DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Statewide Procedure

OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	Number:	10.60.00.PR
Division:	State Controller's Division	Effective date:	October 1, 2007
Chapter:	**Internal Control**		
Part:	**Information Technology**		
Section:			
Approved:	John Radford, State Controller	Signature on file at SCD	

Categories of Information Technology (IT) Controls

.101 In a computerized environment, controls are divided into two principal categories: general controls and application controls.

a. General controls are broad-based, pervasive controls that address the overall operation and activities of the information technology function. General controls apply to all information systems including mainframe, minicomputer, network, and end-user environments. They impact the entire data processing environment, including application systems. General controls address data center and network operations; system software acquisition and maintenance; physical security, environmental protection, disaster recovery, hardware maintenance and computer operations. Other examples include program change controls; controls that restrict access to programs or data; controls over implementation of packaged software or development of new software applications; and controls over system software that monitors the use of system utilities that could change financial data without leaving an audit trail.

b. Application controls, on the other hand, are more specific to individual application systems. They include both computerized and manual controls and are designed to help ensure the completeness, accuracy, and validity of all information processed. When data is transmitted from another system via an interface, application controls must be installed to ensure that all inputs are received and are valid and that all outputs are correct and properly distributed.

Segregation of Duties

.102 A primary aspect of general control includes the organization and operation controls related to the structure of the IT function and how duties are segregated. The IT organization is a support function in that it does not initiate or authorize transactions.

.103 In a well-structured IT organization, the following duties are segregated:

a. *Systems analysts* design the overall computer system. They decide what type of computer network is needed to accomplish management's goals and recommend changes to the overall network. The duties of the systems analyst must be segregated from the duties of the computer programmer and the computer operator.

b. *Application programmers* are responsible for writing the programs. The application programmer also handles the testing of programs, modification of existing programs, and preparation of computer operator instructions. The duties of the application programmer must be segregated from the duties of the systems analyst and computer operator.

c. *Systems programmers* are responsible for maintaining the operating system and related hardware. The systems programmer must not have access to application specific information about programs or data files. The duties of the systems programmer must also be segregated from the duties of systems analyst and computer operator.

d. The *computer operator* is responsible for maintaining live programs and data, scheduling processing activities, running programs, and distributing reports. It is critical that the computer operator and computer programmers be segregated; a person performing both functions would have the opportunity to make unauthorized and undetected program changes.

e. The *control clerk* logs and/or schedules the input and output as well as maintains the error and correction log. The clerk also controls the flow of batches through data entry and editing, monitors processing, and controls distribution of reports and other output.

f. The *IT supervisor* manages the functions and responsibilities of the IT organization and is a member of the external control group defined below.

g. The *external control group* usually consists of the data processing manager and other managers from user organizations. The external control group reviews input procedures; monitors data processing; reviews, approves and handles all reprocessing of errors; and verifies the proper distribution of data output.

h. The *file librarian* stores and protects the files, programs, and tapes from damage and unauthorized use.

i. The *security officer* is responsible for the assignment, maintenance, and timely changing of passwords. Passwords must never be written on paper and left in the workplace. The term *security officer* as used in this procedure refers to the role of the IT organization in controlling general systems access. This term is not synonymous with the term *agency security officer* as used in **OAM 10.70.00**; the agency security officer is responsible for authorizing and requesting access to the following financial systems or databases:

R*STARS (Relational Statewide Accounting and Reporting System)
ADPICS (Advanced Purchasing and Inventory Control System)
OSPA (Oregon Statewide Payroll Application)
Accounting Datamart (R*STARS reporting database)
Payroll Datamart (OSPA reporting database)

j. *System administrators* are responsible for keeping information up-to-date and restricting access. Database administrators update databases and limit access to appropriate personnel. Similarly, network administrators oversee the computer network, while web administrators manage information on the website. Duties of system administrators should, when possible, be segregated from programming and operation duties.

k. *Data input* personnel prepare, verify, and input data to be processed.

Systems Development Controls

.104 Systems development deals with the implementation of new systems and the modification of existing systems. Agency heads and chief information officers (CIOs) must assure all system, implementations, enhancements, and program modifications are appropriately authorized and documented.

.105 Agency heads and CIOs must submit a request identifying the need and outlining the steps to be taken for implementing new IT systems or modifying existing IT systems. Necessary elements include:

a. Proper approval by the State Controller's Division (SCD) and Enterprise Information Strategy and Policy Division (EISPD) to acquire or modify fiscal systems. Refer to **OAM 10.65.00.PO**, *Approval of Proposed Fiscal Systems*, and EISPD statewide policies concerning systems development.

b. Appropriate documentation describing the nature and logic of the proposed changes;

c. A proper methodology for testing and debugging all changes on a test system before incorporating the changes into an operable system;

d. A log of all system enhancements and modifications.

.106 No changes shall be made to programs and files until authorization is provided in writing, and only computer programmers are allowed to make the changes. The same control procedures that apply to the installation or modification of application programs also apply to changes in systems software (e.g., the operating system).

Documentation Controls

.107 There are three levels of documentation that must be maintained. Documentation at each level normally consists of flowcharts and a narrative description.

a. System documentation provides an overview of the programs and data files, how processing occurs, and how different programs within the system interact with each other. In essence, system documentation is documentation of internal control.

b. Program documentation provides a detailed analysis of the data used, the program logic, and the data produced.

c. Operator documentation (also called the "run manual") provides instructions for the computer operator on the use of the program (including required data files, startup instructions, check points, and program output).

Hardware Controls

.108 Necessary hardware controls are usually built into the equipment by the manufacturer and include parity checks, echo checks, and read-after-write checks.

Access Controls

.109 Access to program documentation, data files, programs, and computer hardware must be limited to the extent required by individual job duties. Access controls include the use of multi-level security, user identifications coupled with regularly changed passwords, limited access rooms, call backs and dial-up systems, use of file attributes, firewalls, and encryption of confidential data.

Safeguarding Records and Files

.110 The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) establish worldwide IT security standards that EISPD has adopted as the guide for creating an enterprise information security policy set for the State of Oregon. In accordance with EISPD Statewide Policy 107-004-052 Information Security, each agency shall develop and implement information security plans, policies and procedures that protect its information assets from the time of creation, through the useful life and through proper disposal. All plans and policies must include administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of agency information assets. In addition, each agency must identify, classify and manage its information assets based on the classification schema described in EISPD Statewide Policy 107-004-050 Information Asset Classification.

.111 Each agency shall physically control and protect portable and removable storage devices as well as protect and manage any sensitive information stored on them in accordance with EISPD Statewide Policy 107-004-051 Controlling Portable and Removable Storage Devices. In addition, any agency that sends, receives, or transports confidential or sensitve information to or from another agency is responsible for ensuring that the information is protected appropriately during transit from loss, destruction, or unauthorized access in accordance with EISPD Statewide Policy 107-004-100 Transporting Information Assets.

.112 Agencies must also take precautions to prevent accidental destruction of data. Control measures include the use of internal and external labels, file protection rings, boundary protection, and storing of key master files and records in safe places located away from the work site. It is recommended that copies of files kept on site be in fire-proof containers.

.113 Backup files must also be maintained. The process normally includes reading the previous file, recording transactions being processed, and then creating a new updated master file. The daily (or other interval) transactions are stored separately.

.114 Agencies are required to establish or be part of a disaster recovery plan for continuing operations in the event of destruction of not only program and data files, but also processing capability.

Application Controls

.115 Input control activities. Input controls are designed to provide reasonable assurance that data received for computer processing have been properly authorized and converted into machine-sensible form, and that the data have not been lost, suppressed, added, duplicated, or improperly changed. Computerized input controls include validation procedures such as check digits, record counts, hash totals and batch financial totals. Computerized edit routines include valid character tests, missing data tests, sequence tests and limit or reasonableness tests which are all designed to detect data conversion errors. Various input controls that may be imposed during data entry are described below:

a. Validity tests make sure the code entered is an existing code.

b. Check digits are created by subjecting characters of a field to an arithmetic algorithm. The algorithm yields a single digit that is then appended to the end of a field.

c. A field check verifies that data entered is of acceptable type (e.g., alphabetic, numeric, a certain number of characters, etc.).

d. A limit test checks to see that a numeric field does not exceed a specified limit.

e. A reasonableness check determines whether data in two or more fields is consistent.

f. A sequence check verifies all items in a numerical sequence are present.

g. When loop verification is used, additional information is displayed to confirm correctness or a request is made for explicit confirmation (e.g., “Are you sure you want to delete this employee record? Yes or No.”).

h. Key verification is the re-keying of critical data in the transaction followed by a comparison of the two keyings.

i. Preprinted forms and preformatted screens reduce the likelihood of data entry errors by organizing input data in a logical manner and by using default values whenever possible.

j. Automated data capture eliminates manual data entry by using automated techniques (e.g., scanners).

k. Checkpoint/restart is a processing control whereby a periodic snapshot of all data files is taken. If a system failure occurs, only transactions occurring since the last checkpoint need to be processed.

.116 Processing control activities. Processing controls are designed to provide reasonable assurance that data processing has been performed as intended without any omission or double-counting. Many processing controls are the same as input controls, but they are used during the actual processing phases. These controls include run-to-run totals, control total reports, file and operator controls, such as external and internal labels, system logs of computer operations, and limit or reasonableness tests.

.117 Output control activities. Output controls are designed to provide reasonable assurance that processing results are accurate and distributed to authorize personnel only. Control totals produced as output during processing must be compared/reconciled to input and run-to-run control totals produced during processing. Computer-generated change reports for master files must be compared to original source documents for assurance that data is correct. The following control reports assist in ensuring accuracy and completeness of data processing:

a. Processing reports list all the transactions used to update master files.

b. Error listings report all transactions and/or batches that failed one or more input controls.

c. Application reports are formal, formatted, regularly scheduled reports, usually created by programmers for use by end-users.

d. Ad hoc reports are informal, one-time only reports used to furnish specific information requests. Ad hoc reports are generally limited to database environments and are obtained through query of the system.

.118 The external control group shall receive all data, ensure it is recorded, follow up on errors that occur during processing and verify the proper distribution of output. A list of authorized recipients and a log of report distributions must be maintained. End-user controls supplement the information systems organization controls by performing redundant checks of processing totals and reconciling the results to independently maintained records.

Automated Interfaces Linking Agency Financial Systems to SFMA

.119 Agencies that interface financial data from their own systems into the Statewide Financial Management Application (SFMA), which includes both R*STARS and ADPICS, are responsible for ensuring the transmitted data is timely, accurate, and complete. New interfaces and changes to existing interfaces are reviewed and approved by the Statewide Financial Management Services (SFMS) Analysis and Development (A&D) unit. Interfaces to SFMA are subject to testing and acceptance requirements as specified by the A&D unit.

.120 Approval to establish and continue using an automated interface also depends on an agency’s ability to reconcile data maintained in its internal financial system to data interfaced and posted in SFMA. Agencies are responsible to perform reconciliation procedures as often as data is interfaced and at a level of detail sufficient to ensure all data was transmitted timely, accurately and completely. Each agency head is responsible for ensuring that any discrepancy between an agency’s database and the official financial records in SFMA is promptly and appropriately resolved. When changes to SFMA are made, agencies are responsible to modify their interfaces to adapt to such changes. SFMS is responsible for timely notifying agencies of any changes to SFMA that may impact agency interfaces.

.121 State agencies that transmit data to SFMA are responsible for establishing and monitoring the security of their automated interfaces and ensuring the integrity of the data that is transmitted. These same requirements also apply to entities that host agency applications and control the storage and transmission of data between agency applications and SFMA. In order to protect the data integrity of SFMA, the State Controller’s Division reserves the right to suspend or terminate agency interfaces, or take other remedial actions at the cost of the agency, if the agency does not correct interface errors or appropriately modify interfaces in a timely manner.

Automated Interfaces Linking Agency Time and Attendance Systems to OSPA

.122 Agencies that interface time and attendance data from their own systems into OSPA are responsible for ensuring the transmitted data is timely, accurate and complete. New interfaces and changes to existing interfaces are reviewed and approved by Oregon Statewide Payroll Services (OSPS). Interfaces are subject to testing and acceptance requirements prior to approval.

.123 The approval to establish and continue using an automated interface to transmit time and attendance data also depends upon an agency’s ability to reconcile data maintained in its own time and attendance system to data and hours paid posted to OSPA. Agencies must perform reconciliations as often as data is interfaced and at a level of detail sufficient to ensure all data was transferred timely, accurately, completely and for the correct pay period. Each agency head is responsible for ensuring that time reporting discrepancies are promptly and appropriately resolved.

.124 When changes to OSPA are made that necessitate changes to the time and attendance interfaces, agencies are responsible for modifying their interfaces to adapt to such changes. OSPS is responsible for timely notifying agencies of any changes that might impact agency interfaces.

.125 State agencies that transmit data to OSPA are responsible for establishing and monitoring the security of their automated interfaces and ensuring the integrity of the data that is transmitted. These same requirements also apply to entities that host agency applications and control the storage and transmission of data between agency applications and OSPA. In order to protect the data integrity of OSPA, the State Controller’s Division reserves the right to suspend or terminate agency interfaces, or take other remedial actions at the cost of the agency, if the agency does not correct interface errors or appropriately modify interfaces in a timely manner.

Third Party Service Organizations

.126 When IT services for financial and accounting processes are outsourced to a third party service organization, state agencies must determine whether a written service level agreement (SLA) needs to be established. The purpose of an SLA is to define expectations and responsibilities based on the agency’s requirements and IT capabilities. Important areas in which roles and responsibilities may need to be formalized include security and confidentiality, program change control, availability, reliability, performance and processing requirements, support, capacity for growth, and backup and disaster recovery.

.127 Other important areas to consider when outsourcing IT include:

a. Agreement regarding the level of logical access contractors or other third party providers will have to system programming or data. While certain access to the application and data may be necessary for operational purposes, unrestricted access or access not known to the agency poses a risk to the integrity and confidentiality of the data and the system.

b. How the service provider will restrict access to system logs.

c. Agreement regarding how security violation reporting and follow-up will occur, including when incidents will be reported, who will be notified, who will conduct investigations, and who will be responsible for resolving security incidents or breaches.

d. Provisions to ensure that application source code and other critical system documentation is properly maintained in escrow to allow for continued operations if the provider prematurely discontinues its operations or experiences an unexpected disruption of service.

.128 Another important consideration centers on independent audit assurance. Any time a service organization hosts or processes data belonging to an agency, the agency must determine whether a provision is needed in the contract that requires the service organization to demonstrate that it has adequate controls and safeguards. This may be accomplished by requiring the service organization to undergo an annual audit conducted by the agency or its designees.

.129 Alternatively, the service organization may already be subject to an annual audit that would satisfy the requirement. *Statement of Auditing Standards (SAS) No. 70, Service Organizations*, provides guidance to enable an independent auditor to issue an opinion on a service organization’s internal controls, including controls over IT and related processes. A formal report known as a Service Auditor’s Report, which also includes the auditor’s opinion, is issued to the service organization at the conclusion of the SAS 70 examination. The service organization then makes this report available to its customers who, in turn, provide it to their auditors (such as Secretary of State, Audits Division) for use in planning the audit of the financial statements.

.130 There are two types of SAS 70 Service Auditor’s Reports. A Type I report contains the service organization’s description of controls at a specific point in time. A Type II report not only includes the service organization’s description of controls, but also includes detailed testing of the controls over the period specified. State agencies that pursue a SAS 70 examination need to request a Type II report.