

OREGON ACCOUNTING MANUAL	
Subject: Accounting and Financial Reporting	Number: 10.60.00.PO
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

Authority [ORS 291.015](#)
[ORS 293.590](#)
[ORS 293.595](#)

Management of Risks, Performance, and Controls in the Information Technology (IT) Environment

- .101 Each **agency head** is responsible for establishing, maintaining, and improving internal controls over the agency's information technology (IT). The design, implementation, and operation of agency IT controls must be adequate to provide an acceptable level of confidence in agency systems and assurance that:
 - a. Management's IT goals and objectives are being accomplished effectively and efficiently;
 - b. IT investments and investment strategies are well planned and adequately funded;
 - c. IT assets are safeguarded; and
 - d. IT operational and investment strategies are executed in accordance with management's direction, authorization, and security and control policies.
- .102 In addition, agencies are required to comply with all statewide IT security policies and initiatives issued by the Department of Administrative Services, Enterprise Information Strategy and Policy Division (DAS-EISPD) and all applicable federal and state laws and regulations pertaining to the confidentiality, integrity and availability of electronic data, including Oregon Laws 2007, Chapter 759.
- .103 State agencies are responsible for providing adequate security and control training and other educational support to employees involved in the design, development, implementation, maintenance, and management of the IT infrastructure/function, as well as the storage and protection of the underlying data. Training is available through a variety of nationally and locally recognized professional associations and through DAS-EISPD.

Review of IT Controls

- .104 Periodically, agency management is responsible for reviewing and testing the performance of the agency's internal controls over information technologies.
- .105 Agency management is responsible for preparing a report that identifies any significant or material weaknesses in the agency's IT controls and gives a status update on IT control

- weaknesses identified in earlier reports or noted by internal or external auditors. The plan for correcting the deficiencies must be described in detail and include estimated dates of completion.
- .106 Agency heads should consider making the IT review process an annual event. The corresponding report would serve to document, as a permanent record, the effective management and control of the agency's IT operations and infrastructure investments.
 - .107 The Secretary of State, Audits Division has adopted CobiT (Control Objectives for Information and Related Technology) as the basis for auditing the IT management function; Agencies are also encouraged to adopt the CobiT framework. CobiT is published by the Information Systems Audit and Control Foundation (ISACF); copies may be obtained at <http://www.isaca.org/>.
 - .108 The Audits Division may review an agency's IT security and internal control management as part of its ongoing audit activities. Such a review will not satisfy the requirements of this policy for agency management to review and be accountable for the adequacy of the design, implementation, and operation of the agency's IT controls. However, suggestions from the Audits Division can be useful to agency managers in conducting IT reviews and formulating corrective action plans.
 - .109 The use of qualified agency internal auditors to assist management in reviewing IT controls is strongly encouraged. A properly staffed internal audit function can provide ongoing monitoring and independent risk assessment. Independent review and analysis are critical elements in a well designed framework of IT controls; particularly, as systems are planned, developed, tested and implemented.