



Auditing for a Better Oregon

October 10, 2006

Victor Merced, Director
Oregon Housing and Community Services Department
PO Box 14508
Salem, Oregon 97309-0409

Dear Mr. Merced:

We have completed a risk assessment of the Oregon Housing and Community Services Department's (department) information technology controls. The objective of this engagement was to support our annual financial audit of the department by evaluating some of the important general computer controls. General controls protect the environment in which software applications operate by ensuring security of data and systems, continuous service, and proper management of systems development and modifications to existing applications.

During our risk assessment, we were aware of the state's initiative to consolidate its data centers and the department's role in that undertaking. During April 2006, the department began transferring custody and operations of its computer infrastructure to the Department of Administrative Services' State Data Center (SDC). This process was expected to be completed by September 30, 2006, when the SDC anticipated it would assume full responsibility for hosting the department's systems. Because of this new outsourcing relationship, department management now shares responsibility for some key computer controls. As a result, we limited this review to controls for which the department continues to have primary responsibility. Those controls included security policy, business continuity planning and applications development and maintenance.

We noted several areas where the department could improve its general controls. Issues of most concern included the following:

Security

Industry standards recommend a security framework that includes the following processes:

- identifying information assets;
- assigning individuals responsibility for those assets;
- determining appropriate security levels for those assets;
- assessing security risks; and

Management Letter No. 914-2006-10-01

- implementing suitable controls, including policies and procedures, to ensure risks are reduced to an acceptable level.

During our risk assessment, we noted that department management had identified critical functions and the resources to support those functions. However, the department's overall security framework was incomplete because data owners had not been assigned to the department's various databases, and data had not been classified according to desired or required security levels. In addition, department management had not fully assessed security risks to help direct the selection of controls to protect against those risks. Department management adopted several policies that described acceptable use of information assets, but had not developed organization-wide security policies to more fully define management's intentions for or commitment to information security.

Furthermore, the department's transition agreement with the SDC described the responsibilities for security that were to be shared between the department and the SDC. However, as we noted in our separate audit report No. 2006-33 on the data center consolidation, SDC consolidation plans had not yet adequately addressed how and when critical security services would be provided.

Without a comprehensive security framework in place, department management cannot assure it is adequately protecting the confidentiality, availability, and integrity of its information assets. In addition, management will not be able to provide the SDC with its expected levels of security for department assets.

We recommend department management strengthen its security controls by assigning data owners and determining appropriate security levels for its data. Department management also should assess security risks and select proper controls to protect against those risks. The department's plan for security should be defined in organization-wide security policies and communicated, as appropriate, to all staff. In addition, department management needs to ensure the service level agreement it negotiates with the Department of Administrative Services meets the department's security needs for assets housed in the SDC.

Business Continuity Planning

Business continuity planning involves the preparation, testing, and maintenance of specific actions to protect against losses due to extended data processing service outages. Industry guidelines recommend several phases in the development of business continuity plans:

- business impact analysis to identify time-critical aspects of the critical business processes, and determine maximum tolerable downtime;
- strategy planning to identify and select appropriate recovery alternatives that meet the recovery time requirements outlined in the business impact analysis;
- plan design and development to document the results of the business impact analysis findings and recovery strategies; and
- testing, maintenance, awareness and training to establish the processes for testing the recovery strategies, maintaining the business continuity plan, and ensuring that individuals involved are aware of and trained in the recovery strategies.

We found that department management had prepared a business impact analysis and identified time-critical aspects of critical business functions. In addition, management had determined maximum tolerable downtimes for those functions. However, fully documented and tested continuity plans had not been developed, including recovery strategies and recovery alternatives for each of the critical functions. The department's transition agreement with the SDC provided that the scope of the SDC's disaster recovery services included recovery and continued operations of system components designated in the department's disaster recovery plans. Because the department had not completed those plans, it was not clear how recovery services would be provided at the SDC.

Without fully developed and tested business continuity plans, the department cannot ensure the timely resumption of critical business functions in the event of a disruption to normal data processing operations.

We recommend department management complete and test business continuity plans that include recovery strategies and recovery alternatives to minimize the disruption of operations and ensure an orderly recovery after an outage. In addition, department management should ensure that services from the SDC meet the department's expectations and needs for continuous data processing services by defining those requirements in a service level agreement with the Department of Administrative Services.

Change Management

Effective change management controls include formal procedures to ensure modifications to production applications are authorized, prioritized, tested, approved, and documented. Development and test environments should be separate from the production environment to ensure the integrity of production data. In addition, programmers should not be responsible for migrating changes to production unless mitigating controls, such as management review, exist to ensure only authorized changes are migrated. Procedures should be in place to ensure emergency fixes can be performed without compromising the integrity of the system, typically with the use of special logon IDs that grant a programmer temporary access to the production environment during these emergency situations. Change control procedures should be applied retroactively to emergency fixes.

During our risk assessment, we noted the department had developed practices to collect and prioritize change requests and to test and approve modifications to its applications. Also, the department had separated its development, test, and production environments. However, the department had not developed written change management procedures, established requirements for formal testing plans or required management review of all modifications. The department also had not established minimum standards for documenting changes and did not have procedures for documenting test results and retaining testing documentation. In addition, because modifications to mature applications typically were less extensive than changes to newer applications, department management did not have the same expectations for controls over each application. Because the department did not have written procedures that delineated the differences, it was not clear when and how change management processes should be followed; therefore, department management could not ensure that desired processes were followed.

Furthermore, although department management prevented programmers from having logical access to the production environment for one of the department's applications, it allowed programmers unrestricted and unsupervised access to production for other critical applications. As a result, programmers could migrate modifications to production for those applications without supervisory oversight. Consequently, the department could not ensure that only authorized modifications were made to the applications.

We recommend department management formalize its change management procedures by developing written procedures that define expectations for controls over applications in various stages of maturity. Department management also should establish requirements for formal testing plans, management review, and documentation. In addition, department management generally should not allow programmers to access the production environment, and should monitor programmers' activities on those occasions when their access to production cannot be avoided.

We appreciate the time and effort your staff provided as we completed this work. Should you have questions concerning these issues, feel free to contact me at (503) 986-2351.

Sincerely,
OREGON AUDITS DIVISION

V. Dale Bond, CPA, CISA, CFE
Audit Manager

VDB:brk
cc: Lindsay Ball, Director, Department of Administrative Services