Secretary of State Audit Report

Kate Brown, Secretary of State

Gary Blackmer, Director, Audits Division

State Data Center Operations Are Stable, But Some Areas Need Improvement

Summary

The Department of Administrative Services (DAS) is responsible for providing centralized computer services to state agencies, including operating the State Data Center (SDC). State agencies rely on SDC resources to operate hundreds of computer applications they use to carry out their operations. The SDC is comprised of a complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure.

Our specific audit objectives were to determine whether the SDC provided a controlled and stable operating environment for agency and enterprise applications, and the necessary security framework to protect agency and enterprise applications and their data.

We found that the SDC provides a stable operating environment to ensure day-to-day processing occurs for hosted state agency computer applications. Specifically, SDC staff ensured controls were in place to protect infrastructure from environmental hazards, provide routine back-ups and job monitoring, resolve production problems and incidents, and allocate operating costs according to the agreed-upon cost recovery model.

However, other important operational controls need further attention. Specifically, SDC customer service level agreements have not been established with all agencies; management of IT asset configurations and capacity was not adequate; and, while disaster recovery capabilities improved since our last audit, more preparation is needed.

Although these issues did not significantly hamper the SDC's ability to provide day-to-day operations, they adversely affect staff's ability to respond to disaster events or make changes to enhance data center efficiency.

Recommendations

To address these control weaknesses, we recommend that SDC management establish better service level agreements with all its customers, implement a configuration management system, implement processes for performance measurement and capacity management, and create and test more robust disaster recovery plans. Our recommendations are detailed at the end of the report.

Agency response

The agency response is attached at the end of the report.

Background

The Department of Administrative Services (DAS) is responsible for providing centralized computer services for state agencies, including operation of the State Data Center (SDC). The approved budget for the SDC for the 2009-2011 biennium is approximately $165 million. To cover operating costs, the SDC charges agencies for services according to a predetermined rate schedule.

The 2005 legislature authorized DAS to create the SDC by consolidating data centers previously operated by state agencies. One of the primary goals of consolidation was to develop an enterprise structure to provide better service and cost savings. By the beginning of 2007, 11 agencies had transferred their data center operations to the SDC. Because of difficulties encountered during this project, DAS management opted to relocate agency data centers to the SDC in their "as-is" state, stabilize operations, and then proceed with projects to reengineer the environment.

The SDC is comprised of a complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure. State agencies use these resources to operate hundreds of computer applications, including mission critical systems. In addition, the SDC provides Internet service and networking for the majority of state agencies.

Providing an appropriate computing environment for hosting this diverse set of Information Technology (IT) resources and customers is an enormous managerial task. Best practices indicate that a controlled and stable data center would ensure:

- customer service level expectations are appropriately defined and managed;
- adequate capacity is available and optimally used to meet required performance needs;
- IT services are available as required and controls are present to ensure customers experience only a minimum business impact in the event of a major disruption;
- operating costs are correctly and fairly allocated to users;
- information assets are protected from unauthorized access, disclosure or loss;
- a suitable physical environment exists to protect people and equipment from man-made and natural hazards;
- problems and incidents are resolved and appropriately investigated to prevent recurrence; and
- a record of IT components and configurations is maintained to facilitate sound change management.

For managerial purposes, the SDC is divided into five operational units: Plans and Controls; Enterprise Systems; Distributed Systems and Storage; Network, Security and Voice Services; and Operations. Overall SDC governance is provided through a complex structure of interrelated committees and subcommittees made-up of customer agency and SDC staff.

Last year, we began an audit of SDC computer controls. We performed this audit to provide internal control information to support our annual financial audits of agencies utilizing the SDC, and to provide DAS management information regarding SDC risks and controls. Our specific audit objectives were to determine whether the SDC provided a controlled and stable operating environment for agency and enterprise applications, and the necessary security framework to protect agency and enterprise applications and their data.

On March 5, 2010, we issued a separate public report titled "*State Data Center: Faster Progress Needed on Security Issues*" that addressed management elements related to the security portion of this audit. In addition, we communicated sensitive security findings and recommendations to DAS under separate cover in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure.

The purpose of this report is to communicate the results of our audit work relating to operational controls at the SDC.

Audit Results

State Data Center Operations Are Stable But Further Improvements Are Needed

Managing the complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure at the SDC requires competent staff performing the day-to-day activities. In addition, managing these operations efficiently and cost-effectively requires well designed and consistently applied controls.

We found that the SDC provides a stable operating environment to ensure day-to-day processing occurs for hosted state agency computer applications. To accomplish this, SDC staff ensured controls were in place to:

- monitor and control the SDC physical environment to ensure infrastructure was appropriately protected from environmental and man-made hazards;
- provide routine back-ups for agency applications and appropriately manage the SDC data media library;
- monitor processing and ensure production problems and incidents are appropriately investigated and resolved; and
- allocate operating costs according to the agreed-upon cost recovery model.

However, some other important aspects could be improved. Specifically, we found that SDC:

- customer service level expectations were not adequately defined;
- management of IT asset configurations and capacity was inadequate; and
- disaster recovery capabilities improved but current strategies continue to be insufficient.

Although these issues did not significantly hamper the SDC's ability to provide day-to-day operations, they adversely affected staff's ability to respond to disaster events or make changes to enhance data center efficiency.

Customer Service Level Expectations Were Not Adequately Defined

IT control best practices indicate that data centers should establish a framework for managing customer service level requirements and expectations by publishing a complete catalog of available services and by establishing formal service level agreements with customers. Properly crafted service level agreements establish a common understanding between

a service provider and its customers regarding critical operational elements such as service availability, reliability, performance metrics, capacity for growth, levels of support, continuity planning, and security.

SDC publishes an extensive catalog of services that it makes available to customers, and has taken action to establish service level agreements with its customer agencies. However, additional effort is needed on service level agreements so that they define all the operational expectations and requirements of each state agency.

During 2009, the SDC applied additional resources toward resolving the issue by sponsoring a project to develop a standard service level agreement for the largest SDC customers. By April 1, 2010, seven agencies signed a standard agreement developed through the project. However, SDC management indicated that one SDC customer declined to approve the agreement and other customer agencies would not be asked to establish service level agreements with the SDC.

Development of the standard agreement was a positive step toward a better understanding between the SDC and its customers. However, it does not fully resolve the problem. For example, successful recovery of SDC functionality after a disaster requires agreement between SDC staff and each individual state agency regarding which computer systems will be restored, what services will be available, and when and who will be responsible for managing and staffing the joint recovery effort.

Because the standard agreement was designed as a common solution and was not adopted by all SDC customers, it did not adequately define all agencies' specific requirements, responsibilities or expectations for these and other important operational areas such as security, capacity planning, and staffing.

Management of IT Asset Configurations and Capacity Was Inadequate

Generally accepted IT standards indicate that data centers should document and manage asset configurations. This is accomplished by maintaining a record of current hardware configurations, network and system architecture, application and system software parameters, firmware versions, and tools and operational procedures. Controls should also exist to ensure all changes to configurations are authorized and a blue print is available for restoring the systems should that become necessary. Processes should also exist to maintain performance metrics to facilitate analysis planning for future capacity needs.

We found that SDC staff had standards for managing IT assets and configurations. However, they had not yet developed the necessary procedures or tools to implement the standards. Specifically, staff did not maintain a repository for documenting and maintaining data center configurations, including virtual devices, and did not have a complete and accurate list of all physical IT assets under its control.

Management indicated the SDC had purchased an automated configuration management tool and contracted with a firm to implement the tool. However, during implementation the contractor determined the planned system architecture would not work in the current SDC environment and would need to be changed. After revising the implementation, contractors installed the software in three agency environments. Subsequently, new problems arose and additional requirements surfaced, forcing a higher degree of customization than was planned. Due to these issues, SDC management stopped further development and shifted its resources to other projects. The manager responsible indicated that no project is underway to continue developing configuration management.

SDC staff also had not developed or implemented appropriate modeling techniques to forecast future performance and capacity needs. Rather, managers relied on platform managers' experience and ad hoc methodologies and tools to manage this process.

The above configuration and capacity management weaknesses adversely impacts SDC staff's ability to provide efficient and cost effective services, and appropriately plan for future needs. For example, not having a repository of current data center asset configurations significantly impacts the SDC's ability to provide other vital data center services such as disaster recovery and security. In addition, without attention to capacity and performance metrics, SDC staff is less able to ensure the efficient use of resources.

Disaster Recovery Capabilities Improved But Current Strategies Continue to be Insufficient

Restoring SDC operations after a disaster or other serious disruption would require significant advance planning, training, testing, and coordination between all affected parties. Best practices indicate that data centers should mitigate the risks associated with serious disruptions in service by developing and periodically testing formal disaster recovery and business continuity plans. These plans should be based on agreed-upon customer requirements and should be regularly updated to reflect changes to the computing environment.

Disaster recovery and business continuity plans should provide a framework for restoring data center infrastructure and services to their before-incident state and establish a means of providing critical services in the interim. Developing and maintaining such plans requires a great deal of coordinated and concerted effort by SDC staff, state agency application owners and operators, and external vendors or service providers.

Since our last audit, the SDC expended considerable time and effort to improve disaster recovery capabilities. Specifically, staff held numerous planning meetings to help state agencies identify disaster recovery needs. In December 2009, staff also conducted a limited test at their alternate

processing site to determine whether some key components could be restored.

These accomplishments were noteworthy, but much more work is needed to ensure the SDC and its customers are better prepared to cope with a disaster or other serious incident. Specifically, the SDC has not yet developed a comprehensive plan to restore data center infrastructure in the event of a disaster or major service disruption, or to relocate its critical processing capability to its designated remote processing facility. In addition, full disaster recovery testing is needed to ensure critical applications could be restored. Also, as mentioned earlier, the SDC needs service level agreements with all state agencies.

Disaster recovery planning is a resource intensive task that historically has not been given priority when matched with projects having more immediate or certain payback. However, inordinate delays in restoring some computer systems after a disaster could severely impact state agencies' ability to provide mission critical services to Oregon citizens.

Recommendations

In order to establish a common understanding with the majority of its customers regarding which critical services will be required or delivered at the SDC:

- We recommend that SDC management establish more robust service level agreements with all its customers.

In order to provide efficient and cost effective services and appropriately plan for future needs:

- We recommend that SDC implement a configuration management system with associated procedures.
- We also recommend that management implement processes to develop and maintain performance metrics, and plan for future capacity needs.

In order to reduce delays in restoring state computer systems after a disaster:

- We recommend that SDC management assign a higher priority to disaster recovery and allocate sufficient resources to create and test disaster recovery plans to ensure timely restoration of the SDC operating environment.

Objectives, Scope and Methodology

The purpose of our audit was to provide internal control information to support our annual financial audits of agencies utilizing the SDC, and to provide DAS management information regarding SDC risks and controls. Our specific audit objectives were to determine whether the SDC provided:

1. a controlled and stable operating environment for agency and enterprise applications; and

2. the necessary security framework to protect agency and enterprise applications and their data.

We expanded our audit work to determine why prior audit findings relating to security were not resolved. The result of that work is included in our March 5, 2010, audit report titled "*State Data Center: Faster Progress Needed on Security Issues*". Because of its sensitive nature, we communicated detailed information relating to security findings and recommendations to DAS under separate cover in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure. This report addresses our conclusions and recommendations pertaining to operational controls as stated in our first audit objective.

During our audit, we interviewed various department and customer agency personnel, reviewed department documentation, and conducted various tests. To determine whether the SDC provided a controlled and stable operating environment, we evaluated controls, processes and procedures for:

- establishing customer service level agreements;
- managing performance and capacity;
- ensuring continuous service;
- identifying and allocating costs;
- managing problems and incidents;
- controlling infrastructure configurations;
- managing data;
- protecting the physical environment; and
- managing operations.

To determine whether the SDC provided the necessary security framework to protect agency and enterprise applications and their data, we evaluated SDC:

- security plans, policies, procedures, standards, and performance metrics;
- asset, system, and configuration inventory information and documentation relating to network architecture;

- internal and external audit, risk, and vulnerability assessment reports, and the status of prior report findings;
- selected logical and physical access listings, access policies, and the related system parameters;
- processes and practices governing security testing, surveillance and monitoring;
- processes for reporting and resolving security violations and incidents;
- use of encryption; and
- processes and tools for managing and protecting operating system configurations.

We used the IT Governance Institute's publication, "Control Objectives for Information and Related Technology," (COBIT), the Office of Government Commerce's IT Infrastructure Library (ITIL) and the United State's Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM) to identify generally accepted control objectives and practices for information systems.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Oregon
Theodore R. Kulongoski, Governor

Department of Administrative Services
Office of the Director
155 Cottage Street NE, U20
Salem, OR 97301-3966
(503) 378-3104
FAX (503) 373-7643

May 4, 2010

Gary Blackmer, Director
Audits Division
Office of the Secretary of State
255 Capitol Street NE, Suite 500
Salem, OR 97310

Re: Audit report entitled, *State Data Center Operations are Stable, But Some Areas Need Improvement*

Thank you for providing the Department of Administrative Services with the audit report noted above. The report identified issues that have not significantly hampered the State Data Center's ability to provide services; however, it makes recommendations about the state's ability to respond to disaster events and other efficiencies. I have outlined our response to the recommendations below.

Recommendation: *In order to establish a common understanding with the majority of its customers regarding which critical services will be required or delivered at the SDC: We recommend that SDC Management establish service level agreements with all its customers.*

DAS Response:
Management partially agrees with this recommendation. The SDC has obtained signed service level agreements from the majority of it customers (agencies that receive more than 90-percent of the computing services offered by the SDC). The Secretary of State validated seven of these agreements by April 1, 2010, and by April 15, the remaining agencies had signed agreements. We believe having these agreements in place satisfies COBIT (Control Objective for Information and Related Technology) – "Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities." The SDC's other customers submit Technical Support Orders or Service Requests. We believe these documents are sufficient when combined with the SDC Service Catalog, Roles and Responsibilities Matrices, and service rates sheets.

Recommendation: *In order to provide efficient and cost effective services and appropriately plan for future needs: We recommend that SDC implement a configuration management system with associated procedures. We also recommend that management implement processes to develop and maintain performance metrics, and plan for future capacity needs.*

DAS Response:
Management agrees with this recommendation. Developing and maintaining service-level performance metrics is scheduled for completion by the end of this year. Formal configuration and capacity management processes have been planned for next biennium and will only be superseded by plan changes that result in initiatives with either higher cost efficiency or service benefits. The SDC's strategic plan for implementation of 29 of these types of key processes is based on the industry recommendations for Information Technology Service Management. ITSM implements a guided process and controls for an enterprise-level computing environment. These recommendations include ensuring that other key supporting processes are implemented prior to configuration management, performance metrics and capacity management. For example, implementing service level agreements to ensure that cost-justifiable capacity and performance are available to sustain the agreed-upon workloads.

Or, implementing a single source asset repository and processes to monitor and record changes to assets. The service level agreements' asset repository and change management tools and processes have all been implemented.

Recommendation: *In order to reduce delays in restoring state computer systems after a disaster: We recommend that SDC management assign a higher priority to disaster recovery and allocate sufficient resources to create and test disaster recovery plans to ensure timely restoration of the SDC operating environment.*

DAS Response:
Management agrees with this recommendation. The SDC has kept disaster recovery as it number one priority for the last year and will continue to do so. As the audit points out, much work and testing has been accomplished; however, more work is planned as well as a need to ensure long-term, regular ongoing testing. The SDC is working with the state's DR vendor to complete regular updates to a comprehensive plan to restore data center infrastructure. The next update to the plan is scheduled for completion in December 2010 and again in June 2011. This plan provides the strategies, resources, procedures and disaster time checklist required to recover from any short- or long-term technology interruption. It has been used for the periodic disaster testing conducted to date. In concert with what the SDC is doing and coordinating, the agencies also are preparing by developing for their critical systems the application and data recovery plans, data dependencies, and designation of their needed application recovery sequences. Backup, Restore and Recovery Service are defined in the current service level agreements, SDC Service Catalog, and Roles and Responsibility Matrices.

Closing
We appreciate your audit team's diligent effort over the past year to address operational controls and recommend opportunities for improvement at the SDC. Since the team completed its field work in June 2009, we have endeavored to implement many of its recommendations and will continue to make progress as described above.

If you have any questions about this response, please don't hesitate to contact Julie Bozzi, SDC Administrator, at 503-378-4578.

Thank you again for the recommendations and helpful insight that your audit has provided us.

Sincerely,

Scott L. Harra
Director

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of the Executive, Legislative, and Judicial branches of Oregon government. The division audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

Audit Team
William K. Garber, CGFM, MPA, Deputy Director
Neal E. Weatherspoon, CPA, CISA, CISSP, Audit Manager
Mark A. Winter, CPA, CISA, Principal Auditor
Teresa L. Furnish, Staff Auditor

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained from:

internet: http://www.sos.state.or.us/audits/index.html

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310

The courtesies and cooperation extended by officials and employees of the Oregon Department of Administrative Services during the course of this audit were commendable and sincerely appreciated.