



City of Seattle – City Light Department Points of Discussion with Management

Information Technology

System Development Life Cycle and Change Management

To ensure that new systems and changes to existing systems that impact financial reporting are implemented with data confidentiality, integrity, and availability controls, standard processes that include functional testing and management approval should be in place for all critical systems that impact financial reporting. Baker Tilly Virchow Krause, LLP (Baker Tilly) recommends the following:

1. Expand the scope of existing system development life cycle and change management policies and procedures to include PowerOps, or develop specific system development life cycle and change management policies and procedures that meet the needs of PowerOps.

Management Response:

City Light's System Development Lifecycle (SDLC) processes will be implemented for PowerOps and the entire suite of Sungard software solutions by the end of quarter 3. Changes to the SDLC will be made on an exceptions basis, to meet unique power marketing business needs. For example a formal intake process is being developed in collaboration with the business to formalize change management practices.

2. Implement a mechanism (e.g., ticketing system) to document and retain approvals for all software development, acquisition, and change management efforts for PowerOps.

Management Response:

This will be addressed by the end of quarter 3, as part of the implementation of the SDLC and new intake process for PowerOps.

Logical Security

To prevent unauthorized and inappropriate system access, critical systems that impact financial reporting should require:

- > A unique login ID for each user
- > Strong passwords
- > Standard user access management policies and procedures
- > Limited access to install, modify, and update production systems
- > Periodic access reviews

Baker Tilly recommends the following:

1. Delete the shared accounts that currently exist within CCSS. If shared accounts are required based on business need, implement a monitoring mechanism to track and regularly review actions performed by each shared account.

Management Response:

Review of shared accounts for all critical applications including CCSS will be included in the System Administrator Access Audit project to be fully implemented in 2013, starting with CCSS in 2012. Monitoring mechanisms will be considered as part of this project.

2. Implement strong password parameters for PassPort, ICSB, WAMS, Maximo, and PowerOps, where it does not break the application or incur substantial resources to remediate an application that will be phased out. Questions to consider when setting password parameters include:
 - > Are passwords at least six characters long?
 - > Do passwords expire in no more than 90 days?
 - > Do passwords require a combination of alphanumeric and special characters?
 - > Are accounts locked out after three invalid login attempts?
 - > Is password history checked to prevent password recycling?

Alternatively, City of Seattle – City Light Department (“Department”) may wish to use the organization’s password guidance within the Application Security Policy as the Department’s standards.

The Department has begun incorporating this recommendation into existing processes as part of the Application Security Policy Development project.

Management Response:

City Light has established password standards in the draft Application Security Policy. All critical application leads will be asked sometime over the next several months to assess the feasibility of implementing the standards for existing applications.

3. Implement a formal process to grant, modify, and remove access to PowerOps based on job responsibility. This process should include formally documenting (e.g., via a ticketing system) access requests and necessary approvals. Further, expand the existing Human Resources notification process to include the PowerOps application team to ensure that access is updated to reflect the current status of employees.

Management Response:

City Light’s Risk Management group is leading this effort. ITSD is collaborating to incorporate new processes into the integrated intake process that will be implemented by the end of quarter 3.

4. Delete the shared accounts that are used to install, update, or modify the network operating system, databases, or applications that support Active Directory, PassPort, CCSS, ICSB, WAMS, Maximo, and PowerOps. If shared accounts are required based on business need, implement a monitoring mechanism to track and regularly review actions performed by each account. The Department may wish to include this recommendation as part of the Administrative Rights Approval and Audit project.

Management Response:

Review of shared accounts for all critical applications including CCSS will be included in the System Administrator Access Audit project to be implemented in 2013. Monitoring mechanisms will be considered as part of this project.

5. Implement a formal process to review user access rights for appropriateness based on job responsibility for PassPort, Maximo, PowerOps, and WAMS. The Department has begun incorporating this recommendation into existing processes as part of the User Access Audits project.

Management Response

This project has already been initiated and a policy and procedure for critical applications has been drafted. The initial audit of CCSS is already underway and initial audits for all critical applications will be completed for 2012.

System Security Monitoring

To ensure that security violations are identified and resolved, internal and external security violations to critical systems that impact financial reporting should be monitored, logged, and reviewed. Baker Tilly recommends the following:

1. Continue moving forward with IT's planned initiative to formally review the audit logs of database-level security events for all critical systems that impact financial reporting.

Management Response

Work is in progress to formally audit and review database level security events for all critical systems that impact financial reporting. Work is expected to be complete by end of 2012.

Physical Security

To prevent unauthorized and inappropriate physical access, servers supporting critical systems that impact financial reporting should be restricted through the use of a lock, swipe card, or a similar device. Approval should be required to be granted access to these servers and a list of approved individuals should exist and be reviewed on a regular (i.e., at least annual) basis. Baker Tilly recommends the following:

1. Formalize the existing access review process for the server room to ensure that documentation exists to evidence review and approval.

Management Response

Servers hosting critical apps reside in the Department of Information Technology's (DoIT) Data Center. ITSD will collaborate with DoIT to formalize access review process.

System Backups

To ensure that data is retained based on the Department's business needs, system backups should be performed on all critical systems that impact financial reporting. Additionally, the status of each backup should be monitored and procedures should be in place to respond to backup errors. All backups should be stored offsite and a procedure should be in place to test the restoration of backups on a scheduled basis. Baker Tilly recommends the following:

1. Continue moving forward with IT's planned initiative to meet with the teams that use PassPort, Maximo, and ICSB to understand backup needs and expectations for each system.

Management Response:

Work is in progress and is expected to be completed in 2012.

2. Continue moving forward with IT's planned initiative to auto-verify that all backup jobs performed for PassPort, Maximo, ICSB, and PowerOps (i.e., all backups managed by RMAN) are successfully started and completed.

Management Response

Work is in progress. Task has been assigned to a DBA and will be complete within the next 2 months

3. Implement a formal backup restoration testing process to ensure that all database and server backup restores are performed at least annually and the results of each restore are formally documented.

Management Response:

Database Backup: This work is in progress. The DBA team has scheduled the testing of database restore process for all the critical applications.