

# Port of Seattle

## 2008 Interim Fieldwork Results

Presented to the Audit Committee on February 27, 2009



# MOSS-ADAMS LLP

999 Third Avenue, Suite 2800

Seattle, WA 98104-4019

206-302-6500

## BACKGROUND

---

Generally-accepted auditing standards require that we consider the Port of Seattle's internal control over financial reporting (internal control) as a basis for designing our auditing procedures and for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Port's internal control. Additionally, OMB Circular A-133 requires we perform procedures to obtain an understanding of internal control over federal programs sufficient to plan the audit to support a low-assessed level of control risk for major programs. We use the Committee of Sponsoring Organization (COSO) framework when evaluating the Port's internal control.

### COSO Framework

COSO defines internal control as a process, affected by an entity's board of directors (i.e., Port Commission), management, and other personnel, designed to provide reasonable assurance regarding the achievement of defined objectives.

These objectives are:

- Effectiveness and efficiency of operations, which involves the organization's basic business objectives, performance and profitability goals and the safeguarding of resources.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

### Components

Internal control consists of five interrelated components. All five components are relevant and important to achieving the organization's objectives. The components are:

- *Control Environment* — The core of any business is its people, their individual attributes, including integrity, ethical values and competence, and the environment in which they operate. The control environment is the foundation for all the other components as it provides structure to an organization.
- *Risk Assessment* — The organization must be aware of and deal with the risks it faces. It must set objectives, integrating activities from all divisions, so that the organization is operating in concert. It also must establish mechanisms to identify analyze and manage the related risks.
- *Control Activities* — Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achieve the organization's objectives are effectively carried out.

- *Information and Communication* — Surrounding these activities are information and communication systems. These enable the organization's people to capture and exchange the information needed to conduct, manage and control its operations.
- *Monitoring* — The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

In summary, the *control environment* provides an atmosphere in which people conduct their activities and carry out their control responsibilities. Within this environment, management *assesses risks* to the achievement of specified objectives. *Control activities* are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant *information* is captured and *communicated* throughout the organization. The entire process is *monitored* and modified as conditions warrant.

Internal controls only provide reasonable assurance to management and those charged with governance that the organization's objectives are being achieved. This is because as with any system that is operated by people, there are inherent limitations. These limitations include: the realities that human judgment in decision-making can be faulty; persons responsible for establishing controls need to consider their relative costs and benefits; and, breakdowns can occur because of human failures such as simple error or mistake. Additionally, controls can be circumvented by collusion of two or more people. Finally, management may have the ability to override the internal control system.

We factor these limitations in the design and conduct of our internal control procedures.

### **Enterprise Risk Management**

Enterprise Risk Management (ERM) framework is designed to achieve the following objectives:

- Strategic — High-level goals, the organization's mission
- Operations — Effective and efficient use of its resources
- Reporting — Reliability of reporting
- Compliance — Compliance with applicable laws and regulations

The framework overlays two additional components in addition to those of COSO's internal control framework:

- *Objective setting* — Management has a process in place to set objectives that are aligned with the entity's mission.
- *Event identification* — Management is identifying risks and opportunities (both internal and external) in place affecting achievement of the entity's objective.

While the focus of our procedures is with the five components of COSO, we believe that it is important to note that the COSO framework is an integral part of the ERM framework. Additionally, as the primary focus of the audit is to form an opinion of the fairness of presentation of the financial statements as well as audit and report on the administration of

federal awards – both of which are part of the four ERM objectives mentioned above – the results of our audit helps the Port understand the extent to which those objectives are met.

## **OUR AUDIT APPROACH AND RESULTS**

---

Our firm follows a top-down approach when evaluating internal control from entity-level controls to controls that relate to specific financial statement assertions as follows:

- Obtain and assess the Port’s entity-level controls including information technology environment and the effect on the internal control structure. (*Control environment, information and communication, risk assessment*)
- Identify significant accounts and processes.
- Obtain copies of system, policy, and procedure documentation from various departments. (*Control activities, control environment*)
- Obtain knowledge of design and implementation of controls relevant to financial statement assertions and compliance with laws and regulations that have direct and material effect on determination of financial statement amounts. (*Control activities, monitoring*)
- Perform tests of controls that relate to financial statement assertions and integrate with tests of controls and compliance related to the Port’s federal awards. (*Control activities*)

### **Entity-Level Controls**

We consider entity-level controls to be very important because they have a pervasive impact on all other specific controls and procedures. As such, we evaluate the effectiveness of entity-level controls first because if compromised, controls at the process or transaction level may not work even though they are well-designed and operate effectively. Some of the common entity-level controls at the Port include:

- Tone at the top
- Delegation of authority
- Policies and procedures
- Audit committee
- Internal audit

The results of our testing enabled us to rely on the Port’s entity-level controls.

## Information Technology

We review the Port's information technology environment in order to obtain an understanding of how the Port's information technology (IT) affects control activities that are relevant to the audit. When IT is used to initiate, authorize, record, process, and report transactions or data that is included in the financial statements, the system may include control related to the corresponding significant accounts or may be critical to the functioning of manual controls.

IT control activities can be viewed in terms of general controls (ITGCs) and application controls. ITGCs are Port-wide policies and procedures that ensure the proper function and control of information technology. ITGCs include controls over data center and networks operations; system software acquisition, change, and maintenance; access security; and application system acquisition, development, and maintenance. ITGCs are important because they affect applications and data that becomes a part of the financial statements.

We evaluate ITGCs using the five COSO components. For example we assess whether:

- Technology staff are competent and management provides support for technology staff. *(Control environment)*
- Technology conditions are stable. *(Risk assessment)*
- Sufficient controls exist to review performance. *(Control activities)*
- Roles and responsibilities are defined and communicated to IT staff. *(Information and communication)*
- Performance is tracked and the quality of IT controls is assessed. *(Monitoring)*

Application controls apply to the processing of individual applications. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. We test application controls in conjunction with financial statement controls.

We placed special emphasis on the newly-implemented Marina Management System, ERP Gateway, and Clarity Budgeting System.

## Significant Accounts and Processes

We review the Port's financial statements and assess which accounts and classes of transactions have a significant element of risk of material misstatement. We consider items such as susceptibility to error, complexity, volatility of recorded amounts, changes in the account balance or process, degree of subjectivity, compliance issues, etc., when determining the level of risk for each account or class of transaction.

Underlying the significant accounts and classes of transactions are significant processes.

We've identified the following accounts and processes as significant to the Port:

- Administration of federal grants
- Billings, cash receipts, and receivables
- Signatory Lease and Operating Agreement
- Procurement, cash disbursements, and payables
- Payroll
- Capital projects
- Treasury and investments
- Debt and related accounts
- Pollution remediation obligation and contingencies
- Third party management
- Financial close and reporting
- Budget

### **Assessing Design and Implementation of Internal Controls**

In order to obtain an understanding of the Port's internal control over these accounts and processes, we evaluate the design of controls and determine whether they have been implemented. The objective of performing an evaluation of the design of controls is to assess whether the controls are capable of preventing, detecting, or correcting misstatements. Assessing implementation is determining whether the controls are in place as designed. We consider the design and implementation of both manual and application controls or a combination of both.

We assessed the design and implementation of controls for all the significant accounts and processes listed above.

### **Walkthroughs**

In addition to assessing design and implementation of controls, we performed walkthroughs of certain processes, whereby we reviewed a few transactions within each system from beginning to end (i.e., cradle-to-grave method). Some of the walkthrough procedures we perform are re-performing the control, examining source documents, observing real-time application of the control, and performing corroborative interviews with Port personnel.

### **Test of Controls**

After concluding on the design and implementation of controls, we determine which areas we want to perform tests of operating effectiveness of internal controls. We prefer testing internal control wherever possible so as to reduce the amount of substantive testing at final fieldwork.

While internal control is a process, its effectiveness is a state or condition of the process at a point in time. To test for effectiveness, we look to ensure that the control achieves management's objectives, financial statements are prepared reliably, and that applicable laws and regulations are complied. Depending on the frequency of the control, we test a sample of two-to-twenty-five transactions for each instance of the controls. For example, for controls occurring annually and bearing low risk, we may select two instances whereas for daily controls we would select twenty-five instances of the control.

We have obtained the intended level of reliance on internal controls as determined by our audit approach decision model.

## **Compliance Testing**

Major programs identified in 2008 are the Airport Improvement Program and Transportation Security Grant which, as of September 30, 2008, represented about \$31 million or 91% of total federal expenditures at that date.

We also performed test of controls and substantive testing of compliance for all direct and material compliance requirements. In March, we will perform additional testing for grant claims filed in the fourth quarter. Administrative requirements tested included the following:

- Allowable costs
- Cash management
- Davis-Bacon Act
- Equipment management
- Matching
- Period of availability
- Procurement
- Real property acquisition
- Reporting
- Special tests and provisions

## **Passenger Facility Charge Program (PFC)**

In March, we will perform tests of internal control in conjunction with the audit of PFC cash receipts and disbursements.

## **Results of Interim Procedures**

- We obtained the planned level of reliance on internal controls.
- There were no material weaknesses identified as a result of our testing.
- There were no findings or instances of non-compliance noted in our tests of the controls governing federal awards.

## AUDIT PROGRESS

AUDIT SCHEDULE	TIMING
<b>Audit Planning</b>	
Meet with accounting staff to set up the year-end audit timeline, identify and resolve pertinent issues, perform a risk assessment, and address any concerns of management or members of the audit committee or Port Commission.	<i>Completed</i>
Provide management with a detailed comprehensive list of account analyses and other materials to prepare prior to the start of the audit. Work closely with those involved in the audit process to clearly identify roles and responsibilities during the audit.	<i>Completed</i>
Meet with the audit committee to provide an overview of the planned scope and timing of the audit in our engagement service plan.	<i>Completed</i>
Meet with Port management to discuss new Port transactions or activities and new or pending accounting and auditing guidance.	<i>Continuous</i>
<b>Audit Fieldwork</b>	
Perform interim field work to perform testing of the Port's internal controls and to facilitate planning for year-end audit fieldwork. Test certain accounts such as revenue recognition, leases, environmental liabilities, and construction in progress.	<i>Completed</i>
Perform procedures related to administration of federal awards in accordance with Federal Circular OMB A-133.	October – December 2008 and April 2009
Perform the year-end audit fieldwork of the Port's account balances (financial statement audits and testing of fourth-quarter data in Schedule of Federal Awards).	February – March 2009
Perform the audit on PFC receipts and expenditures and related internal controls.	April 2009
<b>Report Preparation</b>	
Issue our opinion on the financial statements and schedule of Net Revenues Available for Revenue Bond Debt Service.	On or before April 30, 2009
Issue Single Audit reports and PFC program audit report.	On or before June 30, 2009
Issue the draft management letter of recommendations.	On or before June 30, 2009
Meet with the Port Commission and management to present audit results.	As requested