



The Connection

A QUARTERLY NEWSLETTER REPORTING NEWS & INFORMATION FROM STATEWIDE ACCOUNTING

in this issue

- 2012 Single Audit – 1**
- Fiscal Year is Coming to a Close – 1**
- Cash Management Focus – 2**
- Fiscal Year-End Training – 2**
- Time, Leave, and Attendance – 3**
- Training – 4**
- Resource Updates – 5**
- Security Related to EFS – 6**
- Is your Technology Access Secure – 7**
- Do you have the SOC[K]s You Need ? – 8**
- Internal Control Update Coming – 9**



2012 Single Audit

The 2012 Single Audit Report is now available online at <http://www.ofm.wa.gov/singleaudit/2012/default.asp>. The Single Audit must be filed with the federal clearinghouse within nine months of the fiscal year end. While it was a scramble at the end, we were able to meet the filing deadline. We thank all agencies who contributed to making this possible.

The 2012 Single Audit reported:

- Federal assistance expenditures of \$15.8 billion
- 63 findings
- \$4 million in questioned costs

There were 13 findings related to subrecipient monitoring and two for failure to obtain Data Universal Numbering System (DUNS) numbers from subrecipients prior to awarding federal dollars. If your agency passes federal funds through to subrecipients, now is a good time to review subrecipient monitoring requirements to ensure that you are complying with federal regulations. We are planning to offer some form of training on subrecipient monitoring later this spring.

There were eight findings on failure to comply with reporting requirements of the Federal Funding Accountability and Transparency Act (FFATA). FFATA requires information on federal awards (federal financial assistance and expenditures) be made available to the public via a single, searchable website. Federal awards include grants, subgrants, loans, awards, cooperative agreements and other forms of financial assistance as well as contracts, subcontracts, purchase orders, task orders, and delivery orders. The legislation does not require inclusion of individual transactions below \$25,000 or credit card transactions.

(continued on page 3)

Another Fiscal Year is Coming to a Close

Now is the time to prepare for closing fiscal year 2013. Here are the important fiscal year-end dates to keep in mind:

Reporting Item	Due Date
Last day of the fiscal year; cash cutoff (refer to OST's closing schedule memo)	June 28, 2013
Disclosure Form application opens	July 15, 2013
Interagency billings must be mailed	July 23, 2013
Phase 1 closes - Agency Accruals	July 31, 2013
Phase 1B closes – certain state disclosure forms are due*	Aug. 23, 2013
Phase 2 closes - Agency Adjustments completed, State and Federal Disclosure Forms are due	Sept. 6, 2013
State Financial Certification form is due	Sept. 18, 2013
Federal Assistance Certification form is due	Dec. 6, 2013

*New for FY13, Phase 1B is an earlier due date for certain state disclosure forms (3 Bond forms, 3 Cash & Investment forms, and Certificates of Participation on the Liabilities form). Details will be included in the SAAM Chapter 90 update issued in May. If your agency cannot complete some or all of the Phase 1B forms by August 23rd, you will need to request an extension by sending a memo to your assigned OFM accounting consultant. The memo should list the form(s) for which an extension is needed and the date by which your agency can complete the form(s). The requested date can be no later than the end of Phase 2, September 6, 2013. Remember that completion of the disclosure forms requires all AFRS entries related to those forms to be complete.

(continued on page 5)

Cash Management Focus

To ensure good cash management over federal grants, the Financial Management Service of US Department of the Treasury implemented the Cash Management Improvement Act (CMIA) of 1990. The CMIA governs the transfer of funds between the federal government and states. The goal is to make cash activity related to federal assistance programs interest neutral

The state of Washington has a number of federal assistance programs that are governed by the CMIA through inclusion in our Treasury State Agreement (TSA). The TSA is renewed annually and for fiscal year 2013 included federal assistance programs that had expenditures over \$30 million. The TSA specifies the techniques used by state agencies to draw grant funds from federal agencies. Many federal grants have been on the TSA for several years and the techniques used to draw federal funds have remained static.

Periodically, it is in the best interest of the state to review the techniques in the TSA to ensure that they represent good cash management from the state's perspective. As part of the process of preparing the fiscal year 2014 TSA, we are working with agencies to review all techniques currently used to draw federal funds and, if applicable, to recommend more effective methods. In addition, we are required to complete a warrant clearance pattern study on selected federal awards this year. OFM and the State Treasurer's Office are working with agencies involved this Spring.

Agencies with federal grants that are not on the TSA should also review current methods used to draw federal funds and ensure that they incorporate good cash management. If you have questions related to cash management related to federal assistance programs, please contact Bret Brodersen at (360) 725-0229 or bret.brodersen@ofm.wa.gov.

Fiscal Year-End Training

Classes on both state and federal year-end closing procedures will be held in June. For those with year-end closing experience, we offer two short (1.5 hours) classes that focus on current year changes and other important items that we want to emphasize.

Class Name	Dates	Times	CPE Hours
OFM-Fiscal Year-end Closing (CAFR) - Update	6/6/2013 6/12/2013 6/20/2013	8:30 - 10:30 8:30 - 10:30 1:00 - 3:00	1.5 hours
OFM-Fiscal Year-end Closing (Federal) - Update	6/12/2013 6/20/2013	10:30 - 12:00 3:00 - 4:30	1.5 hours

The state and federal fiscal year-end closing updates will also be presented at the Financial Management Advisory Council (FMAC) meeting on May 23rd along with cut-off information presented by the Office of the State Treasurer. For a schedule of FMAC meetings visit OFM's website at <http://www.ofm.wa.gov/accounting/fmac.asp>.

For those new to year-end closing, we also offer two half-day (4 hours) workshops. One workshop focuses on expenditures and payables; the other workshop focuses on revenues, reconciliations, and Phase 2 adjustments. These workshops are hands-on with exercises, and are intended for people who are new to the fiscal year-end process. Space is limited in these workshops, so we ask that you read the detailed class descriptions and coordinate within your office so that each agency sends the appropriate staff to each class. Staff may sign up for either one or both workshops if needed.

Class Name	Dates	Times	CPE Hours
OFM-Fiscal Year-end Expenditures and Payables Workshop	6/5/2013 6/13/2013 6/18/2013	1:00 - 5:00 1:00 - 5:00 8:00 - 12:00	4.0 hours
OFM-Fiscal Year-end Revenues, Reconciliations, & Phase 2 Adjustments Workshop	6/5/2013 6/13/2013 6/18/2013	8:00 - 12:00 8:00 - 12:00 1:00 - 5:00	4.0 hours

To view class descriptions and register, go to the Learning Management System website at <http://elearn.dop.wa.gov>.

For assistance or additional information, please contact your assigned OFM accounting consultant.



Update on the Time, Leave, and Attendance Program

Work continues on the Time, Leave, and Attendance (TLA) Program. As noted in prior issues of The Connection, TLA is a first step in modernizing the state's financial and administrative systems by providing an enterprise time, leave, and attendance solution. The program's goal is to deliver a solution that can be made available throughout state government.

The activities for TLA during this past winter mostly consisted of work on the Request for Proposal (RFP). The RFP was released as planned on February 26, 2013 to WEBS and the public TLA website. Evaluations of the RFP responses are expected to begin on April 17, 2013.

The Business Policy and Process (BPP) Project is currently revisiting policy issues and reviewing demo scripts. These items will be presented to the business sponsors and the executive steering committee. BPP is also working with the human resource, payroll, and labor relations communities to (1) validate and draft business rules needed for system design and configuration and (2) identify business policies that require review or standardization.

The Enterprise Technology Preparation (ETP) Project has been diligently working on TLA Enterprise Process Model reviews. These reviews with representatives from the BPP, OFM's Statewide Accounting, and Office of the State Human Resources Director, the two pilot agencies (WSDOT and Ecology), and DES's Enterprise Technology Solutions are high-level walkthroughs of the proposed business process flow that incorporates the TLA solution into the current state environment. Each review session allows for refining and validating the proposed process flow from an enterprise perspective as well as each participant's unique perspective. The next steps for the ETP project will be defining the enterprise architecture along with system and gap analysis.

The TLA Program is very appreciative of the agency involvement over the past few months. More work lies ahead and the Program is counting on continued agency support.

Regular communications are planned through the Financial Management Advisory Council, the Personnel Payroll Association, and the Human Resource Managers to keep you informed of progress and opportunities for involvement. More information can be found on the TLA website at: www.des.wa.gov/tla.

2012 Single Audit - *(continued from page 1)*

Each agency is responsible for its own reporting to the FFATA Subaward Reporting System (FSRS). More information is available at http://www.whitehouse.gov/sites/default/files/omb/open/Executive_Compensation_Reporting_08272010.pdf. If you currently have policies and procedures for compliance with FFATA reporting and are current with your reporting, good for you! If not, you should make it a priority.

If you have any questions or comments, please contact Wendy Jarrett at (360) 725-0185 or wendy.jarrett@ofm.wa.gov.

Training Offered on a Variety of Subjects

We are pleased to announce that several important training classes will be offered by Statewide Accounting and the IRS this quarter. There are a wide variety of subjects, ranging from federal compliance to accounting basics. All classes will be taught by Statewide Accounting, with the exception of the Compliance: Independent Contractor or Employee class, which will be taught by the IRS.

Please note that fiscal year-end training will be offered throughout the month of June.

Class Name	Dates	Times	CPE Hours
Accounting for Payroll	April 4	8:30 - 4:00	7.5 hours
Internal Control: Basics	April 9 May 13 June 18	8:00 - 12:00	4.0 hours
Compliance: Independent Contractor or Employee?	April 11	9:00 - 4:00	7.0 hours
Accounting for Capital Assets	April 16	8:00 - 12:00	4.0 hours
Payroll Revolving Account Reconciliation	April 24	8:30 - 4:00	7.5 hours
Compliance: Travel Policies	April 30	8:30 - 4:00	7.5 hours
In-Process Report Training	May 2 May 28	1:00 - 4:30	3.5 hours
General Ledger Review	May 2	8:30 - 11:30	3.0 hours
Introduction to GAAP in WA State	May 21 June 12	8:00 - 3:30	7.5 hours
Health Insurance Reconciliation	May 29	8:15 - 12:00	3.75 hours
Fiscal Year-End Expenditure & Payables Workshop	June 5 June 13 June 18	1:00 - 5:00 8:00 - 12:00	4.0 hours
Fiscal Year-End Revenues, Reconciliations, & Phase 2 Adjustments Workshop	June 5 June 13 June 18	8:00 - 12:00 1:00 - 5:00	4.0 hours
Accounting for Revenue, Receivables, and Cash Receipts	June 6	9:00 - 11:30	2.5 hours
Fiscal Year-End Closing (State) - Update	June 6 June 12 June 20	8:30 - 10:30 1:00 - 3:00	2.0 hours
Fiscal Year-End Closing (Federal) - Update	June 12 June 20	10:30 - 12:00 3:00 - 4:30	1.5 hours
Internal Control: Payroll	July 11	8:30 - 4:00	7.5 hours

Space is limited in the classes, so we ask that you read the detailed class descriptions and coordinate within your office so that you and your staff attend the right class.

To view class descriptions and register, go to the Learning Management System website.

For assistance or additional information, please contact your assigned OFM accounting consultant.

Administrative and Accounting Resource Updates

The following sites have been recently updated. Check them out at <http://ofm.wa.gov/resources/default.asp>:

- **Travel**
 - o Travel do's and don'ts: Updated to reflect state agency changes per ESSB 5931 (Department of Enterprise Services).
 - o Quick reference guide: Updated to reflect all travel related internal required policies including international travel.
 - o Frequently used travel internet sites: Updated links.
 - o If you have any questions, please contact Bret Brodersen at 360-725-0229 or bret.brodersen@ofm.wa.gov.
- **Transportation**
 - o Added: How to request a motor vehicle waiver.
 - o If you have any questions, please contact Bret Brodersen at 360-725-0229 or bret.brodersen@ofm.wa.gov.
- **Payroll**
 - o Pay dates and holidays: Added 2014.
 - o IRS training materials: Added the December, 2012 IRS Form 1099 and backup withholding training materials and removed the 2011 version.
 - o Reconciliation: Added 2013 reconciliation templates and year-end 2012/beginning 2013 information.
 - o Salary overpayments: Updated Overpayment identification/recovery and collecting prior year overpayments to include current year examples.
 - o If you have any questions, please contact Steve Nielson at 360-725-0226 or steve.nielson@ofm.wa.gov.
- **Miscellaneous**
 - o Guidelines on paying for professional employee certifications, memberships, or training: Updated verbiage to focus on what an agency should consider in lieu of more directive language.
 - o If you have any questions, please contact the OFM Accounting Consultant assigned to your agency.

Another Fiscal Year is Coming to a Closing - *(continued from page 1)*

As discussed previously, the financial community is seeking more timely financial information. In response to this, we initiated our "faster CAFR" initiative a couple of years ago. Thanks to all of you, we were able to meet our goal last year and issue the CAFR on November 15th. Our goal for this year is November 8th. In order to make this year's goal, we are stressing the importance of meeting the interagency billing due date of July 23rd and trying out the new Phase 1B. We continue to look for ways to lean the CAFR process and welcome your suggestions.

Chapters 90, State Reporting, and 95, Federal Assistance Reporting, in the State Administrative and Accounting Manual are updated every year to reflect changes in reporting requirements. The Chapter 90 update will be issued in May and Chapter 95 will be updated immediately following the issuance of the Office of Management and Budget's Circular A-133 Compliance Supplement. For additional information, please contact your assigned OFM accounting consultant.

Security Considerations related to Economic Feasibility Studies

Washington state agencies have been actively pursuing electronic payment applications in order to increase efficiency or respond to customer requests for alternative payment methods. State law (RCW 43.41.180) and State Administrative and Accounting Manual (SAAM) Chapter 40 require all agencies to submit an Economic Feasibility Study (EFS) to the Office of Financial Management (OFM) for approval prior to accepting or disbursing payments electronically, with certain exceptions.

For more information about the EFS process, refer to SAAM Chapter 40 (<http://www.ofm.wa.gov/policy/40.htm>) and the OFM E-Commerce Resources website (<http://www.ofm.wa.gov/resources/ecommerce.asp>).

In addition to the EFS requirements, there are security considerations to be aware of when agencies are accepting credit or debit card payments from customers. The **Payment Card Industry (PCI) Security Standards Council** sets security standards to protect cardholder data. All merchants/agencies that accept credit or debit card payments must follow PCI Data Security Standards (PCI DSS).

The standard includes 6 goals and 12 requirements for any merchant/agency that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment. PCI compliance can be boiled down to three essential steps: assess, remediate, and report.

Step 1 – Assess

The primary goal of assessment is to identify all technology and business process vulnerabilities that pose risks to the security of cardholder data that is transmitted, processed or stored. You should constantly monitor access and usage of cardholder data.

Step 2 – Remediate

Remediation is the process of fixing vulnerabilities – including technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data. The best practice is to not store cardholder data unless you need it.

Step 3 – Report

Regular reports are required for PCI compliance. All merchants and processors must submit a quarterly scan report. There are four merchant levels depending on the number of transactions processed per year. The degree of PCI compliance that you are subject to gets stricter as the number of transactions increases. Merchants/agencies with large transaction volume must do an annual on-site assessment. Merchants/agencies with small transaction volume may be required to submit an annual Attestation within the Self-Assessment Questionnaire.

Many agencies seek out a third party vendor to provide customers with the option to pay with a credit or debit card, and they may think that they are passing the responsibility for PCI compliance on to that third party vendor. However, that is not true. Ultimately, the agency is responsible for ensuring PCI compliance. Also, keep in mind that each payment card brand has its own program for compliance, validation levels and enforcement.

(continued on next page)

(continued from previous page)

For more information on PCI compliance, refer to the PCI Security Standards Council website at <https://www.pcisecuritystandards.org/>.

In addition to PCI compliance, the **Office of the Chief Information Officer** has policies that agencies must follow on securing information technology assets. This includes personal information that is collected, managed, used, and stored by agencies. Agencies are responsible for protecting the integrity, availability, and confidentiality of information collected in the course of accepting electronic payments that is held by an agency or a third party.

For more information about the OCIO statewide technology policies, refer to <http://www.ofm.wa.gov/ocio/policies/default.asp>.

Is Your Technology Access Secure?

We cannot escape the topic of security. In other articles in this edition of the Connection, you can read about security over payment card holder data and data in control of a third party. In addition to those areas, security over technology access in our own agencies is also important.

Proper security controls limit access to technology systems to only those who need it. Problems can occur when controls are designed, implemented, or operating improperly. While nothing can fully replace an agency testing its own controls, audit issues often point out areas of deficiency. In conjunction with the last CAFR audit, the State Auditor's Office sent 14 management letters to agencies they audited. Of the 14, nine included recommendations for improvements to internal controls. Of the nine, seven included one or more access related recommendations, which are summarized below:

- Excessive or improper electronic access to modify programs
- User access to program screens, tables, or databases that is broader than needed to perform the job
- "Super user" access that is not adequately controlled
- Access given to an excessive number of users who can maintain information
- Access that allows changes to information without an adequate audit trail.

What can agencies do? Here is a partial list.

- Implement a procedure to timely revoke user access when an employee, volunteer, or contractor leaves the agency or no longer needs their current level of access. Remember to do this when an employee is promoted or moves to another section as well.
- Implement a procedure to periodically review access for all employees to all systems. This should be done by someone who does not have the ability to change access. Remember to make changes when needed.
- Get further information.
 - o The Office of Chief Information Officer (OCIO) Policy No. 141, ***Securing Information Technology Assets***
 - o Statewide Accounting Resource ***HRMS Audit – Payroll Considerations***
 - o Your agency's IT department, internal control policies, and internal audit personnel

As a final note, access security is a broad and complex subject that involves many areas of an agency in addition to finance. This article is **not** meant to be a comprehensive study on the topic; it is meant to stimulate conversation and, where necessary, action.

Do You Have the SOC[K]s You Need?

Since the first byte of state data was stored on the first computer, the state has been responsible to secure electronic data and implement adequate controls in technology applications and related processes. A lot has changed since the early days of computers! Part of what has not changed is the state's responsibility. Part of what has changed is that third parties, called service organizations, are increasingly in control of state data and technology applications. For example:

- State information may be stored in "the cloud" as it can be with e-mail
- A vendor may own and run software that processes financial transactions for the state
- A third party vendor may process credit and debit card transactions for a state agency's web purchasing or point of sale system.

What happens when a service organization is involved? When a service organization has control over the state's information, whether the organization is merely storing it or processing transactions, the state is still responsible to know the information is being handled with adequate controls in place. A Service Organization Control (SOC) Report helps give that assurance. While there are 3 levels of reports, SOC 1 and SOC 2 Reports are the most common.

Who requests the SOC Report? Ideally, the request should be part of an agency's contract with the service organization.

Who prepares the SOC Report? Usually the service organization hires an independent auditor to audit the service organization and prepare the SOC Report so all of the service organization's clients can use the same report. Audits and reports are usually done annually.

Who uses a SOC Report? Agency management uses a SOC Report to help fulfill their responsibility for effective internal control. The State Auditor's Office may use a SOC Report when auditing information generated by service organizations.

Who decides what kind of SOC Report is needed? This varies, but the agency contracting with the service organization, OFM, the State Auditor's Office (if they will be relying on the report in an audit), and the service organization need to be in agreement about the specifics of the report.

What is a SOC 1 Report and when is it used? A SOC 1 Report reports on controls relevant to internal control over financial reporting. Generally, it is used when a service organization provides financial transaction processing for amounts that are part of the state's Comprehensive Annual Financial Report (CAFR). In addition, bond covenants, contracts and agreements can require a SOC 1 Report.

What is a SOC 2 Report and when is it used? A SOC 2 Report reports on controls relevant to the five trust principles: security, availability, processing integrity, confidentiality, and privacy. A SOC 2 Report is used when a service organization has control over sensitive state information and it's important to know the service organization's controls over one or more trust principles are in place and working.

How do you know if a SOC Report is needed? A SOC Report may be needed in any of the 3 examples initially cited in this article and whenever a third party is in control of or processes the primary version of state information or any version of sensitive state data. If in doubt, contact your OFM accounting consultant.

An Internal Control Update is Coming Soon!

What publication is being updated? The Committee of Sponsoring Organizations of the Treadway Commission (COSO) announced recently that the updated Internal Control–Integrated Framework (Framework) is expected to be released soon. The original framework, published in 1992, is used globally as a leading framework for designing, implementing, and maintaining internal control. In fact SAAM Chapter 20 Internal Control and Auditing is based largely on the original Framework.

Why is the change needed? In the 20 years since original publication, business and operating environments have changed dramatically, becoming increasingly complex, technologically driven, and global. At the same time, stakeholders are more engaged, seeking greater transparency and accountability for the integrity of systems of internal control.

What is changing? Much of the original Framework has been retained, including the five framework components, but there are certain enhancements. One of the more significant enhancements is the formalization of fundamental concepts as principles. These 17 principles provide additional clarity for the user in designing and implementing systems of internal control and for the auditor in testing internal control.

What will the principles accomplish? Because the 17 principles are drawn directly from the framework components, an entity can achieve effective internal control by applying all principles. Conversely, effective internal control may not be present and functioning if any of the principles is not applied.

What are the principles? The principles and their related framework component are listed below.

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

(continued on next page)

(continued from previous page)

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

What are the next steps? Because our environment is ever changing, your documentation should be viewed as a work in progress. You should continue to review your internal control documentation, to evaluate how the principles align and to add controls and documentation where needed.

How can you get more information? If you have any questions, contact Kim Thompson at 360-725-0224 or kim.thompson@ofm.wa.gov.

