The Audit Connection

Welcome to WASBO 2024! The Office of the Washington State Auditor is delighted to see everyone in person again this year, and share all the ways we can work together on #GoodGovernment.

Check out our sessions

- Basic enrollment reporting
- Keep ASB accounts neat and tidy
- Protect data from cybercrime
- Cultivate strong teams
- Fight fraud with SAO
- What's new for schools in FIT

Stop by our exhibitor booth

- Come see your district's FIT profile
- Learn what trainings we offer
- Meet SAO staff and ask questions

McCarthy's Corner

We've all heard the observation, "The only constant is change." It's attributed to the ancient Greek philosopher Heraclitus, and it is as true for us today as it was for him 2,500 years ago.

Continued on page 2

Have a peek inside

McCarthy's Corner –
Continued from page 1

Rarely have we seen so much change, so quickly as we have over the past four years. Just from the perspective of public finance, we witnessed an abrupt shift in funding models to deal with the COVID-19 pandemic, a subsequent tsunami of emergency federal support for government, followed by the end of those emergency measures and today's increased expenses in many areas.

I know the Washington Association of School Business Officials is working to assist members as they navigate such constant change, no matter where they come from across the state, or the size of their district.

And, as always, we at the Office of the Washington State Auditor are ready to assist, with a host of resources and information, including this special addition newsletter, just in time for the annual association conference.

You will find articles on topics like improvements to our Financial Intelligence Tool, FIT, which is now mobile-friendly. And, later this year, school district data in FIT will be available to anyone interested in the metrics and finances of Washington's nearly 300 districts. You can also read about properly accounting for associated student body funds – a common area for audit issues.

But beyond these pages, you can also talk to us! We will host a booth at the conference where you can ask our staff questions, learn more about the training we offer, and check out your district's profile on FIT.

We are presenting on several topics, as well, including cybersecurity and fighting fraud. As the State Auditor, I can tell you these issues are "trending." Cybersecurity has never been more important as threats to local governments increase, and we've seen an unsettling tendency for fraudsters to be more brazen in their schemes.

Of course, we will be present to listen, as well. It's important to us to hear the concerns of school districts and learn more about the issues you face. We know many of your districts are facing fiscal challenges, and we continue to partner with WASBO and governments across the state to support strong financial stewardship.

Pat McCarthy
Pat.McCarthy@sao.wa.gov, (564) 999-0801

State Auditor Stewardship Award: Oak Harbor S.D.

In April, the Office of the Washington State Auditor recognized Oak Harbor School District with a State Auditor Stewardship Award. The District's Finance Department, under the leadership of retired Business Director Vicki Williams, has a strong internal control environment. This was especially clear during the District's annual financial reporting and implementation of several new accounting standards. District staff were proactive and thorough in developing their understanding of these new financial standards, and the documentation staff retained clearly supported their decision-making process. The documentation was so detailed and thorough that it was used as a "best practice" model for SAO auditors when evaluating the implementation of the same standards at other school districts.

From left to right: Board President Lynn Goebel, Coleman Wilson, Heidi Macaluso, Rachel Frankwich, Michele Leslie, Kristi Coffey, Auvie Astorga, Fiscal Services Supervisor Michele Laiblin, State Auditor Pat McCarthy, Board member Nicole Tesch, Board member Sharon Jensen, Finance Director Amber Porter, Team Bellingham Audit Manager Deena Garza, and Superintendent Dr. Michelle Kuss-Cybula.

Pop quiz

Where can you find top financial resources for schools in one spot?

(hint)

SCAN CODE

We've compiled links to some of our most useful resources and articles in one blog post, so you can easily find what you need, when you need it. Procurement, federal grant programs, internal controls—we have plenty of tools to help you improve your policies and processes!

Scan the code above and get started today, or go old school and visit **sao.wa.gov/school-top-resources** to learn more. Keep this link handy – we'll post our updated financial statement checklist just for schools later this summer.

#ToolsForSchools

FIT for schools will be fully in session this summer

We are excited to announce that our Financial Intelligence Tool (FIT) has received a myriad of improvements and updates since we introduced it at last year's WASBO annual conference! FIT will soon allow all Washingtonians to easily explore the finances of all 295 school districts in one place.

FIT is a user-friendly, customizable database from SAO's Center for Government Innovation that allows free online access to a decade's worth of financial data from nearly 2,000 local governments throughout the state, plus four years of financial data from nearly 300 school districts.

The goal of FIT is to allow people to easily access financial data in an easy-to-understand way. Users can filter and arrange this data all in one place, personalizing the way you can view the information that's important to you. You can:

- Find your own district's financial profile, plus profiles of 294 other school districts in Washington
- See how your district compares with others based on revenues, expenditures and enrollment
- Take a wider look at statewide activities of all school districts, helping you answer questions like, "How much in total property taxes do school districts collect?"
- Examine and assess indicators of financial health for individual districts and overall, for all of Washington's districts
- Access other relevant information like audit reports from the comfort of your laptop, smartphone or tablet

While these features have been publicly available for most local governments for several years now, only those who worked for a school district could access district information. This summer we will complete our latest FIT upgrade, making this school information available to everyone and increasing access for not only school business professionals like you, but also students and other members of the public.

WASBO Session Alert

Interested in learning more about FIT and how you can use it to converse better with non-technical crowds?

Join us

Thursday, May 9, 3:40 p.m. to 4:30 p.m., GTCC 403

for our "Are you smarter than a 5th grader…" session, where we'll walk you through FIT, step-by-step. By the end you should be able to ace a pop quiz about your district using FIT!

FIT FINANCIAL INTELLIGENCE TOOL
Office of the Washington State Auditor

Remember to check the conference app for the latest schedule.

Take charge of your credit card program. Implement our updated best practices today!

How long has it been since your government evaluated its credit card program? Was it when we published our original best practice resource in July 2019, just before the start of the COVID-19 pandemic?

Time sure flies, but don't worry – we have **updated best practices** to help guide you today, whether you have a small credit card program with just some activity or a full-on procurement card program with millions of charges. We've added more best practices to our resource, about 14 in total, to help you better manage the risk that comes with having a credit card program.

Plus, we have a few key tips below as well.

A word to the wise: Don't underestimate the risk

The risk with credit card programs is real. Cardholders have tremendous control over a single transaction, which places considerable pressure on your monitoring controls. All too often, governments do not monitor enough and fail to identify unallowable charges. Performance audits from around the country often find questionable credit card purchases such as personal expenses, gifts, food and refreshments – even when a local government's internal audit department performs audits annually. These audits also report frequent problems with split transactions, where employees find ways to circumvent single transaction limits.

To help you mitigate these risks, our updated monitoring best practices booklet focuses on three themes: implement a robust review process, perform central transaction monitoring, and conduct a thorough annual card review.

Best practice theme 1: Implement a robust review process

We recommend the cardholder's direct supervisor or manager review their purchasing activity. Supervisors and managers know their employees' activities, so they are in the best position to identify questionable transactions. But you might also consider a second reviewer, someone well-versed in policy requirements who might detect something supervisors have overlooked. You could always opt for a review checklist, to make sure that reviewers cover all the important bases. Lastly, impose a strict deadline for all the reviews to take place.

Best practice theme 2: Perform central transaction monitoring

You should assign someone to centrally review and monitor transactions, as frequently as daily. You might say you don't have the resources to do this, but remember, many credit card programs generate rebate

revenue. This revenue can and should be used to pay for the extra monitoring. And you should perform a risk-based review, which means you won't look at everything.

Our updated resource includes a comprehensive list of items to review. For example, you might find it helpful to review declined and disputed transactions, to identify areas of concern and other red flags. In addition, you might review for transactions that exceed your single purchase transaction limit. Vendors can process transactions manually and override your established limit, so you want to check that.

Best practice theme 3: Conduct a thorough annual card review

We've expanded our guidance on how you should conduct an annual card review. During this process, you should physically verify the cards, make sure that your provider's active cardholder list aligns with your own records, and double-check credit limits. Consider lowering any exceedingly high credit limits and closing infrequently used cards. Otherwise, you unnecessarily expose yourself to potential fraudulent activity.

You can find our **Best Practices over Credit Card programs** in our Resource Library. Download a copy and get started on strengthening your internal controls today. If you use your credit cards for travel expenses, you'll also want to review our recently updated **Best Practices for Travel and Reimbursable Expenses**.

Visit our Resource Library

All our guidance is available online at no cost. We have a lot of great information to share, so spend a few minutes in **SAO's Resource Library** to see what we have to offer!

How to reach us for more assistance

Remember, SAO can help. If you have technical questions, submit them using our **HelpDesk** in the client portal.

WASBO Session Alert

Attend the SAO Audit Update to learn about recent audit issues, GASB updates, and key changes to the School District Accounting Manual.

Thursday, May 9, 9:00 a.m. to 9:50 a.m., Marr Chambers II

Remember to check the conference app for the latest schedule.

SAO examines performance in pandemic practices, dual credit programs and special ed

The State Auditor's Office often conducts performance audits examining various aspects of Washington's K-12 educational system and related areas pertaining to student health or learning opportunities. In the year since the 2023 WASBO conference, performance auditors have explored three areas of interest to educators, and this work is likely to inform school and district decisions in the coming years.

K-12 Education During and After the Pandemic (November 2023)

When schools were closed to in-person learning, the state gave school districts great flexibility in how they ensured students' access to instruction. **This audit, published in November 2023,** surveyed 11 school districts and Impact Public Schools (which operates four charter schools in Washington). We also spoke with representatives of Educational Service District 113 and used their responses and conversations to build a list of creative and nontraditional teaching practices applied over the past three years that may be useful for other educators. The 25 identified practices – explored in detail in the report – fell into five broad categories:

- Individualized instruction
- Access
- Student and family engagement
- Teacher training
- Social-emotional needs

Dual Credit Programs in Washington (in progress)

Students in dual credit programs earn high school and college credit simultaneously, and benefit from these programs partly because of their early exposure to college coursework and reduced college education cost. However, two- and four-year colleges and universities establish their own policies and procedures to determine how the credits students earned in a high school dual-credit program are transferred to and accepted by other colleges the students may later attend. This audit will assess a sample of eight colleges and universities to learn how they accept dual credits that students earn in two of Washington's large dual credit programs: Running Start and College in the High School. Although our auditees are higher education institutions, the final report will likely contain results and recommendations that will interest all schools and districts. We anticipate publishing it in early fall 2024.

Improving Recruitment and Retention of Special Educators (in progress)

Washington has a significant shortage of people qualified to work in special education including teachers, paraeducators and support specialists like speech pathologists and psychologists. Each of these roles can be critical to the academic success of students with disabilities. According to the Office of Superintendent of Public Instruction, turnover is high in this field, with vacancies four times higher than in general education. This audit will identify factors contributing to the shortage and turnover of special educators and consider strategies that educational agencies can use to improve recruitment and retention. We plan to publish this report in summer 2024.

WASBO Session Alert

Learn how auditors test basic enrollment, what documentation supports enrollment reporting, and how to minimize errors.

Thursday, May 9, 11:30 a.m. to 12:20 p.m., Marr Chambers 1

Remember to check the conference app for the latest schedule.

Bank statement review is a top-notch fraud-fighting tool. Here's how to do it

One of the best tools in your fraud-fighting toolbox is a bank statement review. Whether you are a finance professional, a department head, or even an elected or appointed official, reviewing the bank statements can greatly increase your odds of deterring and detecting fraud.

Why is bank statement review important?

Your government's bank account activity is how anyone can see where your money is coming from and where it is going. This is why many fraud schemes show themselves – boldly or subtly – on the bank statements. For example, statements can reveal:

- Key information about the government's financial position, including the amount of cash in the bank and the level of monies flowing in and out.
- Details for risky transaction types, such as wire transfers, automatic withdrawals and other electronic payments.
- Unusual activity, such as duplicate check numbers clearing the bank.

Reviewing bank statements each month also will help you build expectations of what is "normal" – typical transaction types, payees and activity levels – to apply in your future reviews.

The Office of the Washington State Auditor has investigated many losses that governments could have detected sooner through a simple bank statement review. Our staff have detected several misappropriations when reviewing bank statements as part of a regular audit.

Even a short, 15-minute scan by an independent reviewer can be the difference between deterring loss and identifying it early, or having it go undetected for a long period of time.

Your bank statement review playbook

If you aren't sure what to look for in a bank statement, or aren't confident you'd notice anything risky – don't worry! We've made a five-part playbook for you to follow.

Playbook chapter 1: Obvious red flags

Keep an eye open for these transactions, which are high-risk indicators for potential fraud schemes:

1. **Electronic payments to employees,** such as wire transfers. Direct wire transfers to employees are hardly ever valid. Employees should be paid only through your normal payroll and accounts payable process. Reimbursements, travel advances and any other payments also should follow a normal process.

2. **Cash and ATM withdrawals.** Governments don't withdraw cash from ATMs. If a government needs cash, staff should write an accounts-payable check and cash it at the bank. Any cash withdrawals should be scrutinized thoroughly.

3. **Payments to unknown or unusual vendors.** You will likely recognize most of your government's vendors – especially ones receiving electronic payments and/or high-dollar amounts. If you see a vendor you don't recognize, ask staff for payment support documents (not just a verbal explanation).

4. **Payments to non-traditional banks and money servicing apps that are unlikely to be used by those doing legitimate business with a government.** Governments generally don't make payments using, for example, PayPal or Western Union; nor do they typically pay vendors who use GoBank or GreenDot. Question those if you see them.

5. **Check if the payee is unexpected or doesn't match the endorsement.** If your bank statements include scanned copies of checks, glance at the payee line

to look for unexpected or suspicious payees, such as the names of employees or their family members, for example. If the statement also includes a scan of the check's back, look at the endorsement to see if it matches the payee.

Playbook chapter 2: Altered bank statements

Because bank statements are so revealing, fraudsters often alter them before someone else independently reviews them. That's why original bank statements are best. If possible, access the statements directly from the bank. But even if you get the statements from staff, be on the lookout for red flags indicating the statements may have been altered. Some examples:

1. Inconsistent formatting or alignment of rows, sections or columns
2. Missing bank header, footer or page numbers
3. Mathematical errors
4. Nonsequential checks without notation. Banks often indicate a gap in check sequence with an asterisk or other marking. Missing marks could indicate someone altered the statement to remove a check they didn't want seen.

Playbook chapter 3: Trends

Reviewing bank statements over time helps you gain an understanding of normal activity, and allows you to notice suspicious trends. Some examples:

1. Declining account balance
2. Repetitive payments that don't make sense. Most vendors expect to be paid monthly at most. Paying the same vendor more than once in a period can be a red flag for disbursement fraud.
3. A new vendor payment that you haven't seen in prior statements. While this activity could be appropriate, you should ask to see supporting documents. New electronic payments to vendors can be a red flag for either fraud by an employee or an external cyber-related loss.
4. A high volume of transfers to other accounts. Ask to see the statements for those accounts, and inquire what the transfers are for.
5. Multiple payments for things that usually are renewed annually or quarterly – things like software licenses, insurance or taxes.
6. Decreased frequency or dollar amount of deposits. This can indicate a cash-receipting fraud.

Playbook chapter 4: Overdraft fees and other oddities

Here are other items you should notice if you review bank statements regularly.

Governments should have sufficient cash in the bank to cover expenses. Declining financial condition can be an indicator that a fraudster is diverting cash receipts or creating inappropriate payments. Be on the lookout for:

1. A negative account balance at any point in the month
2. Overdraft fees or other penalties

Another red flag is deposits made in even-dollar amounts, especially if you collect fees from customers. When was the last time you paid a bill without any "cents" at the end of the amount?

Playbook chapter 5: Your judgment

Apply your knowledge of your government, its operations and activities to the bank statements. Do you see payments to a contractor when your government isn't doing any construction? Payment to an escrow company when your government hasn't purchased any real estate? Combine your knowledge and judgment with a healthy level of skepticism when reviewing the statements.

Recent case studies

Our Office has issued some fraud investigation reports for cases in which a simple secondary review of the bank statement activity could have identified the fraud sooner. We've included a summary of each case and links to the full reports below.

- **City of Kahlotus**, issued Feb. 16, 2023. The Clerk/Treasurer withdrew $1,237 in cash from the City's bank account, and used the City's credit card for personal purchases totaling $4,464. We also identified an additional $6,538 in questionable purchases.

- **Town of Springdale**, issued March 7, 2022. The Mayor used the Town's bank account and related debit card to make personal purchases, cash withdrawals, and mobile payments to her personal bank account. Additionally, she wrote a $5,000 receipt for a donated item, but never deposited the proceeds. Total misappropriation was $15,252.
- **City of Tenino**, issued Jan. 13, 2022. As a result of a phishing email appearing to be from a local government association, the Clerk/Treasurer made 20 electronic payments totaling $336,968 to multiple out-of-state bank accounts. When the Clerk/Treasurer eventually asked for the Council's preapproval to write some checks to the association, he did not disclose that he had already sent $45,090 through electronic payments.
- **Camas Washougal Economic Development Association**, issued May 14, 2020. The Executive Director obtained a debit card to make purchases without approval, misappropriated $19,311 in purchases, and made questionable purchases of $45,029 from February 2013 to March 2019.
- **Pierce County Housing Authority**, issued Dec. 16, 2019. Between July 2016 to February 2019, the Finance Director misappropriated $3,237,712 in vendor ACH disbursements. She did this by changing vendors' bank account information in the accounting system to her personal bank account information. She also wired $3,050,000 to her personal bank account from January 2019 to July 2019, and wired $635,000 to make personal property purchases in 2018.
- **City of Mossyrock**, issued Dec. 14, 2017. The Clerk/Treasurer used the City's bank account to set up a monthly automatic withdrawal for her personal mortgage payments, resulting in a $58,895 misappropriation.

SAO's other fraud-prevention resources

We have several other resources to help you prevent, detect and deter fraud in your government. Here are just a few from our Resource Library and Audit Connection Blog:

> **Trust, but verify: A guide for elected officials & appointed boards to prevent fraud**

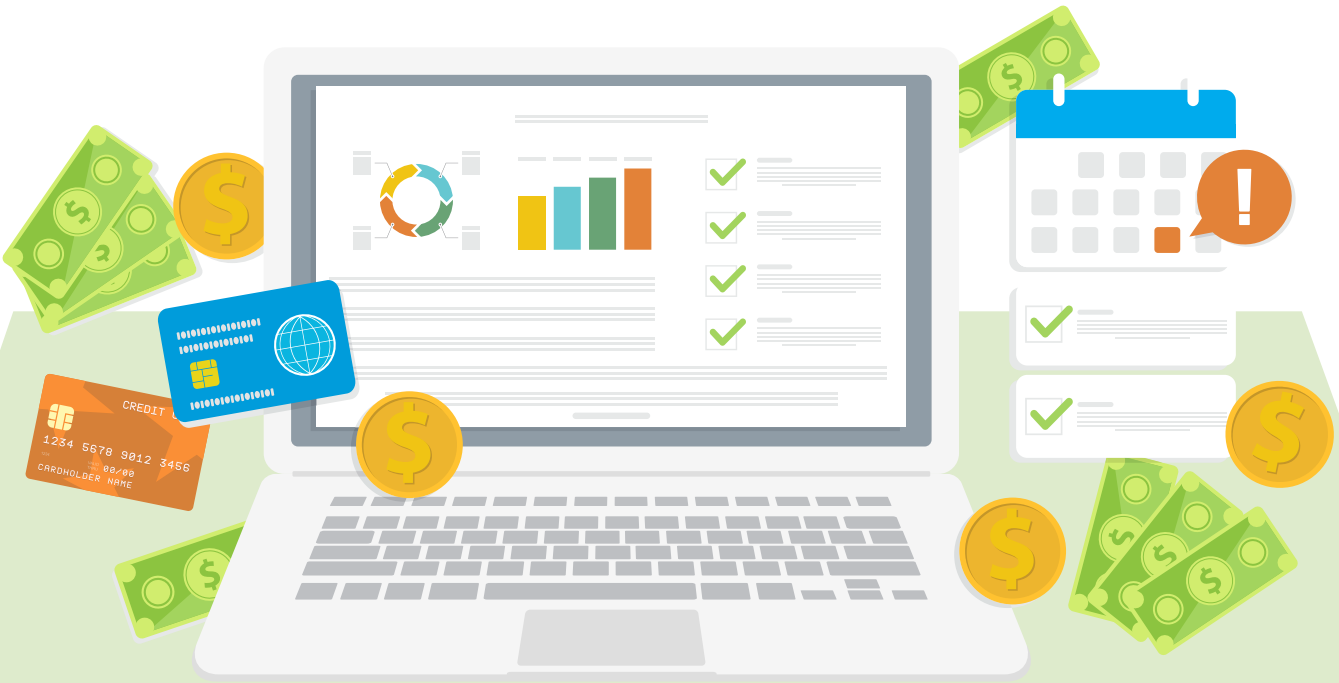
> **Best Practices: ACH electronic payments**

> **Best Practices: Sending wire transfers**

> **How to prevent ACH and bank fraud, published Sept. 18, 2020**

> **Start the year off right: New best practices and tools for bank reconciliations**, published Feb. 7, 2020

> **Positive Pay can help protect your organization from check fraud**, published June 30, 2017



Expect the unexpected: SAO releases new guide on protecting unanticipated revenue from fraud

Local governments rely on predictable and stable revenues from things like property and sales taxes, various charges and fees, and transfers from state and other local governments.

But not every revenue is predictable. Most governments also receive revenues from rebates, donations, collection agency payments, agreements with annual payments, or one-time fees. These revenues are infrequent or unanticipated, making them a prime target for misappropriation.

According to the 2022 Report to the Nations from the Association of Certified Fraud Examiners, fraud of unanticipated revenue accounts for about 17 percent of all asset-misappropriation schemes, with a median loss ranging from $45,000 to $50,000. These schemes typically last for 14 to 16 months before being detected.

Washington is no exception, and SAO's Special Investigations Team has developed a guide to help you: "**Expect the Unexpected: How to protect unanticipated revenue from fraud**." This resource has best practices and other tips to help you evaluate your internal controls around unanticipated revenue, and how to improve them.

Here's a look at some of what's included:

- A list of common types of unanticipated revenue, to help you know what to look for
- Common tactics fraudsters use to swipe these funds
- Ideas for how to prevent this type of fraud in your government
- Behavioral red flags to watch for
- Best practices for detecting this type of fraud

Additional resources

SAO's Resource Library offers a variety of free guides, checklists, and best practices to help Washington's governments improve their internal controls to prevent fraud.

SAO's Preventing Fraud webpage contains multiple internal control assessment tools, guidebooks, free training links, and additional resources to help combat fraud related to cash receipting.

WASBO Session Alert

Find out about the latest fraud schemes, including case studies, and also how to make sure they don't happen to your District.

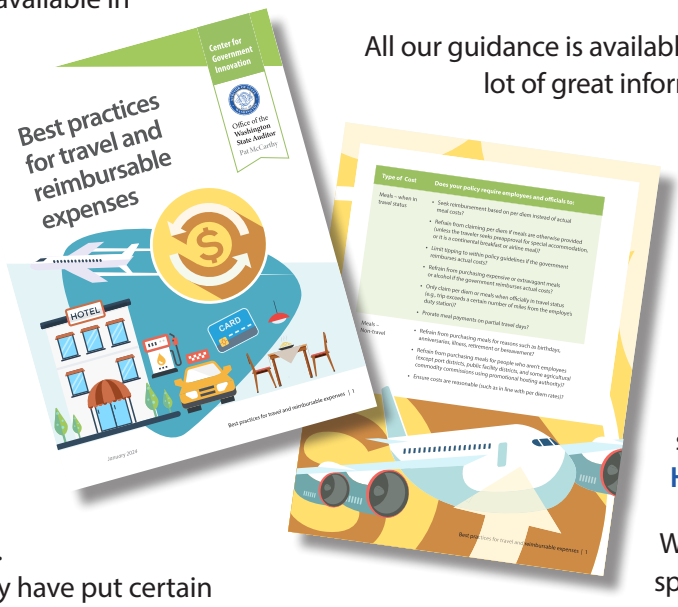
Thursday, May 9, 2:40 p.m. to 3:30 p.m. for Part I; 3:40 p.m. to 4:30 p.m. for Part II, Marr Chambers I

Remember to check the conference app for the latest schedule.

Planes, trains and travel expenses: Upgrade your government's internal controls with our updated resource

Employees are on the road again, traveling to trainings, conferences and handling other work-related business. Now's a good time to ensure your governments' internal control systems for processing employee reimbursements and travel claims are ready to handle this activity while preventing waste, loss or abuse.

We are here to help, with an **updated best practice guide on travel expenses** now available in our Resource Library.



Many governments adapted control processes for employee reimbursements during the COVID-19 pandemic, when travel was at an all-time low and employees worked from home. And since employees were not traveling and seeking reimbursement, you may not have prioritized updating your policy or control system – even when it came due for an update. In some cases, governments may have put certain key internal controls on hold during the pandemic emergency. With more people traveling again, it may be time to reinstate them.

Your policy should describe the key elements of your control system for processing travel claims and other employee reimbursements. The **Government Finance Officers Association** recommends updating travel policies every three years, and we agree. You can use our newly updated resource, as well as **guidance from the Municipal Research and Services Center**, to reevaluate.

You'll find our updated *Best practices for travel expenses and other reimbursements* **here**. During this update, we:

- Added new best practices, such as ideas to reduce the administrative burden of travel advances, a tip to comply with IRS regulations, and a list of travel-related performance metrics you could use
- Expanded the list of economical travel considerations
- Created a new section for travel expense fraud schemes, which you can use to develop in-house training for travel claim reviewers and approvers

Download a copy and get started on strengthening your internal controls today.

Visit our Resource Library

All our guidance is available online at no cost. We have a lot of great information to share, so spend a few minutes in **SAO's Resource Library** to see what we have to offer!

How to reach us for more assistance

Remember, SAO can help. If you have technical questions, submit them using our **HelpDesk in the client portal**.

We also have internal controls specialists at SAO's Center for Government Innovation available to talk with you about best practices and resources. For assistance, reach out to us at **Center@sao.wa.gov**.

WASBO Session Alert

Learn how to protect travel and other expenses from fraud, waste, and abuse – featuring a new travel resource from SAO's Center for Government Innovation.

Thursday, May 9, 9:00 a.m. to 9:50 a.m., Marr Commerce

Remember to check the conference app for the latest schedule.

Small-dollar transactions, big responsibilities: What you need to know about ASB fundraising and cash receipting

Whether from yearbook sales, prom tickets or direct donations, **the money raised by Associated Student Body groups are public funds.**

State law (RCWs **28A.325.020** and **.030**) makes plain that ASB funds are designated as public funds of the school district. This means districts must safeguard and account for ASB funds the same way they guard levy dollars or apportionment funds. It also means if ASB funds go missing or are stolen, you must report the loss to SAO.

Since fundraisers often involve lots of transactions for small dollar amounts being collected by students, they are a high-risk activity that call for strong controls and oversight. Ensuring you have strong cash handling procedures in place will go a long way to protecting these public funds. Some key steps to take for every fundraiser:

1. **Document all the money you receive as soon as you receive it.** Lots of methods can achieve this goal: cash register receipts, reports from a point-of-sale system or old-fashioned receipt books. (If you use receipt books, just make sure they're printed with the district and school name on them as a fraud-prevention measure.) If you have to void a receipt, two people must witness and sign it.

2. **Do a cash count.** If it's a multi-day event, do it at the end of each day. At one high school, SAO auditors conducted their own cash count and found the ASB fund was $1,161 short. A school official was aware of the shortage, but did not quickly report it to management. That meant the loss of public funds was not reported to law enforcement or SAO as required by state law.

3. **Deposit the funds each day**, in the same cash or check composition noted on the receipts and cash counts. (To deposit less frequently requires a waiver from your County Treasurer (**RCW 43.09.240**). SAO auditors once discovered an ASB holding more than $15,000 in the ASB office. This substantially increases the risk of fraud or loss.

   > Money collected at an after-school event should be locked in the school safe or deposited in the night drop at the district's bank.

4. **Ensure the fundraising receipts are reconciled** to the fundraising documents and revenue projections at the end of the event.

Other best practices include ensuring you provide annual training for ASB staff and students on the role of ASBs; establish procedures for activities that involve goods or money; and having rigorous staff oversight of ASB activities to ensure everyone follows district policies and procedures.

SAO offers resources and an on-demand training to make sure your cash handling procedures are strong:

- **Cash Receipting Guide and Checklist:** Find tips and best practices for managing your cash collections. The guide includes a suite of short, one-to-two-page resources for leaders, managers, supervisors and payroll clerks. You can print the guide in sections, and customize the checklist to meet your needs.
- **Cash receipting: Fraud Prevention and Internal Controls on-demand training**: Follow an actual fraud case while learning about important best practices for internal controls.

WASBO Session Alert

ASB funds are a common source of losses and errors. Learn about important controls you can use to reduce the risk of waste, fraud or abuse.

Thursday, May 9, 3:40 p.m. to 4:30 p.m., GTCC 316

Remember to check the conference app for the latest schedule.

Cyber checkups: Common results from the first year of reviews

The Center for Government Innovation at the State Auditor's Office is celebrating: its newest service, the **cyber checkup**, is one year old. These checkups provide a fast, no-cost, independent review of local government cybersecurity programs. Cyber checkups aren't substitutes for an audit – and won't find all vulnerabilities – but they give local governments actionable recommendations and resources to help address any weaknesses.

So far, the Center has completed 45 checkups for all types of local governments, from cities and towns to fire districts and school districts. Our checkups have helped governments both large and small, including those with annual revenues as high as $661 million and as low $225,000.

To celebrate the first year of this service, we identified some common results of these checkups, including areas where local governments are doing well or could use improvement.

Top three cyber successes

- **Scanning email attachments.** The checkup tests to see if the government's email software prevents executable files from being delivered in an email. Malicious software can't be installed if it never reaches a computer, so governments should ensure their email software won't deliver attachments that are executable files. Nearly all the governments we have assessed had this scanning software in place.
- **Updating antivirus software.** Cybercriminals are regularly creating new computer viruses, so local governments must keep their antivirus software updated. Keeping antivirus software updated is especially important because it can also stop spyware, adware, and other malicious software. Most of the governments we assessed kept their antivirus software current.
- **Applying patches regularly.** Keeping other software updated is also crucial for keeping a secure information technology environment. When vendors learn about a security vulnerability, they will develop a patch to secure the software or hardware. However, it is up to users to apply the updates. Patches are applied to both software and hardware; patches to hardware can be overlooked, but they are important to apply to ensure the hardware runs securely. Many of the governments we assessed regularly applied patches developed by their software and hardware vendors.

WASBO Session Alert

Schools are in the crosshairs of cybercriminals. Find out how you can strengthen your cybersecurity program and learn about SAO's free cyber checkup program.

Thursday, May 9, 10:30 a.m. to 11:20 a.m., GTCC 403

Remember to check the conference app for the latest schedule.

Top three areas for improvement

- **Adopting written IT policies**. As part of our checkup, we look at whether governments have seven key IT policies in place. These policies cover things like multifactor authentication, acceptable use, and password requirements. None of the governments we assessed had the seven policies in place. Refer to our **March 2024 blog post** for more information on adopting specific IT policies as part of your government's cybersecurity program.
- **Naming a designated lead for incident response**. Only a handful of the governments we assessed had named people as the designated lead and backup lead for responding to cybersecurity incidents. In addition to naming a designated lead, it is important to identify a backup in case the lead person may be unavailable. Backup leads are also necessary in extended cases that require an incident command rotation to allow people to take breaks. Governments can respond to incidents faster when they have named people for these positions, and it allows these employees to prepare for the responsibilities.
- **Maintaining contact list information**. Governments should keep a list with the current contact information of their service providers and emergency contacts. The list should be printed, and key personnel should have copies or know where to find one in situations where computers are not working. Some of the governments we assessed had complete contact lists; others had partial lists or did not have one at all.

Ready for a checkup?

Whether your government has an established cybersecurity program or is just starting to build one, the Center's checkups can give you actionable steps to improve your overall cyber health. **Contact us** today to schedule your cyber checkup!

How to reach us for more assistance

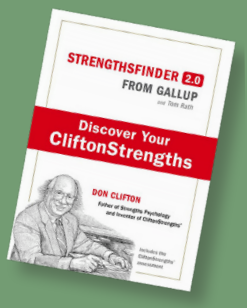
Do you have questions about cybersecurity? The Center's cybersecurity specialist is available to talk with you about best practices and resources. For assistance, reach out to us at **Center@sao.wa.gov**.

WASBO Session Alert

Increase efficiency by building on your team's unique strengths

- **Strengthen** team cohesion
- **Increase** productivity
- **Improve** employee satisfaction

And more – all at no cost to you.



SCAN CODE TO GET STARTED

Center for Government Innovation

Join us for

The Care and Feeding of Teams: How to cultivate employees to stand strong as work keeps changing

Thursday, May 9, 2:40 p.m. to 3:30 p.m., GTCC 407

Remember to check the conference app for the latest schedule.

Cybersecurity services we offer to Washington governments

The State Auditor's Office continues to expand its program of work around cybersecurity and information technology systems at both state agencies and local governments. Our goal is to help diminish the likelihood government organizations, no matter how large or small, will fall prey to hacking, malware or phishing schemes. Here's a snapshot of services we offer.

Cyber checkups

While not intended to be a replacement for a detailed audit, these checkups are designed to be a high-level assessment of a local government's cyber health to identify gaps that could leave its IT systems vulnerable to common threats. Every checkup offers ideas on how to improve. Performed by SAO's Center for Government Innovation, these checkups are built on the framework developed by the Center for Internet Security (CIS) in its Critical Security Controls. The checkups are done remotely and can be completed in less than a month, depending on a government's availability. There's no waitlist! To schedule a cyber checkup, governments should contact the Center at **center@sao.wa.gov**.

Ransomware audits

These audits examine a government's resiliency to ransomware, a type of cyberattack designed to deny access to a computer system or the data it stores until the victim pays the demanded ransom. We examine five control areas that apply to distinct facets of ransomware prevention, detection and response. These audits can benefit governments large enough to employ cybersecurity staff as well as smaller governments that use contracted IT services.

Critical infrastructure audits

These audits are designed around the special security needs of governments that provide essential services such as hospitals, power stations and water. These smaller scoped audits focus on finding "low-hanging fruit" for improvements. We look at internet-facing assets, such as public websites, to identify vulnerabilities that an attacker anywhere in the world could leverage. We also interview IT staff and assess publicly available information to identify risks including compromised email accounts and potential data breaches.

Cybersecurity audits

Our full cybersecurity audits dig deep into IT systems used in government operations to identify weaknesses that could expose the government to a wide range of possible risks. Audit teams conduct penetration and technical tests, and interview IT staff and managers to learn about controls already in place. Auditors then propose solutions to help strengthen those systems. To learn more about the cybersecurity audits listed here, or to request one, governments should email **SAOITAudit@sao.wa.gov**

How to learn more

*I*n September 2023, we published a new report that summarizes the results of FY 2023 cybersecurity audit work. You can also view a roll-up report touching on all aspects of this work on our website at **sao.wa.gov**.

New OPMA materials to help local governments navigate recent changes

The Open Public Meetings Act (OPMA) was enacted to make the conduct of Washington's governments more accessible and open to the public. The OPMA underwent significant changes in 2022 when the Legislature modified the law in response to how local governments had adapted and continued to hold their governing body meetings during the COVID-19 pandemic.

With all these changes, the Municipal Research and Services Center (MRSC), in partnership with SAO's Center for Government Innovation, decided to revamp and expand our OPMA materials to help local governments better navigate the new requirements.

OPMA Guide

We've reorganized the **OPMA Guide** to better reflect how a local government would apply the law. This includes step-by-step instructions regarding:

- Applicability — detailing which local agency bodies are subject to the OPMA
- What is a meeting? — breaking down the definition of a meeting
- Exemptions — explaining which types of meetings are fully exempt
- Procedural requirements — walking through the procedural requirements applicable to regular, special and emergency meetings
- Executive sessions — adding context for executive session topics
- Penalties and enforcement
- Training requirements
- Recommended resources

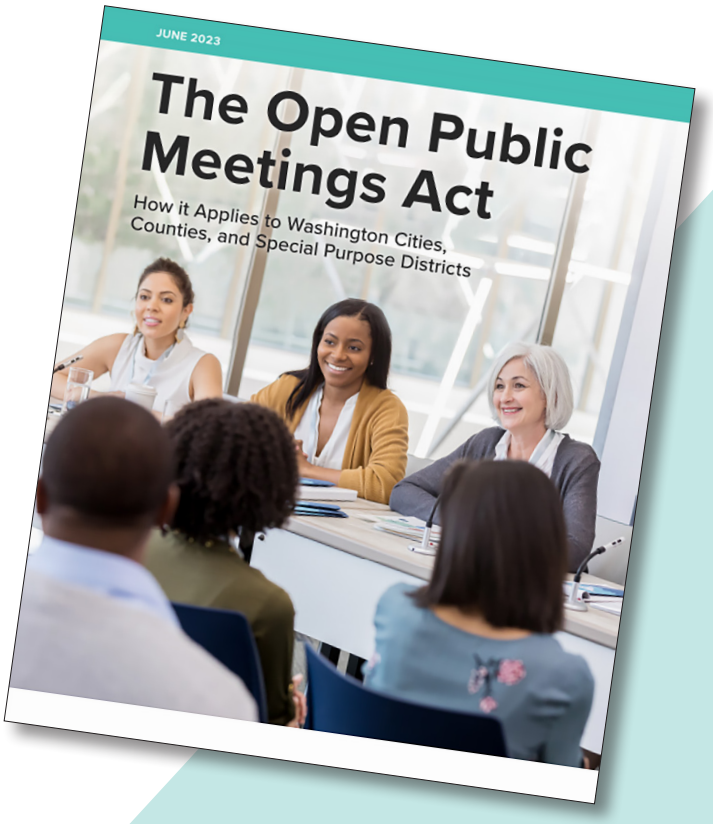
We've also incorporated and highlighted recent and significant legislative changes that occurred in response to the COVID-19 pandemic, including:

- New sections on serial, hybrid and remote meetings
- Additional detail on emergency meetings
- New guidance on meeting cancellation and adjournment
- A detailed explanation of the public comment requirements for regular meetings at which the governing body takes final action

Plus, we've updated the "Selected Questions" section included after each chapter by providing answers to those questions most frequently asked by local governments over the last few years.

OPMA Practice Tips Guidance Sheets

We've expanded our collection of **OPMA Practice Tips Guidance Sheets** to include **developing and modifying agendas** and **minutes**. These new guidance sheets not only provide the legal obligations for modifying agendas and taking minutes, but also practical tips and recommended practices. You can also find guidance sheets for OPMA **basic requirements**, **notice requirements**, **executive sessions** and **electronic communications**.



Updated contracting requirements tool can help ease your procurement woes

Procurement and competitive bidding laws can be complicated, often varying based on government type, the nature of the procurement, and the estimated cost, and it can be difficult to wade through existing requirements or stay updated on new ones.

That's why SAO, in partnership with the Municipal Research and Services Center (MRSC), developed the **Find Your Contracting Requirements** tool in 2015. This free tool helps local governments identify and understand their statutory legal requirements for purchasing and contracting. The tool asks up to three simple questions, then provides you with a summary of your competitive bidding and contracting requirements.

We recently upgraded the tool to include the option of additional project types, an expansion of the types of governments, and guidance on federal funding. Here is a summary of our additions:

New procurement type for electronic data processing/telecommunications

- Procuring electronic data processing or telecommunications equipment, software, or services to support your government's internal administrative functions can be confusing. Procuring things like computer hardware, custom or off-the-shelf software, or various audio, video, internet and data systems can lead to several questions—is it an equipment purchase? A service? Would installation be considered a public work?
- To answer these questions, a new project type has been added to question No. 1: "What type of procurement is this?" You can now select "Acquisition of electronic data processing or telecommunications equipment, software, or services" to learn the requirements, including a review of the optional competitive negotiation process under **RCW 39.04.270**.

Expanded agency types

- For public works and purchases, we have updated the menu options to make it easier to find housing authorities and public development authorities (public corporations). These government types were included previously, but they were harder to find.

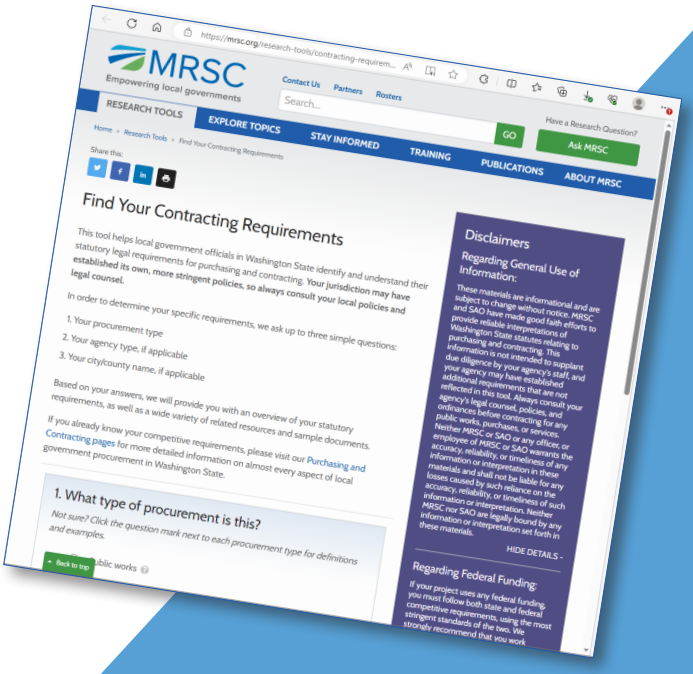
Federal funding sections added

- Each project result page now has a section that provides specific information regarding federal funding requirements based on the unique project type selected. However, if your procurement involves federal funds, you will still need to work closely with your granting agency and carefully review state and federal requirements, using the most stringent of the two.

While **Find Your Contracting Requirements** is based on reliable interpretations of Washington statutes relating to purchasing and contracting, we encourage you to work with your legal counsel and to consult local ordinances and policies before contracting for any public works, purchases or services.

In addition to updating the contracting tool, we've also created the **Alternative Public Works Contracting Methods** web page that describes design-build contracting, general contractor/construction manager contracting, and job order contracting.

You can also find a variety of resources about purchasing, bidding, and contracting on **SAO's** and **MRSC's** websites.



SAO launches improved annual filing system

The Office of the Washington State Auditor released an improved, interactive and more efficient annual filing system in early 2024.

The system has many upgraded features to help clients with their legally required annual reports, including:

- A new client dashboard that shows how much of the annual report is completed, as well as edit checks highlighting possible errors that the client needs to resolve before filing.
- Icons that provide more information about possible errors in the report, including guidance on how to fix them plus links to additional instructions.
- An integrated help feature where clients can submit a HelpDesk ticket or send an email to our Local Government Support Team directly in the filing system.
- Simplified navigation that groups together the required components of the annual report.
- A new and more efficient interface for the Schedule 22 that allows clients to import prior-year responses to select questions. Questions are now organized by category, using collapsible headers.

If you have questions or would like further assistance, feel free to use the Auditor Helpdesk at **sao.wa.gov** or email **LGCSFeedback@sao.wa.gov**.

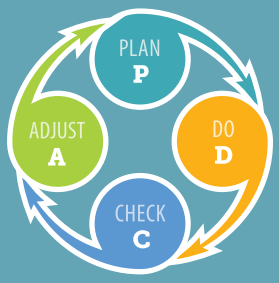
WASBO Session Alert

Ensure your government runs efficiently with Lean Services

Lean Services help you to:

- Quickly **identify** problems
- **Improve** how work gets done
- **Optimize** processes

And more – all at no cost to you.



SCAN CODE TO GET STARTED

Center for Government Innovation

Join us for

Nuts, bolts and hands-on practice: Improve your business processes with fundamentals of Lean

Wednesday, May 8, 4:10 p.m. to 5:00 p.m., GTCC 405

Remember to check the conference app for the latest schedule.

How to print this newsletter:

- Move your mouse curser to the bottom of your browser window. A bar will appear with several icons. Click the "download PDF" button.
- Open the downloaded PDF, and choose the "print" option from your PDF reader.
- Consider "printing on both sides, flip on long edge" to save paper.
- Finally, decide whether you want full color or grayscale – we know folks rooted in #GoodGovernment are judicious with printer ink.