



Paul D. Joyce, CPA
State Examiner

INDIANA STATE BOARD OF ACCOUNTS

302 WEST WASHINGTON STREET
ROOM E418
INDIANAPOLIS, INDIANA 46204-2769
Telephone: (317) 232-2513
Fax: (317) 232-4711
www.in.gov/sboa

THE STATE AGENCY BULLETIN

October 2025

IN THIS ISSUE

Items to Remember	1
Standard Operating Procedures – A Policies and Procedures Program (Part 2)	2
State Subaward Agreement - Updated	3
Entity Annual Reports (E-1)	4
Fraud Series – Part 4	5

ITEMS TO REMEMBER

If there are certain items or dates that would be beneficial to include in future calendars, please let us know by emailing StateAgencyAdvisory@sboa.IN.gov.

November

- Holiday – Veteran’s Day November 11th
- Holiday – Thanksgiving Day November 27th
- Holiday – Lincoln’s Birthday November 28th
- Review State Comptroller ACFR Survey for Deliverables this month.
- Complete accounting information and approvals in PeopleSoft for TOS approved AR/ROC.
- Review requirements for FFATA Reporting; File FFATA reports as applicable.
- Cleanup GL, AP and AR entries prior to month-end.

December

- Holiday – Christmas Day December 25th
- Holiday – Washington’s Birthday December 26th
- Review State Comptroller ACFR Survey for Deliverables this month
- Complete accounting information and approvals in PeopleSoft for TOS approved AR/ROC
- Review requirements for FFATA Reporting; File FFATA reports as applicable.
- Cleanup GL, AP and AR entries prior to month-end.

January

- Holiday – New Year’s Day January 1st
- Holiday – Martin Luther King, Jr. Day January 19th
- Review State Comptroller ACFR Survey for Deliverables this month.
- Complete accounting information and approvals in PeopleSoft for TOS approved AR/ROC.
- Review requirements for FFATA Reporting; File FFATA reports as applicable.
- Cleanup GL, AP and AR entries prior to month-end.

STANDARD OPERATING PROCEDURES – A POLICIES AND PROCEDURES PROGRAM (PART 2)

In our last Standard Operating Procedures Program (Part 1) article, we covered how to organize Standard Operating Procedures (SOPs) numerically so that they are well-organized, identifiable to a particular agency and department, and can be easily retrievable. In Part 2, we will cover another important aspect of maintaining a successful SOP Program – management buy-in.

Management buy-in starts with obtaining support from your agency head and leadership. It is recommended that the SOP Program Administrator/Owner create a SOP program charter explaining the scope, goals, and management of the program and discuss this with your agency leadership. Having everyone on the same page at the beginning will help ensure the program is headed in the right direction and has management buy-in.

Next, you will want to work with each department head through a series of meetings to create an initial list of policies and procedures for their department. These SOPs will be subject to updates due to process changes, personnel changes, and other factors. On this list you will want to include the SOP Number, SOP Name, SOP Description, Process Owner, Reviewer, Target Completion Date, Last Revision Date, Last Walkthrough Date, Key Controls, Risk Rating, Comments, and Other Information. These will be critical elements to track to have a robust program that drives accountability for the documents and reduces risk.

The policies and procedures list is the joint responsibility of both the SOP Administrator and each department. The SOP Administrator will work with each department to keep their list up to date, help document SOPs as needed, and schedule walkthroughs of completed SOPs. The SOP Administrator will also provide a policy template and an SOP template that each department can use to document their SOPs.

The policies and procedures list should be saved in a secure location with controls over read-only and editing access. It should be readily accessible to appropriate personnel.

In our next bulletin we will discuss SOP quality standards.

STATE SUBAWARD AGREEMENT - UPDATED

2 CFR 200 requires certain elements to be included and identified in grant agreements, including subawards.

Previously, agencies have been including additional information beyond what was required to be identified in the previous boilerplate grant agreement, either as an exhibit or an attachment to satisfy these requirements.

IDOA has updated the boilerplate grant agreement language to allow additional elements to be listed. This not only improves agency compliance with federal requirements but also allows the SBOA State audit team to easily identify and test part of the subrecipient monitoring compliance requirement as required by the OMB Compliance Supplement.

The following highlighted attributes have been added to collect information about subrecipients.

(1) Federal Award Identification

- I. Subrecipient name (which must match the name associated with its unique entity identifier).
- II. Subrecipient's unique entity identifier.
- III. Federal Award Identification Number (FAN).
- IV. Federal Award Date (see the definition of Federal award date in § 200.1 of this part) of award to the recipient by the Federal agency.
- V. Subaward Period of Performance Start and End Date.
- VI. Subaward Budget Period Start and End Date.
- VII. Amount of Federal Funds Obligated by this action by the pass-through entity to the subrecipient.
- VIII. Total Amount of Federal Funds Obligated to the subrecipient by the pass-through entity including the current financial obligation.
- IX. Total Amount of the Federal Award committed to the subrecipient by the pass-through entity.
- X. Federal award project description, as required to be responsive to the Federal Funding Accountability and Transparency Act (FFATA).
- XI. Name of Federal awarding agency, pass-through entity, and contact information for awarding official of the Pass-through entity.
- XII. Assistance Listings number and Title; the pass-through entity must identify the dollar amount made available under each Federal award and the Assistance Listings Number at the time of disbursement.
- XIII. Identification of whether the award is research and development.
- XIV. Indirect cost rate for the Federal award (including if the de minimis rate is charged) per 2 C.F.R. 200.414

(2) Other Requirements

Subrecipients shall adhere the following requirements to ensure that the Grant is used in accordance with Federal statutes, regulations, and the terms and conditions of the Grant:

ENTITY ANNUAL REPORTS (E-1)

In the State Subaward Agreement, information is provided to subrecipients about their responsibility to file Entity Annual Reports (E-1). These reports are public and are maintained in Gateway. We would like to highlight this information's usefulness for State Agencies while monitoring for subrecipient compliance.

Agencies could determine if subrecipients have fulfilled their requirement to have audits performed by reviewing E-1 reports in [Gateway](#) and by searching the SBOA audit report filings [portal](#). Additional information included in E-1 reports may also be helpful to agencies when performing subrecipient monitoring activities.

We have created a [training video](#) introducing the topic of E-1 reports and how they may be utilized by state agencies.

Below is additional information that explains E-1 reporting in more detail.

Entities are defined as providers of goods, services, or other benefits that are maintained in whole or in part at public expense or supported in whole or in part by appropriations, public funds, or taxation. The definition does not include the state or municipalities but does include for-profit and not-for profit corporations, unincorporated associations and organizations and individuals.

Financial assistance is defined as payments received in the form of grants, subsidies, contributions, aid etc. Entities are primarily non-governmental organizations, many of which conduct their business as a not-for-profit corporation. By contract or other form of agreement, these entities provide a service or benefit to the public on behalf of and paid for by government.

IC 5-11-1-9 delegates the "oversight" responsibility of these entities to the State Board of Accounts. Specifically, the State Board of Accounts is to ensure that audits, in accordance with agency guidelines, are performed for all entities receiving financial assistance from state or local government sources. The State Board of Accounts is also required to establish a system of review, follow-up, and resolution of any findings of noncompliance identified during the audit process.

All entities receiving assistance from state and local government, involving federal or non-federal dollars are subject to audit by state law.

IC 5-11-1-9 requires an organization-wide audit of an entity when the public funds disbursed by that organization are equal to or greater than 50% of its total disbursements. The State Examiner may waive the audit requirement if the public funds disbursed are less than 50% of its disbursements or if public funds disbursed are at least 50% of total expenditures but public funds expended are less than \$750,000.

Additionally, fee-for-service arrangements with governmental entities are required to be reported on the E-1 report per the Uniform Compliance Guidelines. It will be the determination of the State Board of Accounts, and not the entity, as to whether the funding arrangement meets the definition of fee-for-service. Copies of contracts and other information may be required to be submitted and will be reviewed to determine the proper categorization of funding.

Entities subject to the requirements of IC 5-11-1-9, are required to file an Entity Annual Report (E-1) with the State Board of Accounts annually. The submission is due within sixty days of the entity's fiscal year-end.

FRAUD SERIES – PART 4

In the last bulletin we discussed fraud risk assessment and how to think like a fraudster to identify what your agency could be vulnerable to.

This is the fourth in a series of articles on establishing and maintaining a system of internal controls related to managing fraud risk.

In this segment, we are focusing on the second phase of a 5-phased approach to create a robust anti-fraud program.

Fraud Risk Assessment (Phase 2 Part 4) – Discover What You Don't Know

Conducting a fraud risk assessment helps you understand exactly where your processes might be vulnerable to fraud and allows for a holistic and detailed look at the fraud risks across the agency. Every enterprise faces a variety of risks from both internal and external sources, and a fraud risk assessment is a tool that your agency can leverage to identify and understand risks and provide the basis for how risks are managed. Further, the fraud risk assessment process is a proactive measure that can increase the perception of detection.

Therefore, the process should be visible throughout your agency, which means you should communicate broadly, promoting the process at all levels. It is important to remember that risk assessment is an art and not a science, so your fraud risk assessment methodology or approach should be tailored to the unique vulnerabilities and strategic goals of your agency.

Steps of a Fraud Risk Assessment:

1. Establish the fraud risk assessment team
2. Determine your starting point
3. Identify all fraud schemes
4. Estimate the likelihood and significant of each fraud scheme
5. Identify existing controls and assess effectiveness
6. Prioritize fraud schemes
7. Assess and respond to high-priority or significant fraud schemes
8. Document the risk assessment
9. Reassess periodically

Below are some key questions to assist in developing a fraud risk assessment

- Who will be on your fraud risk assessment team? What are their roles and responsibilities?
- Where do you want to start your fraud risk assessment?
- Does your agency leverage a likelihood and impact scale for other risk assessment efforts that you can leverage for assessing fraud risk? If not, how do you plan to develop those scales?
- How will you educate stakeholders on the fraud risk assessment process to ensure understanding of key terms and procedures?
- How will you document and evaluate existing fraud controls throughout the assessment process?
- What factors should you consider when prioritizing fraud risks? Will this be based solely on likelihood and impact scores, or will other information be considered?
- How will you respond to high-priority risks identified? How can you leverage your roadmap and strategy to inform this process?
- How often will you perform a fraud risk assessment? What changes will initiate a reassessment?

In the next bulletin we will be discussing the next phase (fraud control activities) of creating a robust anti-fraud program