

# THE STATE AGENCY BULLETIN

AND UNIFORM COMPLIANCE GUIDELINES  
ISSUED BY STATE BOARD OF ACCOUNTS

October 2023

Volume 6

## IN THIS ISSUE

Items to Remember.....	1
Internal Controls Series – Part 4.....	2
Training Video Requests.....	3
Glossary of Accounting and Audit Terms.....	4

## 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](mailto:stateagencyadvisory@sboa.in.gov).***

### November

- Holiday – General Election Day November 7<sup>th</sup>
- Holiday – Veteran’s Day (substitute) November 10<sup>th</sup>
- Holiday – Thanksgiving Day November 23<sup>rd</sup>
- Holiday – Lincoln’s Birthday November 24<sup>th</sup>
- 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 25<sup>th</sup>
- Holiday – Washington’s Birthday December 26<sup>th</sup>
- 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 1<sup>st</sup>
- Holiday – Martin Luther King, Jr. Day January 15<sup>th</sup>
- 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.

### **INTERNAL CONTROL SERIES – PART 4**

In the July 2023 State Agency Bulletin (Internal Control Series - Part 3), we briefly discussed the Risk Assessment component of internal controls and principles 6 through 9 from the COSO framework.

In this segment, we are focusing on Control Activities, which includes Principles 10 through 15 from the COSO Framework.

#### **Principle 10. Management designs control activities to achieve objectives and respond to risks.**

Control activities are designed to fulfill defined responsibilities and address identified risks. An evaluation of the purpose of the control activity is performed as well as an evaluation of the effect a deficiency would have on objectives. Control activities may be either automated or manual. The Green Book identifies a list of control activity categories that are meant only to illustrate the range and variety of control activities; the list is by no means all inclusive, but is reproduced here for reference purposes:

- Top-level reviews of actual performance.
- Reviews by management at the functional or activity level.
- Management of human capital.
- Controls over information processing.
- Physical control over vulnerable assets.
- Establishment and review of performance measures and indicators.
- Segregation of duties.
- Proper execution of transactions.
- Accurate and timely recording of transactions.
- Access restrictions to and accountability for resources and records.
- Appropriate documentation of transactions and internal control.

#### **Principle 11. Management designs the political subdivision's information system and related control activities to achieve objectives and respond to risks.**

Control activities are designed to support the completeness, accuracy, and validity of information processing by technology including the design of security management. Management evaluates changes to systems and updates control activities in response. For example,

- Disaster Recovery ensures that critical accounting information will be processed in the event of interruption of computer processing capacity.
- Back-Up Processing provides for accounting information to be backed up on a periodic basis sufficient to allow restoration of the information in a timely manner.
- Physical Security protects the computer system and the associated telecommunications equipment from environmental damage and unauthorized access.

### **INTERNAL CONTROL SERIES – PART 4 (Continued)**

- Logical Security requires access to accounting information and processes be controlled by operating system software and by the computerized accounting application through user identification codes and passwords.
- Change Controls are internal controls over changes made to the accounting system's computer programs.
- Audit Trails allow for sufficient documentation to trace all transactions from the original source of entry into the system, through all system process, and to the results produced by the system.
- Input Controls provide input edits and controls to assure that information entered into the system is accurate, that all appropriate information is entered into the system.
- Segregation of Duties can be achieved within information technology systems by appropriate assignment of security profiles that define the data the users can access and the functions they can perform.
- Output Controls are features that assure all accounting information is reported accurately and completely.
- Interface Controls allow for information generated in one computer application system to be transferred to another computer application system accurately and completely.
- Internal Processing provides written verification procedures and actual verification results that document accurate calculating, summarizing, categorizing, and updating of accounting information on a periodic basis.

#### **Principle 12. Management implements control activities through policies.**

Management works with each office or department in determining the policies necessary to address the objectives and related risks for the operational process. Further defined policies through day-to-day procedures may be warranted. These policies are periodically reviewed for continued relevance and effectiveness.

### **TRAINING VIDEO REQUESTS**

We are expanding our library of training videos on a variety of topics including, but not limited to: Audit Issues, Compliance, Accounting Procedures, Best Practices, Internal Controls, Uniform Compliance Guidelines, and more. If there is a training topic you believe would be of assistance to you, please send your suggestions to [stateagencyadvisory@sboa.in.gov](mailto:stateagencyadvisory@sboa.in.gov).

### **GLOSSARY OF ACCOUNTING AND AUDIT TERMS**

We have created a glossary of accounting and auditing terms that are relevant to the audit work conducted within the State of Indiana and our agency which can be found on our website.

The glossary contains definitions of accounting, reporting, and auditing terms that are commonly used while conducting our engagements and often appear in the reports issued by our agency.

We have provided sources for these definitions for further reference. The most authoritative source is provided but additional sources may be available. There are terms listed within this glossary that are not explicitly defined in authoritative guidance. In these instances, the State Board of Accounts has compiled definitions based on research and our staffs' knowledge and experience.

To find the glossary, you can visit our website ([www.in.gov/sboa](http://www.in.gov/sboa)) and navigate to the 'About Us' section on the left navigation pane and select 'SBOA Glossary of Accounting and Audit Terms' or click on the following link. [SBOA Glossary of Accounting and Audit Terms](#)