# THE STATE AGENCY BULLETIN

AND UNIFORM COMPLIANCE GUIDELINES
ISSUED BY STATE BOARD OF ACCOUNTS

January 2025 Volume 11

## IN THIS ISSUE

## 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.***

February

- 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.

March

- 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.

April

- Holiday – Good Friday April 18th
- 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.

## CYBERSECURITY INCIDENTS

IC 4-13.1-2-9 states:

> "A state agency (as defined in IC 4-1-10-2), other than state educational institutions, and a political subdivision (as defined in IC 36-1-2-13) shall:
>
> > (1) report any cybersecurity incident using their best professional judgment to the office without unreasonable delay and not later than two (2) business days after discovery of the cybersecurity incident in a format prescribed by the chief information officer; and
> >
> > (2) provide the office with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident described in subdivision (1) before September 1, 2021, and before September 1 of every year thereafter.
>
> Nothing in this section shall be construed to require reporting that conflicts with federal privacy laws or is prohibited due to an ongoing law enforcement investigation."

State agencies are required to report any cybersecurity incident, using their best professional judgement, to the Indiana Office of Technology (IOT) without unreasonable delay and not later than two business days after discovery of the cybersecurity incident.

A cybersecurity incident may consist of one or more of the following categories of attack vectors: (1) Ransomware, (2) Business email compromise, (3) Vulnerability Exploitation, (4) Zero-day exploitation, (5) Distributed denial of service, (6) Web site defacement, (7) Other sophisticated attacks as defined by the chief of information officer and that are posted on the officer's Internet web site. (IC 4-13.1-1-1.5)

Cybersecurity incidents can be reported on IOT's web site at the following webpage. https://www.in.gov/cybersecurity/report-a-cyber-crime/

## SBOA YOUTUBE CHANNEL

The State Board of Accounts has a YouTube Channel!

The State Advisory Services team plans to periodically release short training videos on internal controls, fraud prevention, best accounting practices and other topics. If there is a topic you think would make a good training video, please let us know (Stateagencyadvisory@sboa.IN.gov).

You can subscribe to our channel to receive updates via YouTube notifications. To access the SBOA State agency playlist on YouTube you can use this link.

## FRAUD SERIES – PART 1

In the last bulletin we introduced concepts of fraud risk management.

But what exactly is fraud risk management and how can this be implemented? This is the first 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 first phase of a 5-phased approach to create a robust anti-fraud program.

**Fraud Risk Governance (Phase 1) -** Understand where you are and where you want to be.

Fraud risk management should be tailored to the unique needs of the agency. Business units with limited fraud exposure may not need rigorous or time consuming procedures in place to combat fraud. The level of maturity in an agency's fraud risk framework should be considered when deciding how to address fraud. It is important to ensure resources are effectively utilized in areas of high impact and high priority.

If there are no fraud mitigation procedures in place, the first step is to understand where your agency's fraud risks lie and what controls are currently implemented. Once you understand the current environment you can identify long-term goals and a vision to work towards a mature fraud risk management program.

We recommended creating a roadmap that leads towards the future goal of having a strong fraud risk management program. Any previously identified gaps should be immediately remedied if feasible. An effective way to develop a roadmap is by conducting a maturity assessment. Below are some key questions to assist in identifying how mature your current fraud risk management program is.

- Is the organization aware of the need of a formal fraud risk management program?
- Are fraud risk management processes organized, reviewed periodically, and updated to reflect updates in processes?
- Are internal controls developed and documented specific to both external and internal fraud?
    - Are fraud controls monitored for effectiveness?
- Is information about prior known fraud instances aggregated and analyzed to improve procedures?
- Is ongoing anti-fraud training provided to all employees?
    - Do employees understand what fraud is?
    - Have the consequences of fraud been made clear?
    - Do employees know where to seek advice on potential unethical situations?
    - Has a zero-tolerance policy been communicated through words/actions?
- Is an effective fraud reporting mechanism in place?
    - Do employees know how to use it?
    - Is there more than one reporting channel?
    - Do employees trust reports are confidential?

  - Has it been made clear that reports will be acted upon promptly?
  - Do reporting policies extend to external parties?
- To increase employees' perception of detection, are these measures being taken?
  - Is fraud sought out rather than dealt with passively?
  - Are internal surprise audits performed?
  - Are data analytics used to identify variances?
  - Are controls reviewed and monitored?
- Is management's tone at the top one of honesty and integrity?
  - Are employees surveyed to determine if management acts with integrity?
  - Are performance goals realistic?
  - Have fraud prevention goals been identified?
  - Have internal control policies been implemented and tested?
- Are fraud risk assessments performed to proactively identify and mitigate the agency's vulnerabilities to fraud?
- Are strong anti-fraud controls in place and operating effectively? This could include:
  - Proper Segregation of Duties
  - Use of Authorizations
  - Physical Safeguards
  - Job Rotations
  - Mandatory Vacations
- Does the internal audit department, if one exists, have adequate resources and authority?
  - Does the internal audit department operate without undue influence from management?
- Is an open-door policy in place that allows employees to speak freely about pressures?
- Are regular, anonymous surveys conducted to assess employee morale?

In the next bulletin we will be discussing fraud risk assessment in part 2 of this fraud series.