Emerging and Potential Audit Issues Volume 26 • 2020 Annual Edition

# Illinois Audit Advisory

Frank J. Mautino, Auditor General

## Auditor General's Message

This year has marked historic challenges for state government and the agencies that serve the good people of Illinois. The worldwide pandemic has left its mark on all facets of life in our society. The people of Illinois have endured historic levels of unemployment, dramatic changes to our social structure, and increased levels of financial, physical, and emotional stress as a direct result of COVID-19.

During this time, the agencies of the State of Illinois provided relief, comfort, and critical services. This they accomplished while working remotely under high-pressure and constantly evolving work place conditions. They should be commended for their dedication, ingenuity, and ability to keep state operations running.

Mr. Frank Mautino

The purpose of the Illinois Audit Advisory is to share information that may make state agency operations more efficient, effective, and/or increase compliance with State law. In this issue we will look at the effects of the pandemic on the audit process. We will also review crisis management planning, risk identification, and cyber security. In the coming year, tracking of expenditures of state and federal dollars to combat COVID-19 will be important in determining, evaluating, and improving our reaction to this or any future crisis.

As always, my Office looks forward to working with you in a cooperative manner during this audit cycle.

## Impact of COVID-19 on the Audit Process

On January 30, 2020, the World Health Organization declared a public health emergency. On March 20, 2020, Governor Pritzker issued a stay-at-home order that went into effect the next day. This means any State agencies undergoing a fiscal year 2020 audit will have been affected by the COVID-19 pandemic during the audit period. Auditing these agencies will present unique challenges and heightened risk.

When the stay-at-home order was issued, agencies shifted from working in an office to working remotely. Since an agency's relevant controls may have changed to accommodate remote working, the risk of a breakdown in internal controls is increased. Auditors need to be aware of risks and modify audit approaches accordingly.

It is important to note that while auditing standards address what evidence needs to be obtained, the standards don't dictate how to meet the requirements. Auditors can work remotely and still meet auditing standards. However, in some cases, auditors may encounter scope limitations such as performing physical inventory observations, accessing agency records, and testing internal controls.

The following are procedures that can be utilized that allow the audits to proceed while limiting exposure to both auditors and agency staff:

- Holding interviews, including fraud interviews, via video conferencing technology;
- Avoiding travel to audit locations except when absolutely necessary;
- Conducting video observation of inventories, eligibility case file documentation, voucher support, etc.;
- Considering alternate inventory solutions, such as postponement of inventory counting to when the environment is more relaxed and possibly performing roll forward and roll back procedures; and
- Providing auditors remote access to IT systems for various detail transactions testing.

Under the current circumstances, effective communication is more important than ever. The auditee agency should immediately notify auditors of any issues that will impact both timeliness and its ability to fully respond to audit requests. The agency and the auditor should work together to resolve any obstacles. While delays in responding to audit requests can be expected, the pandemic should not be used as a justification for not cooperating and needlessly delaying the audit.

## Developing a Crisis Management Plan

If your agency does not have a crisis management plan in place, now may be a good time to start the process of developing one while the current crisis is fresh in our minds. Also, keep in mind during the process that there are a myriad of types of crises that you may need to plan for such as natural disasters, a technology crisis, or a personnel crisis. Below are some key steps that will help guide your agency through the process.

### 1. Assess your risks and identify types of crises

To get started, the first step is a risk assessment, which identifies potential crises that could disrupt your functions and/or processes. Work with members of your agency's leadership and other key stakeholders to begin listing all relevant threats and vulnerabilities that could have an impact. These might include cyber-attacks, data breaches, and natural disasters.

### 2. Determine the impact on your agency

Quantify the potential impact a crisis could have on your agency's operations. This can reveal a variety of potential effects, including:

- Client dissatisfaction
- A tarnished reputation
- Lost or delayed revenues
- Increased expenses (for example, paying for overtime or acquiring materials to address the crisis)

### 3. Identify possible actions

Begin identifying which actions will help your agency respond effectively to each crisis situation. Think about the steps that would be required to resolve a given crisis, the resources needed, and how employees assist.


### 4. Develop plans

Once you've determined possible actions for each potential crisis, develop the plans with input from relevant stakeholders including key employees and contractors. Agency staff can help to provide insight into available resources and potential hurdles. As you work your way through the plan, keep in mind any relevant regulatory requirements, and determine how you will continue to meet them, even in the midst of a crisis. For example, if your organization must remain compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), be sure to account for this regulation in each crisis scenario.

### 5. Familiarize and train employees

Employees should understand their roles during a crisis. Consider ways to quickly and effectively communicate and distribute your crisis plan including access to current documents and other needed information. Also, employees and stakeholders should be regularly trained on your crisis management plan.

### 6. Revisit and update the plan

Once your plan is in place, be sure to revisit it on a regular basis. It is important to keep the plan up to date, especially as employees join or leave the organization, new technologies are implemented, and other changes occur.

## Crisis Planning and Fraud Risk Management from an Agency Perspective

The COVID-19 pandemic has resulted in unprecedented social and economic upheaval in the US. In Illinois, many State agencies transitioned to a remote workforce during most of the final quarter of FY20. Although existing technologies such as video and teleconferencing services have helped facilitate a new normal, working in this new environment still poses numerous challenges.

As a result of this crisis, agencies should have a heightened awareness of the risk for fraud and misconduct that might occur. During this crisis, agency employees may have been faced with increased pressure and urgency to respond to requests. Even though most people behave ethically, agencies and their management should review their controls, processes, and procedures to assess the risk of fraud during a crisis.

Fraud prevention should not be an afterthought in crisis planning and response; it should be a starting point. There are several steps agencies can take in order to effectively manage fraud risk during a crisis. Questions for agency leaders to consider include:

- Is the agency reinforcing its code of conduct and policies and procedures?
- Are there resources dedicated to monitoring compliance (i.e. a whistleblower hotline)?
- Is the agency emphasizing a safe environment for employees to speak up?
- Are processes still in place to identify red flags and warning signs?
- What gatekeeping functions or internal controls might be compromised that may pose a risk?
- What measures are being set in place to boost employee morale and prevent culture erosion?

(*Portions excerpted from the Center for Audit Quality's Managing Fraud Risk, Culture, and Skepticism During COVID-19*)

## Cybersecurity

Public Act 100-914 amended the Illinois State Auditing Act (30 ILCS 5/3-2.4 new) to specifically include Cybersecurity as part of our Compliance Examination program with an effective date of January 1, 2019 (see inset below).

> ***Sec. 3-2.4. Cybersecurity audit.***
>
> *a) In conjunction with its annual compliance examination program, the Auditor General shall review State agencies and their cybersecurity programs and practices, with a particular focus on agencies holding large volumes of personal information.*
>
> *b) The review required under this Section shall, at a minimum, assess the following:*
>
> *1) the effectiveness of State agency cybersecurity practices;*
>
> *2) the risks or vulnerabilities of the cybersecurity systems used by State agencies;*
>
> *3) the types of information that are most susceptible to attack;*
>
> *4) ways to improve cybersecurity and eliminate vulnerabilities to State cybersecurity systems; and*
>
> *5) any other information concerning the cybersecurity of State agencies that the Auditor General deems necessary and proper.*

To address the amendment, on the audits for the period ending June 30, 2019, we did the following:

- Updated the Compliance Audit Guide to include specific questions concerning cybersecurity practices, policies and procedures, training, roles and responsibilities, risk assessments, and data classifications. In addition, we provided guidance to assist audit staff and contractors in obtaining and reviewing documentation to support responses.
- Performed detailed testing at 20 agencies considered higher risk as part of the June 30, 2019 compliance examinations. We provided these agencies with detailed information regarding our analysis and if appropriate we developed material or immaterial findings.

To promote agency's responsibility to ensure that confidential information is protected from accidental or unauthorized disclosure, we generally recommend they:

- Establish and document cybersecurity roles and responsibilities.
- Establish and communicate policies, procedures, and processes to manage and monitor the regulatory, legal, environmental and operational requirements.
- Perform a comprehensive risk assessment to identify and ensure adequate protection of confidential or personal information most susceptible to attack.
- Classify data to establish the types of information most susceptible to attack to ensure adequate protection.
- Ensure all employees annually complete cybersecurity training as outlined in the Data Security on State Computers Act (20 ILCS 450).

Our 2021 Annual Report will have a section with additional information on the results of cybersecurity testing and general recommendations for improvement. An approach similar to 2019 will be used in the June 30, 2020 compliance examinations.

## Identifying Fraud Risks and Preventing Fraud from an Auditing Perspective

The new environment resulting from the COVID-19 pandemic has created an increased risk of fraud and improper financial reporting. As such, auditors, both internal and external, should be on a heightened alert for fraud. The COVID-19 pandemic presents a near perfect storm for fraud risk. With the increases in unemployment and uncertainties in the economy, employees may have felt pressure particularly if they experienced personal financial difficulties. Couple this with potential breakdowns in internal controls or management overrides of internal controls, the opportunities for fraudulent activities is increased.

In response to the current crisis, many agencies and organizations have changed working protocols to enable remote working. This can lead to an increased risk of fraud if internal controls are circumvented as a result of the change in practices. The International Auditing and Assurance Standards Board highlight in a COVID-19 staff alert, the need for auditors to have heightened awareness of the possibility of fraud or error, with the importance of the exercise of professional skepticism when performing audit procedures.

> ***Professional skepticism*** *is an attitude that includes a questioning mind, being alert to conditions that may indicate possible misstatement due to fraud or error, and a critical assessment of audit evidence.*

Fraud can occur both within an agency and outside the agency as clients may try to take advantage of new opportunities to commit fraud. Auditors should be alert to see if agencies have taken steps to strengthen fraud prevention such as:


- Updating fraud risk assessment programs;
- Examining and updating internal controls to address new risk factors; and
- Underscoring prevention policies with employees and making sure they understand who to report to if they suspect fraud.

## COVID-19 Expenditures

COVID-19 expenditures are likely to be scrutinized in future audits. Agencies should be aware of guidance issued by the federal Department of the Treasury. The federal Coronavirus Aid, Relief, and Economic Security Act (CARES Act) established the Coronavirus Relief Fund. The Fund was used to make payments for specified uses to State and local governments. The CARES Act provided that payments from the Fund may only be used to cover costs that:


1) are necessary expenditures incurred due to the public health emergency with respect to the Coronavirus Disease 2019 (COVID–19);
2) were not accounted for in the budget most recently approved as of March 27, 2020 (the date of enactment of the CARES Act) for the State or government; and
3) were incurred during the period that begins on March 1, 2020, and ends on December 30, 2020.

The Department of the Treasury issued guidance on its interpretations of the permissible use of funds. The requirement that expenditures be incurred "due to" the public health emergency means that expenditures must be used for actions taken to respond to the public health emergency. These may include expenditures incurred to respond directly to the emergency, such as by addressing medical or public health needs, as well as expenditures incurred to respond to second-order effects of the emergency, such as by providing economic support to those suffering from employment or business interruptions due to COVID-19-related business closures. Funds may not be used to fill shortfalls in government revenue to cover expenditures that would not otherwise qualify under the statute.

The Department of the Treasury's guidance listed examples of eligible expenditures under the following categories:

1) Medical expenses;
2) Public health expenses;
3) Payroll expenses;
4) Expenses of actions to facilitate compliance with COVID-19 related public health measures; and
5) Expenses associated with the provision of economic support in connection with the COVID-19 public health emergency.

Specific guidance can be found at the Department of Treasury's website at https://home.treasury.gov/.

## GASB Effective Dates

On May 8, 2020, the Governmental Accounting Standards Board (GASB) issued Statement No. 95 which postponed the effective dates on several statements and implementation guides. Most effective dates were postponed by one year with two being postponed by 18 months. Go to GASB's website at https://www.gasb.org/home for more information.

**Office of the Auditor General**
• Iles Park Plaza, 740 East Ash Street
Springfield, Illinois 62703-3154

• Michael A. Bilandic Building,
160 N. LaSalle Street, Suite S-900
Chicago, Illinois 60601-3103

Phone: 217-782-6046
Fax: 217-785-8222

TTY: 1-888-261-2887
Fraud Hotline: 1-855-217-1895

E-mail: oag.auditor@illinois.gov
Website: www.auditor.illinois.gov



Recycled Paper • Soybean Inks • Printed by Authority of the State of Illinois • LPU Order 00000 • July 2020 • 525 copies