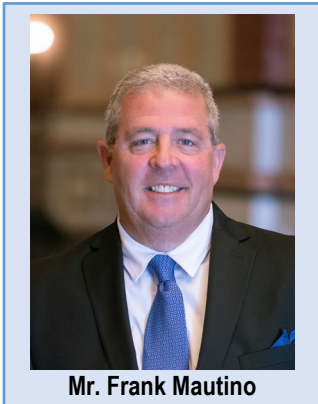


Illinois Audit Advisory

Frank J. Mautino, Auditor General

Auditor General's Message

The year 2024 will be a year of change in state government operations, as well as for the Office of the Auditor General. It is our mission to work with internal auditors, agency managers and public officials. Part of our responsibility is to listen to and react to changes in internal controls, reporting requirements, auditing practices, and standards. This issue of the Illinois Audit Advisory will look at a few of these changes. We have listened and heard concerns of internal auditors and agency managers throughout State government and have made changes to our compliance examinations beginning in fiscal year 2022. In doing so, we have eliminated certain report components. These changes should help to save time and effort by agency staff while providing vital information to the legislature and citizens of Illinois.



Mr. Frank Mautino

On May 31, 2023, the State of Illinois and the Department of Innovation and Technology was breached by ransomware via the MOVEit transfer protocol. The attack was not limited to the State of Illinois, but was a global assault on industries and governments, both foreign and domestic. This issue will also look at changing technologies and the importance of encryption. We all must recognize our changing environment in the IT world and be diligent in protecting both business and personal data.

The Office of the Auditor General remains committed to assist agencies in their mission to efficiently and effectively protect the resources of the State of Illinois.



Importance of Data Encryption

Data encryption standards are protocols used to protect data from unauthorized access. They can be used to encrypt data at rest and in transit, making it unreadable to anyone without the proper keys or authorization.

The Auditor General's office strongly recommends the use of encryption capabilities for portable devices (i.e., laptops, USB flash drives) and also for desktop computers that store confidential information. Encryption is a cost-effective way to secure data and greatly reduces the risk of disclosure of confidential information resulting from a breach.

Per Security Magazine, in 2022, the average cost of a data breach reached \$4.4 million: a 13% increase since 2020. One of the significant costs associated with a breach is the notification to individuals impacted by the breach. Another cost is the standard practice of providing free credit monitoring or identity theft protection to individuals affected by the breach.



In Illinois, the Personal Information Protection Act (815 ILCS 530/12) requires any State agency that collects personal information to notify such persons at no charge if there has been a breach of security of the system data or written materials. However, the Act removes the notification requirement when the personal information is encrypted.

There are many available options for hard drive encryption, including Micro Focus ZENworks FDE, Apple FileVault 2, Sophos Central Device Encryption, and BitLocker Drive Encryption.

BitLocker is a Microsoft Windows security and encryption feature that is included with certain newer versions of Windows. BitLocker enables users to encrypt everything on the drive Windows is installed on, protecting that data from theft or unauthorized access. BitLocker protection can also be added to USB flash drives.

BitLocker and Apple FileVault are free as they are provided with newer versions of operating system software.

Another method to encrypt data (and provide digital certificates) is through the Department of Innovation & Technology's (DoIT) Public Key Infrastructure (PKI) Cryptography.

(Continued on next page)

(Continued from page 1)

DoIT, by Legislative directive, is the sole source of digital certificates (and the associated encryption capability) for State of Illinois agencies, boards, commissions,



universities and those who do business with them. DoIT currently provides PKI encryption capability at no cost to users.

When sending confidential data via email or using a file sharing service to transfer confidential data, PKI can be used to encrypt the data. Data can be encrypted by a registered user for secure

transfer and subsequent use by other registered user(s). If such data is breached, it will be unreadable and of no value to unauthorized individuals. However, the authorized party can read the data after decrypting the data through the PKI service. For additional information on this service go to [Public Key Infrastructure Cryptography \(illinois.gov\)](https://www.illinois.gov/public-key-encryption).



In the current environment of frequent and widespread attacks to expose data for profit, encryption is an effective method to limit the exposure of confidential information.

Can ChatGPT Be Used in Auditing

The auditing profession is constantly adapting to technologies and techniques to improve processes and increase efficiency. Artificial intelligence (AI) is a relatively new technology which is making an impact in auditing. One of the latest AI tools is ChatGPT, an artificial intelligence chatbot developed by OpenAI. While its uses in auditing are open for debate, we asked ChatGPT a simple question to get its opinion.



We asked: **How can ChatGPT be used in the auditing profession?**

ChatGPT's response:

ChatGPT can be utilized in the auditing profession in various ways to enhance efficiency, accuracy, and productivity. Here are a few potential use cases:

- 1. Data analysis and anomaly detection: ChatGPT can assist auditors in analyzing large volumes of financial data and identifying potential irregularities or anomalies. By feeding the model with relevant financial information, auditors can leverage its natural language processing capabilities to extract insights and detect patterns that may require further investigation.*
- 2. Risk assessment: Auditors can use ChatGPT to evaluate the risk profiles of different clients or companies. By inputting relevant financial data, the model can provide risk assessments, identify potential red flags, and help auditors prioritize their efforts based on the identified risks.*
- 3. Compliance and regulatory guidance: ChatGPT can be used to stay up-to-date with ever-evolving regulations and compliance requirements. Auditors can interact with the model to ask specific questions related to auditing standards, regulatory frameworks, and industry-specific guidelines, enabling them to provide accurate and consistent guidance to clients.*
- 4. Documentation and report generation: ChatGPT can assist auditors in generating audit documentation and reports. By inputting key findings, observations, and supporting evidence, the model can help streamline the report writing process, ensuring accuracy, consistency, and adherence to auditing standards.*
- 5. Knowledge sharing and training: ChatGPT can act as a knowledge repository for auditors, providing access to a wide range of auditing information, best practices, and industry-specific knowledge. It can be used for training purposes, allowing auditors to ask questions, seek guidance, and learn from the model's responses.*
- 6. Fraud detection: ChatGPT can aid auditors in identifying potential fraud schemes or suspicious activities. By leveraging its language understanding capabilities, the model can assist auditors in analyzing narratives, transaction descriptions, and other textual data to flag potential fraudulent behavior for further investigation.*

It's important to note that while ChatGPT can be a valuable tool in the auditing profession, it should complement and augment human auditors' expertise rather than replace them. Auditors should exercise professional judgment and critical thinking when interpreting and acting upon the model's outputs.

Not a bad answer!!

Compliance Examination Report Changes – Elimination of Report Components

Our State Compliance Examination Reports are conducted in accordance with attestation standards (AT-C) established by the American Institute of Certified Public Accountants (AICPA), the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States (GAS), the Illinois State Auditing Act (Act), and the *Audit Guide*. Historically, the State compliance examination reports released by the OAG have contained multiple components (Report Components) and were included after any findings presented. These Report Components included schedules, variance explanations, narratives of agency functions and planning, etc.

A new understanding of what is allowable within compliance attestation reports resulting from our discussions with the AICPA necessitated a change. Based on the guidance received from the AICPA and the fact we do not want to be out of compliance with professional standards, the Auditor General decided, beginning with the FY22 engagements, we will no longer include these Report Components in our compliance examination reports. Please know that although these Report Components will no longer be included within our reports, this information is still readily available as noted below. In addition, this does not mean we are auditing any less. We will still perform all necessary procedures over appropriations, receipts, equipment, travel, personal services, etc. as we have in previous engagements, and, if exceptions are noted, we will still report findings outlining the deficiencies noted.

The Report Components were originally included within the State compliance examination reports to provide the public with information that was not easily accessible at the time (i.e. pre-electronic age). Now, however, this information is largely accessible online through the Comptroller's website and agency websites. In addition, the amount of time spent both by the agencies and auditors on preparing/reviewing the Report Components is significant, and in our opinion outweighs any potential benefit of continuing to include these Report Components in our compliance examination reports.

The removal of the Report Components from our compliance examinations allows this Office to be in conformity with professional standards and still provide a valuable service to the Legislative Audit Commission by continuing to report deficiencies in compliance and internal control as we have since the Office's inception. In the State's current environment whereby all agencies are having to do more with less, this approach also alleviates unnecessary time and effort for the agencies we audit as well as our Office's staff and Special Assistant Auditors in reporting on information while providing no opinion or assurance on that information.



Updates to the Legislative Audit Commission's University Guidelines

On May 16, 2023, the Legislative Audit Commission (LAC) adopted significant changes to their *University Guidelines*, first adopted on November 30, 1982.

A new understanding of what is allowable within compliance attestation reports from the Office of the Auditor General's (OAG) discussions with the AICPA necessitated a change from past practice of including the majority of the reporting requirements from the Legislative Audit Commission (LAC) *University Guidelines* within the State compliance examination reports for the universities. In late summer 2022, the OAG outlined a plan for the required reporting to be moved into the financial statement reports. The universities raised significant

concerns with this plan, particularly regarding timeliness of financial statement audits, so the OAG developed both a short-term plan and long-term solution. The short-term plan was a single year "grace period" from the requirements to publish certain information as required by the *University Guidelines*. The long-term solutions focused on determining the usefulness and applicability of the *University Guidelines* to the legislature and other users of the university reports. Since the *University Guidelines* originated prior to significant changes in financial reporting and the availability of substantial information via electronic means, some of the requirements were outdated or irrelevant.

In carrying out the long term solutions, the OAG provided an opportunity for Universities to participate in an initiative to update the LAC University Guidelines. The universities established a group with representatives from all Illinois public universities to develop a formal review process and provide input to the OAG.

Through fall 2022 and winter 2023, a group of typically 20-25 individuals representing all Illinois Universities held meetings to systematically review each section of the guidelines and develop a joint document containing suggestions, rationale, and other information for consideration by the OAG. The OAG met periodically with the group and provided feedback on the suggested changes. At the end of April 2023, the universities presented their request to modernize the *University Guidelines* to the LAC. The LAC reviewed the proposed changes, and during their May 16th meeting, they adopted the changes after just a single question to the university representatives present. The OAG has since developed a testing program for our special assistant auditors to use to test compliance with the updated *University Guidelines*, which has been shared with the universities.



Disaster Recovery Plans

In late December 2022, the Office of the Auditor General experienced a need for its disaster recovery plan. A severe cold snap caused our pipes to burst, flooding a substantial portion of the building including our IT room. Fortunately, all of our systems and data were backed up and nothing was lost. We were able to get critical applications up and running quickly. We were also able to seamlessly switch to a full-time work-from-home policy as needed thus minimizing any disruption. Some of this can be credited to having a disaster recovery plan in place.



The Contingency Planning Guide for Information

Technology Systems published by the National Institute of Standards and Technology (NIST) requires entities to have an updated disaster recovery plan. Such a plan should include a review and analysis of the IT environment and contain guidance to help ensure the timely recovery of applications and data.

The lack of a disaster recovery plan or an out-of-date disaster recovery plan has been a finding reported in past compliance examinations for various State agencies.

Findings have included the following issues:

- The disaster recovery plan had not been updated during the examination period.
- Prioritization of applications and data, based on criticality, had not been completed.
- Not all backups were encrypted.
- Detailed recovery scripts for the recovery of the environment, applications, and data were not documented.
- The business continuity plan had not been reviewed or updated.
- The network disaster recovery outline was outdated.
- Disaster recovery testing was not conducted.

Every agency needs to be able to recover quickly from an occurrence that disrupts operations. Without a disaster recovery plan, an agency can suffer data loss, reduced productivity, and reputational damage.



Office of the Auditor General
• 115 Park Plaza, 740 East Ash Street
Springfield, Illinois 62703-3154
• Michael A. Blandin 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
E-mail: audgen@auditor.illinois.gov
Website: www.auditor.illinois.gov