Introduction to Information Technology (IT) Auditing

June 11, 2025

Table of Contents

Introduction

This document provides a general overview of Information Technology Auditing (IT Auditing). However, not all aspects discussed here will apply to every Illinois State government organization. For instance, the Department of Innovation and Technology's (DoIT) client user agencies do not conduct penetration testing. Instead, such functions are either performed by DoIT or carried out in collaboration with DoIT.

IT auditing is a systematic evaluation of an organization's information technology systems, processes, and controls. It aims to assess the effectiveness, security, and compliance of IT resources and to ensure that they align with business goals and regulatory requirements.

IT audit is essential for organizations to:

- Effectively manage IT risks associated with IT systems.
- Comply with regulatory requirements and industry standards.
- Safeguard information assets by assessing the effectiveness of internal controls over IT processes and access.
- Improve efficiency and effectiveness of IT operations by identifying areas of improvement.
- Ensure data confidentiality, integrity, and availability. Verify the accuracy and reliability of data processed and stored by IT systems. Data integrity ensures that an organization's data remains accurate, consistent, and reliable.
- Ensure system development and implementation align with organizational goals and mitigate risks.
- Evaluate how changes to IT systems are managed to ensure they do not introduce new risks. Change management includes software updates, configuration changes, and system migrations.
- Ensure business continuity and ensure business can recover quickly from disruptions including natural disasters or cyber incidents.

IT audits are similar to non-IT audits in many respects. They both follow the same workflow. IT audits and non-IT audits share similarities in their fundamental goals of assessing controls, ensuring compliance, evaluating governance processes, and improving organizational processes. Auditors in both fields document findings and provide recommendations to management. However, they differ significantly in their focus, methodologies, and areas of expertise.

Key Differences Between IT Audits and Non-IT Audits:

- **Focus:** Evaluates the IT controls, security, and reliability of information systems, data governance, and technology infrastructure.
- **Scope:** Focuses specifically on IT systems, applications, and interfaces including hardware, software, security applications, networks, databases, and cybersecurity controls.
- **Expertise:** Require specialized knowledge in information technology, cybersecurity, data management, and IT governance frameworks.
- **Methodologies:** Involves testing of IT controls, vulnerability assessments, penetration testing, and reviews of IT governance.
- **Regulations and Standards:** Compliance is measured against IT standards and frameworks, as well as regulatory requirements related to data protection and privacy.

Examples of Regulatory Requirements:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - HIPAA Privacy Rule
  - HIPAA Security Rule
- Personal Information Protection Act (PIPA) (815 ILCS 530)
- Data Security on States Computer Act (20 ILCS 450)
- Illinois Information Security Improvement Act (20 ILCS 1375)
- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA))
- Uniform Electronic Transactions Act ("UETA") (Public Act 102-0038)

Please see "Regulations and Standards" section on page 14 for additional information.

Examples of Frameworks/Standards/Guidelines:

- Cybersecurity Maturity Model Certification (CMMC) 2.0 Federal DOD compliance
- IRS Publication 1075 (Relevant to federal tax information (FTI))
- Payment Card Industry Data Security Standard (PCI DSS)
- Control Objectives for Information and Related Technologies (COBIT)
- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- Institute of Internal Auditors (IIA) Cybersecurity Topical Requirements and Global Technology Audit Guides (GTAGs)
- IRS Safeguard Control Security Evaluation Matrices (SCSEM) for use in preparing an IT environment that will receive, process, or store FTI

IT Ownership

When IT systems are put in place, there is a purpose behind IT, as well as potentially multiple owners. All owners have knowledge over the different facets of IT and are considered key stakeholders. It is only when taking into consideration all owners that IT risks can be properly identified. These different owners include, but are not limited to:

- Business Owner
    - Define and assess the business requirements that the IT must follow from the business process standpoint.
    - Define and assess the security requirements, including by not limited to:
        - Defines data classification which will be used in determining minimum security requirements.
        - Defines Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Maximum Tolerable Downtime (MTD).
    - Define compliance requirements (policy, statutory, best practices, etc.) and ensure obedience with the requirements.
    - Communicate requirements with Technical Owner
- Technical Owner
    - Design, develop, or procure the IT in consultation with Business Owner.
    - Communicate with the Business Owners regarding their business, security, and compliance requirements.
    - Work with the Business Owners to ensure the application meets the business and security requirements.
    - Work with the Business Owners to ensure compliance requirements are met.
- Data Owner
    - Responsible for classifying data as well as monitoring access rights, back up procedures, and ensure data sanitizing of the data set.
- Data Custodian
    - The maintainer of the data in terms of ensuring protected (confidential), appropriately controlled (integrity) and backed up (available).

Assessing IT Risks

I. Audit Plan

The Audit Plan involves identifying, analyzing, and understanding potential risks that could impact the success and reliability of an audit engagement. Integrating IT risk assessments into an audit plan enhances the effectiveness of the audit process and ensures that potential risks are adequately addressed.

II. Audit Engagement

Conducting an IT risk assessment as part of an audit engagement involves a systematic approach to identify, evaluate, and manage risks associated with information technology systems and processes.

Common IT Audit Topics and Key IT Controls

- IT Governance
- IT General Controls
- Compliance
- System Development Life Cycle (SDLC)
- Application/System Specific Risks
- Vendor Risk Management
- Identity Access Management
- Cybersecurity
- Information Security
- Network Security
- Data Privacy
- Incident Response Preparedness
- Disaster Recovery and Business Continuity
- IT Asset Management
- Encryption
- Endpoint Security
- Patch Management
- Physical Security
- Security Awareness Training
- Secure Configuration Management
- Security Logging and Monitoring
- Batch Job Processing
- Artificial Intelligence (AI)
- Logical Access Controls Over Infrastructure, Applications, and Data
- Program Change Management
- System and Data Backup and Recovery
- Computer Operation Controls

III. IT Project Management

Conducting an IT risk assessment for IT projects is crucial to identifying potential risks and ensuring that projects are completed successfully, on time, and within budget.

Pre-implementation Audits

The Illinois Fiscal Internal Control Auditing Act (FICAA) [30 ILCS 10] requires State agencies to conduct system development reviews of major implementations of new information technology systems or major modifications to existing information technology systems to ensure appropriate controls exist within the system and ensure the needs of the users of the system are being addressed in the new system. These reviews also verify that there are business and technical owner approvals regarding the security and functionality throughout the system being implemented. Unlike a typical audit, these reviews are typically conducted throughout the development of the new system, although at times, some agencies may also conduct these reviews after the fact. The reason for the timing of conducting the review throughout the development of the system is that it is less costly to make appropriate changes, based upon the input of Internal Audit, as the system is being developed. These reviews involve all key stakeholders.

Agile System Development Life Cycle

Most new system development projects utilize the agile System Development Life Cycle (SDLC). Agile development is designed to encourage teamwork and allows the product to adapt to changes quicker than a traditional waterfall development. The waterfall model is linear and sequential where each phase (e.g., requirements, design, implementation, testing, deployment, maintenance) is completed before moving to the next whereas the agile SDLC breaks the development work into small increments (also known as iterations or sprints) that typically last from two to four weeks. Frequent, short standup meetings (or scrums) keep all the team members informed of the product progress. Each iteration consists of a full cycle of planning, analysis, design, coding, unit testing, and user acceptance testing. The planning, analysis and design is defined in a product backlog that is comprised of user stories, bugs, and technical tasks. Adherence to the tasks or stories included in each iteration minimizes system development scope creep and helps each team member to understand their role in the iteration. The product backlog items are prioritized before each iteration and discussed with the product owner(s). Each iteration is concluded by demonstrating the working iteration user stories or features to the product owner(s). After each iteration, and before the beginning of the next iteration, the development team meets for a Sprint Retrospective that provides an opportunity for the development team to conduct self-reflection and create a plan for improvements to be enacted during the next sprint.

Agile development is designed to encourage teamwork and allows the product to adapt to changes quicker than traditional waterfall development. Even though planning and analysis work is included in each iteration, it is also pertinent that proper project planning and analysis is completed before the system coding work begins. For example, there must be proper governance for the SDLC, the project scope must be defined, project schedule must be refined, resources must be planned, initial backlog must be compiled, etc. Typically, in these first stages a system and the data are categorized based on confidentiality, availability, and integrity. Using the

categorization, the auditor can determine a baseline of security controls needed. Further, the system may have a security plan. Best practices include the use of a control document checklist, prepared before the coding begins, that includes and tracks all required documentation for the project. The control document checklist may be adjusted during the project with proper management approval. For a successful system development, there should be a comprehensive plan for any additional infrastructure needs and the data plan for the project (e.g., business process/data flow, interfaced data, and will data be converted from an old system, or will the data be archived, data required for reporting, etc.) should be place. Many information technology solutions utilize Cloud Service Providers for storage and services. This introduces other risks and considerations that must be taken into account prior to the implementation of the system, such as concerns centering around clear ownership, protection of the data, and exit clauses.

Throughout the project, there are governance checkpoints and management approvals for the project to progress to the next phase of the project. Also, a proper segregation of duties between development, testing and productions environments should be maintained.

All testing and training is completed, as well as help documents and procedures are in a written format before the project is put into production to be used by the end users. These documents include procedures for how to use the system as well as for user and developer on-boarding and off-boarding. Also, a written disaster recovery plan, or information system contingency plan, must be in place for the system with proper recovery time and recovery point objectives. Recovery Time Objective is the business owner's determined amount of time the system can be inoperable. The Recovery Point Objective is the business owner's acceptable level of data loss.

Disaster recovery covers the complete recovery process, which can include technical IT as well as process/business owners. Due to this, there may be multiple plans in place covering the recovery efforts which identify the roles and responsibilities of the different owners.

Note: While participating in meetings during planning, design and development, the auditor should be actively looking for any security risks or confidential data that must be protected and either ensure that those risks are addressed or bring the risks to the attention of the development team.

Third Party System Development

Many new systems fall under the implementation of a procured or Third-Party software. Third-Party systems fall into two categories: a third party is procured to develop an entirely new system, or they are procured to modify a commercial off-the-self (COTS) software to fit the business needs. The most typical procurement path for an Information Technology (IT) solution is the Request for Proposal (RFP). Contracts awarded for RFPs are made to the responsible offeror whose proposal is determined to be the most advantageous for the business needs taking into considerations price and the evaluation factors set forth in the RFP.

When a system is being developed by a third party, the focus shifts more from the controls in place by the development team to protecting agency or organization data and needs. The RFP defines all mandatory requirements and spells out any licensing provisions. It is also pertinent that proper project planning and analysis is completed before the system development work begins. For example, system and the data are categorized based on confidentiality, availability, and integrity, there must be proper governance for the system development, the project scope must be defined, project schedule must be refined, resources must be planned, fit-gap analyses are documented, etc. For a successful system development, there should be a comprehensive plan for any additional infrastructure needs and a data plan for the project (e.g., business/process data flow, interfaced data, and will data be converted from an old system, or will the data be archived, data required for reporting, etc.) should be in place. It is also important to determine where the data will be stored. Many Third-Party information technology solutions now utilize the storage of the software and/or the storage of your data in the cloud. This introduces other risks and considerations that must be taken into account prior to the implementation of the system, such as concerns centering around clear ownership and protection of the data.

Throughout the project, there are governance checkpoints and management approvals for the project to progress to the next phase of the project. Before the project can be put into production, all the testing and training is completed, and help documents and procedures are in a written format. These documents include procedures for how to use the system and for on-boarding and off-boarding. Also, a written disaster recovery plan must be in place for the system with proper recovery time and recovery point objectives.

When using a Third-Party Service Provider, at least 2 disaster recovery plans should exist.

- One which covers the Service Providers environment and responsibilities. It may be developed and retained by the Service Provider
- The other covers the organization contracting out. It should contain information such as:
    - Organizational roles and responsibilities relating to communication between key staff and technical SME.
    - Organizational controlled elements (interfaces, databases, sign-on mechanisms, etc.) used within the system, the priority to bring them back up, and how to do so.

Note: During the planning, design and implementation processes, the auditor should be actively looking for any security risks or confidential data that must be protected and either ensure that those risks are addressed or bring the risks to the attention of the management.

IV. Cloud Services

Cloud services are becoming more critical for organizations as they seek options for efficient digitalization and cost savings. Moving to cloud-based services provides many benefits including greater scalability, cost efficiency, improved agility, improved reliability, and improved business continuity. However, using Cloud Services increases overall risk for an organization. This can

happen when control of the internal control environment is transferred. Increased risk can include:

- Loss of control and oversite (reduced visibility and lack of transparency)
- Security and data privacy risks (third party access and compliance risks)
- Dependence on the Service Provider (Single point of failure and vendor lock-in)
- Quality Assurance and Performance Risks (Inconsistent service deliver and lack of customization)
- Regulatory and Compliance Challenges (Unclear Accountability and Changing Regulations)
- Intellectual Property (IP) and Confidentiality Concerns (Data loss or exposure and inadequate safeguards)
- Communication and Coordination Challenges (Time Zone Barriers and Misaligned Priorities)
- Increased Complexity in Management (Complex Contracts and SLAs and Coordination Between Teams)
- Risk of Vendor Insolvency or Business Disruption (Provider stability)
- Difficulty in Transitioning Back In-House (Exit strategy)

Cloud platforms have delivery models such as:

- **Software-as-a-Service (SaaS**). SaaS based software or applications are not located on TA's devices or premises. Instead, they are accessed by a web-browser or Application Programming Interfaces (API). This allows a more efficient way for the service provider to manage upgrades and security benefiting the user agencies since they are no longer required to maintain the software installs and updates.
- **Infrastructure-as-a-Service (IaaS).** IaaS is when a vendor provides clients pay-as-you-go access to storage, networking, servers, and other computing resources in the cloud. IaaS clients are responsible for managing aspects such as applications. IaaS allows clients to bypass the cost and complexity of buying and managing physical servers and datacenter infrastructure.
- **Platform-as-a-Service (PaaS).** Unlike SaaS that provides "ready-to-use" software, PaaS provides a platform for software creation. This typically includes operating system, programming language execution environment, database, web server etc.
- **Function-as-a-Service (FaaS).** FaaS is a serverless computing model where developers can execute code in response to events without managing servers. Examples include AWS Lambda, Google Cloud Functions, Azure Functions.

Below are some of the deployment options for cloud service:

- **Public Cloud.** A third-party cloud service provider owns and operates all the cloud resources (like servers and storage). The services are provided over the internet.
- **Government Cloud.** Government cloud is designed for government entities (federal, state, or local). Government cloud can meet the standards (FedRAMP, HIPAA, CJIS, etc.) and several security and compliance requirements of many government agencies. Data on US government cloud resides only in the US.

- **Private Cloud.** The cloud resources and infrastructure are operated and maintained on a private network and dedicated to an organization. The private cloud can be located on the organization's on-site datacenter or hosted by a third party.
- **Hybrid Cloud.** A hybrid cloud combines private cloud with a public and/or government cloud. Data and applications can move between the different environments.
- **Community Cloud.** Community cloud is a shared environment to a limited set or organizations or employees. Community clouds are used by organizations like government agencies, financial institutions, and healthcare providers. These organizations usually have industry-specific security and privacy requirements.
- **Multi-cloud.** Multi-cloud utilizes multiple cloud services from different providers. It also reduces dependency on a single vendor, enhances redundancy, and optimizes performance.

As agencies implement more of their IT computing functions and data storage into cloud resources, it becomes increasingly important for auditors to provide added value by giving adequate assurance that agencies' controls provide security and efficient and effective operations. Auditor should review and verify the agency is requesting a SOC 2 Type 2 report over the contracted control environment where the data will be hosted. Auditor should also verify the SOC report was reviewed by the agency, and the review was documented to address any concerns.

V. System and Organization Controls (SOC) Reports

SOC 2 stands for System and Organization Controls 2. It is a set of standards designed to help companies manage customer data based on five key principles: security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports are an independent auditor's assessment of organizations IT controls and processes.

SOC 2 Report Types:

- Type 1 assesses the design of controls at a specific point in time.
- Type 2 assesses both the design of controls as well as their effectiveness of controls over a period of time, most commonly over 12 months.

There are five **trust service criteria (TSC)** for a SOC 2 report:

1. **Security**
   Safeguarding against unauthorized access includes access controls, network security, and monitoring systems for security events and ensuring they are securely configured.

2. **Availability**
   Maintaining uninterrupted service requires ensuring system uptime, having disaster recovery plans, and ensuring resources are available to meet demand.

3. **Processing Integrity**
   Delivering accurate and complete information requires ensuring that data is processed accurately and without errors. Also, checks should be implemented to verify data integrity and processing.

4. **Confidentiality**
   Data should be protected through encryption during storage and transmission. Protecting sensitive information also requires limiting access to confidential information to authorized users only. Data Retention Policies should be in place to ensure confidential data is stored and disposed of properly.

5. **Privacy**
   There are increasing concerns regarding data privacy, and data protection requires compliance with privacy regulations regarding the collection, use, and sharing of personal data. Organizations should also have procedures in place to address potential data breaches affecting personal information.

Auditors should be aware that, with the exception of security TSC, a SOC 2 report is not required to address all five trust service criteria. The SOC 2 report should include trust service categories relevant to the service provided and should cover the solution being acquired. It is crucial for management to review SOC 2 Type 2 reports because these reports play a pivotal role in safeguarding an organization's security posture and ensuring effective risk management. Among other things, management should note where the SOC report highlights areas where controls are weak or ineffective and note any Complementary User Controls, also known as Complementary User Entity Controls (CUECs). CUEC's are specific responsibilities or controls outlined in the SOC report that a user organization must implement to ensure the effective operation of a service provider's controls.

SOC 2 reports are the reports that are aligned with the objectives of most IT audits, there are other SOC reports to be aware of. SOC 1 reports cover Internal Controls for financial statements and reporting when a Service Organization provides a service that can impact a client's financial statements (for example, collection agencies, payroll providers, payment processing). SOC 3 reports are the result from a SOC 2 report but tailored for a general audience, which usually means that any confidential information is redacted and are used for marketing purposes.

It is also important to remember that a Service Organization cannot be SOC "certified". A SOC report is an "attestation report" which provides an opinion on the controls examined and, in Type 2 reports, tested based on a specific audit period.

VI. Enterprise Risk Management/Governance Risk and Compliance

A systematic approach that organizations use to identify, assess, and mitigate potential risks. Part of this process is conducting a Business Impact Analysis (BIA). A BIA is a systematic process to determine and evaluate the potential effects of an interruption to critical business functions as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's disaster recovery plan, the output of which is a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied.

The following steps are part of the systematic approach agencies must take:

1. Maintain an inventory of all IT related assets.
2. Document which systems/applications are most critical and dependencies between systems or functions.
3. Determine Recovery Time Objective (RTO).
4. Determine Recovery Point Objective (RPO).
5. Identify potential risks.
6. Identify the resources (including, staff, technology, facilities, etc.) necessary for recovery efforts.
7. Prioritize/rank functions for recovery.

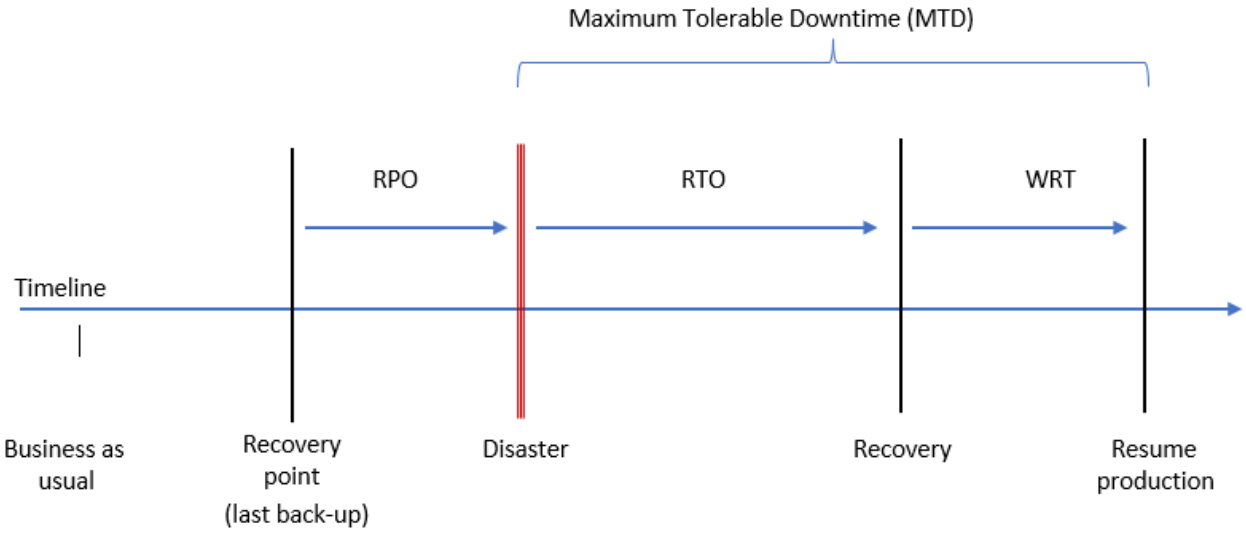
RPO, **RTO**, and **WRT** are key terms used in the context of business continuity and disaster recovery planning. They help organizations define their recovery strategies and set expectations for data loss and downtime.

Maximum Tolerable Downtime (MTD) - The maximum amount of time a business can tolerate the outage of a critical business function. Sometimes referred to as Maximum Tolerable Outage (MTO), the MTD consists of two elements, the systems recovery time (RTO) and the work recovery time (WRT). Therefore, MTD = RTO + WRT.

Recovery Point Objective (RPO) - The point in time, prior to a disruption or system outage (e.g., end of previous day's processing). RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that might need to be recreated after the systems or functions have been recovered. (I.e., how much data can be afforded to be lost)

Recovery Time Objective (RTO) - The period of time within which a system shall be recovered after an outage (e.g., one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. (I.e., how long can the business afford for the system be down)

Work Recovery Time (WRT) - The period of time within which critical business functions are recovered and running once the systems are restored.



IT Audit Criteria

Audit Criteria for IT audits can look similar to non-IT audits. Criteria includes statutes and regulations as well as internal policies, procedures, and standard operating guides. In addition, there are industry recognized frameworks or standards published by National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), Payment Card Industry (PCI) Security Standards Council, Open Worldwide Application Security Project (OWASP), and other well recognized industry partners that publish best practices, frameworks, and standards. They are generally publicly available on their trusted websites and may be downloaded and reviewed to identify relevant best practices. Some frameworks require a membership and/or purchase such as ISO 270001 and COBIT.

Common Frameworks and Standards

- **Organizational Standards**

  Organizational Standards are the organization's own policies, procedures, and processes used to manage and monitor compliance or alignment with the organization's mission, business environment, legal environment, risk tolerance, privacy and security risks, and operational requirements.

- **National Institute of Standards and Technology (NIST)**

  "NIST is a U.S. federal agency that develops and promotes measurement standards, guidelines, and technologies. It plays a crucial role in various fields, including information technology, cybersecurity, manufacturing, and environmental science. … Its guidelines are

widely referenced by federal agencies and are often adopted by private sector organizations to enhance their cybersecurity posture" (NIST.gov).

NIST publishes the NIST Cybersecurity 2.0 (NIST CSF 2.0) and various guidance such as *NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations* and *NIST Cybersecurity Framework* free of charge on their website.

- **Center for Internet Security (CIS)**

  "CIS is a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data" (cissecurity.org). CIS Controls are best practices designed to help organizations improve their cybersecurity posture, and CIS Benchmarks are configuration recommendations aimed at strengthening organizations' defenses against cyber threats.

- **ISACA**

  ISACA is a global professional association focusing on IT Governance and offers IT Audit Framework as a set of standards and best practices. ISACA's Control Objectives for Information and Related Technologies (COBIT) is a framework for the governance and management of enterprise information and technology.

- **International Organization for Standardization (ISO)**

  ISO standards often emphasize risk assessment and management. IT auditors can use these principles to evaluate how organizations identify, assess, and mitigate risks related to information security and data protection. ISO standards such as ISO 27001 (Information Security Management Systems) or ISO 27002 (Code of Practice for Information Security Controls) can be used for evaluating an organization's processes and controls.

- **Institute of Internal Auditors (IIA)**

  State Internal Audit Advisory Board (SIAAB) promulgates a set of professional standards based on the standards of the IIA among others. The IIA also publishes information technology guidance such as Global Technology Audit Guides (GTAGs) and Cybersecurity Topical Requirements.

- **Cloud Security Alliance (CSA)**

  IT auditors use the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) as a framework to evaluate the security posture of cloud service providers (CSPs). The CCM provides a comprehensive set of security controls specifically designed for cloud computing, and auditors use the CCM to identify potential risks associated with cloud services. The matrix allows auditors to assess specific controls related to various domains such as data security, identity management, and compliance.

- **Other legal standards or regulations such as HIPAA, PCI, GDPR, etc.**

  There are additional legal and regulatory requirements the IT auditor should be familiar with to ensure that organizations comply with laws and standards related to data protection, cybersecurity, and IT governance.

While IT auditing is focused on evaluating internal controls over existing systems and organization, it is also always evaluating future opportunities and risks. Currently emerging technologies include Artificial Intelligence (AI), Internet of Things (IoT), and blockchain among other things. Agencies must adapt to everchanging information technology and stay diligent in updating policies or writing new polies (such as AI Policy) as new technology emerges and cyber threats continue to evolve.

Regulations and Standards

- Biometric Information Privacy Act 740 ILCS 14
    - Regulates the collection, use, safeguarding, and destruction of biometric identifiers and information by private entities in Illinois.

- California Consumer Privacy Act (CCPA)
    - Grants new privacy rights to California consumers.

- Data Security on States Computer Act (20 ILCS 450)
    - Established to protect sensitive data stored on State-owned electronic data processing equipment to be (i) disposed of by sale, donation, or transfer or (ii) relinquished to a successor executive administration.

- General Data Protection Regulation (GDPR)
    - The European Union's (EU) General Data Protection Regulation (GDPR) is a comprehensive set of privacy and security laws adopted by EU member states to protect the personal data of EU citizens.

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - HIPAA Privacy Rule – establishes national standards to protect individual's medical records and other identifiable health information (collectively defined as "protected health information").
    - HIPAA Security Rule – establishes national standards to protect individual's electronic personal health information that is created, received, used, or maintained by a covered entity.

- Illinois Information Technology Accessibility Act (IITAA) 30 ILCS 587
    - Requires Illinois state agencies and universities to ensure that their websites, information systems, and information technologies are accessible to people with disabilities.

- Illinois Information Security Improvement Act (20 ILCS 1375)
    - Aims to enhance cybersecurity measures across state and local government entities.

- Illinois Personal Information Protection Act (PIPA) 815 ILCS 530
    - Establishes specific guidelines for how businesses and organizations must handle sensitive information.

- Illinois State Auditing Act - Section 30 ILCS 5/3-2.4
    - Section of the Illinois Compiled Statutes that pertains to the Office of the Auditor General (OAG) and its responsibilities regarding audits of state agencies. Specifically, it addresses the OAG's role in auditing State agencies' cybersecurity programs and practices, with a particular focus on agencies holding large volumes of personal information.

- Illinois Uniform Electronic Transactions Act (UETA) 815 ILCS 333
    - Provides a legal framework for electronic transactions and signatures.

- The International Organization for Standardization (ISO)
    - ISO standards provide a wide range of standards for information technology (IT) to help organizations and industries maintain quality, security, and efficiency in their systems and processes covering a wide range of areas and are internationally agreed upon by experts. ISO IT standards include:
        - ISO/IEC 27001: Information Security Management
        - ISO/IEC 27002: Code of Practice for Information Security Controls
        - ISO/IEC 20000: IT Service Management
        - ISO/IEC 22301: Business Continuity Management
        - ISO/IEC 29100: Privacy Framework
        - ISO/IEC 9001: Quality Management Systems (QMS)
        - ISO/IEC 12207: Software Life Cycle Processes
        - ISO/IEC 25010: Software Quality Models
        - ISO/IEC 15504 (SPICE): Process Assessment
        - ISO/IEC 19770: Software Asset Management (SAM)
        - ISO/IEC 17025: General Requirements for the Competence of Testing and Calibration Laboratories
        - ISO/IEC 11801: Information Technology – Generic Cabling for Customer Premises

- IT Audit and Assurance Standards (ITAF™)
    - ISACA's IT Audit and Assurance Standards (ITAF™) are a set of globally recognized guidelines and practices designed to help IT auditors, professionals, and organizations ensure that their IT systems and operations are properly assessed, controlled, and improved. The ITAF provides a structured approach to auditing IT systems and helps organizations effectively evaluate their information technology environments.

- Payment Card Industry (PCI) Data Security Standards (DSS)
    - Set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It was created by the Payment Card Industry Security Standards Council (PCI SSC) to enhance cardholder data security and reduce credit card fraud.

Glossary

Access Rights - Also known as access permissions or access control, refer to the privileges granted to users or systems, determining their ability to read, write, modify, delete, or otherwise interact with computer files, applications, or systems. (soffront.com) The primary components of access rights include:

- **Identification**: The process of recognizing a user or system, typically through a unique identifier such as a username or user ID.
- **Authentication**: Verifying the identity of the user or system, often using methods like passwords, biometrics, or security tokens.
- **Authorization**: Determining the specific actions or resources the authenticated user or system is permitted to access or modify. (www.bcsconsultants.com)

Artificial intelligence (AI) - Technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy. (ibm.com)

Batch Job – Jobs that can run without end user interaction, or can be scheduled to run as resources permit, are called batch jobs. Batch processing is for those frequently used programs that can be executed with minimal human interaction. (ibm.com)

Business Continuity - Paradigm for maintaining operations, even if in a temporarily limited capacity, in the event of unexpected or planned disruptions to normal business processes. These disruptions can include natural disasters, cyberattacks, armed conflict or other force majeure, global pandemics, power outages due to storms or flooding, infrastructure failures, planned maintenance activities, and even the unexpected departure of a key employee. (oracle.com)

Change Management - Practice designed to minimize disruptions to IT operations while making changes to critical systems and services. A good change management process is also vital for information security because it helps organizations protect their most sensitive assets during changes to systems, processes, and technology. (iso.org)

Confidentiality, Integrity, and Availability (CIA triad) – Essential objectives that organizations must prioritize when designing, implementing, and managing security systems, networks, and policies.

- **Confidentiality**: Ensuring that sensitive data is accessed only by authorized individuals or systems.
- **Integrity**: Ensuring data remains accurate, consistent, and unaltered during transmission or storage.
- **Availability**: Ensuring data and network resources are accessible to authorized users when needed. (Cybersecuritynews.com)

Data Classification – Specialized term used in the fields of cybersecurity and information governance to describe the process of identifying, categorizing, and protecting content according to its sensitivity or impact level. In its most basic form, data classification is a means of protecting your data from unauthorized disclosure, alteration, or destruction based on how sensitive or impactful it is. (learn.microsoft.com)

Disaster Recovery - Disaster recovery is the process by which an organization anticipates and addresses technology-related disasters. The process of preparing for and recovering from any event that prevents a workload or system from fulfilling its business objectives in its primary deployed location, such as power outages, natural events, or security issues. (aws.amazon.com)

Encryption - Process of transforming readable plaintext into unreadable ciphertext to mask sensitive information from unauthorized users. Organizations regularly use encryption in data security to protect sensitive data from unauthorized access and data breaches. Encryption works by using encryption algorithms to scramble data into an indecipherable format. (ibm.com)

Endpoint Security - Protects end users and endpoint devices—desktops, laptops, mobile devices, servers, and others—against cyberattacks. (ibm.com)

Identity and Access Management - The administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users. (csrc.nist.gov)

Incident Response – Strategic, organized response an organization uses following a cyberattack. The response is executed according to planned procedures that seek to limit damage and repair breached vulnerabilities in systems. Six steps of an Incident Response Plan:

1. Prepare - how well an organization will be able to respond in the event of an attack.
2. Identify - determining whether an incident has occurred.
3. Contain - limit and prevent any further damage.
4. Eradicate - ensure that malicious content has been removed from affected systems and systems have been thoroughly cleaned to prevent the risk of reinfection.
5. Recover - bring affected systems back into the production environment and ensures another incident does not occur.
6. Learn - review their incident response and adapt their approach for future attacks.

(fortinet.com)

Information System Contingency Plan – A type of Disaster Recovery plan. This plan is a set of procedures and strategies designed to ensure the continuation or recovery of a particular IT system and data in the event of a disruption, disaster, or emergency. It outlines actions to restore services, protect data, and minimize downtime, helping an organization maintain operations during unexpected events. (isaca.org)

IT Governance - The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals (www.gartner.com). It involves aligning IT strategy with business strategy, managing IT-related risks, ensuring compliance with regulations, and optimizing IT investments to deliver value to the organization (www.cio.com)

IT Risk - The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (csrc.nist.gov)

IT Systems - A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. (csrc.nist.gov)

Logical Access - The tools and protocols used in computer information systems for identification, authentication, authorization, and accountability. It involves controlling access to hardware and software resources through remote interactions, as opposed to physical access, which involves direct interactions with hardware in a physical environment. (www.techopedia.com)

Patch Management - Process of applying vendor-issued firmware and software updates to close security vulnerabilities and optimize the performance of software and devices.

Penetration Testing (Pen Testing) - Penetration testing is a simulated cyberattack that's used to identify vulnerabilities and strategize ways to circumvent defense measures. There are different forms of Pen Testing. Some examples:

- Network Pen Testing
- Social Engineering Pen Testing
- Web Application Pen Testing
- Wireless Pen Testing
- Internet of Things (IoT) Pen Testing
- Cloud Pen Testing
- Database Pen Testing
- Mobile Device Pen Testing

(EC-Council)

RFP - A Request for Proposal (RFP) is a formal document issued by an organization to solicit detailed proposals from potential vendors or service providers. The RFP outlines the organization's specific requirements, project goals, timelines, and evaluation criteria, inviting vendors to submit their solutions and pricing. This process enables organizations to compare different offerings and select the most suitable provider for their needs. (techtarget.com)

RFQ - An RFQ, or Request for Quotation, is a formal document issued by a buyer to solicit detailed pricing and terms from potential vendors for specific products or services. This process allows organizations to compare offers and select the most suitable supplier based on cost, quality, and delivery timelines. (wrike.com)

SOC 1 Report – (System and Organization Controls 1) is an independent evaluation that assesses a service organization's controls relevant to a user entity's internal control over financial reporting. These reports are specifically designed to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements, in evaluating the effect of the controls at the service organization on the user entities' financial statements. (aicpa-cima.com)

SOC 2 Report – An independent evaluation that assesses a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy. These reports are intended to meet the needs of a broad range of users who require detailed information and assurance about the controls at a service organization relevant to the security, availability, and processing integrity of the systems the service organization uses to process users' data, and the confidentiality and privacy of the information processed by these systems. (aicpa-cima.com)

SOC 3 Report - (System and Organization Controls 3) is an independent evaluation that assesses a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy. Unlike SOC 2 reports, SOC 3 reports are intended for general public distribution and provide a high-level overview of the organization's controls without detailed information. This makes them suitable for marketing purposes, allowing organizations to demonstrate their commitment to data security and privacy to a broad audience. (techtarget.com)

System Development Life Cycle (SDLC) - The system development life cycle is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases. For any SDLC model that is used, information security must be integrated into the SDLC to ensure appropriate protection for the information that the system will transmit, process, and store. (csrc.NIST.gov)

Vulnerability Assessment - Systematic review of security weaknesses in an organization’s information systems. Vulnerability analysis works as a form of threat assessment, as it is used to evaluate how susceptible a network may be to future cyberattacks or attempted hacks. (EC-Council)