SIAAB Guidance #08
Internal Audit Coverage, Risk Assessment, FCIAA Compliance
Adopted February 13, 2018

Revised In Accordance with 2024 Standards – Effective January 7, 2025

**** Note: The State Internal Audit Advisory Board (SIAAB) requires Illinois Internal Auditors to follow the Global Internal Audit Standards (GIAS) of the Institute of Internal Auditors (IIA). The structure of GIAS consists of 5 Domains, 15 Principles and 52 Standards. Any references made to GIAS will begin with the Domain, then Principle followed by a (.) and then the Standard. For example, Domain II, Principle 3, Standard 4 would be referenced as GIASII 3.4.*

The terms "Chief Executive Officer" or "Agency Head" as utilized in this document are interchangeable and shall refer to the individual who has been designated by the Governor as the head of an agency under the Governor or the Constitutional Officer, in the case of those entities which do not fall under the direct jurisdiction of the Governor. The term "Agency" as utilized in this document, refers to an agency under the Governor or the Constitutional Office, in the case of those entities which do not fall under the direct jurisdiction of the Governor.

The terms "Chief Internal Auditor," "Chief Audit Executive," "Director Internal Audit" or similar positions describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of GIAS and ensuring the quality of the performance of internal audit services. This document uses those terms interchangeably. The specific job title and/or responsibilities of the chief audit executive may vary across organizations. In Illinois, the Fiscal Control and Internal Auditing Act refers to this position as Chief Internal Auditor. The Chief Internal Auditor or others reporting to the Chief Internal Auditor, will have the appropriate professional certifications and qualifications.

SIAAB Interpretation

Chief Internal Auditors (CIAs) must strike a balance between adhering to internal audit requirements and the best use of their limited resources to provide appropriate internal audit coverage in an effective and efficient manner. This should be accomplished by the CIA conducting an annual risk assessment. This is required by both FCIAA and the GIAS.

GIASIV 9.4 states, "The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. The assessment must be performed at least annually."

The Fiscal Control and Internal Auditing Act (FCIAA) in 30 ILCS 10/2003 requires each Chief Internal Auditor to develop a two-year Audit Plan that covers "Audits of major systems of internal accounting and administrative control conducted on a periodic basis so that all major systems are reviewed at least once every 2 years." Specific areas noted within FCIAA include the following:

obligation, expenditure, receipt and use of public funds and those held in trust, grants, reviews of the design of major new or major modifications to existing information technology systems and special audits.

Although not specifically referenced in the audit section of FCIAA, historical practice has included giving consideration to the 11 general transactional categories listed in the Statewide Accounting Systems Manual (SAMS). The rationale that has been given for this practice is that since management is required to certify the adequacy of their internal controls after giving consideration to these general transactional categories, internal auditors should give them consideration during their audit planning. This is because management relies on internal auditors to notify them of any internal control weaknesses, they discover during the various audits they conduct of the agency's activities. It is important to note that these 11 SAMS categories are generally not the audits themselves but rather transactional categories that should be given consideration by the CIA during their risk assessment process. Because each agency is unique, the CIA must give consideration to the unique environment in which the agency operates. Therefore, a CIA must make their assessment based upon their professional judgement as well as the best use of their available resources.

GIASIV 9.4 states, "One approach to preparing the internal audit plan is to organize potentially auditable units within the organization into an audit universe to facilitate the identification and assessment of risks. An audit universe is most useful when it is based on an understanding of the organization's objectives and strategic initiatives and aligned with the organization's structure or risk framework. Auditable units may include business units, processes, program, and systems. The chief audit executive can link those organizational units to key risks in preparation for a comprehensive risk assessment and the identification of assurance coverage throughout the organization. This process enables the chief audit executive to prioritize the risks to be evaluated further during internal audit engagements."

It is SIAAB's position that in order to develop a risk-based Audit Plan that relates to the activities of the agency, the Internal Audit shop should develop an "audit universe" or "auditable units" for the agency. An "Audit Universe" or "Auditable Units" are internal audit industry terms that refer to a compilation of the activities responsibilities, processes and programs of the various business units, departments, and groups of the organization. They are an inventory of the activities or functions of the agency that should be given consideration during the risk assessment process. The audit universe should be created based upon the organizational structure of the agency. This enables Internal Audit to directly link the Internal Audit Plan to the risks based upon the primary owner of the process. The key to maintaining a good schedule of auditable units is to periodically verify that there have been no changes or additions to the auditable units. The auditable units should be updated to reflect any changes in structure, functions or responsibility at least annually. When responsibility changes occur, historic data should be retained to reflect the previous responsibilities and audit coverage that was given. The development of the auditable units for the agency provides many benefits including but not necessarily limited to the following:

- Provides the framework for monitoring the internal control structure of the operational area and provides the foundation for the risk assessment process;
- Allows Internal Audit to communicate with each division or office of the agency in a standardized manner to monitor the internal controls;
- Provides a mechanism for confirming whether all processes have been captured and given consideration;
- Provides a means for monitoring historic audit coverage for all functions and activities;
- Demonstrates compliance with the standards and laws that govern the Internal Audit function; and
- Considered an Internal Audit best practice.

The 11 SAMS categories should be given consideration as part of the risk assessment process against the functions and activities defined by the audit universe/auditable units of the agency. The risk assessment may reveal that certain SAMS categories may not be the highest risk areas just as certain audit universe/auditable units may not be the highest risk. Therefore, coverage may not be given to all 11 SAMS categories during a 2-year cycle. The CIA must retain documentation to support this conclusion. In addition, generally an audit universe/auditable units is too large to cover over a 2 year period so coverage is provided based upon covering those areas that pose the highest risk first. It is important to understand that a risk assessment is a prioritization of audit coverage. If all high-risk items are covered during the period and if time and resources are available, the CIA may elect to conduct audits of additional lower risk areas. Audits of these areas will also provide benefit to management, but the risk assessment is utilized to ensure that those areas which pose the highest risk are given audit coverage first. Environments and conditions change quickly so the audit plan may need to be adjusted during the period. This should be communicated in some manner to the head of the agency.

GIASIV 9.2: The chief audit executive must develop and implement a strategy for the internal audit function that supports the strategic objectives and success of the organization and aligns with the expectations of the board, senior management, and other key stakeholders. An internal audit strategy is a plan of action designed to achieve a long-term or overall objective. The internal audit strategy must include a vision, strategic objectives, and supporting initiatives for the internal audit function. An internal audit strategy helps guide the internal audit function toward the fulfillment of the internal audit mandate.

GIASIV 9.4 states, "The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives. The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually.

The internal audit plan must:

- Consider the internal audit mandate and the full range of agreed-to internal audit services.

- Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
- Consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.
- Identify the necessary human, financial, and technological resources necessary to complete the plan.
- Be dynamic and updated timely in response to changes in the organization's business, risks, operations, programs, systems, controls, and organizational culture."

"The chief audit executive must review and revise the internal audit plan as necessary and communicate timely to the board and senior management:

- The impact of any resource limitations on internal audit coverage.
- The rationale for not including an assurance engagement in a high-risk area or activity in the plan.
- Conflicting demands for services between major stakeholders, such as high-priority requests based on emerging risks and requests to replace planned assurance engagements with advisory engagements.
- Limitations on scope or restrictions on access to information."

GIASIV 9.4 goes on to state, "The chief audit executive must discuss the internal audit plan, including significant interim changes, with the board and senior management. The plan and significant changes to the plan must be approved by the board."

SIAAB is issuing the follow framework as a recommended methodology for complying with all of these requirements. We believe this methodology for having a documented risk assessment, satisfies the requirements of the IIA Standards, FCIAA and SIAAB By-Laws. Because the risk assessment utilized to develop the audit plan is based upon the unique activities of each agency, we recognize that there should be considerable flexibility allowed to account for the CIA's professional judgment, however; these decisions must be documented. The written procedures of the Internal Audit Office should provide direction for compliance with each element of the following compliance framework as appropriate for each agency.

1. A documented risk assessment performed on an annual basis.
2. A determination of the organization's audit universe.
3. Establishment of assessment criteria to be applied to the audit universe, including fraud considerations and threats to internal control.
4. The development and utilization of appropriate assessment tools to effectively gather information from each auditable unit in regard to the identified criteria.
5. The maintaining of sufficient documentation to support the evaluation and conclusions drawn.

Documented Risk Assessment

The CIA must establish written procedures that outline the audit plan development and risk assessment process to be followed by their agency and the related supporting documentation. Because the environment and activities are unique to each agency, the process should be uniquely tailored to each agency. As internal auditors know, written procedures provide the road map that should be followed to ensure consistent application of the audit planning process. The professional judgement of the CIA and their knowledge of the activities of their agency is critical to ensuring the limited internal audit resources are applied in an efficient and effective manner.

The creation and retention of sufficient documentation to support the audit planning process is also a critical component. The State Records Act requires documentation to support decisions that are made in the course of conducting business on behalf of the State. The specific documentation necessary to support these decisions will be unique to the environment of each agency but should consist of information sufficient for a professional internal auditor to arrive at similar conclusions.

Determination of Audit Universe

The methodology must provide that the audit universe for the organization be determined and documented. The audit universe/auditable units should represent the uniqueness of the organization and should be tied to the organization’s goals, as prescribed by the IIA Standards.

An “Audit Universe” or “Auditable Units” are internal audit industry terms that refer to a compilation of the activities responsibilities, processes and programs of the various business units, departments and groups of the organization. They are an inventory of the activities or functions of the agency that should be given consideration during the risk assessment process. An audit universe/auditable units provides the audit categories that are to be given consideration during the risk assessment process. The structure of the audit universe/auditable units should be determined at the discretion of the CIA based upon the activities of the agency and the CIA’s professional judgment. As noted in the IIA Standards there is considerable flexibility allowed to account for the CIA’s professional judgment. There are various ways in which compliance may be accomplished. Because the audit universe/auditable units are unique to the agency, approaches will vary between agencies and will be highly dependent upon the CIA’s professional judgment. Some elect to place emphasis around a business unit structure, others place emphasis on the programmatic activities, others focus on consideration of functional activities, physical location or various other approaches. Whatever methodology is adopted by a CIA, they must develop audit universe/auditable units and document the selected approach. The development of the audit universe/auditable units provides the following benefits:

a. Provides the foundation for the risk assessment process.

b. Provides the framework for monitoring the internal control structure within the organization.

c. Allows Internal Audit to communicate with each identified unit in a standardized manner.

d. Provides a mechanism for confirming whether all processes have been captured.

e. Provides a means for monitoring historic audit coverage for all functions and activities of the organization.

f. Demonstrates compliance with the Standards and the law that govern the internal audit function.

g. Considered a best practice under the IIA Standards.

Establishment of Assessment Criteria

To perform a sufficient risk assessment, criteria must be established on which each auditable unit is to be assessed. The CIA may utilize the organization's risk management framework which documents the types of risks or risk categories that are important to the organization's Board or the unique operations of the organization. If a documented framework does not exist or the CIA prefers their own methodology, the CIA shall use his/her own judgment of risks after consultation with senior management and the board. Some examples of risk categories on which the auditable units could be assessed are:

- Strategic
- Operational
- Financial
- Personnel
- Regulatory
- Governance
- Reputational
- Fraud
- Technological

Factors that should be considered when developing the criteria for the assessment may include the following:

- Financial Exposure;
- Significance of Area;
- Changes to Laws, Rules and Regulations;
- Adequacy, Effectiveness & Quality of Controls including written policies and procedures;
- Major Changes in Information Technology;
- New Programs or Initiatives;
- Complexity of Operations;
- Rapid Growth, Competence & Experience of Staff and Management;
- Previous Internal or External Findings;
- Cause or Suspicion of Fraud;
- Time Since Last Audit;
- Political or Press Exposure;
- Ethical Climate;

- Low Employee Moral or Problematic Personnel and Opportunities to Achieve Operating Benefits;
- Volume or complexity of transactions;
- Confidential or protected information.

Consideration may also be given to the major threats to internal controls, which include the following:

- **Management Override -** Controls that are readily set aside at the option of management or personnel. This is equivalent to no controls at all.
- **Optional or Incomplete Controls -** Controls that say "may" or those that give options without guidance for making decisions about how to proceed are not effective. They should include clear direction regarding the choice that should be made.
- **Form Over Substance -** Controls appear to be well designed but there is no substance to them or they are ineffective or miss their intended mark.
- **Conflicts of Interest -** Causes personnel to place their interest above that of the organization.
- **Access to Assets -** Having improper access to assets can result in theft, misuse or abuse.
- **Inadequately Trained or Uninformed Personnel -** Results in personnel not being able to properly perform required tasks. Personnel not understanding the reason for a particular control and the desired result may not properly execute the necessary steps. It does not matter how well the procedures are written if personnel cannot execute them properly. The end result is the same as if no controls were in place.
- **Segregation of Duties-** One individual having access to too many aspects of a transaction process can result in errors, theft, misuse or abuse.

Additional consideration may also be given to the reasons why non-fraud related issues occur. These might include the following:

- The process becomes routine and this familiarity causes steps in the process to be overlooked;
- Information concerning a law, rule or procedure was never communicated to a unit or employee;
- Employees are not properly trained or instructed;
- Personnel do not recognize the importance of a step or process or its potential impact on another area;

- Personnel fail to handoff to another area or there is confusion over which area is responsible for particular processes or procedures (each area incorrectly thinks the other is handling the process);
- Time constraints;
- Inadequate resources devoted to the process;
- Employees unknowingly overlook something;
- Personnel become too close to the process to think of improvements (married to the existing process);
- It is difficult to proofread your own work.

Consideration may also be given to the reasons why fraud related issues occur. These might include the following:

Fraud, by definition entails intentional misconduct designed to evade detection. There are three types of fraud to consider when performing a risk assessment. These include misappropriation of assets, fraudulent financial reporting and corruption. Misappropriation of assets involves misuse and/or theft of the organization's assets. Fraudulent financial reporting involves intentional and deliberate misstatements or omissions of financial accounting information with the intent to deceive. Corruption is a form of dishonest or unethical conduct by a person entrusted within the organization.

GIASIV 9.4 "The internal audit plan must consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas." A fraud risk assessment should anticipate the behavior of a potential fraud perpetrator and consider ways fraud may be perpetrated within the organization's processes. Brainstorming about fraud is an effective method to assess the agency's fraud vulnerability. This generally includes a discussion regarding incentives, pressures, and opportunities to commit fraud; risks of management override of controls; and the population of fraud risks. The establishment of criteria provides the foundation for the risk assessment, in that it sets the parameters/boundaries for the areas to be assessed.

The Global Practice Guide "Internal Auditing and Fraud" provides further guidance on the internal auditor's role in detecting, preventing, and monitoring fraud risks and addressing those risks in audits and investigations.

Assessment Tools

The preferred method of assessment should be determined by the CIA and documented. The determination of the assessment method should be based on many factors which are unique to the organization, including the number and physical location of auditable units, internal audit resources, time constraints and availability of electronic means of delivery. Methods of assessment may include but not be limited to meetings with key organization personnel and Board members, paper surveys directed toward key personnel, or complex electronic surveys directed toward a larger audience. While the method of assessment will vary based on the uniqueness of the organization, the chief audit executive should document the method to be used and justify its sufficiency under the circumstances.

Evaluation

Once assessment criteria have been obtained from each of the auditable units, the CIA has the responsibility to document and evaluate the information gathered. In doing so, it is necessary to assess the results, based on calculated risk, in order to determine which auditable units will be placed on the audit plan. Approaches to ranking audits may differ from one organization to another. Some chief audit executives may choose to assign numeric values to the results, while others may make assessments simply based upon the information gathered to determine which areas are considered high risk. However, in either scenario, the chief audit executive should maintain sufficient documentation to provide support for the auditable units identified as posing a higher risk as compared to those that do not.

GIASIV 9.1 states, "To develop an effective internal audit strategy and plan, the chief audit executive must understand the organization's governance, risk management, and control processes.

GIASIV 9.1 goes on to state, "To understand risk management and control processes, the chief audit executive must consider how the organization identifies and assesses significant risks and selects appropriate control processes. This includes understanding how the organization identifies and manages the following key risk areas:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws and/or regulations."

GIASIV 9.4 states, "The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives. The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually."

"The internal audit plan must:

- Consider the internal audit mandate and the full range of agreed-to internal audit services.
- Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
- Consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.
- Identify the necessary human, financial, and technological resources necessary to complete the plan.
- Be dynamic and updated timely in response to changes in the organization's business, risks, operations, programs, systems, controls, and organizational culture."