**SIAAB Guidance # 08**

**Internal Audit Coverage, Risk Assessment, FCIAA Compliance**

**Adopted February 13, 2018**

**** Note: 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.*

*"Chief Audit Executive (or Chief Internal Auditor) 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 the International Professional Practices Framework. The Chief Audit Executive (or Chief Internal Auditor) or others reporting to the Chief Audit Executive (or Chief Internal Auditor) will have the appropriate professional certifications and qualifications. The specific job title 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.]*

*It is accepted practice to use the terms "Audit Universe" and "Auditable Units" interchangeably as they both refer to the activities, functions and responsibilities of the agency. However, as a means of simplification in this document we refer to an "Audit Universe" as a collection of "Auditable Units" and an "Auditable Unit" as an individual component of an "Audit Universe."*

## 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. The International Standards for the Professional Practice of Internal Auditing (IIA Standards) 2010.A1 states the "internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken 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 transactional categories that a CIA should consider during their risk assessment process; they do not necessarily represent titles of individual audits. 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.

The IIA suggests as a best practice that internal audit functions develop an Audit Universe as a means of assessing the activities of the agency. The Institute of Internal Auditors' Implementation Guide 2010 states, "The audit universe includes projects and initiatives related to the organization's strategic plan, and it may be organized by business units, product or service lines, processes, programs, systems or controls." An audit universe is an inventory of the activities, functions and responsibilities of the agency that should be given consideration during the risk assessment process. The 11 SAMS categories should be given consideration as part of the risk assessment process against the activities, functions and responsibilities defined by the audit universe of the agency. The risk assessment may reveal that certain SAMS categories may not represent the highest risk areas just as certain 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 is too large to cover over a 2-year period so coverage is provided based upon 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 can 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 and board, if applicable. *(See SIAAB Guidance 04 Internal Audit Plan Development and Amendment in State of Illinois Government).*

SIAAB recommends the following framework methodology for complying with all of these requirements. We believe this methodology for documenting a 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, it is recognized 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 the following 5 core elements of the framework. The approach for demonstrating compliance with these 5 core elements is based upon the professional judgment of what the CIA deems appropriate for their 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 to assess risk within the audit universe.
5. Maintenance 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 for the determination and documentation of the audit universe for the organization. The audit universe should represent the uniqueness of the organization and should be tied to the organization's goals, as prescribed by the IIA Standards.

The IIA Implementation Guide 2010 states, "The audit universe includes projects and initiatives related to the organization's strategic plan, and it may be organized by business units, product or service lines, processes, programs, systems or controls." An audit universe provides the audit categories that are to be given consideration during the risk assessment process. The structure of the audit universe 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 is 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 an audit universe and document the selected approach.

The development of the audit universe 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 the CIA to effectively communicate the results of the risk assessment in a standardized manner.

d. Provides a mechanism for confirming whether all activities, functions and responsibilities have been captured.

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

f. Demonstrates compliance with the Standards, SIAAB By-Laws and the law that governs 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 to assess risk within the audit universe. 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, if applicable 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 their own judgment of risks after consultation with senior management and the board, if applicable. Some examples of risk categories that may be used to assess the auditable units are:

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

Factors to consider 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, such as 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.

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. 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 organizations 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.

According to IIA Standard PS-2120.A2, **the internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk**. A fraud risk assessment anticipates the behavior of a potential fraud perpetrator and considers 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 IPPF 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 the auditable units, internal audit resources, time constraints and the availability of electronic data. Methods of assessment may

include but not be limited to meetings with key organization personnel and board members, if applicable, data analytics, 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 CIA should document the method to be used, and justify its sufficiency under the circumstances.

## Evaluation

Once assessment criteria have been evaluated against the audit universe, the CIA has the responsibility to document and evaluate the information gathered. In doing so, it is necessary to assess the results, based on 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 CIAs may choose to assign numeric values to the results, while others may make professional judgment assessments based upon the information gathered to determine which areas are considered high risk. However, whatever the scenario, the CIA should maintain sufficient documentation to provide support for the auditable units identified as posing a higher risk as compared to those that do not.

**References:**

**Fiscal Control and Internal Auditing Act**

> (30 ILCS 10/2005) (From Ch. 15, par. 2005) Sec. 2005. Internal Audit Advisory Board.
>
> ***The Board shall be responsible for: (1) promulgating a uniform set of professional standards and a code of ethics (based on the standards and ethics of the Institute of Internal Auditors, the General Accounting Office, and other professional standards as applicable) to which all State internal auditors must adhere;***
>
> In response to this section of the statute, SIAAB promulgated guidance applicable to the internal auditing activities for the State, which are discussed in the section below.
>
> (30 ILCS 10/2003) (from Ch. 15, par. 2003) Sec. 2003. Internal auditing program requirements.
>
> *(a) The chief executive officer of each designated State agency shall ensure that the internal auditing program includes:*
>
> *(1) A two-year plan, identifying audits scheduled for the pending fiscal year, approved by the chief executive officer before the beginning of the fiscal year. By September 30 of each year the chief internal auditor shall submit to the chief executive officer a written report detailing how the audit plan for that year was carried out, the significant findings, and the extent to which recommended changes were implemented.*

*(2) 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.* ***The audits must include testing of:***

***(A) the obligation, expenditure, receipt, and use of public funds of the State and of funds held in trust to determine whether those activities are in accordance with applicable laws and regulations; and***

***(B) grants received or made by the designated State agency to determine that the grants are monitored, administered, and accounted for in accordance with applicable laws and regulations.***

***(3) Reviews of the design of major new electronic data processing systems and major modifications of those systems before their installation to ensure the systems provide for adequate audit trails and accountability.***

***(4) Special audits of operations, procedures, programs, electronic data processing systems, and activities as directed by the chief executive officer or by the governing board, if applicable.***

*(b) Each chief internal auditor shall have, in addition to all other powers or duties authorized by law,* ***required by professional ethics or standards****, or assigned consistent with this Act,* ***the powers necessary to carry out the duties required by this Act.***

**State Records Act**

The State Records Act (5 ILCS 160/8) states in part, "The head of each agency shall cause to be made and preserved records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency designed to furnish information to protect the legal and financial rights of the state and of persons directly affected by the agency's activities."

**SIAAB Bylaws**

The SIAAB Bylaws were developed as a result of Section 2005 of FCIAA. Per Section III - Professional Auditing Standards (2.3.1 PROFESSIONAL AUDITING STANDARDS), "***All audits performed by the internal audit staffs of State agencies shall be conducted in accordance with Standards adopted by the Board as provided by FCIAA.*** *(10 ILCS 30/2005(f)(1)).* ***These Standards*** *shall be summarized in the Quality Assurance Matrix on the Board's website and* ***shall include the****:*

- *Mandatory Guidance published by the Institute of Internal Auditors:*

- *International Standards for the Professional Practice of Internal Auditing **(Standards);***
- *Definition of Internal Auditing;*
- *Code of Ethics (See also 2.4.1);*
- *Core Principles for the Professional Practice of Internal Auditing;*

- *some implementation guidance (**practice advisories**) and supplemental guidance*
- *some (**practice guides**) published by the Institute of Internal Auditors and adopted by the Board;*
- *some government auditing standards published by the U.S. General Accounting Office and adopted by the Board; and*
- *internal audit requirements contained in the Board's Bylaws*

**IIA Standards**

The Standards (2010 – Planning) require "The chief audit executive **must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals**. To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes. **The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls."**

The Standards further state:

*2010.A1* *The internal audit activity's plan of engagements **must be based on a documented risk assessment**, undertaken at **least annually**. The input of senior management and the board must be considered in this process.*

*2010.A2* *The chief audit executive must identify and consider the expectations of senior management, the board and other stakeholders for internal audit opinions and other conclusions.*

*2010.C1* *The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.*

**Glossary of Definitions:**

**Internal Audit Plan Risk Assessment**

Risk Assessment is the identification and analysis of risks as they pertain to the functions of the agency and its ability to the achieve the organization's objectives for the purpose of developing a prioritization of audit coverage to be included in an Internal Audit Plan to determine the adequacy and the effectiveness of the agency's internal controls.

## Audit Universe or Auditable Units

IIA Implementation Guide 2010 states, “The audit universe includes projects and initiatives related to the organization’s strategic plan, and it may be organized by business units, product or service lines, processes, programs, systems or controls.”

## Record

The State Records Act (5 ILCS 160/2) " ‘Record’ or ‘records’ means all books, papers, born-digital electronic material, digitized electronic material, electronic material with a combination of digitized and born-digital material, maps, photographs, databases, or other official documentary materials, regardless of physical form or characteristics, made, produced, executed, or received by any agency in the State in pursuance of State law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its successor as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the State or of the State Government, or because of the informational data contained therein.”