SIAAB Guidance #04

Internal Audit Plan Development and Amendment in State of Illinois Government

Adopted April 14, 2015

Revised In Accordance with 2017 Standards – Effective January 1, 2017

**** 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. Illinois Administrative Procedures Act (5 ILCS 100 Section 1-25) states, "'Agency head' means an individual or group of individuals in whom the ultimate legal authority of an agency is vested by any provision of law."*

"Chief Audit Executive (or Chief Internal Auditor) is a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the Definition of Internal Auditing, the Code of Ethics, and the Standards. 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.]

SIAAB Interpretation

An acceptable audit planning process within Illinois State Government must balance the requirements of the Fiscal Control and Internal Auditing Act (FCIAA) and the International Standards for the Professional Practice of Internal Auditing (IIA Standards), published by the Institute of Internal Auditors (IIA). FCIAA 30 ILCS/10 Section 2003 (a) (1) requires each Internal Audit program to include a two year Audit Plan that is approved by the Chief Executive Officer. FCIAA includes a prescriptive approach to internal control and the development of the audit plan in that it actually prescribes certain control activities that must be given consideration. Specifically, FCIAA 30 ILCS 10/2003 (a) (2) states the auditing program must include, *"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."* It goes on to state in part that testing must cover the obligation, expenditure, receipt and use of public funds, grants, reviews of the design of major new information technology systems or major modifications to information technology systems and special audits of operations, procedures, programs and information technology systems. FCIAA 30 ILCS/10 3002 references Internal Control Certification Guidelines that were established by the Comptroller in conjunction with the Department of Central Management Services and approved by the Legislative Audit

Commission. The guidelines list the control activities utilized by management in executing their program responsibilities. They relate to the auditable units but are not generally the auditable units themselves. The auditable units are the major programs or activities of the agency. To show compliance, most audit shops track the FCIAA control areas against their auditable units. Auditing auditable units generally provides coverage to multiple FCIAA control areas. Providing Internal Audit coverage in this manner allows for compliance with FCIAA as well as the Standards. The Comptroller guidelines list the following control areas that should be given consideration:

- Agency Organization and Management;
- Administrative Support Services;
- Budgeting, Accounting and Reporting;
- Purchasing, Contracting and Leasing;
- Expenditure Control;
- Personnel and Payroll;
- Property, Equipment, and Inventories;
- Revenues and Receivables;
- Petty Cash and Local Funds;
- Grant Administration; and,
- Electronic Data Processing.

FCIAA also provides for a State Internal Audit Advisory Board (SIAAB), whose responsibilities outlined in FCIAA 30 ILCS 10/2005 (f) (1) include, *"promulgating a uniform set of professional standards and a code of ethics (based upon 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."* The standards adopted by SIAAB include those of the IIA, which requires a risk-based Internal Audit Plan.

IIA Performance Standard 2010-1 states, *"The Chief Audit Executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals."* 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. 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.

Management input should be one of the factors considered by Internal Audit during the development of the Internal Audit Plan. Meetings with various levels of management should be considered by Internal Audit as part of their risk assessment process to gain a further understanding of the risk and controls of the auditable units. Internal Auditors are the internal control and risk management experts of the agency. The Audit Planning process should be utilized as an opportunity to educate and increase management's understanding of the internal audit function and the risk assessment process, and ensure that there is a common understanding of definitions. Other helpful tools for Internal Audit to consider may be the development of a risk assessment questionnaire as a means of gathering information from the various areas. Factors that may be considered during the risk assessment process include the following:

- Any changes to the auditable units;
- New programs, initiatives or activities;
- Rapid growth or significant increases in funding or expenditures;
- Turnover of key management or key personnel;
- Reviews or audits by a Federal agency;
- Previous internal and external audit findings;
- Fiscal Control & Internal Auditing Act Annual Certification;
- Media exposure;
- Law changes;
- Administrative Rule changes;
- Policy or Procedures changes;
- Complexity of program requirements;
- Information technology that was developed or had major modifications in the last year or any that are currently in process or planned;
- Any fraudulent activity, improper conduct, blatant disregard for procedures, suspected or improper use of assets or State resources;
- Any process or programs management would like Internal Audit to review;
- Management ranking of what they consider to be the five most significant areas or processes for which they are responsible.

The Chief Internal Auditor may also utilize the available work conducted by others as a source of information. In order to place reliance on this work, the Chief Internal Auditor must gain

assurances about the accuracy of the work. The Annual FCIAA Certification listed above is the process the State has instituted for agency management to provide their assessment of the effectiveness of the existing internal control environment. The Chief Internal Auditor may elect to utilize the questionnaires or other documentation that was gathered by the agency during the preparation of the Annual Certification of Internal Controls. This annual certification of internal controls by management is required pursuant to FCIAA 30 ILCS/10 Section 3001. Additional sources of information are the system narratives created by the Auditor General's Office and the external auditors that work for them. This information is gathered as part of the external audit process in order to provide information regarding the various activities of the agency. They usually include the auditor's assessment of the effectiveness of the internal controls over each process that is discussed within the system narrative.

A related activity that is becoming more common in government is the concept of Enterprise Risk Management (ERM). Some agencies have an established ERM process with a designated Compliance Officer. IIA Practice Advisory 2010-2- Using the Risk Management Process in Internal Audit Planning states, *"An effective risk management process can assist in identifying key controls related to significant inherent risks. Enterprise Risk Management (ERM) is a term in common use. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission defines ERM as 'a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.' Implementation of controls is one common method management can use to manage risk within its risk appetite. Internal auditors audit the key controls and provide assurance on the management of significant risks."* The Chief Internal Auditor may elect to rely on the work performed as part of the ERM process if they obtain assurances as to the accuracy of the work.

The Internal Audit Plan is prepared by the Chief Internal Auditor and in accordance with FCIAA it must be approved by the Chief Executive Office of the agency. Specifically, FCIAA 30 ILCS 10/2003 (a) (1) states in part,

> *"(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."*

This is consistent with the IIA Standards which requires the Internal Audit Plan to be approved by the Board. As discussed in SIAAB Guidance #02, Board within Illinois State Government is the Chief Executive Officer or Agency Head, see notation at the beginning of this guidance. IIA Practice Advisory 2020-01 states that *"significant interim changes"* should be communicated to the Chief Executive Officer. FCIAA, Section 2002(b) requires that the Chief Internal Auditor

report directly to the Chief Executive Officer and shall have direct communications with the Chief Executive Officer and the governing board, if applicable, in the exercise of auditing activities. Accordingly, the Chief Internal Auditors should report to the Chief Executive Officer any limitations that may prevent the auditor from completing the audit plan as approved. The manner in which this is reported is left to the discretion of each internal audit activity and their Chief Executive Officer. What is considered "significant" will vary between agencies; however, the key is good, open and timely communication between the Chief Internal Auditor and the Chief Executive Officer.

Internal Audit Plans should take into account the Chief Internal Auditor's best judgment for creating an Audit Plan based upon available information and existing resources. If the Chief Internal Auditor believes there are areas which need to be addressed but can't be due to limited resources, they should convey that information to the Chief Executive Officer. IIA Standard 2020 states in part, "*The chief audit executive must also communicate the impact of resource limitations.*" In addition, throughout the year the Internal Audit shop may experience both decreases as well as increases in staff which will affect the plan. This will also impact the proficiency of the available Internal Audit resources, which may affect the timing of audits due to the availability of appropriate staff. In accordance with IIA Attribute Standard 1210, "*Internal Auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities.*" In addition, the work of Internal Audit is impacted by the number of issues that are found during the course of an audit. The more issues that are identified, the longer the audit takes to complete. It is sometimes difficult to estimate this unknown, which in some agencies may be significant. This can have a significant impact upon the Internal Audit Plan. It is also important that the Chief Internal Auditor conveys the progress towards achieving the Internal Audit Plan and changes to the plan during periodic meetings with the Chief Executive Officer. The Internal Audit Plan should be a flexible document that may require change as the year progresses. This is because priorities and events change over time, in fact situations often change as soon as they are put into writing. A new program, department realignment or reorganization may occur, unexpected occurrences may change management's needs, and some engagements may need to be shifted to a higher priority status because of increased importance by the Chief Executive Officer or Senior Management. IIA Practice Advisory 2130-1 "Assessing the Adequacy of Control Processes" states, "*The CAE (Chief Audit Executive) develops a proposed internal audit plan to obtain sufficient evidence to evaluate the effectiveness of the control processes. The plan includes audit engagements and/or other procedures to obtain sufficient, appropriate audit evidence about all major operating units and business functions to be assessed, as well as a review of the major control processes operating across the organization. The plan should be flexible so that adjustments may be made during the year as a result of changes in management strategies, external conditions, major risk areas, or revised expectations about achieving the organization's objectives.* "

The Internal Audit Plan should be designed to allow the Chief Internal Auditor the flexibility to manage and apply the Internal Audit resources throughout the year and schedule and prioritize

those audits approved in the plan. This allows the Chief Internal Auditor to perform their day to day responsibilities in executing the Audit Plan. However, significant changes should be brought to the attention of the Chief Executive Officer and Board, if applicable. The Chief Internal Auditor should also report to the Chief Executive Officer any limitations that may prevent the auditor from completing the audit plan as approved. How these are communicated should be through a process agreed to by the Chief Internal Auditor and the Chief Executive Officer. Significant changes or limitations may be addressed during the periodic meetings held between the Chief Internal Auditor and the Chief Executive Officer. The documentation of the meeting should reflect the significant changes or limitations that were discussed. An Internal Audit Shop may elect to prepare actual amended plans or written amendments to the plan. An Internal Audit shop may elect to communicate those changes by e-mail to the Chief Executive Officer. We believe any method that communicates the understanding of the significant change or limitation is an acceptable method as long as that documentation is maintained by Internal Audit.

Fiscal Control and Internal Auditing Act

FCIAA 30 ILCS/10 Section 2002 (b) of FCIAA states in part, "The chief internal auditor shall report directly to the chief executive officer and shall have direct communications with the chief executive officer and the governing board, if applicable, in the exercise of auditing activities."

FCIAA 30 ILCS/10 Section 2003(a) states in part, "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."

FCIAA 30 ILCS/10 Section 2003(a) states in part, "The chief executive officer of each designated State agency shall ensure that the internal auditing program includes:

(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."

FCIAA 30 ILCS/10 Section 2005 (f) (1), "The Board (SIAAB) shall be responsible for: "promulgating a uniform set of professional standards and a code of ethics based upon 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."

FCIAA 30 ILCS/10 Section 3001

"Internal controls required. All State agencies shall establish and maintain a system, or systems, of internal fiscal and administrative controls, which shall provide assurance that:

(1) resources are utilized efficiently, effectively, and in compliance with applicable law;
(2) obligations and costs are in compliance with applicable law;
(3) funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use, and misappropriation;
(4) revenues, expenditures, and transfers of assets, resources, or funds applicable to operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the State's resources; and
(5) funds held outside the State Treasury are managed, used, and obtained in strict accordance with the terms of their enabling authorities and that no unauthorized funds exist."

FCIAA 30 ILCS/10 Section 3002

"Certification guidelines for chief executive officers.

(a) By the next March 1 after the date this Act takes effect, the Comptroller, in consultation with the Director of Central Management Services, shall establish guidelines for:
(1) the evaluation by State agencies of their systems of internal fiscal and administrative controls to determine whether the systems comply with the requirements of Section 3001; and

(2) the certification by chief executive officers required by Section 3003.
(b) The guidelines must be approved by the Legislative Audit Commission and may be modified, as needed, with the Commission's approval."

IIA Standards

1210- Proficiency

"Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities."

"Proficiency is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities. It encompasses consideration of current activities, trends, and emerging issues, to enable relevant advice and recommendations. Internal auditors are encouraged to demonstrate their proficiency

by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by the Institute of Internal Auditors and other appropriate professional organizations."

2010 – Planning

"The chief audit executive must establish a risk-based plan 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. "

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."

2020 – Communication and Approval

"The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations."

2120 – Risk Management

2120. A1 – "The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts."

2130 – Control

"The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement."

IIA Interpretation Practice Advisory

Practice Advisory 2010-1

"The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. 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.

1. In developing the internal audit activity's audit plan, many chief audit executives (CAEs) find it useful to first develop or update the audit universe. The audit universe is a list of all the possible audits that could be performed. The CAE may obtain input on the audit universe from senior management and the board.

2. The audit universe can include components from the organization's strategic plan. By incorporating components of the organization's strategic plan, the audit universe will consider and reflect the overall business' objectives. Strategic plans also likely reflect the organization's attitude toward risk and the degree of difficulty to achieving planned objectives. The audit universe will normally be influenced by the results of the risk management process. The organization's strategic plan considers the environment in which the organization operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

3. The CAE prepares the internal audit activity's audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization. Key audit objectives are usually to provide senior management and the board with assurance and information to help them accomplish the organization's objectives, including an assessment of the effectiveness of management's risk management activities.

4. The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the organization. In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the organization's business, operations, programs, systems, and controls.

5. Audit work schedules are based on, among other factors, an assessment of risk and exposures. Prioritizing is needed to make decisions for applying resources. A variety of risk models exist to assist the CAE. Most risk models use risk factors such as impact, likelihood, materiality, asset liquidity, management competence, quality of and adherence to internal controls, degree of

change or stability, timing and results of last audit engagement, complexity, and employee and government relations."

Practice Advisory 2010-2 Using the Risk Management Process in Internal Audit Planning

"The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. 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.

1. Risk management is a critical part of providing sound governance that touches all the organization's activities. Many organizations are moving to adopt consistent and holistic risk management approaches that should, ideally, be fully integrated into the management of the organization. It applies at all levels — enterprise, function, and business unit — of the organization. Management typically uses a risk management framework to conduct the assessment and document the assessment results.

2. An effective risk management process can assist in identifying key controls related to significant inherent risks. Enterprise risk management (ERM) is a term in common use. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission defines ERM as "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Implementation of controls is one common method management can use to manage risk within its risk appetite. Internal auditors audit the key controls and provide assurance on the management of significant risks."

Practice Advisory 2020-1 Communication and Approval

"1. The chief audit executive should submit annually to senior management and the board for review and approval a summary of the internal audit plan, work schedule, staffing plan, and financial budget. This summary will inform senior management and the board of the scope of internal audit work and of any limitations placed on that scope. 2. The approved engagement work schedule, staffing plan, and financial budget, along with significant interim changes, are to contain sufficient information to enable senior management and the board to ascertain whether the internal audit activity's objectives and plans support those of the organization and the board and are consistent with the audit charter."

Practice Advisory 2130-1 Control Processes

"4. The CAE develops a proposed internal audit plan to obtain sufficient evidence to evaluate the effectiveness of the control processes. The plan includes audit engagements and/or other procedures to obtain sufficient, appropriate audit evidence about all major operating units and business functions to be assessed, as well as a review of the major control processes operating

across the organization. The plan should be flexible so that adjustments may be made during the year as a result of changes in management strategies, external conditions, major risk areas, or revised expectations about achieving the organization's objectives."

Practice Advisory 2120-3 Internal Audit Coverage of Risks to Achieving Strategic Objectives

"Executive management is responsible for identifying and managing risk in pursuit of the organization's strategic objectives. It is the board's responsibility to ensure that all strategic risks are identified, understood, and managed to an acceptable level within risk tolerance ranges. Internal audit should have an understanding of the organization's strategy, how it is executed, the associated risks, and how these risks are being managed.

2. To enable internal audit to focus on the critical risks to the organization, the organization's strategy should be a foundational element when developing a risk-based audit plan. This will align internal audit with the organization's strategic priorities and help ensure its resources are allocated to the areas of significant importance.

3. When developing the audit plan, internal audit should leverage the work of management and other assurance functions to help identify the risks that present the most significant threats and opportunities to the achievement of an organization's strategic objectives.

4. Strategic threats and opportunities will drive management's creation and prioritization of the organization's short-term and long-term strategic initiatives or the organization's most significant investments to deliver value to its stakeholders. "

IIA Glossary of Definitions:

- ***Board-*** The highest level of governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

- ***Charter*** - The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

- ***Chief Audit Executive (Chief Internal Auditor)*** – Chief audit executive 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 others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The

specific job title and/or responsibilities of the chief audit executive may vary across organizations.

- ***Code of Ethics*** - The Code of Ethics of The Institute of Internal Auditors (IIA) are Principles relevant to the profession and practice of internal auditing , and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

- ***Standard*** **-** A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.