SIAAB Guidance #10

System Development Reviews Risk Assessment and Scoring

Adopted January 9, 2024

**** 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." According to the Institute of Internal Auditors (IIA) Standards Glossary, 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 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 and/or responsibilities of the Chief Audit Executive may vary across organizations." In Illinois, the Fiscal Control and Internal Auditing Act (30 ILCS 10) refers to the position of Chief Audit Executive as Chief Internal Auditor. The terms Chief Audit Executive and Chief Internal Auditor are used interchangeably.*

<u>Key Statutory References</u>

<u>Fiscal Control and Internal Auditing Act</u>

<u>(30 ILCS 10/2003) (from Ch. 15, par. 2003) Sec. 2003. Internal auditing program requirements.</u>

(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.

<u>Key Related Auditing Standards</u>

1210 – Proficiency

- ***1210.A3*** *– Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.*

1220 - Due Professional Care

- **1220.A2** – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

2110 – Governance

- **2110.A2** – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

Other Suggested Resources:

- IIA Global Technology Audit Guide (GTAG) – Auditing Business Applications
- National Institute for Standards and Technology (NIST)
- Information Systems Audit and Control Association (ISACA)

SIAAB Interpretation

Chief Internal Auditors (CIAs) must strike a balance between adhering to internal audit and other requirements and the best use of their limited resources to provide appropriate internal audit coverage in an effective and efficient manner. This includes ensuring that appropriate internal controls exist and are functioning within the various information technology systems utilized by the Agency. Therefore, CIAs should implement written procedures that address a process they will follow for making a determination of whether a new information technology system or a change to an existing system should be reviewed by Internal Audit. FCIAA requires a system development review to be conducted of the implementation of all major systems, as well as any major modifications to major system. In addition, a CIA may elect to conduct limited or other reviews of system changes that are not major or major modifications, as resources are available, in order to ensure a sufficient understanding of the various systems utilized by their agency.

In order to assist the CIA with making their determination as to whether a system is major or not, SIAAB has adopted this Guidance and an optional assessment tool, which can be used to assist the CIA in making their decision. It should be noted this is merely being provided as a tool to assist the CIA in deciding whether a particular project rises to the level of necessitating a system development review. 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. In the end, the final decision should be based upon the CIA's professional judgment and agency knowledge in making a determination what, if any, review may be required. This tool is not intended to replace the CIA's professional judgment. The CIA knows the agency the best and there are other factors unique to the agency that are not contained within this scoring mechanism. The CIA is also required to strike a balance of work against available resources. SIAAB recognizes 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 this requirement.

Assessment Tool (See Related Tool)

The optional Assessment Tool was developed which can be used to provide a baseline for the CIA to make their determination as to whether a system is major or not. The tool develops a score that arrives at a recommended level of coverage for a particular system development project. This is an initial level determination that then must be reviewed by the CIA to make a final determination. The CIA should then utilize their professional judgement and knowledge of the Agency to arrive at the appropriate, if any, level of review that is required for a particular project.

The scoring sheet is divided into Section A and Section B. Section A includes areas of higher significance and therefore, if any item in this section scores a 5, the project should be brought to the attention of the CIA to determine if at least a Level 2 Limited System Development Review should be performed regardless of the score in Section B, although the scoring of Section B may impact the decision of the CIA. The ultimate decision is still at the discretion of the CIA. A Level 2 Limited System Development Review is not statutorily required by FCIAA.

A Level 1 project designation assigned by the CIA means they have designated the project as a major system development or major modification to an existing system, as referred to in FCIAA. Level 1 projects receive a review that encompasses the entire system development process. A Level 2 is a project designation assigned by the Chief Internal Auditor that means they have determined although it is not a major system development or major modification to an existing system, it can be a significant enough project to have some work performed. A Level 2 project is called a Limited System Development Review. A Level 3 designation is all other projects not designated as a Level 1 or 2. Generally, no specific work is planned for these projects, and they are just monitored for informational purposes. However, the CIA could decide at their discretion to assign work on a Level 3 project if they deem it necessary.

According to the Institute of Internal Auditors (IIA), “As trusted advisors of the organization, internal auditors are expected to have sufficient knowledge of key information technology risks and controls.” The CIA should keep that concept in mind in making their determination. That determination should then be documented in accordance with the CIA’s written procedures.