SIAAB Guidance #06

Pre-Implementation Reviews for non-IT Auditors in the State of Illinois

Adopted December 8, 2015

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

**** Note: Pre-installation review is the term used in the statute; however, pre-implementation review is the current industry term, which will be used in this document.*

Definitions as utilized in this document:

1. *"Agency" 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.*
2. *"Chief Executive Officer" or "Agency Head" 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. 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."*
3. *"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 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.]*

SIAAB Interpretation

The Fiscal Control and Internal Auditing Act (FCIAA) [30 ILCS 10/2003(a)(3)] requires *"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*." This Guidance offers an optional methodology with examples on how to perform a pre-implementation review if the internal auditing shop does not have a process to perform pre-implementation reviews of systems or major modifications of a system and/or does not have an information technology (IT) auditor.

According to Auditing Standards 1210.A3 (IT Proficiency), *"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."*

Ideally, pre-implementation reviews should be assigned to technically proficient IT auditors who conduct testing at a level appropriate for each circumstance. However, the FCIAA pre-implementation review requirement applies to all audit functions, including functions that do not include an IT auditor. Therefore, if an IT auditor is not available, there is still a requirement to perform pre-implementation reviews. This guidance will assist auditors and audit shops that lack specific training in conducting information technology audits.

Auditors may also refer to the IIA guidance (available to IIA members on their website www.theiia.org/technology) from the Global Technology Audit Guide Practice Guides. These guides are intended to provide non-IT auditors with guidance on conducting audits on applications and determining which aspects can be tested by non-IT auditors or when an IT auditor must be engaged. Specific guidance that may be useful are: GTAG 8 Auditing Application Controls, GTAG 1 IT Risks and Controls, and GTAG 12 Auditing IT Projects. Additionally, COBIT, IRS Publication 1075, and the NIST Computer Security Division are also good resources depending on the information in the system that you are reviewing.

Tracking System Development Projects

In order to perform pre-implementation reviews, Internal Audit functions must obtain a listing of new development or modification projects on a periodic basis, track them, and review them to determine which projects are major (as an example see the Risk Assessment Worksheet). Internal Audit functions that have successfully established processes to review projects either review significant projects with development management on a regular basis, i.e. monthly, or have a continuous process in place.

The determination whether a new system or modification is major may be based on one or more factors which may include, but are not limited to:

- How important is the system or modification as it relates to the business functions/operations of the user?
- Is the proposed system or modification mandated by changes in legislation or the agency head?
- Does the proposed system or modification involve complex calculations or edits, multiple transactions types, the addition of a significant number of data fields?
- Is the software development technology relatively new and untested by the project team at the agency?
- Is the system or modification migrating to a new/different infrastructure platform?
- Will this system or modification be a vendor supplied solution?
- Will the system or modification be interdependent or interface with other systems?
- Does the system or modification encompass confidential information?
- How many bureaus, offices, or agencies will the system or modification affect?
- Will this system have an impact on fiscal reporting for the agency?
- Does this project address a previously cited deficiency in internal control?
- Do processes, policies, or workflows for the system or modification exist?

In the Risk Assessment Worksheet example, there are three different levels of system developments. Level 1 is high, which is considered major and should have all applicable steps completed that would normally be done for a pre-implementation review. Level 2 is moderate, which can have a pre-implementation review completed but it does not meet the mandatory FCIAA definition of "major" and is therefore not a required pre-implementation review. In addition, it is usually a limited scope pre-implementation review targeted towards the higher risks of the development project. Level 3 is low risk, which does not require a pre-implementation review.

Note: Consolidated agencies should submit governance documents to the Department of Central Management Services (CMS) Bureau of Communication and Computer Services (BCCS) Governance for all major developments and modifications. These documents, which should be maintained by your agency, may aid in helping make your determination. See bccs.illinois.gov.

Review Program

This guidance will walk through an example of a Level 1 pre-implementation review including elements of projects hosted (the equipment needed to run the application reside) internally at CMS BCCS (internally hosted for non-consolidated agencies) or hosted by a 3rd party, which would generally be all-inclusive of the steps that would be needed for a new development or modification (as an example see both Pre-Implementation Review (Hosted Solution) and Pre-Implementation Review). For the purpose of this guidance, hosted is considered hardware equipment that is setup outside of the State of Illinois. The requirements mentioned can be different based on the underlying information in the system. For instance, if there is federal taxpayer information it would be governed by Publication 1075 from the IRS and there is a warning banner requirement specifically for the IRS. A level 2 pre-implementation review would typically focus on a portion/s of the Level 1 review.

Planning and Organization

All development projects need a team that includes the proper stakeholders. As such, there should be a project team/resource plan. Internal Audit would verify that the appropriate business owner, information technology (IT) personnel, and project manager is involved. If there are 3rd party vendors, they should be able give you a listing that shows the key personnel on their project team. There should be a formal request to begin the project, which would either be a Change Request Form or Governance documentation. There should be documentation of key meetings where the business owner and IT personnel approve major changes in the project. Project plans are one of the most important elements of the project. Lack of a project plan in a system development project is a primary reason projects face major delays and issues. If there are contracts for the system development either for software or hosting facilities, obtain the contract. Verify that the statement of work includes system and business requirements.

Acquisition and Implementation

All developments need system and business requirements. Internal Audit should review them for adequacy and develop tests to ensure they are met. New developments should have role based access. Additionally, the ability to grant access and issue passwords should be limited to a few employees.

If access to a system is controlled by active directory on the Illinois.gov domain most of the requirements in this paragraph have been completed. Passwords should be either masked or blank when entered. Additionally, for systems that have confidential data, passwords should be complex to enter the system. This means passwords should contain one uppercase, one lowercase, one number, one special character and be at least eight characters in length. Prohibit password reuse for 12 generations. Internal Audit should review the password requirements and access rights to reasonableness.

Systems should have specific application logs. Internal Audit should determine what logs are available, ask which logs are enabled, and review for reasonableness. As an example, if there is an error log that has been disabled, you would want to inquire as to why this has been disabled.

Developments should have an adequate test plan. Internal Audit should review the tests anticipated for reasonableness and verify that the plan has been completed and that errors noted in testing have been resolved. Developments with a web component should be scanned by the CMS BCCS Technical Safeguards Unit. Internal Audit should review and verify that risks have been remediated to an acceptable level. Additionally, all projects that are going to multiple users on the system simultaneously should have a load/stress performed. This is one of the main reasons application go-lives fail in the 1st few days. Internal Audit should ask the business management how many users they expect to have logging on the system at the same time.

Systems will need to have Technical Requirements determined up front. This is one of the required governance documents. Technical Requirements include anticipated storage space of the new system. Internal Audit should verify that enough space is available. Capacity planning should be considered as well. For hosted environments, internal audit would want to see a diagram with the equipment (could be virtual) that will house State of Illinois information. Additionally, Internal Audit should inquire about system interfaces if any, which should be included in the Technical Requirements document. Internal Audit should verify if there is an interface rollout plan and for external facing interfaces verify that a virtual private network (VPN) with at least 256 bit encryption is used.

Developments modifying existing systems or upgrade to a new system can have parallel runs of the old system and new system. If information is being entered into both systems, you would want to see a comparison of run-to-run totals. Additionally, these modifications may require a conversion plan, which requires a reconciliation of the legacy data to the data converted to the new system. If part of the information is not being converted into the new system, Internal Audit should ask if the legacy data is being archived.

Delivery and Support

System developments are either deployed all at once, functionality is added with scheduled deployments, or it is deployed agency by agency. As such there should either be an implementation/deployment plan or there should be one incorporated into the project plan. Additionally, system developments that are relying on BCCS for their disaster recovery should be entered into the Enterprise Architecture Taxonomy Database Structure. This is the system that BCCS would use to recover the State of Illinois information systems should a disaster occur (if the agency does not use BCCS there should be some inventory of critical systems with vital information needed to recover those systems). Additionally, Internal Audit should verify that the coding practices of the developers on the project are sufficient. There should be multiple environments: development, test, production, etc. There should be a code migration process that limits who can put code into production. Additionally, there should be emergency code change procedures and peer reviews of code completed. Also, if this is a new system there should be a training manual or if it is an upgrade there should be revisions to the old manual if there are significant changes.

Monitoring

System development projects all have constraints, weaknesses, and risk. As such, every system development project needs a risk assessment performed that documents concerns for the project that should be completed by the project manager in conjunction with the business owner and IT personnel. Additionally, all systems will require some minor changes after deployment; Internal Audit should inquire as to what monitoring will be in place after the development ends.

Internal Controls of the 3rd Party (Hosted developments)

All hosted projects need to obtain a Service Organizational Control (SOC) 2 type 2 report for the entity that hosts State of Illinois data if that data is confidential. The SOC report will need to be reviewed by management during the procurement process prior to signing a contract.

When conducting the pre-implementation review, Internal Audit would need to know who will be reviewing the SOC report, both during the procurement process and annually thereafter. Obtain and document the SOC checklist (as an example see the SOC2 Annual/Initial Audit Checklist) completed by management, the SOC reports and all applicable documents such as a bridge letter. SOC checklists are usually signed off on by the business owner and a technical resource. Internal Audit may complete the SOC checklist as well to verify that there are no significant deficiencies in the SOC report and review the SOC checklist that has been completed by management for potential weaknesses. Additionally, if there are weaknesses identified, consider performing a site visit to the hosting site.

Fiscal Control and Internal Auditing Act

"The chief executive officer of each designated State agency shall ensure that the internal auditing program includes:

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. [30 ILCS 10/2003(a)]