Insert Agency Letter Head

TABLE OF CONTENTS

[INTRODUCTION 1](#_Toc238266618)

[SCOPE, OBJECTIVES AND METHODOLOGY 2](#_Toc238266619)

[REVIEW TESTS 4](#_Toc238266620)

# INTRODUCTION/BACKGROUND

The Division/Office of Internal Audit (D/OIA) will conduct a pre-implementation review of [insert project name]. This review was selected by the D/OIA for review because it meets the definition of a major system development.  This review will be conducted as part of the Internal Audit's Fiscal Year 20[xx] audit plan.

***[Instructions for completing this section. You must delete these instructions before generating the audit program/report.]***

         List a brief description of the area reviewed which identifies the agency, organizational units and activities reviewed and any other relevant explanatory statistical or financial information, which would provide the reader with at least a basic understanding of the area and the process audited.  Summarize the system narrative or flowchart of the process/program.

         State the date of the last internal/external review.  Describe the previous internal/external review findings or affirmatively state none were previously cited.  Note their current status of resolution or implementation of previous recommendations.

# SCOPE AND OBJECTIVES

[Keep one of the following two paragraphs.]

This review will be conducted as part of the Internal Audit’s two-year audit plan required by the Fiscal Control and Internal Auditing Act (30 ILCS 10/2003) and in accordance with the International Standards for the Professional Practice of Internal Auditing promulgated by the Institute of Internal Auditors. FCIAA also 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."  Thus this review was also conducted in accordance with the Control Objectives and Audit Guidelines for Information and Related Technology (COBIT), which was developed as generally applicable and accepted standards for Information Technology (IT) Control.

[or]

This review was conducted at the request of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_and will be completed in accordance with the International Standards for the Professional Practice of Internal Auditing promulgated by the Institute of Internal Auditors.  Special review requests were included as part of the Internal Audit’s two-year plan, which is required by the Fiscal Control and Internal Auditing Act (30 ILCS 10/2003). FCIAA also 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."  Thus this review was also conducted in accordance with the Control Objectives and Audit Guidelines for Information and Related Technology (COBIT), which was developed as generally applicable and accepted standards for Information Technology (IT) Control.

[Keep the following paragraphs. Only update fields surrounded by [ ] before generating the review program/report.]

The review includes tests and procedures considered necessary for the purpose of determining with reasonable, but not absolute, assurance whether the agency established proper controls and complied with applicable laws, rules, regulations, grant or contractual agreement and policy.

The scope of this review is to conduct a systems development review of the [Project Name] to determine if this system is being appropriately implemented.  The review includes procedures and tests considered necessary for the purpose of determining with reasonable, but not absolute, assurance whether the system will function as intended and that controls are in place to ensure that the system includes; adequate audit trails and accountability, data confidentiality, and system integrity.  The review period began on [insert month, date, and year] and is planned to be completed on [insert month, date, and year].

Specifically, the review objectives were to:

|  |  |
| --- | --- |
| Objective 1 | Determine whether business requirements for the system are clearly defined. |
| Objective 2 | Determine whether the system has been designed with an adequate level of built in controls. |
| Objective 3 | Determine whether the system will be implemented in accordance with established policies and procedures. |
| Objective 4 | Determine whether Business Units and IT are aware of controls and requirements of the system. |
| Objective 5 | Determine whether managerial review of IT Internal Controls exists. |

# REVIEW TESTS

**A: Planning and Organization**

|  |  |
| --- | --- |
| Step A.1 | Verify that the appropriate level of management is involved in the project and determine who is on the Project Team/Resource Plan. (Objective 5) |
| Step A.2 | **Obtain the formal project request (Change Request Information Form) and/or project charter. Verify that the request/charter has all relevant information including: summary, description, requestor and supervisor. Verify that the requestor and supervisor are not the same person and the requestor is the Business or Process owner or a designee. If a charter was completed, verify that the project has been approved by the BCCS Governance process or a waiver has been issued by the State Chief Information Officer. (Objective 5)** |
| Step A.3 | **Obtain documentation of key meetings. Verify that the documentation generally notes that user personnel are involved in meetings and that appropriate user management or a designee approves major changes to the initial plan and approves go-live. (Objectives 4 and 5)** |
| Step A.4 | Obtain the Project Plan/Project Schedule. Verify that it contains critical phases including: testing phases, user training (if applicable), conversion (if applicable), and rollout plan. For major tasks or milestones verify that it specifies start and end dates or planned budgeted hours and resource assignments. (Objective 5) |
| Step A.5 | If applicable (vendor software) obtain and inspect a copy of the contract. Verify that it was executed by both parties and the statement of work was defined. Verify that the agreement has adequate provisions (i.e. for training, user guides, and end user documentation, technical support, issue/error troubleshooting, interface operations, server maintenance, user administration, etc.). Verify that the contract contains provisions stating either that the State owns the source code, or there is a source code escrow agreement in place if the vendor ceases to exist. Verify that the state maintains ownership of the data. Verify that there are an appropriate number of licenses given the expected number of users. |

**B: Acquisition and Implementation**

|  |  |
| --- | --- |
| Step B.1 | Obtain System and Business Requirements and verify documented system/business requirements are adequate. If applicable to the development (vendor solution) verify that the system and business requirements are included in the contract or attachments. (Objectives 1, 3, and 4) |
| Step B.2 | Develop application control (completeness, validity, identification, authentication, authorization, and input) tests, to ensure complete and accurate processing of data, from input through output.  Document tests and results.  Inputs can include: validity of data formats (i.e. dates, zip codes, etc.), completeness checks, (i.e. required fields), and range checks (i.e. birthdates must occur in the past etc.)  Outputs can include: Batch job completeness (i.e. balancing reports are available to employees), date/time checks (i.e. making sure dates are current on reports etc.) (Objective 2) |
| Step B.3 | Obtain a listing of users and the role based access that they are allowed. Verify that the access is appropriate for those users who are granted access. (Objective 2) |
| Step B.4 | Determine who has the ability to grant access and/or issue passwords. Verify that this employee works in the user department and that all access granted is documented. (Objective 4) |
| Step B.5 | Determine how passwords are displayed when typed or displayed on the screen. Verify that they are masked or are blank. (Objective 2) |
| Step B.6 | Determine what types of application logs are available for the application including both business and security logs. Determine which of these logs will be turned on. Verify that the business owner agrees with the application logs that are enabled. Verify that there is an individual who is assigned to monitor these logs on a periodic basis. (Objective 2) |
| Step B.7 | Obtain the Test Plan. Verify that the plan selects appropriate tests i.e.; Unit Test, Peer Review, Integration Test, Regression Test, Functionality Test, Usability Test, Interface Test, Compatibility Test, Security Test, HTML Validation Test, Load Test, System Test, Accessibility Test, Vulnerability Test, and User Acceptance Testing. Review the results to determine if testing was adequate. Verify that there is a log of bugs based on testing, that there are resolutions to the bugs identified, or business owner acceptance of the bug prior to go-live. (Objective 4) |
| Step B.8 | Obtain the Technical Requirements as required in Enterprise Program Management (EPM), and review to see if the storage requirements are adequate. Verify with Infrastructure Services Division, that there is enough space to accommodate the project and that it will be hosted on one of the virtual servers (Objective 2) |
| Step B.9 | If applicable, determine if the application password parameters are consistent with industry best practices (minimum length, expiration duration, complexity, number of failed login attempts, history of previous passwords) and are appropriate. (Objective 2) |
| Step B.10 | If applicable to the development, obtain all capacity planning documentation and review to determine whether all required hardware components have been identified; including computer (PCs, server, mid-range, etc.), printer, modems, telecom lines, and other equipment; and are in place prior to implementation and determine if there was a written plan/schedule for the hardware installation and review it for reasonableness. (Objective 2) |
| Step B.11 | If applicable to the development, interview project staff to identify the application interfaces with other systems (should be included in the Technical Requirements).  Determine whether interface roll-out plans have been properly documented. Interface roll-out plans should address: security of the interface (VPN with at least 256 bit encryption for external interfaces), automation of manual processes, elimination of redundant data entry, enhanced controls over data validation and accuracy, and business and system owner approval of the plan. (Objective 4) |
| Step B.12 | If applicable for the development, obtain volume/stress testing prior to deployment and review to see if the application can handle the anticipated amount of users. (Objective 2) |
| Step B.13 | If applicable for the development, obtain the conversion plan. Verify that the conversion plan was approved by user management and was adequate including a reconciliation of legacy data transferred. Conversion plan should consider either access to a legacy system in order to get old data or archiving the data from the legacy system. (Objectives 4 and 5) |
| Step B.14 | If applicable for the development, determine if a parallel run was used prior to the actual switchover to a new system. Verify that run-to-run totals were produced during the parallel runs and that any discrepancies were investigated. (Objective 2) |
| Step B.15 | If applicable (web based applications) verify that the system/application has had vulnerability testing/preproduction scans performed by the DoIT Technical Safeguards Unit. (Objective 2) |

**C: Delivery and Support**

|  |  |
| --- | --- |
| Step C.1 | Obtain Implementation Plan/look at Implementation Plan specified in the Project Plan and verify that the schedule/plan includes details of the project for its various stages/phases. (Objective 4) |
| Step C.2 | Inquire with project staff and determine if disaster recovery procedures/back-up recovery plan has been entered into the EPM business application. Look specifically to verify that the System Owner and Business Owner are identified and the DR Category, RTO Stage, and Disaster Recovery Justification have been provided. For major modifications, determine if the Enterprise Architecture Taxonomy Database Structure should have been updated based on the modifications made and verify that the modifications have occurred. Additionally, verify that a disaster recovery plan exists. (Objective 2) |
| Step C.3 | Interview project staff and determine whether the development, testing, and production environments have been distinctively defined. (Objective 2) |
| Step C.4 | Inquire about the customized code migration process and determine whether:   1. there is proper version control, 2. access to migration tool is limited, and 3. documentation of customizations is maintained. (Objective 2) |
| Step C.5 | Interview project staff and determine whether controls are in place to prevent programmers from normal access to production code and data. (Objective 2) |
| Step C.6 | Interview project staff and determine the plan in place to detect unauthorized access to Production program libraries is adequate, by completing the following steps:   1. Identify what is needed to gain access to Production  program libraries. (Who has access to the Production   libraries)   1. Identify what security monitoring exists on production program libraries. (Objective 2) |
| Step C.7 | Inquire about emergency program changes and verify whether procedures and controls have been established. (Objective 2) |
| Step C.8 | Interview project staff and determine whether quality checks/peer reviews are performed on modified software to ensure standards are followed, and documentation and testing are complete before moving the changes into production.  (Objective 5) |
| Step C.9 | If applicable to the development, obtain the Training Plan and Materials/ User Manual and determine if they appear sufficient for user and IT support upon implementation of the system. Training topics should include data entry, report generation, user operations; and if applicable; backups, management reporting, and disaster recovery. Verify that the appropriate levels of staff were trained prior to go-live. (Objective 4) |
| Step C.10 | If applicable (mainframe applications), verify that at least 60 days of backups are occurring. |

**D: Monitoring**

|  |  |
| --- | --- |
| Step D.1 | Obtain and review the Impact Assessment/Risk Assessment and assess whether Internal Controls appear adequate. (Objective 5) |
| Step D.2 | Interview project staff to determine whether monitoring controls exists to provide reliable and useful feedback in a timely manner after implementation of the system. (Objective 5) |