

Review and Assessment of Internal Access Controls for Human Resources Information Systems

The Inter-American Development Bank Senior Management team, Auditor General and the Budget and Financial Policies Committee, initiated the Review and Assessment of Internal Access Controls for Human Resources Information Systems. The purpose was to conduct an evaluation of the scope of activities and requirements for the Bank to meet current best practices for internal controls. These best practices call for the adoption and implementation of a formal control framework to enable Management to issue an annual report regarding the effectiveness of internal controls over financial reporting.

Internal control is defined as a process effected by an organization's board of directors, management, and other personnel that drives business success in three categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The review supported the Bank's efforts to meet current best practices for internal control, and established a roles and responsibility center with the following entities:

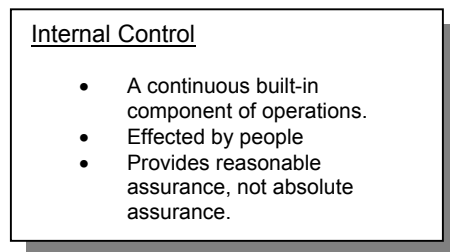
- *Management* (President and Vice-President for Planning and Administration and Finance Manager directly responsible for internal controls;
- *Risk and Control Unit* (RCU) will (i) the redesign of business units control reports; (ii) conduct risk and control assessment meetings with the business unit; (iii) compiled and evaluated information for management's report on the effectiveness of internal controls over financial reporting; (iv) oversee the unit level representation letter process; (v) manage and maintain the internal control database; and (vi) support the external auditors in conducting their audit of management's report on internal controls;
- *Establish Business Units* as the owners of the processes and controls. A unit level representation letter process will be in place to report about the effectiveness of the internal controls under its responsibility;
- *External Auditors* will attest on Management's report and will provide technical advisory consulting regarding the auditing of internal controls;
- *Audit Committee* will assist the Board in overseeing the Bank's financial reporting, risk management and control process, the internal and external audit functions and the Bank's activities in promoting institutional integrity with regards to matters involving fraud or corruption.

The initial objective of the project was to address the issues of (a) Segregation of duties and responsibilities and (b) Policies and procedures.

Internal Control

Internal control is a major part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals and objectives and supports performance-based management. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. Internal control is synonymous with management control, helps program managers achieve results through effective management of the Bank's resources.

Internal control is not one event, but a series of actions and activities that occur throughout an entity's operations and on an ongoing basis. Internal control should be recognized as an integral part of each system that management uses to regulate and guide its operations rather than as a separate system within an agency. Internal control is management control that is built into the entity as a part of its infrastructure to help managers run the entity and achieve their aims on an ongoing basis.



Internal Control Standards

There are currently five standards for Internal Control

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

These standards define the minimum level of quality acceptable for internal control and provide the basis against which internal control is to be evaluated.

In a *control environment*, the Bank's management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and effective management.

Internal control should provide for an *assessment of the risks* the Bank is exposed to from internal and external sources. A precondition to *risk assessment* is the establishment of clear objectives. Risk assessment is the process of analyzing and interpreting risk, is comprised of three basic activities: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results. Risk assessment is associated with achieving internal control objectives and provides the basis for determining how risks should be managed.

Control activities are the policies, procedures, techniques, and mechanisms that enforce management directives. To control the risks of operating an information system, HRD managers and users need to

know the vulnerabilities of the system and the threats that may exploit them. Control activities occur at all levels of functions operations. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, maintenance of security, and the creation and of maintenance of related records, which provide evidence of execution and appropriate documentation.

To address *information and communications*, information should be recorded and communicated to HRD management and other staff within the department within a timeframe to support efforts for internal control. HRD senior staff needs both operational and financial data to determine whether they are meeting the Bank's strategic and annual performance plans. For example, operating information is required for the development of financial reports. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and on a day-to-day basis to make operating decisions, monitor performance, and allocate resources. Pertinent information should be identified captured, and distributed in a form and time frame that permits people to perform their duties efficiently. In addition to internal communications, management should ensure there are adequate means of communicating with and obtaining information from external stakeholders that may have significant impact on the Bank achieving its goals.

Internal control *monitoring* should assess the quality of performance and ensure the findings of audits and other reviews are promptly resolved. Monitoring refers to an ongoing activity that examines either the system or the users. Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. Monitoring should be performed continually and defined as a "best practice" in the Bank's operations. Key components in the monitoring process are regular management and supervisory activities, comparisons, reconciliations, and other actions managers perform.

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate the Bank's operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates the findings and recommendations do not require management actions.

Logical Access Controls

Logical access controls provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make. Access is the ability to do something with a computer resource. *Access control* is the means by which the ability is explicitly enabled or restricted in some manner, usually through physical and system-based controls. Computer-based access controls are called *logical access controls*. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection). The term access is often confused with *authorization* and *authentication*.

- *Authorization* is the permission to use a computer resource. The application or system owner grants permission directly or indirectly.
- *Authentication* is proving (to some reasonable degree) that users are who they claim to be.

Roles

Access to Human Resources Information Management Systems information may also be controlled by the job assignment or function, for example, Recruiting and Staffing Officers, Insurance Officers, Benefits Officers, Administrative Officers and Administrative Assistants, Training Coordinators and Budget Officers. PeopleSoft security policies and procedures include specific guidance on the use of correction mode, i.e., restrictions on assignment to user profiles, procedures for assigning correction mode. PeopleSoft security has been established to restrict access to only appropriate and authorized users commensurate with their roles and responsibilities. Policies and standards are documented to define the critical records and record field that are to be logged for changes.

Segregation of Duties Questionnaire

1. Segregation of Duties. Authorization-Data Owner - (Who can authorize access?).
2. Describe process used to identify authority that determines security settings, roles and other configurations
3. Describe process to initiate and monitor security settings
4. Identify Critical Panels, Tables, Fields (Who has access) Determine Level of Confidentiality, i.e., Availability, Integrity, Confidentiality
5. Identify Reports Produced
6. Identify Interfaces - Who has access, describe access, i.e., read, create, modify, delete, execute program, use external connection) - identify interfaces with other systems
7. Identify Process to Grant Access to Data/Reports
8. Identify Process to Monitor Changes to Production Data
9. Determine Level of Confidentiality (System), i.e., Availability, Integrity, Confidentiality
10. Read-Only Access Privileges [Identify User Profiles] Staff Levels
11. Create-Only Access Privileges [Identify User Profiles] Staff Levels
12. Modification Access Privileges [Identify User Profile] (Delete, Insert) Staff Levels
13. File Deletion-Only Access Privileges [Identify User Profiles] Staff Levels
14. Execute a program -Only Access Privileges [Identify User Profiles] Staff Levels
15. External connection -Only Access Privileges [Identify User Profiles] Staff Levels (Regions)
16. Security Procedures Used For Monitoring
17. Description of Input Data Validation Process
18. Identify Approval Authority for Review of Reports for Accuracy and Completeness
19. Identify Procedures Used to Identify and Correct Process Errors
20. Identify Review Process to Initiate and Monitor Security Settings
21. Responsibility for Maintenance (Assigned to who)

The information collected during this phase was used to develop the internal access control matrix which was designed to measure the performance of IDB internal access controls and the basis for the development of security policy and standards for Human Resources Information Systems.