

Policy Title: Internal Controls Policy

Type: Internal Controls

Policy Number: #03-30-01

Responsible Office: Business and Finance

Responsible Executive: VP for Business and Finance and Strategic

Retention

Applies to: All Wiley College Employees

Policy Number/Title #03-30-01 Internal Controls Policy

CONTACT(S)

Scope

This policy defines the College's responsibility for integrating internal controls at all levels throughout the organization.

Reason for Policy

This policy establishes the key areas of internal control and related responsibilities for systems and processes outside of the College's standard business practices.

Policy Statement

The College and many of the external readers of the financial statements rely on the integrity of the College's financial reports and processes that is enhanced by strong internal controls. Management of the College at every level is responsible for designing, implementing and enforcing internal controls appropriate for business processes. Every employee is responsible to know and implement applicable internal controls related to the following five components: control environment, risk assessment, control activities, information and communication and monitoring.

Every manager and employee is responsible for the systems and processes that fall under their sphere of influence. College departments need to especially focus on designing and implementing systems of internal control around processes outside of the College's Jenzabar environment that affect the College's fiscal processes. As part of this responsibility, managers and employees must ensure that every process contains adequate internal control activities to help ensure the following key objectives are achieved:

Completeness: All valid transactions for a given period have been processed and individual or groups of transactions have not been omitted or misdirected. A common control is to have transactions grouped by "batch" and to prove each batch as it is processed. Another example is to develop a control total of transactions that should be processed today and verifying that total against the totals reported on system reports, or verifying today's deposit against the transactions posted to the ledger.

Authorization: Only those transactions that meet management's criteria are processed. Some ways to accomplish this objective include requiring documentation of the authorization, such as the manager's initials, signature, or electronic approval on all transactions being processed. Additional ways include edit checks within the system to detect "improper" transactions and the timely approval of transactions. Individuals who approve transactions must have the authority to do so and knowledge to make informed decisions. An individual should not approve a transaction for which they are the payee.

Accuracy: Transactions are accurate in amount, posted appropriately, and consistent with the originating transaction data.

Timeliness: Transactions are recorded within the appropriate reporting period. All transactions must be processed within the applicable accounting period and recorded before there is opportunity for amounts to be misdirected.

Safeguarding of Assets: Access to physical assets and information systems is controlled and properly restricted to protect against misappropriation, misuse, accidental loss, and ensure accountability. Examples of physical security include a safe, locked doors, locked cabinets or drawers, card key systems, and computer passwords. This control objective is most common for inventories of supplies, cash, and investment securities, but also includes the safeguarding of data.

Managerial Review: Sufficient oversight of activities ensures controls are functioning as intended and the detection of unauthorized activities and material errors. Managerial review includes activities taken by the manager to gain assurance that controls are functioning or provide a warning before a malfunction significantly impacts operations. There are a number of tools a manager can employ to achieve this objective, including:

- Reviewing and testing reconciliations to ensure they are performed correctly.
- Reviewing an aging of accounting balances
- Reviewing reconciliations
- Performing balance fluctuation analysis
- Comparing rates of occurrence.

Definitions

Internal Control is broadly defined as a process, affected by an entity's people, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations.

Internal control consists of five interrelated components. These are derived from the way the College is managed, and are integrated with the management process.

Control Environment - The control environment sets the tone of the College, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the Board of Trustees.

Risk Assessment - The College faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.

Control Activities - Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the College, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

Information and Communication - Pertinent information must be identified, captured and communicated in a form and timeframe that enable employees to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. The employees deal not only with internally generated data, but also information about external events, activities and conditions necessary for informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. The employees must understand their own role in the internal control system, as well as how individual activities relate to the work of others. Employees must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Monitoring - Internal control systems need to be monitored--a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management/leadership and the Board of Trustees. There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the College's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions.

Accountabilities

Every employee:

- Is responsible to know and follow appropriate policies and procedures for their job.
- Has a responsibility for internal controls.
- Is responsible for the execution of control activities.
- Must be aware of opportunities to increase the reliability and integrity of the College's accounting systems.
- Notify supervisors of weaknesses in, and opportunities to enhance internal controls.

Managers:

- Are responsible for establishing appropriate controls in their sphere of influence.
- Are responsible for monitoring the effectiveness and functioning of controls.
- Provide employees with appropriate training and guidance to accomplish job responsibilities

