EMORY UNIVERSITY

FINANCIAL INTERNAL CONTROL BEST PRACTICES
Provided by the Internal Audit Department

OBJECTIVES

The Internal Audit Department wishes to share "best practice" internal controls for select business processes. We envision this document, along with the accompanying Self-Assessment, to be tools that chief business officers can use to:

- Enhance awareness of internal controls within their business unit through a shared framework and understanding of best practice internal controls for select financial and operational areas/risks
- Self-assess both areas of strength and potential opportunities within their business unit, and remediate if applicable
- Promote visibility and discussion on common enterprise-wide strengths and potential opportunities.

DOCUMENT LAYOUT

The document is divided into business processes. For each business process, the following information is provided:

- Primary Control Objective: Describes what risk the control is designed to prevent/detect.
- Why this Control Matters: Describes "what could go wrong" and provides historical Emory experiences. This is not intended to suggest that these are current issues/concerns. The issues described occurred in the past and enhanced internal controls were implemented in the affected business unit. However, a summary of the internal control gap and steps taken to remediate the risk may not have previously been shared broadly across Emory.
- Leading Industry Practices: Describes recommended internal controls to have in place.

PROCESS

- Share best practice document within your business unit.
- Complete the self-assessment document and forward results to Internal Audit
- Internal audit to conduct follow up discussions with business units

DESIRED OUTCOMES

- Internal control discussions between internal audit and the business units, and sharing of best practices amongst the business units at EFN

  Note: Internal Audit will not be issuing any "audit report". This process is designed to be a collaborative discussion around risks and internal controls.

Key Program Revenue*

*** Note: Program revenue excludes tuition, endowment, and sponsored awards, and any other contract revenue identified in the next section.**

Control Objective

Ensure Separation of Duties (SOD) controls are in place (including invoicing, collections, deposits, reconciliation, and monitoring) over school/business unit revenue sources.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, Emory units have experienced fraud resulting from the diversion of program revenues, which is damaging to the unit and to the University. In these fraud cases, the primary root cause was the lack of segregation of duties (one person was responsible for registration, invoicing, payment receipt and posting); and the fraud was not detected timely due to the lack of routine reconciliations (i.e., a simple reconciliation of # of registrant's times the course fee compared to actual revenue received) that would have identified these frauds earlier. More importantly, a unit known to lack these procedures creates an environment to enable fraud.

Leading Industry Practices Applicable to Emory

Standard SOD controls regarding revenue include the following examples:

- Separate individuals should be responsible for registration and collection activities.
- Separate individuals should be responsible for each of the following tasks: receiving cash, recording revenue, reconciling revenue to the supporting activity (i.e., registrations, sales, etc.), and posting adjustments to the general ledger. Collaborating with related departments to share these responsibilities should be structured if a department is not staffed to support the internal controls needed for a program.
- Deposits are made to Emory University bank accounts that are reconciled to the general ledger regularly by a central finance employee, and reviewed and approved by a different individual than the reconciliation preparer
- The person who receives funds should not initiate or approve the write-off of receivables
- Credit notes, write-offs of bad debt, and other entries to reduce revenue or reverse accounts receivable transactions are reviewed by a different individual than the preparer
- The person who opens the mail and/or receives cash or checks should not deliver the funds to the bank or record the receipts in the general ledger
- All billing/invoicing should be processed through the financial systems (i.e., Compass, at Emory) and not through paper invoicing (using Word, Excel, or other applications) distributed by the unit. This will generate the related revenue transaction in the ledger.

Other Contract Revenue*

*** Note: Contract revenue excludes research and programs listed in the "Program Revenue" section above; includes contract revenue from any other internal, affiliate, and/or external organizations/entities (e.g., Conference Center, CHOA, other revenue shares).**

Control Objective

Ensure contract revenue controls are in place (including contract management, invoicing, collections, deposits, reconciliation, and monitoring) over school/business unit revenue sources.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, controls in this area could reduce the risk of misstatement of revenue, premature revenue recognition, or recording fictitious revenue.

Leading Industry Practices Applicable to Emory

Standard SOD controls regarding contract revenue include the following examples:

- Separate individuals are responsible for Contract Administration (i.e., review and monitoring the rights of the parties, payment terms, and performance obligations of a contract, etc.).
- *School/unit provides services* - All billing/invoicing are processed accurately, timely (only when performance obligations are fulfilled) through the financial systems (i.e., Compass, at Emory) and not through paper invoicing (using Word, Excel, or other applications) distributed by the unit. This will generate the related revenue transaction in the ledger.
- *School/unit receives revenue share* - Any arrangements where school/unit receives a percentage of revenue from an external entity managing a program, a school/unit management representative reviews and confirms incoming payments are received as expected**.**
- Separate individuals are responsible for each of the following tasks: receiving cash, recording revenue, reconciling revenue to the supporting activity, and posting adjustments to the general ledger. Collaborating with related departments to share these responsibilities should be structured if a department is not staffed to support the internal controls needed for a program.
- The person who receives funds should not initiate or approve the write-off of receivables
- Credit notes, write-offs of bad debt, and other entries to reduce revenue or reverse accounts receivable transactions are reviewed by a different individual than the preparer.

Research Participant Payment Funds (RPPF)[1]

Control Objective

Ensure Segregation of Duties (SOD) controls are in place (including custody, recording, distribution, reconciliation, and monitoring) over RPPF funds.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, the theft of RPPF funds is one of the most common fraud experienced by Emory. Inadequate physical/access security is the primary control deficiency (funds are not adequately stored in secured/locked receptacle with access limited to a limited number of accountable employees).

Leading Industry Practices Applicable to Emory

Standard SOD controls regarding RPPF include the following examples:

- Separate individuals should be responsible for each of the following tasks: ordering RPPF, custody of the RPPF, recording (both purchase and distribution), distributing RPPF, conducting inventory counts of RPPF, reconciling RPPF funds (i.e., between purchasing records, distribution records, etc.), adjusting the general ledger, and approving the general ledger adjustments. Collaborating with related departments to share these responsibilities should be structured if a department is not staffed to support the internal controls needed to manage an RPPF program.
- Inventory logs should be maintained detailing RPPF funds on hand (if gift cards, serial numbers and/or other identifying information should be recorded.
- RPPF reconciliations should be completed on a timely /periodic basis.
- RPPF inventory counts should be completed on a periodic basis and supplemented with at least one surprise count a year.
- RPPF should be physically secured (i.e., in a lockbox, safe, etc.)
- Physical access to the RPPF should be limited to as few people as possible. Access should be recorded (e.g., sign in sheet or electronic records).
- Total amount of RPPF physically available at any time should be kept at a minimum to lower possible loss from theft or fraud.

[1] RPPF funds can include cash, gift cards and CliniCards.

Tableau Travel and Expense Dashboards

Control Objective

Review the Tableau travel expense and unused airline tickets dashboards to determine whether they are operating effectively.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, use of the Tableau dashboards allows effort to be focused on looking for trends/unusual items and can result in time savings to a business unit (effort can be reallocated to other tasks). There are a couple of key dashboards that CBO's should ensure they staff are reviewing: 1) unused airline tickets (so credits can be applied to future trips); 2) Non-Reimbursable Expense Reports by Employee (instances of an employee using a corporate card multiple times for personal purchases can be identified on this report, and appropriate consequences initiated; such as the suspension of card privileges); 3) Duplicate Expenses (this is a new dashboard that identifies potential duplicates…i.e., employee submitted the same expense more than one time for reimbursement).

Leading Industry Practices Applicable to Emory

Standard controls regarding the travel and expense analytics process include the following examples:

- Accountable employees are designated to review the travel dashboards at least monthly. Random spot-checks are deemed appropriate for University transactions less than $250.
- Maintain documented reporting and escalation procedures to outline scenarios that require further escalation.
- Provide regular trainings and reminders on requirements and available tools, resources, and analytics to individuals responsible for monitoring travel expenses.
- Direct bill charges (from travel agent) are reviewed for appropriate business purpose.

Vendor Contract Management/ Signature Authority

Control Objective

Verify that approval authority requirements (i.e., signature authority, delegation letters) are established for the review of contracts for goods and services.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, a common internal audit observation is that employees obligate Emory funds to be spent (purchase orders, contracts, or invoice attach) when they do not have authority to do so. In addition, situations where one employee can engage a vendor (typically via a sole source decision) are frequently reported to the Emory Trust Line for investigation. In many of these instances, the employee had an undisclosed conflict of interest with the vendor.

Leading Industry Practices Applicable to Emory

Standard controls regarding the vendor/contract signature authority process include the following examples:

- The University should maintain policies and procedures that govern the vendor/contract signature authority processes, including clear guidelines for the delegation and sub-delegation of authority and signature responsibilities.
- A signature authority matrix (i.e., a listing of all employees and the authority delegated to them from the school/business unit) should be maintained, periodically reviewed, and updated, distributed to applicable personnel, and integrated into automated workflows as possible.
- Proper training should be provided to all individuals who are assigned signature authority to ensure policies and procedures are followed and the individual manages their authority appropriately.
- All vendor/contract signature authority activities should be correct and compliant with University policy, and proper documentation should be maintained for all delegation activities.
- An annual review of all delegation of authority activities should be performed to ensure that all contracts are approved appropriately, and all guidelines are followed.
- New delegation of signature authority documentation should be created if authorized uses or limitations change or if staff terminate employment.
- An independent review (i.e., internal audit) of vendor/contract signature authority should be performed periodically, which may include a review for improvements of vendor/contract signature authority processes to identify potential changes to make the process more accurate and efficient.

Procurement (Check Request Purchases)

Control Objective

- Verify that approval authority requirements are in place for the review of check request purchases.
- Verify that access controls around Emory Express are designed and implemented appropriately.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, Emory policies and procedures define expectations for utilizing appropriate procurement methods. In general, all purchases should have a purchase order generated, even if associated with a contractual statement of work for services. Purchase orders should be generated through Emory Express. Certain non-purchase order transactions, such as low-cost department supplies may be charged to a P-Card. Data indicates low levels of compliance with procurement policies, as purchases are made using inappropriate procurement methods (check request purchases). These situations are more prone to potential fraud, and often result in increased costs and unfavorable terms to Emory.

Leading Industry Practices Applicable to Emory

Standard controls regarding non-PO purchases include the following examples:

- The University should maintain policies and procedures that govern the check request purchasing process (e.g., travel purchases, procurement card (Picard) transactions, contracts, sole source agreements), including purchasing mechanisms, approval processes and thresholds, and required supporting documentation.
- The University should maintain, distribute, and regularly update a signature authority matrix that captures required approvals at various thresholds for different purchasing mechanisms.
- All submitted transactions should be correct and compliant with University policy, and proper supporting documentation for all check request purchases should be maintained.
- Check request purchases should be evaluated during the Emory Express approval process to verify that the contracting/engaging individual had authority to do so based on signature authorization letters. If individual is deemed to not have authority, processes are in place to flag and discuss the transaction with appropriate faculty and/or staff.
- A review of all check request purchases should be performed to ensure that all payments are allowable, acceptable, and accurate.
- Separation of duties should be maintained between individuals who initiate, authorize, and pay for check request purchases. The equivalent approval workflow of PO transactions should be followed and documented for check request purchases. These approvals should be completed prior to the supplier's work performance.
- Purchases should be made using system workflows to automate controls regarding separation of duties, approvals, purchase thresholds, and allowable transactions.
- An independent review (i.e., internal audit) of check request purchases should be performed periodically, which may include a review for improvements of check request purchase processes to identify potential changes to make the process more accurate and efficient.

Physical Access/Building Security

Control Objective

- Review physical access and building security controls to verify proper safeguards are in place.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, theft of assets (both Emory assets, and employee/student personal assets) from building is a common occurrence due to the open nature of campus. Criminals know that they can freely enter most buildings and thefts of opportunity routinely occur (unsecured asset left in open). In addition to the monetary loss associated with the stolen assets value, electronic devices that store confidential information are a frequent target, and their theft exposes Emory to potential data breach penalties.

Leading Industry Practices Applicable to Emory

Standard controls regarding physical access and building security include the following examples:

- Each unit should maintain policies and procedures that govern physical access and building security to verify access is monitored and buildings are secure
- The unit should monitor activity of all buildings during business hours
- The unit should keep premises and secured areas locked via key or card swipe during non-business hours to prevent theft, damage, and unauthorized access
- Access to specific buildings and secure areas should be properly controlled by appropriate safeguards (e.g., proximity cards, swipe cards, keys) and only given to those who require access to perform their job functions. The University should perform regular reviews of these buildings/areas to verify whether access controls are operating effectively
- The unit should maintain separation of duties between individuals responsible for administering, approving, and reviewing physical access to buildings
- The unit should maintain a detailed log of all employees, assets, and functions within each building
- Building access logs and appropriate supporting documentation should be maintained to track all distribution and management activities of physical keys and swipe cards, including their assignment to individuals
- The unit should conduct regular reviews of access control logs to verify all employees have appropriate levels of access and that terminated individuals no longer have access
- Master keys should be appropriately maintained by an authorized individual. Access to master keys should be limited, and any distribution of the master key to others should be logged (provision, and return).

Space Planning

Control Objective

- Review space planning controls to verify assets are being managed effectively.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, campus physical plant space use is a significant system wide asset, and the operations of the physical plant typically represents 15% or greater of all campus operating costs. Savings in physical plant issues can be spent for improvement in facilities or betterment of the academic programs. Strong, proactive space management is important to: A) Operating facilities with optimum efficiency and utilization. B) Recruiting efforts in an increasingly competitive environment. C) Providing flexibility to better respond to program needs. D) Better understanding space needs to plan for future projects. E) Establishing appropriate teaching, research, and community service resources. F) Providing a platform for innovative educational program delivery.

Leading Industry Practices Applicable to Emory

Standard controls regarding space planning include the following examples:

- Each unit should maintain policies and procedures that govern space utilization (standard size, furniture/equipment, and configuration; scheduling rooms, etc.).
- The unit should maintain an inventory of all spaces by type (office, classroom, research lab, conference room, other, etc.).
- The unit should provide guidance on space sizes and utilization (for each type of space).
- The unit should use a space management/scheduling tool to reserve spaces for use (particularly classrooms).
- All requests for space should flow through a central process for consideration and assignments.
- The unit should establish utilization targets for spaces (classrooms, conference rooms, etc.).
- The unit should generate or have access to space utilization reports (hours used, seat utilization, etc.).
- The unit should regularly review space utilization reports and take actions where necessary to improve utilization.
- The unit should review all spaces to ensure they are accessible (compliance with regulations).

Employee Separation Process, Non-Time Payroll, and Honorarium

Control Objectives

- Review the employee separation process to ensure it is operating effectively.
- Review the approval authorization and monitoring of non-time payroll (e.g., extra duty, bonuses).
- Review approval authorization of honorariums.

Why This Control Matters

Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, historically Emory has not experienced significant payroll fraud. However, non-time payroll can be abused if proper segregation of duty controls (approval of request) and approval (request in accordance with policies, proper justification provided/no indication of bias in the payment to select employee).

Several recent instances have occurred where terminated Emory employees were able to take data with them (on electronic devises, flash drives, or emailed). Monitoring of the separation process is important to ensure that exit procedures are followed, particularly for high-risk positions (faculty, business officers, etc.).

Leading Industry Practices Applicable to Emory

Standard controls regarding the employee separation process include the following examples:

- The University Human Resources should maintain policies and procedures that govern the employee separation process to ensure that termination payments are correct, timely, all University assets are returned prior to termination, and access to Information Technology (IT) systems and premises are removed prior to termination.
- All terminated employees (i.e., voluntary, involuntary, resignations, retirements) should complete a separation checklist or form to ensure consistency across all employee separations and to help alert the University if key actions do not occur. The employee's supervisor and Human Resources (HR) should review the checklist and share the checklist with any other impacted departments (e.g., IT).
- The University should ensure that proper documentation is maintained on all steps throughout the employee separation process.
- Designated unit HR representatives or University Employee Relations should host an exit interview or exit survey before the terminated employee's departure.
- Each business unit should establish processes to ensure that a terminated employees' access is revoked timely.

Standard controls regarding the non-time payroll process include:

- The University should maintain policies and procedures that govern the process to ensure that non-time payroll transactions are properly recorded and authorized, that paychecks are appropriately distributed, and that employees are paid accurately.
- The University should maintain separation of duties between individuals responsible for hiring and promoting personnel; recording, maintaining, and reviewing timecards and non-time payroll approvals; preparing/inputting payroll information and authorizing/ processing payroll.
- The University should maintain documentation of justifications and approvals for non-time-related payments, such as bonuses, and verify that these payments are within any University limits or thresholds.
- An additional, separate individual should regularly review payroll reports to ensure all payroll actions are appropriate.

- Access to employee records should be restricted to prevent unauthorized use and unauthorized changes to an employee's marital status, withholding allowances, or deductions.
- Proper documentation should be maintained on all activities that occur throughout the payroll process, including reviews and approvals.

Standard controls regarding the honorarium process include:

- The University should maintain policies and procedures that govern the honorarium process to ensure that appropriate costs are incurred, and all payments made are necessary and authorized.
- Separation of duties should be maintained between the individuals authorized to prepare, approve, and review and reconcile honorarium payments.
- Access to honorarium information should be limited to only designated employees who need the information to perform their job functions.
- Monthly ledger reconciliations should be performed to confirm that honorarium activities have been approved and billed correctly.
- A review of contract and grant terms, gift restrictions, and other fund restrictions should be conducted to ensure that honorariums charged are allowable.
- All submitted transactions should comply with University policy and be supported by proper documentation.

Financial Review Procedures

Control Objective:
Determine whether financial review procedures/checklist activities are performed timely (monthly, quarterly, annually) to ensure accurate reporting.

Internal Control Note:
Controls in this area matter because they reduce the risk that questionable or inappropriate activities happen (i.e., help to prevent) and/or remain without identification/resolution (i.e., help to detect). For example, the failure to perform financial review procedures/activities (monthly, quarterly, etc.) in a timely manner contributes to the potential for inappropriate/overspend, and/or inaccurate reporting.

Leading Industry Practices Applicable to Emory:
Standard controls regarding the financial review process include the following examples:

- Procedures/checklists that govern the financial review process, including guidance for the preparer and reviewer, timelines to complete accounting activities, and documentation requirements are maintained and updated.
- Financial review procedures, including analysis of key reports (i.e., suspense accounts, Aged A/R, fund balance reports, etc.) are performed timely and reviewed by an appropriate manager.
- Journal Entry procedures (including RSTs, journal mover, etc.) are reviewed, approved, and adequately supported by supporting documentation and retained within Compass.