The Engagement Process: A Collaborative Effort

Our objective is to have you involved at every stage so that you understand what we are doing and why. The process for most engagements consists of four stages: (1) Planning; (2) Fieldwork; (3) Reporting; and (4) Follow-up.

Planning

During this phase, we explain our risk-based approach, gather information about risks and controls, and determine the objectives for fieldwork. We will hold a Welcoming Meeting and conduct an Engagement Risk Assessment. When planning our review, we welcome input from management on areas they would like to include.

Fieldwork

The Fieldwork phase is when the actual work of the audit is performed through testing of controls. This typically includes:

- determining whether controls are operating efficiently and effectively.
- assessing accuracy of financial reporting.
- verifying that policies and procedures are available, up to date and address risks adequately.
- reviewing compliance with applicable laws, regulations and policies.

Testing results will be discussed with you and your management team both during the fieldwork phase, as well as at the engagement's conclusion.

Reporting

- Draft Report — During a closing meeting, we will discuss the draft report and make any appropriate revisions.
- Final Report – Management's action plans, including responsible parties and a timeline for completion, are added to the report. The final report is distributed to management, appropriate University leadership, and the Board of Trustees.
- Dashboard – The Dashboard summarizes the activities and procedures reviewed, and provides an assessment of the areas reviewed and related internal controls.

Follow-Up

Follow-up is the final stage of the process. Follow-up activities will be performed periodically and conclude when action plans are completed. We maintain a tracking report to record open audit recommendations which is shared with the Audit and Compliance Committee of the Board of Trustees at quarterly meetings.

Other Relevant University Resources:

University Policies

University Policies are formal policies and procedures at the University of South Carolina that have campus-wide or system-wide application.

Contact: (803)777-2808 http://www.sc.edu/policies/

Enterprise Risk Management

Program including risk assessment, control, insuring and financing alternatives to reduce potential loss.

Contact: Brian Hann - Hann@mailbox.sc.edu, (803)777-2828

Finance

The Finance organization houses the Controller's Office, Budget Office, Bursar, Capital Finance, Contract and Grant Accounting, Financial Reporting and Payroll. These offices provide support for financial operations for the University of South Carolina System. http://adminfin.sc.edu/finance.shtml

Office of the VP for Research

Provides the resources for those conducting research at the University.

Contact: (803)777-5458 http://www.sc.edu/about/offices_and_divisions/research/index.php

Purchasing

The Purchasing department strives to ensure all procurement transactions are conducted in a legal, ethical, and professional manner.

Contact: (803)777-4115 http://purchasing.sc.edu

UTS IT Security Office

Outlines requirements for the appropriate protection of technology assets and data; to report a data compromise or other IT security incident.

Contact: (803)777-1800 http://security.sc.edu

Columbia 24-hour 911 / Communications

Maintaining emergency communications center, dispatch/911 services, monitoring burglar/fire alarms, Carolina Alert and University card access systems.

Contact: (803)777-4215 http://les.sc.edu/

Audit & Advisory Services

1600 Hampton Street, Suite 610
Columbia, SC 29208
(803) 777-2752
http://www.sc.edu/audit

UNIVERSITY OF SOUTH CAROLINA

About Audit & Advisory Services

Audit & Advisory Services (AAS) enhances and protects organizational value by providing risk-based assurance, advice and insight. We function as an independent appraiser of university activities and use a systematic, disciplined approach to evaluate and improve effectiveness of governance, risk management and control processes.

Our staff is committed to assisting the University of South Carolina in functioning at the highest level possible regarding compliance with regulations and university policies, financial stewardship, ethics and internal controls. We are guided by a charter which establishes our authority, role and responsibilities. Our charter is University Policy BTRU 1.06, *Audit & Advisory Services.*

Pamela A. Doran
Chief Audit Executive
Audit & Advisory Services

USC Integrity Line

The University of South Carolina has established a 24-hour Integrity Line that enables you to report concerns about questionable or unethical behavior anonymously. To submit a report, please visit the following website:

http://www.sc.edu/uscintegrityline

What are Controls?

Control objectives are an integral part of managing daily business transactions. With risks arising from potential error, material misstatement, or non-compliance, it is important that proper controls are in place and functioning.

Developing sound controls provides reasonable assurance that operations are effective and efficient, produce reliable financial report and comply with applicable laws and regulations.

The first step is identifying the risks applicable to your organization, followed by a prioritization of those risks based on their impact to the organization if they occur.

Control policies and procedures are established to help ensure these risks are effectively mitigated and the entity's objectives are efficiently carried out.

In addition:

- Controls cultivate strong teamwork and productivity.
- Controls provide information for continuous improvement.
- Controls reduce errors and provide restraints and barriers to illegal access and acts.
- Controls help establish an environment conducive to integrity and honesty.

We have provided examples of potential risks, and related controls, to consider during your evaluation.

Potential Risks and Controls

Assets/Inventory

Risk: Assets or inventory may be subject to theft or become obsolete.

Controls: Assets and inventory should be physically secured through the use of locks, cameras, etc., including cash and checks, computers and capital assets. Assets and inventory records should be periodically reviewed for accuracy and obsolescence.

Audit Trails

Risk: Erroneous or fraudulent transactions may not be detected.

Control: All systems and processes should have a log of critical transactions processed, who processed them and the date they were processed. Logs should be periodically reviewed for unauthorized or unusual activity.

Business Continuity/IT Disaster Recovery

Risks: Inability to recover lost critical data and resume core business functions.

Inaccurate financial reporting due to loss of data.

Controls: Disaster recovery and business resumption plans should be developed, tested, and maintained.

Critical data and software should be backed up daily and rotated off-site.

Data Access/Authentication

Risks: Data may be compromised, leading to disclosure of confidential faculty, staff, and student information to unauthorized individuals.

Sensitive information might be used for fraudulent purposes.

Controls: Only authorized personnel should have access to sensitive and confidential data; system access levels should be assigned in accordance with job function and should be periodically reviewed by management.

Strong passwords should be used to control access and user names and passwords should never be shared amongst staff.

Data Integrity

Risks: Financial and operational data may be inaccurate, leading to loss of the University's credibility.

Reports may not reflect the entire financial activity.

Controls: Management should review monthly financial reports for unusual items. All unusual items should be investigated and resolved in a timely manner.

Manual adjustments to data should be properly documented and approved.

Management should ensure that all data is protected in accordance with University requirements.

Expenses/Procurement

Risks: Budget overruns could occur.

Prices of goods and services may be inflated by vendor or contractor.

Inappropriate or fraudulent transactions could go undetected.

Controls: Management should ensure effective controls are in place to approve expenses.

Duties should be appropriately separated, having more than one person required to complete a transaction.

Adequate documentation supporting the business purpose should be maintained.

Budget to actual comparisons should be prepared and reviewed with management.

Petty cash accounts should be reconciled.

External Funding

Risk: Sponsored program budgets may be under or over expended, leading to possible fines, loss of current and future funding, and subjecting the University to reputational risk.

Controls: Changes in regulatory requirements should be monitored to determine their applicability.

Time and Effort reporting should be periodically validated.

Sponsored program expenses should be regularly reviewed for compliance with the terms of the contract and the approved budget.

IT System Security

Risk: The server/system could be compromised and confidential information could be exposed.

Control: Information technology assets and data are secured in accordance with University requirements.

Reconciliations

Risks: Problems resulting from daily processing may not be managed or responded to timely.

Unnecessary resources and time could be spent if data errors are not corrected timely.

Incorrect data may be erroneously reported.

Recognizing revenue/expenses in the wrong period could distort financial data/statements.

Controls: Departmental reports should be reviewed for accuracy, and errors should be resolved within established time frames.

Accounts should be properly reconciled to supporting detail and differences should be appropriately researched and resolved.

Revenues

Risk: Funds could be misappropriated or could be assigned to the wrong account.

Control: Funds should be collected, deposited timely, applied to the appropriate account, and reconciled. These duties should be appropriately separated.

Training/Personnel Considerations

Risk: Critical operations could be seriously interrupted if key personnel are not available due to illness or attrition.

Controls: Key personnel should be appropriately cross-trained.

Roles and responsibilities should be defined, documented, and communicated to applicable personnel.

Transaction Authority

Risk: The University could be liable for unfavorable terms resulting from improper contract negotiations.

Controls: Contracts should be actively monitored, renegotiated, and authorized as appropriate.

Potential Conflicts of Interests should be disclosed and appropriately managed.