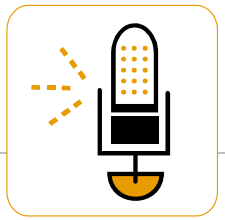
The STRAIGHT and NARROW

July 20, 2007
Volume 1, Issue 1

Office of Internal Audit, Board of Regents of the University System of Georgia, (404) 657-2237

Special Interest Articles:



From the Desk of Ron Stark

Welcome to the Office of Internal Audit's first issue of *The Straight and Narrow.*

This quarterly publication is intended to provide an informal learning opportunity for campus personnel as well as a regular communication tool for matters that may affect your campus.

We also want to make it well known that the Office of Internal Audit is a System resource for questions, concerns and exchange of ideas so that we may assist you in the continuously changing accounting and reporting environment that we all face. Your feedback is always welcome!

Internal Control - 101

You have probably heard reference to "internal controls" on more than one occasion. What do we really mean by this term? Although there are many definitions, simply put, internal controls are the methods, systems, and procedures for 1) protecting resources from waste, loss, theft or misuse, 2) ensuring that resources (monetary and non-monetary) are used in accordance with laws, and 3) producing reliable financial information based on accurate and verifiable data.

Some examples of internal controls include:

- Top level reviews of actual performance – tracking results to plans, goals, and established objectives.
- Physical controls over vulnerable assets – examples include limited access to cash, inventories, and equipment that may be vulnerable to risk of loss or unauthorized use.
- Segregation of duties – separating the responsibilities for authorizing, processing, and recording of transactions so that no one individual controls key aspects of the transactions or events from initiation through completion.
- Proper execution of transactions – assuring that transactions or events are authorized and executed only by persons acting within the scope of their authority. The authorizations should be clearly communicated to managers and employees.
- Appropriate documentation of transactions – source records that support the directives, approvals and actions taken by the authorized individuals.
- Information technology controls–a variety of activities that ensure automated information processing provides accurate results such as edit checks, control totals, limited access to data, files and programs.
- Reconciliation of accounts – processes used to ensure that key balances (such as cash) are valid or correct at a specific point in time as supported by documentation, calculations and clear and complete explanations. In other words, making sure what you think you have in an account is what you actually have.

Designing and establishing effective internal controls is not a simple task. A well designed internal control structure can enhance your department's efficiency and effectiveness as well as reduce the risk of loss or theft. For further advice and assistance in designing internal controls appropriate for your operation, you may contact Internal Audit at 404-656-2237.

"Creating A More Educated Georgia"
www.usg.edu

From the Office of Internal Audit – Reporting Department

AFR Due Date Reminder:

August 1st – *Institutions receiving Agreed Upon Procedures*

August 8th – *Institutions receiving Modified Disclosure Management Reports*

August 15th – *Institutions receiving full audits*

Don't Let History Repeat Itself!

For the University System, there were 127 AFR reporting inaccuracies as noted by the State Auditors for fiscal 2006.

There were some common themes for many of the reported inaccuracies:

- Unrecorded or unsupported Accounts Receivables
- Unrecorded or unsupported Accounts Payable
- Capital Assets: capital vs. expense; depreciation; missing inventory items
- Bank reconciliation items
- Compensated absences liability

Please keep these areas in mind when completing the fiscal 2007 AFR.

Tip: Look at your institution's subsidiary account balances on a Budgetary and GAAP basis to identify Asset accounts with credit balances and Liability accounts with debit balances. These balances must be reclassified for BOTH Budgetary and GAAP Reporting. The year-end journal entries that address this are GAAP ledger entries. Note that reclassification entries may be made in the Actuals ledger to accomplish both objectives.

A Capital Idea?

If your institution is one of the growing number to enter into rental agreements for privatized housing and other projects with your Foundations, know that in most cases, the rental agreements should be accounted for as Capital Leases.

The criteria for capital lease determination follow:

1. Ownership transfers to the institution at the end of the lease term. The wording in the agreement may indicate that the Foundation will 'gift' the improvements.
2. The lease contains a bargain purchase option.
3. The net present value of the minimum lease payments exceed 90% of the estimated fair value of the project
4. The lease term is greater than 75% of the estimated remaining useful life of the project. The lease term should include the primary plus all renewal lease terms.

If any one of these criteria is met, capital lease treatment is warranted.

Call BOR Reporting with any questions about capital lease accounting.

Did you know?

Check payment detail reports for GSFIC projects should now be requested from Yvette Usher. Her e-mail address is:

yvette.usher@usg.edu

Significant Adjustments are misstatements that exceed the State auditors' materiality threshold and are required to be adjusted in the financial statements.

Uncorrected Misstatements are reporting inaccuracies that exceed the State auditors' materiality floor but fall below the materiality ceiling and are not required to be corrected in the year being audited.

Financial Aid Call Center Contracting

According to a leading education finance and marketing services company focused on providing a broad set of student loan products and services, call center agreements with third-party companies have advantages and disadvantages. Call center contracting reduces the burden and cost of a financial aid office. However, call center employees may recommend their employer (the lender) over other lenders, even if other lenders have products with better benefits or lower rates.

If your institution decides to enter into an agreement with a financial aid call center, please ensure the following items have been addressed:

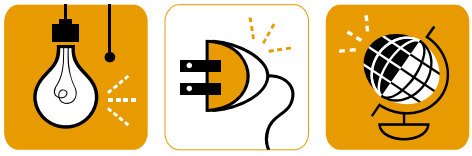
- Follow State Procurement Guidelines: http://statepurchasing.doas.georgia.gov/vgn/images/portal/cit_11783501/53901646procurementmanual.pdf
    - solicit bidding prior to awarding contracts for services greater than $5,000.
    - contract must be annually renewable and five years or less.
    - obtain all proper signature approvals.
- Adhere to US Department of Education Blue Book Chapter 3: General Participation Requirements - Contracts with Third-Party Services (http://www.ifap.ed.gov/bbooks/attachments/1005BlueBookCh3GeneralRequirements.pdf) pages 1-15 & 1-16. Examples of functions that are covered by this definition are:
    - providing student consumer information services.
    - certifying loan applications, servicing loans, or collecting loan payments.

According to policy, schools are required to notify the Department of all existing third-party service contracts. If a school has not notified the Department, the school immediately must do so by completing Section J of the Application for Approval to Participate in Federal Student Aid Programs (E-App).

- Review contract language to ensure it includes:
    - reference to the Gramm-Leach-Bliley Act of 1999 and the Family Educational Rights and Privacy Act of 1974 relating to protection/confidentiality of student data.
    - provisions to prevent the company from using its access to information as part of its sales of student loans and loan consolidations. Additionally, the agreement should include specific contract language that protects student confidential information.
    - ability to audit company procedures to ensure there is a “firewall” between financial aid administrative services and student loan sales/servicing.
    - specific provisions on how student information will and will not be used.

Recently, the University of West Georgia opened a new campus-operated Call Center to help with their financial aid and registration questions. The center is a cooperative effort between the offices of Financial Aid and the Registrar. The Call Center provides assistance, guidance and answers questions regarding registration and financial aid. According to Kimberly Jordan, Director of Financial Aid, and Bonnie Stevens, Registrar, “they hope the center will make life less stressful for university staff and students.”

Remember, educational institutions should exercise due diligence in protecting the financial interests of students and should ensure that outside organizations providing services to students also adequately protect student interests.



Who is watching over your Credit Card Data? (And why do you have it at all?)

Due to substantial losses in the last few years, credit card issuers have worked hard to ensure that credit card data is properly handled and protected. The outcome of this work has resulted in a comprehensive set of requirements known as the Payment Card Industry – Data Security Standard (PCI DSS). PCI DSS was first released in January 2005 but has since been enhanced and is now published as PCI DSS version 1.1.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Any Institution which processes, stores, or transmits credit card numbers must be PCI DSS compliant or they risk substantial fines and loss of the ability to process credit card payments. These Institutions must validate compliance through an audit by a PCI DSS Qualified Security Assessor (QSA) company. This assessor will ensure that the Institution meets the requirements of the Standard. Organizations that fail to comply, risk not being allowed to handle cardholder data and fines of up to $500,000 if the data is lost or stolen.

In order to be compliant with PCC DSS, the standard requires the following:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Mgmt. Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to card-holder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

Compliance is required of *all* merchants and service providers that store, process, or transmit cardholder data and applies to all payment channels: at the point of sale, over the Internet, on the phone, or through the mail.

Monitoring of compliance with PCI DSS depends on the volume of credit card transactions that an Institution/Merchant processes. An Institution with between 20,000 and 1,000,000 transactions is defined as a Level 3 merchant. Proof of compliance requires an annual self-assessment and quarterly network scans. An Institution with less than 20,000 transactions is a Level 4 merchant and requires an annual self-assessment and annual network scan.

If your institution stores credit card data or credit card data passes through your systems, then you must meet PCI DSS standards. One method to ensure that you do not run into problems with PCI DSS is to ensure that you do not store credit card data on your systems or allow credit card data to transit your systems. Use of payment gateways, such as Touchnet, where the web sessions is redirected to the payment gateway for processing will allow an institution to meet PCI DSS standards.

All institutions should review their management of credit card data. If you store or transmit credit card data, then you need to understand and comply with PCI DSS.

Board of Regents of the University System of Georgia
Office of Internal Audit
270 Washington Street S.W.
Atlanta, GA 30334-1450

Phone
(404)657-2237

Fax
(404) 651-9444

"Creating A More Educated Georgia"
www.usg.edu

We're on the Web!
See us at:
www.usg.edu/offices/audit.phtml