The STRAIGHT and NARROW

April 1, 2009
Volume 3, Issue 8

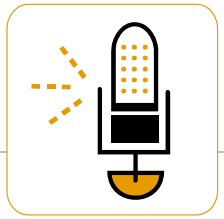
Office of Internal Audit, Board of Regents of the University System of Georgia, (404) 657-2237

The Office of Internal Audit has a position opening for an Auditor III. See the link below for additional details: *http://www.usg.edu/employment/jobs/*

****Reminder****

The FY2010 Audit Plan for the University System of Georgia will be presented at an upcoming Board of Regents Audit Committee Meeting. In order for us to complete the system-wide plan, we need to have your completed risk assessments and audit plans by March 31, 2009

Quarterly Status of Audit Activity Reports are due by April 30, 2009



From the Desk of Ron Stark

Today, we find ourselves dealing in difficult economic times and we must be aware of spending every dollar wisely. Being cognizant of our expenditures, especially those that relate to travel, we must control our costs and follow policy and procedures. All institution personnel should be aware of the travel regulations found in the USG Business Procedures Manual (BPM).

Personnel using commercial air transportation should be reminded to be cost effective and efficient. Internal Audit has recently noted an issue related to airline travel that I would like to bring to your attention. In addition to seeking approval for expenses prior to date of travel, employees must follow these steps:

Choose the lowest available airfare – a non-refundable coach ticket, make reservations 21 days in advance and submit original receipts for reimbursement

In general, it is the State's policy that State employees traveling by commercial air carrier travel is the most cost-effective manner and utilizes the lowest possible coach fares.

Employees traveling by commercial air carrier will not be reimbursed for the portion of non-coach (first class, business class, etc.) airfare that exceeds the cost of the lowest, available fare on the same flight. For instance, if an institution employee upgrades his/her coach ticket to first class at an additional expense, documentation showing the cost of a non-refundable coach ticket must also be submitted with the original receipt for the first class ticket. The employee will be reimbursed for only the non-refundable ticket price. In circumstances precluding the above conditions, pre-approval must be sought and appropriate documentation must be submitted.

Further guidance will be provided in a memorandum that I will issue shortly to the Chief Business Officers. Additionally, we will update Chapter 4 in the Business Procedure Manual.

Ron Stark, Chief Audit Officer and Associate Vice Chancellor of Internal Audit for the Board of Regents of the University System of Georgia (USG), will be leaving the USG at the end of April for a similar position at the King Abdulla University of Science and Technology (KAUST) in Saudi Arabia. It is with mixed emotions that the Office of Internal Audit bids Ron farewell. We will miss his leadership, talents and invaluable contributions to the University System. However, we know that his new position is truly a unique, once-in-a-lifetime opportunity to help build and shape a major new research university. We wish you the best Ron!

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

Inside this Issue:

Who We Are

Internal auditing is an independent appraisal activity authorized by the Board of Regents to examine, evaluate and advise components of the University System of Georgia (USG). We offer objective reviews for the purpose of providing an assessment on governance, risk management, and control processes. This is accomplished through:

- Financial engagements
- Performance engagements
- Compliance engagements
- IT engagements

The Compliance and Ethics (COMET) Program is also managed by the Office of Internal Audit with responsibility to:

- Prevent misconduct through education and training
- Detect misconduct through reviews, anonymous reporting, and other means
- Protect the USG from the potential repercussions associated with misconduct by USG employees.

The COMET program accomplishes these objectives through:

- Managing a USO compliance program
- Advising USG and institution management on significant compliance risks
- Coordinating and supporting institutional compliance functions
- Conducting investigations and reviews as needed.

Website: www.usg.edu/offices/audit.phtml
Phone: (404) 656-2237
Fax: (404) 463-0699

Study Abroad

By Matthew Harrell

Students today are offered many opportunities to enhance their experience in college. One such opportunity is a Study Abroad program. Part of the University System of Georgia's (USG) Strategic Plan emphasizes renewing excellence in undergraduate education, and includes increasing participation in Study Abroad as one of the objectives. With an increase in Study Abroad programs around the system and the importance of such programs to the USG strategic plan, the Office of Internal Audit (OIA) included a review of Study Abroad as a focus area during FY2009. In February, the OIA completed its review which concentrated on the areas of guidelines and approvals, required program charges, and fund reporting associated with the administration of a Study Abroad program. The following are areas/issues to consider when creating or maintaining a Study Abroad program:

- Pay Faculty Travel and Expenses from E&G Funds. However, if funding is insufficient in the E&G Account, then student program fees (agency funds) may be used. If student program fees are used, the funds must be transferred to the appropriate E&G account before being disbursed.

- Ensure that each Study Abroad program is approved by the institution's President or President's designee. The approval form is located at the following website: http://www.usg.edu/oie/facstaff/policies/usg_rfa.pdf

- Prepare a Study Abroad Handbook which should include the following:
  - How to obtain the proper authorization (forms, signatures, etc)
  - How to set up an Agency Account
  - How to educate students and faculty on institutional and BOR Travel policy
  - What academic considerations are needed
  - How to develop a budget and budgetary guidelines
  - Who collects the fees
  - How to pay for expenses and reconciliation of expenses and accounts
  - What to do in case of an emergency (Risk and Emergency Management Plans)

- Provide instructions on where to deposit the funds if foundations provide financial assistance, i.e., deposit into a specific Study Abroad agency account.

- Ensure that faculty salaries are paid from the appropriate E&G account and not from agency accounts. If there are excess funds remaining in the associated Agency account after the program has concluded, then the funds must be used for future Study Abroad programs. If the specific program has ended and will not continue the following year, then excess funds remaining in the agency account must be transferred to another Study Abroad program's account or the general fund.

- Develop appropriate waiver and release forms for faculty, staff, and students.

- Institute policies and procedures to discuss program requirements with students and parents/guardians.

Understanding Identity and Access Control Management

By Erwin (Chris) Carrow

Overview:
In various reviews of the business functions (e.g., service level agreements with external agencies, university departments management of related services and resources) associated with the management of user credentials (the means by which users might log onto and use various systems or resources, e.g., the provisioning and de-provisioning of student, faculty, staff, and outside agencies identities), and the mechanisms in place to allow logical or physical access to sensitive or confidential information (permit or deny the use of a particular resource by a particular entity e.g., technical or administrative controls to allow or deny access to file shares). The following problems were consistently identified and would prove to be beneficial for all USG universities to evaluate their current business practices.

Problem:
The handling of sensitive and confidential information and access rights administered by departments was not effective or systematic. There was a divestment of the various roles' (e.g., business owner, trustees, and data stewards) authority and responsibility to safe-guard information and information systems, which introduced unnecessary risk. The business practices were not clearly defined and documented to ensure sensitive and confidential information for operational procedures were being implemented consistently and correctly throughout all campus departments. Likewise these practices should be periodically evaluated to validate the level of implementation effectiveness. The risk introduced into the university environment could include:

- Lack of IT security governance and misaligned IT security controls to organizational objectives
- Unprotected IT systems or information assets or unauthorized changes to hardware and software
- Identity and access management failing business requirements and compromising the security of business-critical systems
- Unspecified security requirements for all sensitive or confidential information or information systems
- Compromised sensitive or confidential information or system information or unnecessary exposure of sensitive or confidential information

Solution:
Ensure the policies, standards, and procedures for receiving, handling, storing, and destroying of sensitive or confidential information is being effectively implemented for all department level operational practices. To avoid and mitigate risk, business functional processes involving sensitive or confidential information should be defined, documented, and periodically reviewed to ensure consistency in how data is received, handled, stored, and destroyed. These functional processes associated with sensitive or confidential information should be formally acknowledged and understood by all personnel. Practically applications of these requirements should be defined and documented at the department level to the specific roles or responsibilities that handle sensitive or confidential information. Therefore, you should:

- Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable.
- Enable user identities via automated authentication mechanisms.
- Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities.
- Ensure that user access rights are requested by the users' management, approved by system owners and implemented by the security-responsible person.
- Ensure applicable policies, standards and procedures exist to safe-guard sensitive and critical information.

The following graphic depicts the "Life Cycle" of IAM considerations for properly managing your business processes, e.g., policy requirements, how data is produced, who is involved, and where the information resides or travels throughout your university.

Please direct questions that you might have about Identity & Access Control Management to Erwin (Chris) Carrow at ewrin.carrow@usg.edu or 404-657-9890.

Malfeasance Reporting Explained

By John Fuchko, III

The malfeasance reporting requirements to the System Office have changed significantly over the past year. Previously, Business Procedures Manual (BPM) Section 16.4 (http://www.usg.edu/fiscal_affairs/bpm_acct/bpm-sect16.pdf) was the only source of guidance on malfeasance reporting. BPM Section 16.4.5 stated, in part, that:

All reports prepared as mentioned in Section 16.4.4 above must be provided to the Associate Vice Chancellor for Internal Audit. Additionally, any fraud activity investigated must be reported to the Associate Vice Chancellor. This includes those fraud incidents that are administered by the Triage committee, as well as those incidents that are turned over to the institution's Internal Audit Department to investigate.

The Associate Vice Chancellor for Internal Audit should be notified when it has been determined that a "high likelihood" of impropriety greater than $1000 has occurred. Periodic updates should be forthcoming as the situation dictates. A written report should be submitted to the Associate Vice Chancellor for Internal Audit at the conclusion of the investigation.

The P-Card audit identified the need for some changes in the malfeasance reporting process. One change to this process was an agreement between the USG and the Attorney General's Office that requires the USG to collect and report on *all* instances of employee malfeasance involving the institution. The Compliance Program within the Office of Internal Audit was charged with the responsibility of collecting employee malfeasance reports for submission to the Attorney General's Office. These reporting changes were introduced in a May 5, 2008 memo from the Chancellor and a May 6, 2008 follow-up memo from Ron Stark. The reporting requirements will also be integrated into BPM Section 16 in the coming months.

The purpose of this note is to clarify some of the reporting requirements. Institutions should note the following:
All instances of employee malfeasance should be reported to Ron Stark and John Fuchko; this requirement is not limited to P-Card violations.

Employee malfeasance "generally includes instances of embezzlement, misappropriation, alteration or falsification of documents, false claims, theft of any assets, inappropriate use of computer systems to include hacking and software piracy, bribery or kickbacks, etc."

Employee malfeasance does not include students (unless acting as employees) or outside parties.

Reports should be submitted once an initial determination has been made that employee malfeasance was likely; institutions are not authorized to negotiate a promise to not report employee malfeasance in return for the employee's resignation, restitution, etc.

Please direct questions that you might have about malfeasance reporting to John Fuchko at john.fuchko@usg.edu or 404-656-9439.

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) 463-0699

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

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