The STRAIGHT and NARROW

July 1, 2009

Internal Audit, Board of Regents of the University System of Georgia. 404- 656-2237

Volume 3, Issue 9

Office of Internal Audit's (OIA) mission is to support the University System of Georgia management in meeting its governance, risk management and compliance (GRC) responsibilities while helping to improve organizational and operational effectiveness and efficiency. The OIA is a core activity that provides management with timely information, advice and guidance that is objective, accurate, balanced and useful. The OIA also promotes an organizational culture that encourages

We have three strategic priorities:

1. Anticipate and help to prevent and mitigate significant USG GRC issues.

2. Foster enduring cultural change that results in consistent and quality management of USG operations and GRC practices.

3. Build and develop the OIA team.

Inside this issue:

From the Chief Audit Officer

John M. Fuchko, III

The more cynical auditors will tell you that the two biggest lies in auditing are: Auditor - "We are here to help" AND Auditee - "We are happy to see you." While most people may recognize the theoretical value of an independent and objective review of operations, an internal audit can still prove to be a demanding and frustrating experience even when the end-result is worth the effort.

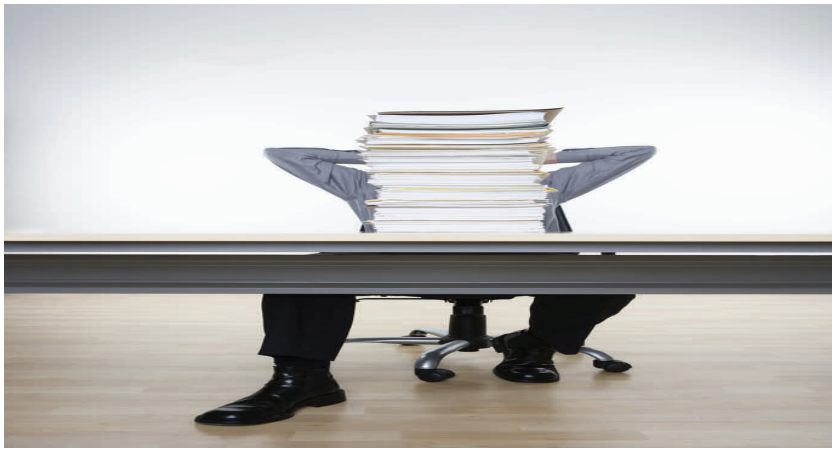
Some of these challenges flow from the logistics associated with an audit. Auditors traditionally have less time in the field and so often request large volumes of information with an expectation of a quick turn-around. Auditors learn by interviewing executives, managers and staff performing daily business functions. Conducting these interviews takes time and may appear redundant. Finally, auditors may create a certain degree of frustration when making recommendations that the auditee already knew needed to be done. However, the auditor has not addressed the auditee's real issues around resource constraints, process improvement or training challenges.

While these challenges are somewhat perennial to internal audit, the USO Office of Internal Audit (OIA) is working very deliberately to remain an effective tool for management while, potentially, reducing some of the frustrations associated with traditional audits. Specifically, OIA has:

- Re-balanced our FY10 audit plan by reducing the number of assurance (audit) engagements from our normal 15 to nine traditional audits
- Increased our FY10 audit plan focus to include more consulting engagements at both the campus-level and system-wide
- Committed to providing ongoing support to Stimulus Fund Oversight and the Time and Leave Reporting Committee

Additionally, OIA is working to enhance our access to HR and accounting information systems so that we can pull some data using our own internal resources instead of relying on institution personnel to provide us this data. This approach to data queries should reduce the demands on campus staff while increasing the quality of our analyses.

Finally, we are developing a survey tool as a means to gather feedback from auditees as to the audit process, results, etc. We look forward to hearing from auditees as to how we can improve our own processes. In the meantime, please feel free to call us at 404-656-9439 or email us at: john.fuchko@usg.edu.



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, & control processes.

This is accomplished through:

1. ***Financial engagements***
2. ***Performance engagements***
3. ***Compliance engagements***
4. ***IT engagements***

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

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

The COMET program accomplishes these objectives through:

1. ***Managing a USO compliance program***
2. ***Advising USG and institution management on significant compliance risks***
3. ***Coordinating and supporting institutional compliance functions***
4. ***Conducting investigations and reviews as needed.***

Websites: ***www.usg.edu/offices/audit.phtml***

www.usg.edu/compliance/

Phone: (404) 656-2237

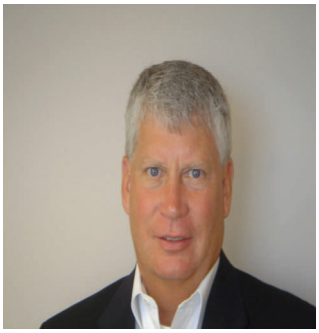
Fax: (404) 463-0699

Spotlight on James F. Winters

Due to the growth, complexity and exposure of the Public Private Venture Program (PPV), an auditor position was created to aid in the review of potential and current projects. **Jim** reports through the Office of Internal Audit but will work closely with the Office of Real Estate and Facilities.

In his position, Jim will review and audit current PPV projects while also providing recommendations on how to mitigate risks for new projects. Jim's review of current projects will include compliance with various lease and contract terms, compliance to bond requirements, and monitoring compliance of obligations for the Georgia Higher Education Facilities Authority (GHEFA) transactions.

Jim's past working experience will be beneficial in filling this new role. In his most recent assignment, he spent four years as Controller/ Accounting Manager with the Georgia State University Foundation. Jim has 30 years of banking experience with SunTrust and Wachovia with the majority of that time spent in the Trust Division working with Foundations. Jim is a CPA and has maintained his Series 27, Financial Operations Securities License.



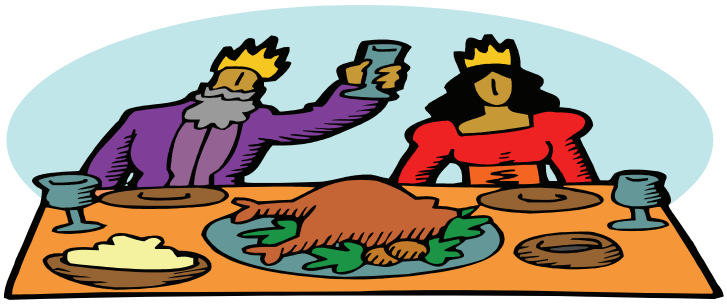
Spotlight on Michelle A. Frazier

Michelle Frazier recently relocated to Atlanta, Georgia from Minneapolis, Minnesota. Prior to joining the Office of Internal Audit with the Board of Regents of the University System of Georgia,

Michelle worked as a senior auditor with the Federal Reserve Bank of Minneapolis in Minneapolis, Minnesota. Michelle attended Kent State University in Kent, Ohio and earned a Bachelor of Business Administration degree with a major in Finance and also attended the DePaul University College of Law and earned a Juris Doctor degree.

An interesting fact about Michelle is that she has lived in five states. Michelle's hobbies include reading, listening to music, playing the piano & watching movies.

Banquets and Balls by John Fuchko, III



No one ever said that higher education administration was easy. Actually, higher education administration is a very challenging field of endeavor. This is certainly true in the University System of Georgia. As a distinct community of learners, each USG institution must find a way to further academic excellence, conduct cutting-edge research, perform service to the larger community (city, region, state, nation, and world) and develop a sense of belonging for students, faculty and staff. As a part of state government, USG institutions must do all of these things while still complying with the state laws, rules and regulations (in addition to BOR, Federal, grantor, and contractual requirements) that other state agencies must also follow.

The difficulty faced by institutions in balancing these multiple requirements is reflected in the many questions that the Office of Internal Audit receives pertaining to food. Recently, an institution requested clarification on the food policy (USG BPM Sections 19.7 and 19.8) as it pertains to a traditional end-of-year awards banquet held in honor of student assistants, RAs, etc. Specifically, the institution wanted to know if it was allowable to use auxiliary fees (Fund 12XXX) to pay for the banquet costs.

The short answer to this request was no. What was the rationale for this response? First, the banquet participants were being invited in their capacity as employees and not as students or volunteers. Second, the proposal involved the use of institutional funds. Institutional funds are defined in BPM Section 19.8 as follows: "Institutional funds include all funds to which an institution holds title, such as student fees, auxiliary revenues, state appropriated funds, etc." This meant that either BPM Section 19.7 (Employee Group Meals) or BPM Section 19.8.3 (Food for Employees) would apply.

BPM Section 19.7 is designed to address meals scheduled as part of a day-long meeting where the meal is provided in order to facilitate better use of everyone's time in that participants do not leave to obtain lunch (see BPM Section 19.7.1 for more details and requirements). Additionally, 19.7 addresses the purchase of food for conferences involving multiple institutions (see BPM Section 19.7.2 for more details and requirements). Clearly, an awards banquet falls into neither of these categories.

BPM Section 19.8.3 addresses those instances when institutional funds may be used for food for employees:

1. **Safety.** Water or other hydration products may be purchased insofar as these products are required by OSHA or are necessary to prevent serious harm to an employee.

2. **Academic Programs, Student Events, and Educational or Business Meetings Involving Predominantly Non-Employees.** When conducting a program, event or meeting involving predominantly non-employees (of any institution of the Board of Regents) where attendance by the employee is essential and in furtherance of an official institutional program, and the meal is an integral part of the meeting, an employee can partake in the meal and be reimbursed for his or her actual meal cost up to the per diem limits established in BPM Section 4.3. An employee may not be paid a reimbursement unless the employee actually incurs a cost.

Additionally, there are instances pertaining to recruitment activities and prior grant/contractual arrangements that may result in an allowable food purchase (see BPM Section 19.8.3 for more details).

Once again, the banquet fails both of these tests in that it is not a safety requirement to hold the banquet and it is not an event involving predominantly non-employees.

Where does that leave the institution that wants to build community among its student employees? For one, the institution could seek Foundation funds for use in paying for this event. Next, the institution may use student fees to hold an event open to all students where the purpose of the event is to honor student employees.

Please direct questions that you might have about allowable purchases to John Fuchko at john.fuchko@usg.edu or 404-656-9439 or Mike Foxman at michael.foxman@usg.edu or 404-656-3374.

Revisions to P-Card Policy Aimed at Addressing Common Questions by Paul Kurtz

Editors' Note: In FY 2010, we will continue to audit P-Cards. Here is a preview of the program updates.

You are probably aware that the State Purchasing Card, or P-Card, is a simple, secure and cost effective method to pay for official purchases. You also know that exceptions to the Statewide P-Card Policy must be approved in writing prior to use of the card. But did you know that many policy exception requests received by DOAS are not truly exceptions and don't require approval? The revised Statewide Purchasing Card Policy, effective July 1, 2009 includes several updates designed to make using the card easier and more convenient for Board of Regents entities.

New Maximum Monthly Cycle Limit: The most common reason for requests for policy exceptions stemmed from the need to exceed the maximum Monthly Cycle Limit previously set at $10,000. After a review of those requests showed that 99% were approved, the maximum Monthly Cycle Limit has been raised to $25,000. Program Administrators can now manage monthly cycle limits on their cardholders' accounts up to the new limit without prior approval from the State Cards Program Manager. Program Administrators should continue to actively manage cycle limits based on cardholder historical spend & purchasing needs and are encouraged not to default to the maximum allowed under policy.

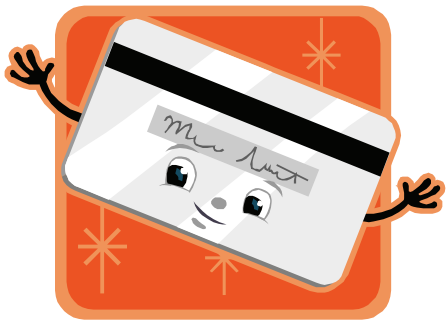
Purchases from Statewide Contracts, Agency Contracts and/or mandatory sources: As in the previous versions of the P-Card Policy, purchases on the P-Card from Statewide Contracts, Agency Contracts and mandatory sources such as Georgia Correctional Industries (GCI) can exceed the $5,000 single transaction limit and the new $25,000 monthly cycle limit. The new policy revision clarifies that P-Card Program Administrators can adjust cardholders' single transaction and monthly cycle limits to accommodate these purchases without prior approval. Documentation should show that the adjustments were made to permit a purchase from one of these sources. Changes to the limits for any other reason still require prior approval.

Clarification of Food Purchases: After limit increases, the second most common request for policy exceptions involved the purchase of food. A category added to the new policy revision in the *Allowable Purchases* section includes "Food provided for consumption at events or services provided to the general public, state benefit recipients and/or state program participants (other than State employees), or purchased for resale in gift shops, bookstores, etc. and other non-employee meal related use." The idea is to allow food purchases for official functions where the meal recipients are any group other than state employees (for whom meal purchases must adhere to the State Accounting Office's *Group Meal Policy)*.

Clarification of "Personal" Purchases: DOAS frequently receives questions about personal purchases. The new policy revision includes a definition of personal purchases as "purchases of goods and services intended for non-work related use or use other than official State business". In other words, personal purchases include items purchased for one's home or individual use versus use in the office, or related to one's job function. Items such as facial tissues, hand gel or cleansers when purchased with official funds and designated for office use by employees and guests are not classified as "personal" purchases. However, purchases of such supplies to be used at an employee's home would be prohibited.

These are just some highlights of the new P-Card Policy. Please see the entire policy on the Department of Administrative Services, State Purchasing Division Website at http://doas.ga.gov . Click on "Purchasing Card Program", then "Learn more…" under *Features* on the right side of the page. Also, be sure to refer to the Board of Regents, Office of Fiscal Affairs "Business Procedures Manual" for more information on the P-Card.

The P-Card remains a convenient and economical way to pay for purchases you are already making. In today's economy it is more important than ever to manage expenses by avoiding unnecessary costs. National benchmark studies indicate that using the P-Card versus a traditional purchase order can save users more than $60 per transaction and reduce the procurement cycle time by almost 70%! For more information about the State P-Card program and how your department can save time and money on your purchases, contact Paul Kurtz, DOAS State Card Program Manager at paul.kurtz@doas.ga.gov or 404-656-5344.



Fiscal Year 2010 Office of Internal Audit Focus Areas by Michael J. Foxman and Scott C. Woodison

The Fiscal Year 2010 audit plan was presented to the Audit Committee at the May 2009 Board of Regents meeting. Internal auditing standards require that the Audit Committee review the annual plan and ensure that internal audit identifies significant risks at the strategic and operational levels. The Audit Committee has the opportunity to validate how internal audit addresses risks through planned engagements.

The audit plan has traditionally been developed using an assessment of institutional risk issues gathered through surveys, financial statement analysis and other quantitative factors. In keeping with the Office of Internal Audit (OIA) Fiscal Year 2010 – 2014 Strategic Plan, the OIA has re-focused our risk assessment on issues that have been identified through a combination of Enterprise Risk analysis, Ethics and Compliance Hotline results, past audits and feedback from campus auditors and campus management. Using this revised risk assessment process, OIA developed a series of planned audit and consulting engagements designed to best address significant risk issues at both the University System of Georgia (System) level and Institutional levels. The sixteen campus-based auditors will continue to prepare their audit plans based upon an institutional risk-assessment process. This article focuses on the System audit plan.

Through our risk assessment, we have identified areas as having potential negative impact should an event occur and the resulting consequences without proper management and administrative controls. Our emphasis during Fiscal Year 2010 has shifted to recognize that OIA must support the entire System in the System's efforts to manage risks. We therefore are placing additional importance on risk "issues" common across institutions as opposed to individual institutions per se. To address the key risks identified, our Fiscal Year 2010 audit plan focus areas includes the following:

Tuition Revenue – In-State vs. Out-of-State: To ensure that a) students are assessed appropriate tuition amounts, and b) the State's residency and out-of-state tuition waiver policies are consistently and properly implemented.

Unrelated Business Income Tax: To verify that Institutions a) comply with Internal Revenue Service regulations on reporting and paying tax on activities directly engaged in which may be considered unrelated to the exempt purposes and b) identify all potential sources of unrelated business income tax.

P-Cards: To review Institutions compliance with **State of Georgia State Purchasing Card Policy** and **BOR Business Procedures Manual Section 3.3 Purchasing Cards**.

Grants and Contracts: To review adherence with State of Georgia, Board of Regents, and institution guidelines and policies related to pre-award, post-award, reporting, and administration requirements.

Emergency Management Operations: To determine if there is an integrated approach to the management of emergency programs and activities related to the mitigation, preparedness, response, and recovery of all types of emergencies and disasters.

Accounts Receivable: To assess whether Institutions have strong fiscal management practices and proper controls over the collection and management of revenues, such as tuition and fees.

Travel: To determine adherence with **State of Georgia Statewide Travel Regulations** and **BOR Business Procedures Manual Section 4.0 Travel**.

Contract Management: To establish whether a monitoring system is in place for ensuring that a) contracts are accomplished and b) vendors meet their responsibilities.

Student Fees: To verify that student fees are a) used for their intended purpose and b) submitted for advice and counsel in accordance with **Board of Regents Policy Section 704.02 Student Fees and Special Charges**.

Time and Leave Reporting: To report whether all faculty and staff have properly and accurately reported leave in accordance with **O.C.G.A. § 47-3-93 Georgia Code** and **Board of Regents Policy Section 802.07 Leave**.

Stimulus Funds: To assist in the assessment of controls for the planning, awarding, managing and overseeing of stimulus funds.

Payment Card Industry (PCI) Requirements: To verify that Institutions correctly manage and control sensitive credit card data such as account numbers, expiration dates, and account names.

Network Security: To determine whether all University System of Georgia information technology networks are secure from "hostile attacks."

Identity Access Management: To ascertain whether a) individuals have access to data through proper authentication techniques and b) access is appropriate to job responsibilities.

Annual Financial Report(AFR): To review controls for ensuring the a) accuracy of financial reports and b) existence of documentation to support the activity of financial accounts.

Understanding Identification & Access Control Management (IAM) of Sensitive or Confidential Information & Information System Services (part 2 of 3) by Erwin (Chris) L. Carrow

This article is the second in a three part series which examines the implementation of an effective IAM process. This article focuses on the hiring, provisioning, transfer and eventual termination of employees.

Overview:

During reviews of IAM processes performed by the Office of Internal Audit (OIA), there continue to be a number of areas which are identified as requiring improved processes and increased controls. At its highest level, IAM involves Identifying a user, ensuring that the person is who they say they are (Authentication) and then granting the user rights to Access specific data or systems, (Authorization). As a user enters or leaves an institution, or a specific position, they must interact with the IAM system.

Problem:

One often noted problem is the failure to implement a comprehensive and effective solution for Identity and Access Control Management (IAM) that addresses the entire employment life cycle for institution personnel or contracted support resources. This process should address program management and the roles and responsibility for "acceptable use" of information, information systems, and other institutional resources. A critical component in this process is the Human Resources (HR) lifecycle for hiring, transferring, or terminating of employees. This program must clearly define and document an individual's identity, rights, and permissions to information and resources and ensure that an employee is only granted the proper access.

More effective standards and communications are typically needed between the Human Resources department and other university entities to ensure proper implementation of operational IAM procedures. The activities involved in the access provisioning and de-provisioning must be effectively defined and documented. An institution's processes for hiring, transferring, or terminating of employees should not be divided among several different institutional agencies. If it is necessary to have these functions in more than one department, the interfaces between departments must be documented and enforced.

This IAM process should include a "non-disclosure" and "acceptable use" policy. These polices should be properly acknowledged by the employee and implemented to clearly identify how the institution's information and information systems may be used. The policies, standards, and operational procedures for activities and requirements associated with "non-disclosure" and "acceptable use" should be enforced with sanctions for non-compliance.

Solution :

A clear understanding and alignment of organizational processes to business strategy should be documented for hiring, transferring and terminating personnel. Organizational processes should address requesting, establishing, issuing, suspending, modifying and closing of user accounts and related user privileges with associated account management procedures. Procedures should include approval procedures defining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users. Management reviews should be performed regularly of all accounts and their privileges.

For the HR lifecycle IAM employee program process to be effective it must be incorporated into all departments' business practices.

Personnel Security Policy and Procedures: The institution must develop, disseminate, and periodically review / update;

1. A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance. This should include high level objectives and clearly address the expectations placed upon departments implementing policy.
2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

- Position Categorization: Assign a risk designation to all positions and establish a screening criterion for individuals filling those positions, e.g., if students have access to the Banner SPAIDEN screen, will they need a background check since high school "minor" information is contained in this database. Ensure there is a process to review and revise position risk designations and that the process is continually monitored. As job positions or descriptions change, a review should be conducted to ensure security requirements support the change.
- Personnel Screening: Ensure there are documented methodologies / checklists for the process of screening individuals requiring access to institutional information and information systems before authorizing access to these resources. Typically, one general process will not meet all security requirements; it must be flexible yet clearly define the level of graduated security needs or requirements.
- Personnel termination: When employment is terminated, the institution, department, or functional business owner must terminate information system access, conduct exit interviews, ensure the return of all organizational information system related property (e.g., keys, ID cards, building passes, etc.), and ensure that appropriate personnel have access to official records created by the terminated employee. A dedicated checklist should exist to ensure all de-provisioning of access was implemented and validated.

(See page 7)

(continued)

- Personnel Transfer: The institution must review information systems / facilities access authorizations, when individuals are reassigned or transferred to other positions within the organization and initiate appropriate actions such as:
    1. Reissuing keys, ID cards, and building passes
    2. Closing old accounts access
    3. Establishing new account access
    4. Changing system access authorizations
- Personnel Sanctions: Ensure the institution employs a formal sanctions process for personnel failing to comply with established acceptable use of institution resources in accordance with associated policies and procedures.
- Acceptable Use policy implementation: An "acceptable use" policy and its objectives must be clearly defined and documented. An official statement of agreement and understanding for proper handling of sensitive or confidential information (to include a "non-disclosure agreement") or "acceptable use" of resources for the institution must be acknowledged by employees. A properly documented and implemented "Acceptable Use" policy and program should include:
    1. What users are and are not allowed to do with the information, information systems, and other resources of the organization.
    2. Define what sanctions will be applied for misuse or misconduct associated with the information, information systems, and other resources of the institution.
    3. Produce signed documentation, identifying that the members of the institution acknowledge and understand their role and responsibilities for use of the information, information systems, and other resources.
    4. Compliance for "non-disclosure" and "acceptable use" should be defined in practical terms by agency or department business owners for trustees (employees of that department) that utilize sensitive or confidential information, information systems, or other resources on or off campus.
    5. Periodic refresher training to reinforce initial understanding and educate users of any policy or program changes.

These lists are not all-inclusive and only represent key elements of what should be given consideration for the needed documentation and implementation of an effective program. Failure to clearly define, document, and periodically evaluate key processes will result in inconsistent and inefficient operational performance outcomes that could pose a reliability or security risk.

Recommendation:

We recommend that all processes and procedures for the management of operational activities and requirements of an institution employee's information access rights provisioning and de-provisioning throughout the various phases of employment be effectively implemented and maintained per the following requirements.

- Define, document, and periodically review the IAM processes for hiring, transferring, or terminating employees per the guidance earlier defined in the managerial overview for this finding.
- Communicate employee life cycle provisioning and de-provisioning requirements to all key shareholders in administration and associated functional departments.
- Ensure departmental operational procedures are established for "personnel employment" or "contracted support" for the IAM employment management life cycle. IAM procedures for hire, transfer, termination, or temporary contracted access must be clearly defined and implemented.
- Require and reinforce the existing "acceptable use" and "non-disclosure" agreements with sanctions and awareness training.
- More effectively implement the existing "acceptable use" policy, operational procedures, so that they are understood and acknowledge by all users of information, information systems, and other resources.
- Test and assess consistency of documented operational processes and controls to ensure they are measurable and support organizational objectives.

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

Phone:
(404)656-2237

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
www.usg.edu/compliance/