The STRAIGHT and NARROW

October 1, 2009

Internal Audit and Compliance, University System of Georgia, 404- 656-2237

Volume 3, Issue 10

Office of Internal Audit and Compliance's (OIAC) 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 ethical conduct.

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 OIAC team.

Inside this issue:

From the Chief Audit Officer

John M. Fuchko, III

It is a continued honor to be able to reach out to each of you and contribute to improving USG institutions. Those of us in the Office of Internal Audit and Compliance (OIAC) remain committed to providing assurance that our institutions are achieving their key objectives and to helping our institutions achieve those objectives through auditing, consulting engagements, guidance (such as this newsletter) and other assistance as required. Let me briefly highlight some of the special initiatives and other changes currently underway at Internal Audit and Compliance.

- Our name has changed from the Office of Internal Audit to the Office of Internal Audit and Compliance. This change reflects our increased focus on compliance per the direction of the Chancellor.
- The Board of Regents is scheduled to vote on a name change for the Audit Committee. The proposed new name is the Committee on Internal Audit, Risk, and Compliance. This proposed change reflects the tri-legged approach to increased accountability in the USG, i.e., internal auditing, Enterprise Risk Management, and the Compliance and Ethics Program.
- Proactive identification of fraud AND appropriate response to suspected cases of employee malfeasance continues to grow in importance – particularly given the various reporting requirements pertaining to recipients of American Recovery and Reinvestment Act (ARRA) funding. I highly recommend reviewing our new website on Fraud, Waste, and Abuse reporting for additional guidance - http://www.usg.edu/audit/compliance/fraud_waste_and_abuse_reporting/.
- OIAC continues to move forward with implementation of the USG Enterprise Risk Management (ERM) program (see http://www.usg.edu/audit/risk/) and the USG Compliance and Ethics Program (see http://www.usg.edu/audit/compliance/). OIAC is in the process of implementing an ERM pilot at the System Office and a Compliance pilot at Georgia Tech.
- OAIC and our campus auditors will be conducting some audit work pertaining to ARRA reporting and internal controls. Recently, the USG Office of Fiscal Affairs issued BPM Section 22 (http://www.usg.edu/fiscal_affairs/bpm_acct/bpm-sect22.pdf) that pertains to the required oversight for ARRA funds. OIAC recommends that each USG institution review these BPM Section 22 requirements and additional guidance issued by the Office of Fiscal Affairs as these will form the basis of future audit procedures.
- OIAC is in the process of forming an advisory council consisting primarily of USG CBOs and USG CIOs. This advisory council will meet on a periodic basis (3-4 times per year) for the purpose of offering advice, feedback and perspective on OIAC operations, risk issues, and opportunities for improvement.

In closing, please do not hesitate to contact our office with questions, concerns, or recommendations. It is an honor to serve.

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.***

Website:

http://www.usg.edu/audit/

Phone: (404) 656-2237

Fax: (404) 463-0699

Study Abroad Reminders

Based on the OIAC's system-wide review of Study Abroad programs, we would like to remind you to please consider the following when creating or maintaining your institution's study abroad programs:

- Faculty travel and expenses should be paid from department E&G funds; faculty salaries must be paid from department E&G funds.
- Study abroad programs must be approved by the institution's president or president's designee and the Board of Regents.
- The recommended approval form is available here: http://www.usg.edu/oie/facstaff/policies/usg_rfa.pdf
- Each institution should provide its own Study Abroad Handbook to include information on paperwork/authorization, communication, risk management, academic considerations, money management, and budgetary guidelines.
- Appropriate waiver and release forms should be available for faculty, staff, and students; policies and procedures should be clearly outlined; and program requirements should be fully communicated to students and parents/guardians.

Each separate program (trip or course) needs a separate, unique Agency account.

Spotlight on Steve Rosenthal

Steve is a student at Georgia State (GSU) who is interning with the Office of Internal Audit and Compliance.

While at GSU, Steve is an accounting major working towards an eventual Master's in Professional Accountancy. Additionally, he is working on earning his Certified Fraud Examiner certification from the Association of Certified Fraud Examiners.

Steve earned his MBA from the University of Phoenix and his Bachelor's of Science in Journalism and Mass Communications from Florida International University.

An interesting fact about Steve is that he is forming an Internal Audit Student Chapter at GSU and is working with one of his professors to have GSU become an Educational Partner with the Institute of Internal Auditors.

New Credit Card Law Affects Students & Affinity Credit Card Programs by Michelle Frazier

On May 22, 2009, President Barack Obama signed into law the "Credit Card Accountability Responsibility and Disclosure Act of 2009" (Act). Title III of the Act (Protection of Young Consumers) is directly relevant to institutions of higher education and their traditional college-aged students (18-21 years old) and to institutions involved in affinity credit card programs. The Act provisions discussed in this article will go into effect on February 22, 2010.

Affect on College Students

According to Title III, Section 301 of the Act, credit card companies can no longer issue credit cards to consumers under the age of 21 unless they have a co-signer. A student's parent, legal guardian, spouse or any other individual at least 21 years old may co-sign the credit card application with the student. Parents, spouses, or legal guardians of students under the age of 21 can continue to add under-age students as authorized users of credit cards of which the parents, spouses or legal guardians are the primary account holders. However, the parents, spouses or legal guardians must approve in writing any requests for an increase in the credit line. In addition, credit card companies are prohibited from issuing unsolicited credit cards to students under the age of 21.

The Act does not restrict all college students from obtaining credit cards. Students at least 21 years of age may still apply for credit cards. However, the students must submit an application for a credit card and include financial information adequate enough to prove that they will be able to independently repay their credit card debt.

Effect on Institutions of Higher Education

Title III, Section 304 of the Act requires institutions of higher education to publicly disclose any contracts or agreements made with credit card companies for the purpose of marketing a credit card. The Act also restricts credit card companies from offering any gifts or other tangible items to college students in order to induce them to apply for credit cards. The gift restriction applies on campus, near campus, and at any events sponsored by or related to the institution.

Furthermore, the Act provides specific guidance to institutions with regard to managing credit card companies' activities on campus and in educating students. Congress recommends that each institution adopt the following policies related to credit cards:

- Require credit card companies to notify the institution of the location(s) at which they plan to market the credit cards to students
- Limit the number of locations on the campus where credit card companies will be allowed to market credit cards to students
- Include credit card and debt education and counseling sessions as part of the new student orientation program.

Affinity Credit Card Programs

Affinity credit cards are those that display the name, emblem, mascot or logo of an institution. These types of credit cards are marketed to individuals with an affinity or close relationship to the institution, e.g., students and alumni. Some institutions of higher education and credit card companies enter into agreements known as affinity credit card programs. The affinity credit card program consists of an institution and/or an institution's alumni association granting the credit card company the right to issue a credit card bearing the institution's name, emblem, mascot or logo. In return, the institution and/or alumni association receives a royalty from the credit card company that is often used to help fund student and/or alumni activities and services.

Affinity credit card programs are not inherently bad. However, Title III, Section 305 of the Act requires that each credit card company submit an annual report to the Board of Governors of the Federal Reserve System (Board) containing the terms and conditions of all college affinity card agreements with institutions of higher education or alumni associations affiliated with institutions. The credit card company's report must include the following:

- The memorandum of understanding between a credit card company and an institution of higher education or alumni association;
- The amount of any payments made from the credit card company to the institution or alumni association during the period covered by the report and how the amounts were calculated; and
- The number of credit card accounts covered by the agreement that were opened during the period covered by the report, and the total number of credit card accounts covered by the agreement that were outstanding at the end of the period.

Subsequently, the Board will submit the credit card companies' reports to Congress, and the reports will be made available to the public via an annual report.

Overall, the institutions comprising the University System of Georgia are encouraged to keep the abovementioned provisions of the "Credit Card Accountability Responsibility and Disclosure Act of 2009" on their radar as fiscal year 2010 gets underway.

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

This article is the third 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 Department 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:

Contractual obligations and operational practices for Limited Access Agreements or Third-Party security requirements were fragmented or non-existent and failed to be effectively defined, documented, or implemented. The root cause was due to management's failure to clearly define, document, and implement requirements for Limited Access Agreements and Third-Party Agreements for day to day operational support and security requirements.

Solution :

A clear definitive understanding and alignment of organizational processes to business strategy should be documented for out-sourced service and support operations and associated security requirements. Policies, standards, and procedures for out-sourced agency agreements will ensure proper management and control of access to resources for: day to day operations, handling of configuration and maintenance changes, defects and identifying of problems and needed solutions. All institutions should define, document, and implement effective and secure policies, standards, and operational procedures for Limited Access Agreements and Third-Party Agreements. You should ensure the processes for service and support are consistent, effectively communicated, and demonstrate measureable expectations and outcomes.

Documentation and operational processes evaluated during the past audits were typically fragmented, incomplete, or non-existent for various departments evaluated. Those processes that were documented were not understood or applied consistently by all departments. Policies, standards, and operational procedures should address the specific tasks needed to demonstrate that Access Agreement and Third-Party Personnel Security were being clearly defined and managed. Those contractual agreement objectives for IAM, must address requirements and have clearly defined and documented measurable practices and procedures.

The policies, standards, and operational procedures associated with Limited Access Agreements and Third-Party Provider Agreements to be effective should be addressed as follows:

- Limited Access Agreements; institution must complete appropriate access agreements (e.g., non-disclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access. These agreements must articulate the roles, responsibilities, and limitations of all parties involved as well as any additional authorization requirements and associated processes.
- Third-Party Personnel Security; institution must establish personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information systems development, information technology services, outsourced application, network and security management) and monitor provider compliance to ensure adequate security is being maintained.

Practical application and outcomes for an effective IAM governed Limited Access Agreements and Third-Party Provider Agreements program should include:

- A consistent understanding of access requirements and constraints by departmental staff to senior management regarding Limited Access Agreements and Third-Party Provider Agreements policies, standards, and procedures.
- An identifiable framework (structure and resources) for processing access interdependencies and requirements for internal agencies and / or departments working with external organizations or out-sourced service and support agencies.
- A definition of key roles and responsibilities related to the agreements / contracts, how those duties are conducted, and the communication and execution of requirements throughout the chain of command for all parties, agencies, or departments involved for the out-sourced support.
- A managed and secure exchange and execution of responsibilities related to information or access to information systems by your institutions' personnel and Third-Party providers.

(continued)

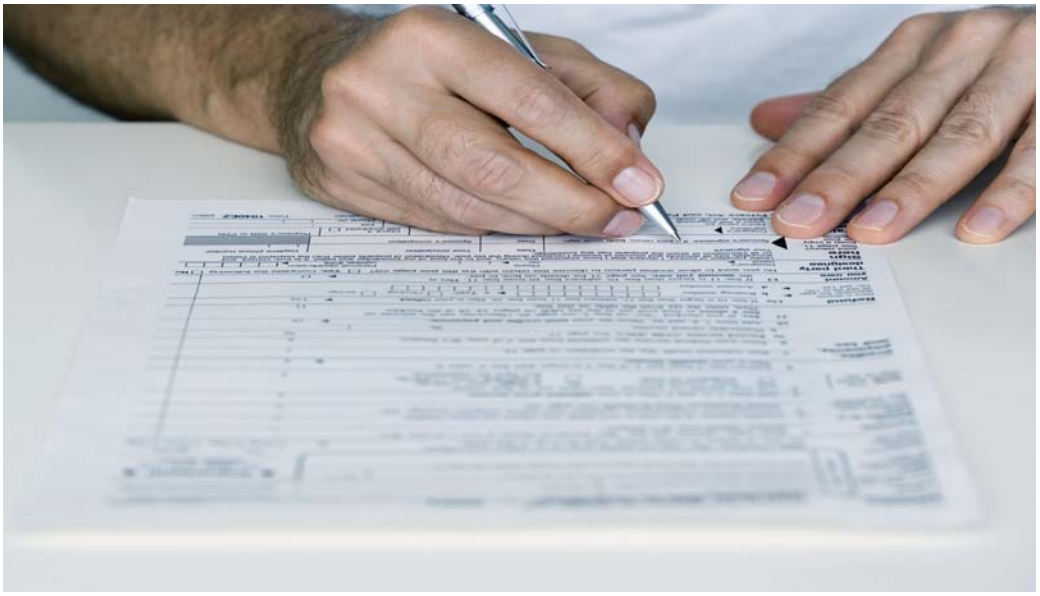
This list is not all-conclusive and only represents key elements to be given consideration for the needed documentation. Failure to clearly define, document, and periodically evaluate key processes will result in inconsistent and inefficient operational performance outcomes that could pose a liability or security risk. These risk could include: inappropriate resource allocation or reduced system availability; increased likelihood of unauthorized change being introduced to key organizational systems; failed understanding of current operations, security requirements, or changes to organizational needs or technology; security breaches; users failing to comply with security policy; and unavailability of critical IT resources or failure to recover IT system in a timely manner.

Recommendation:

It is recommended that all processes and procedures for Limited Access Agreement and Third-Party Agreements be clearly documented for the implementation and maintenance of an institutions information and information system services and support requirements.

- Define and document current process for critical or high risk operations and security controls involving contractual agreements.
    1. Ensure access control procedures exist to control and manage system and application rights and privileges according to the organization's security policies and compliance and regulatory requirements.
    2. Ensure systems, applications, and data have been classified by levels of importance and risk, and that the process' functional business owners have been identified and assigned.
    3. Ensure user provisioning policies, standards and procedures extend to all system users and processes, including vendors, service providers and institutional or business partners.
- Review all current Limited Access or Third party agreements or contracts to ensure your Information Technology department in conjunction with other departments has coordinated access and support requirements.
- Test and assess consistency of documented processes and controls to ensure they are measurable and support organizational support and security objectives.

UBIT – IRS Form 990-T Unrelated Business Income by Sally Carter



A public university may have to file a 990-T by November 15, 2009 if it receives income from business that is not substantially related to the institution's exempt purpose. This means that the income does not contribute importantly to accomplishing the exempt purpose of the institution (i.e., higher education). If the business is conducted on a scale that is larger than is reasonably necessary to perform the exempt purpose, it does not contribute importantly to the exempt purpose.

Risk Assessment:

- Compliance risk is medium to high since a survey questionnaire was sent out by the IRS in October2008 to 400 universities in order to determine compliance levels based on 2006 data. Chances are the IRS will increasingly scrutinize public universities' and associated cooperative organization's 990-T filing in the future.
- Financial risk is low to medium since in most cases unrelated business income is a small portion of college/university income. However, the compliance threshold is low (**unrelated income greater than $1,000 must be reported**) and could easily apply to all schools. Non-compliance is subject to interest and penalties which can increase the tax burden.

Based on discussion with state auditors and several CBOs/controllers at Georgia universities, most CBOs are aware of UBIT either from CBO listserv discussions or NACUBO postings and articles. R1 universities have filed Form 990-T for several years. Medium to large universities knew of the survey and the Form 990-T requirements. However, all USG institutions should review these requirements in order to determine what compliance requirements apply to them.

Board of Regents of the University System of Georgia
Office of Internal Audit and Compliance
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/