The STRAIGHT and NARROW

July 2014

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

We have three strategic priorities:

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

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

3. Build and develop the OIAC team.

Inside this issue:

From the Chief Audit Officer   John M. Fuchko, III

Turning our Focus Towards Information Security

The OIAC will be turning our attention towards Information Security issues in the upcoming months.

The USG stores the personal information of hundreds of thousands of individuals associated with our student and employee records. Cloud computing, social media, mobility tools, and other advanced technologies have created new internal and external security challenges and risks that impact higher education. The OIAC is assessing these risks and looking at ways to partner with Information Security and Information Technology to further define and structure information security programs to counteract these emerging threats.

Our part of the security process is to provide assurance that the USG has implemented proper safeguards to protect vital data. To this end, the USO Information Security (INFOSEC) Audit will assess the effectiveness of information security controls in the University System Office (USO) and the implementation of the USG INFOSEC program. We will assess the adequacy of the governance structure provided by the USG Information Security and ePrivacy team to the USG institutions and other entities.

The IT Security audit will primarily focus on the USO, however, it will extend to USG institutions and other entities for more detailed testing. Our goal is to identify potential weaknesses in USG's IT security protocols in order to adequately address emerging threats and risk.

The OIAC will review specific issues, such as:

- Organizational adherence to the USG IT Handbook and security protocols,
- IT Security Management practices designed to ensure confidentiality, integrity and availability of information, data and IT services
- IT Security Plans outlining the appropriate level of security, asset inventory and risk assessment
- Encryption mechanisms to protect access sensitive data
- Procedures to manage review of user accounts and related privileges; and
- Approaches to addressing and managing responsiveness to a security incident

The OIAC will provide additional information regarding this review in the near future.

I look forward to hearing your thoughts. Please feel free to contact me at john.fuchko@usg.edu or 404-962-3025. Our Rolling Audit Plan may be found on the OIAC website located at: www.usg.edu/audit/internal_audit.

John M. Fuchko, III
Chief Audit Officer & Associate Vice Chancellor

Athletic Program Review

USG Policy on Auxiliary Enterprises and Intercollegiate Athletics

BOR 4.5 Intercollegiate Athletics outlines the policy on establishing and funding intercollegiate athletic programs.

BOR 7.2.2 Auxiliary Enterprises Revenues and Expenditures provides guidance on funds spent and earned through enterprises activities related to the mission of USG institutions.

Auxiliary enterprise operations should operate on a self-supported basis with revenues derived from student fees and other non-state sources. Axillary Enterprises include [but are not limited to]:

- *Housing;*
- *Food Services;*
- *Student Health Services;*
- *Student Activities;*
- *Intercollegiate Athletics;*
- *Parking;*
- *Transportation;*
- *Stores and Shops; and*
- *Vending and Other Services.*

Overview and Purpose

Athletic programs can potentially be one of the most financially promising auxiliary operations managed by a University. Intercollegiate sports in all forms provide Universities with the opportunity to generate revenues for special purposes not payable using "public" funds or tax payer dollars.

Some basic tenets of auxiliary operations include:

- It must be self supporting—each auxiliary operation should generate enough revenue to pay for the expenses incurred by an institution to provide the service. This may include expenses for staffing, plant operations and facility maintenance, etc.

- It must have a dedicated source of revenue—the provision of the service and the expenses attributable to the provision of the service must be self-supported with revenues derived from student fees and other non-state sources.

The amount of resources expended and cash collected through an auxiliary program can create intentional and unintentional opportunities for fraud, waste and abuse, potentially jeopardizing the University's integrity and reputation.

The upcoming USG audit will initially examine one auxiliary enterprise— Intercollegiate Athletics. BOR 4.5— Intercollegiate Athletics outlines USG policy on university athletics. The policy governs an institution's establishment of intercollegiate athletics, expansion of sports, changes in intercollegiate athletic competition levels, and funding of intercollegiate athletics programs." (BoR minutes, March 2013).

The purpose of BOR 4.5 is to define two issues: 1) responsibility to establish the importance of athletic programs, and 2) establish some parameters for implementing and managing the activity *...in an ethically and fiscally responsible manner consistent with the rules, regulations, and principles of the national intercollegiate*

Athletic Program Review

athletic associations and the conferences with which the institutions are affiliated (BoR minutes, March 2013).

The policy also defines the requirements for program oversight, identifies the person/entity responsible for the operation of the athletic program, an finally, establishes the approval process for an athletic program and/or expansion of an existing program. Most significantly, the policy outlines the institutions' responsibility for:

- ensuring athletic program funding requirements are achieved
- distributing athletic scholarships to students
- maintaining financial viability
- and providing audit reports to the USG Chief Audit Officer.

The BOR 4.5 is lengthy and very explicit on the role, responsibilities and requirements for maintaining an athletic program. This policy will establish the basis for the upcoming audit program.

Audit Program Objectives

The upcoming USG Audit will review all existing USG athletic programs.   The audit will consist of an assurance and operational review.   Our first objective is to assure the USO that proper safeguards are in place to adhere to policy, procedure and operational practices.   We will also seek to identify potential best practices and other similar efficiencies that may be relevant to USG operations.

Our second objective is to determine the level of compliance of USG athletic programs with existing policies and procedures, especially those related to internal controls designed to mitigate significant risks (e.g. continued financial viability, inter-athletic conference program participation, safety and athletic students success).

Our review will incorporate many different aspects of athletic operations, including the following:

- Allocation and administration of out-of-state tuition waivers to student-athletes
- Governance structure and characteristics for athletic programs
- Descriptive characteristics of the programs, such as the number of teams, student-athletes, type and gender of sports
- Financial characteristics of athletic programs and teams
- Program and team staffing models

The OIAC is still in the process of developing and testing the sufficiency of the audit program. We want to ensure the program is properly vetted before it is released to institutions. We estimate distributing the audit program by September 2014. It will also be published in the next Straight and Narrow.

Georgia Department of Audits and Accounts: FY 2013 Audit Results
Common Audit Issues
By Ted Beck, OIAC

The Georgia Department of Audits and Accounts (DOAA) recently completed their work for with the FY 2013 audit cycle. These engagements vary across institutions, and take one of three forms: 1) a full financial statement audit, 2) a full disclosure management report, or 3) agreed-upon procedures. The scope and level of detail for these engagements is defined by the audit type, with full financial statement audits being the most comprehensive, and agreed-upon procedures focusing only on selected areas of testing.

The overall results of the FY 2013 audit cycle demonstrate positive change, most notably the identification of only two material weaknesses at a single institution, in comparison to the FY 2012 cycle, which had eight material weaknesses at three different institutions.

The following sections highlight the three most common types of issues across the USG resulting from the FY 2013 audit cycle, as well as recommended resolutions and other means of mitigating these control deficiencies.

Financial Reporting
As DOAA's work as an external auditor is largely concerned with the fair presentation, in all material aspects, of each USG institution's financial position; the most common category of findings was related to the accuracy of financial reporting practices. Forty-one separate

deficiencies, ranging in impact from material weakness findings to verbal comments, were associated with this category of exceptions. The most severe of these exceptions identified "significant and material errors and omissions" within both budgetary and financial statements presented by the institution for audit. Other common deficiencies included the following:

- Subsidiary ledgers that could not be reconciled to the general ledger (or that did not provide appropriate documentation for various journal entries);
- Inaccurate or inadequate tracking of capital assets, including incorrect lease purchase obligation calculations; and,
- Incorrect posting of scholarship allowances, resulting in understatements of allowances and overstatement of fellowships.

Though most deficiencies reported in this category were not of a significant or material nature, repeated or systemic findings in this area could be viewed as evidence of inadequate financial management and accounting controls. We recommend that all USG institutions ensure appropriate resources are dedicated to the financial management and reporting functions, and take advantage of opportunities such as the year-end financial statement workshops. Finally, institutions should seek clarification or guidance from University System Office staff responsible for

# of Issues

- Financial Reporting — 41
- Financial Management — 29
- Financial Aid — 17
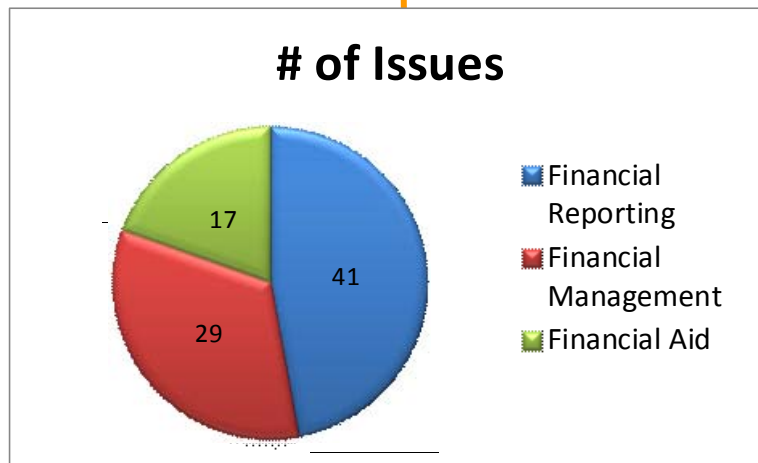
Common Audit Issues, Cont'd

the Consolidated Annual Financial Statements as needed to enhance the accuracy and reliability of these materials.

Financial Management

The second most common category, representing 29 separately identified deficiencies, were exceptions related to financial management practices and, more generally, issues regarding the controls for those practices. Specifically identified issues included the following:

- Incorrect proration of summer tuition between fiscal years;
- Recognition of expenditures and other payables in the wrong accounting periods; and,
- Failure to appropriately collateralize institutional checking accounts.

While the impact and severity of the findings identified in this area were largely of a limited nature, as with exceptions related to financial reporting, repeated or evidence of systemic control issues can result in more significant audit concerns. We recommend that USG institutions carefully assess the internal control structure for their respective financial management processes, and ensure that the associated risks be effectively mitigated. The USG Business Procedures Manual offers substantive guidance for most common business practices within the USG enterprise, to include the appropriate control structures for those activities.

Financial Aid

Findings related to the administration of financial aid at USG institutions represented the third-most common area of exceptions, totaling 17 separately identified deficiencies. Eight of these 17 findings (47 percent) were classified as significant deficiencies,

giving an indication of the severity of the exceptions identified in this area. The most commonly identified deficiencies included the following:

- Incorrect calculation and/or untimely return of Title IV award payments to the U.S. Department of Education for students officially and/or unofficially withdrawing from the institution, including
  ⇒ Improper determination of student financial aid need; and
  ⇒ Errors in the methodology for and/or the assessment of student satisfactory academic progress.

The ability of USG institutions to accurately administer and disburse federal financial aid to students is of critical importance given the system's reliance on this funding as a revenue stream. Financial aid awards represent about 70% of the approximately $2 billion in tuition recognized by the USG each year. Thus, USG institutions must ensure the necessary controls and well-defined business processes related to the administration of federal financial aid are in place. We recommend that USG institutions remain up-to-date on training

Common Audit Issues, Cont'd

and compliance requirements for federal financial aid by participating in collective enterprise meetings such as the USG Financial Aid Directors meetings and other state- and nationally-based organizations such as the Georgia Association of Student Financial Aid Administrators (GASFAA), Southern Association of Student Financial Aid Administrators (SASFAA), and National Association of Student Financial Aid Administrators (NASFAA).

Ted Beck, Audit Manager
Office of Internal Audit & Compliance
Telephone: 404-962-3023
Email: ted.beck@usg.edu

Take-Aways from the
OIAC and the Association of University and College Auditors (ACUA)
Georgia Conference, May 2014

The BOR Office of Internal Audit and Compliance (OIAC) and the Association of University and College Auditors (ACUA) co-sponsored our fifth annual Georgia Audit conference held at Clayton State University Conference Center. The conference theme was Enrollment Management. The program featured elements of Enrollment Management as a continuum, beginning with the process of recruiting prospective students, admitting students, authorizing financial aid, mentoring and implementing strategies for at-risk students assuring campus safety, providing housing, , and finally graduating successful well-educated citizens!

Eleven speakers representing seven USG institutions presented. The President's panel with Dr. Cheryl Dozier, President, Savannah State University; Dr. David Bridges, President, Abraham Baldwin Agricultural College; and Dr. Kyle Marrero, President, University of West Georgia spoke about their perspectives on the importance of enrollment management strategies and how to engage the entire campus community. This was a key take-away—"**enrollment management is everyone's business**".

Our guest speakers included two Special Agents of the Office of Inspector General, Jason Moran who discussed institutional fraud issues and Yessyka Santana who discussed the seriousness of financial aid fraud; Louis Negron of United Way of Atlanta discussed Non-Profit Initiatives Promoting Higher Education; and Attorney Scott Killingsworth presented issues pertinent to Driving Compliance Results through Ethical Leadership and Organizational Culture. These presentations provided training beyond the boundaries of recruitment and admissions and demonstrated comprehensive techniques that can be incorporated into improving enrollment management strategies at institutions. This was a second key take-away—**incorporate subject matter from diverse areas to enhance enrollment management discussions and strategies**.   A third key take-away gleaned from Georgia State University, Dr. Renick's presentation —**use data analytics to help identify students at-risk of not achieving academic progress.**

Many thanks to participants who attended the conference and all of the speakers! Next year, ACUA will sponsor the Mid-year conference in Atlanta, so OIAC invites auditors, accountants, and business officers to attend the ACUA conference.

Sandra Evans, Auditor, OIAC

Institutional Effectiveness
"Think Compliance First"
Guest Contributor: Deann M. Baker, Managing Director
Compliance Advisor Specialists, LLC

You might wonder how it is that a person or an organization would consider or "think compliance first."   We "think compliance first" by contributing to the development of a "Do the right thing" culture. To understand how we all contribute to such a culture, we need to evaluate the following definitions:

1. Culture is the set of shared values and goals that an organization follows. Culture is what sets an organization apart from its peers.

2. Values are often wide-ranging ideals regarding the right course of action.

3. A value system is a set of consistent values and measures.

4. Compliance programs are systematic procedures established by an organization to ensure that requirements of the regulations imposed by a government agency are met.

Organizations communicate their value system through written standards of conduct, often referred to as a *Code of Ethics or a Code of Conduct.* These documents are the foundation of an organization's policies and procedures, and provide statements of the intention to comply with requirements it must meet. Values give us a sense of what is right and wrong, and help us to know the "right course of action" to take. One of the purposes of a compliance program is to help create a "Do the right thing" culture.

There are guidelines that tell organizations how to design and implement effective compliance programs. These guidelines address several requirements, including the need to create an ethical culture by (1) exercise due diligence to prevent and detect criminal conduct; and (2) promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law."

A value system is a set of consistent values and measures. There is an old saying that what gets measured gets done. This is also true of incentives. It is helpful if management ties workforce incentives to expected performance. The guidelines for designing and implementing compliance programs also address incentives, and state: "The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through appropriate incentives to perform in accordance with the compliance and ethics program." An example of compliance activities that can be measured and can incentivize is the participation of the workforce in assigned compliance education and/or completion of certain policies and procedures that address the organization's risks. "Do the right thing" culture.

Everyone has a part in creating an ethical culture, whether it is incentivized or not. When we all do our part to "do the right thing," we are "thinking compliance first."

Information Technology—Understanding Data Breach
Kenyatta Morrison, OIAC

Understanding Data Breaches

Any institution that houses critical assets such as Social Security numbers, Credit Card numbers, intellectual property or other proprietary data is at risk of a data breach. The size of the institution does not matter. A data breach is an incident where personally identifiable data is accessed and/or stolen by an unauthorized source. The data can be compromised by an outside party, such as a hacker, or by an internal party (perhaps a disgruntled or recently terminated employee).

The US Secret Service 2011 Data Breach Investigations Report described common traits of data breaches as:

- *83% of victims were targets of opportunity*
- *92% of attacks were not highly difficult*
- *96% of breaches were avoidable through simple or intermediate controls*
- *89% of victims subject to Payment Card Industry Data Security Standard (PCI-DSS) had not achieved compliance*
- *76% of all data was compromised from servers*
- *86% were discovered by a third party*

But, when a "data breach" is reported, many people associate violations with companies like Target, Neiman Marcus and Michael's. **Why?** Each of these companies have been victims of recent data breaches where the personal information of its customers was compromised.

Data breaches have also occurred at universities across the country.   In February of this year, an outside source gained access to a University's secure records database and obtained more than 300,000 personal records for faculty, staff and students dating back to 1998. The records included name, social security number, date of birth and University identification number. The hackers did not change anything within the University's computer system, but did duplicate the information. In response to the intrusion, state and federal law enforcement authorities investigated the incident. The University contacted each of the affected individuals to offer free credit monitoring service.

Below are examples of data breaches that occurred at other Universities across the country this year:

- Unauthorized access to a database, for one of its grand funded projects administered on the campus, containing personally identifiable information for an estimated 50,000 individuals.
- Staff error left information on 146,000 students exposed for 11 months.
- Names, email addresses and phone numbers of as many as 1,307 current and former students were stolen from a web server and posted online by a hacker.
- Server containing the information of 291,465 former, current, and aspiring students and 784 employees was hacked.

Data Breaches can be costly to Institution

The [Chronicle of Higher Education](#) reported that costs of data breaches at universities can run into the millions. Even though there may not be any reports regarding illegal use of the compromised information, the institution is still required to respond.

Expenses incurred in response to a data breach may include:

- Notifying all affected individuals
- Setting up a call center to field questions from those affected
- Hiring IT forensics consultants to investigate
- Providing credit protection services to all those affected
- Obtaining legal representation for your institution

A 2013 study published by the Ponemon Institute reported that the average cost of a data breach in higher education is $111 per record. This can be an unexpected expense, as few institutions have a line item in their budget for "data breach". In addition, cybersecurity insurance in higher education is a fairly new phenomenon and rarely purchased. While there is data available on the average financial cost to an institution, the damage to an institution's reputation cannot be appraised or determined.

How can an Institution safeguard against data breaches?

The open technology architecture found at universities allows faculty and students to do their work with ease, but open technology architecture opens the environment to exponential security risks. To reduce the chance of a data breach at an institution, the institution must assess its vulnerabilities and take steps to help prevent data breach. Some low-cost steps can include:

- Develop an IT risk management plan that includes a description of all systems used, the data stored and processed, and assign ownership for the protection of the data.
- Educate faculty, staff and students on the need to protect sensitive data and the mechanisms available to provide such protection.
- Delete data that is no longer needed.
- Prohibit the transmission of sensitive information over unencrypted, unprotected email.

EVERYONE has a role in preventing a data breach. It is no longer acceptable to look at data breaches from the "if" perspective, but it must be looked at from the "when" perspective. By treating the protection of data as an ongoing practice, your institution can help reduce the likelihood of exposure, minimize a potentially costly data breach; and be prepared to respond when the notification comes, *"We've had a data breach".*

[Kenyatta Morrison](#)
Director of IT Audit, OIAC
Telephone: 404-962-3028
Email: kenyatta.morrison@usg.edu

PROMOTING AN ETHICAL CULTURE: THE ETHICS & COMPLIANCE REPORTING HOTLINE

HOTLINE CONTACTS

If you are aware of fraudulent activity related to the University System of Georgia or simply want to suggest an improvement to ongoing operations, we want to know about it! You may anonymously report online or call us at: 1-877-516-3466.

Ethics and Compliance Reporting Contacts

In January of 2008 the University System of Georgia's (USG) Ethics & Compliance Reporting Hotline became operational. The hotline is just one part of a comprehensive ethics and compliance program which is designed to promote the highest standards of ethical and professional conduct within the USG. The following are the answers to frequently asked questions regarding the hotline.

Question: What is an Ethics & Compliance Reporting Hotline?

Answer: The hotline is a way to confidentially report concerns regarding fraud, waste, and abuse and any other improper, unprofessional, or illegal activity within the USG. The hotline does not replace existing reporting mechanisms, to include reporting concerns to an employee's supervisor, but rather serves as an additional reporting option, which may be used anonymously.

Question: How do I make a report?

Answer: Reports can be made on-line or by telephone 24 hours a day, 7 days a week. Each institution and the System Office have a hotline web address and a telephone number assigned to it. A list of the web addresses and telephone numbers for each institution and the system office can be accessed from the following web address:

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

Ethics and Compliance Reporting Contacts

🖨 Print friendly   ✉ Email or share

"ETHICS AND COMPLIANCE REPORTING HOTLINES" FOR USG INSTITUTIONS

- Abraham Baldwin Agricultural College
- Albany State University
- Armstrong State University
- Atlanta Metropolitan State College
- Bainbridge State College
- Clayton State University
- College of Coastal Georgia
- Columbus State University
- Dalton State College
- Darton State College
- East Georgia State College
- Fort Valley State University
- Georgia Archives

On the Ethics and Compliance contact page, select the link for your institution.

Question: Who can make a report?

Answer: Reports can be made by any USO employee, student or the public.

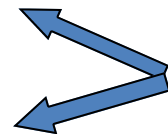**Question: Will my report by confidential?**

Answer: All reports will be treated in a confidential and professional manner. Those who make reports can choose to identify themselves or remain anonymous. The hotline is administered by a 3rd party vendor which provides for confidential communication. Those making reports will be provided with a Personal Identification Number and instructions so they can follow-up with additional information or simply check on the status of a report.

PROMOTING AN ETHICAL CULTURE: THE ETHICS & COMPLIANCE REPORTING HOTLINE

Frequently Asked Questions

Question: What should be reported?

Answer: Employees should report violations of state or federal law and violations of USG policies. Employees should also report concerns regarding unprofessional or unethical practices. Of special concern are fraud, waste and abuse in that these types of malfeasance directly affect our stewardship responsibilities.

Question: What should not be reported?

Answer: The hotline should not be used as a tool to harass, embarrass or undermine co-workers or supervisors or to settle old scores. Reports should only be made in good faith where there is a reasonable belief in the truth or accuracy of the information provided. Any employee who knowingly files a false report may be subject to disciplinary action up to and including termination.

Question: Would I be subject to retaliation?

Answer: State law and USG policy prohibit any employee from retaliating against another employee who, in good faith, has reported concerns or wrongdoing or who has cooperated with an authorized investigation. Employees may make reports of wrongdoing without fear of reprisal.

You can look forward in the next issue of this publication to information concerning the number and types of cases received on the USG hotline since 2008.

Do You Have Questions about Ethics & Compliance Practices or Issues?

What Type of Questions would you like addressed?

I would like to hear from you!

Wesley Horne
Director of Ethics and Compliance, OIAC
Telephone: 404-962-3034
Email: wesley.horne@usg.edu

Reference Reading

Professional Aids

Fraud Auditing and Forensic Accounting, By Tommie W. Singleton, Aaron J. Singleton , John Wiley & Sons, 2012

Effective Interviewing and Interrogation Techniques, By William L. Fleisher, Nathan J. Gordon , Academic Press, 2011

The Internal Auditor's Guide to Risk Assessment, The IIA Research Foundation, Rick A. Wright Jr., 2013

Management Aids

10 Key Techniques to Improve Team Productivity: A Guide to Developing Your Team's Full Potential, The Institute of Internal Auditors Research Foundation, Hernan Murdock, CIA, 2011

Reviewing Kettering Foundation Studies of the Role of HIGHER EDUCATION in American Democracy, Kettering Foundation, 2012

Board of Regents of the University System of Georgia

Office of Internal Audit & Compliance (OIAC)
270 Washington Street, SW
Suite 7093
Atlanta, GA 30334-1450

Phone:
(404) 962-3020

Fax:
(404) 962-3033

Website:
www.usg.edu/audit/

? Ask the Auditor ?

If you have a governance, risk management, compliance or control question that has been challenging you, let us help you find the answer. Your question can help us to become better auditors.

Want to Contribute to the Straight and Narrow?

We invite you to send your questions and ideas for future articles to us for feature in upcoming Straight and Narrow newsletters.

Contact Us: USG-OIACNewsletter@usg.edu