The STRAIGHT and NARROW

Volume 3, Issue 13

July 1, 2010

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

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:

Questions for Leaders Erwin Carrow, Director of IT Audit

We promised to publish a "Questions for Leaders" column in this edition of the "Straight and Narrow." Following are questions (grouped by category) that leaders may wish to ask pertaining to the administration of various programs and processes at their institution. Please note that the questions represent areas that we anticipate including in our audit procedures for future engagements.

Ensuring the Protection and Security of Information Resources - Perimeter and Network Security

Are we securely exchanging sensitive and confidential information throughout our network and with outside agencies? What steps have been taken to protect and monitor these types of secure transmission? Have the appropriate steps been taken to comply with the various federal and industry standards, e.g., FERPA, HIPAA, PCIDSS, etc.? How are inappropriate personnel being denied access to campus Information and resources? How is the campus monitoring for malicious activities that could disrupt normal communications?

Protecting Access to Critical Business Information - Identity and Access Control Management

How is individual access being managed by department leadership to critical business applications that contain sensitive or confidential information, e.g., Banner, PeopleSoft, etc.? How often are access rights and privileges reviewed to ensure appropriate access has been granted and is still needed. How are you ensuring that access granted to an individual from different departments does not violate "segregation of duty" requirements for critical business functions? What method does the Human Resources department employ to ensure new employees understand their role and responsibilities for receiving, creating, handling, storing, and destroying of sensitive or confidential information? How are access rights and privileges being de-provisioned or reallocated for transferred or terminated employees? Do 3rd party agencies' or vendors' contacts contain the appropriate provisions and conditions for network access or exchange of sensitive or confidential information to ensure due diligence?

- Board of Regents Policy Manual, § 7 Information Security Policy http://www.usg.edu/policymanual/section7/policy/7.12_information_security_policy/
- Office of Information Security Policy and Compliance http://www.usg.edu/infosec/policy_management/policies/
- Board of Regents Policy Manual, § 10 Information, Records, and Publication http://www.usg.edu/policymanual/section10/
- USG Business Procedure Manual (BPM) § 12 Protection and Security of Records http://www.usg.edu/fiscal_affairs/bpm_acct/bpm-sect12.pdf
- Health Insurance Portability Accountability Act (HIPAA) § 164 Security Standards http://www.dhhs.gov/ocr/combinedregtext.pdf
- Federal Register, Department of Health Services, Health Insurance Reform: Security Standards; Final Rule; Vol. 68, No. 34, http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf
- Higher Education Opportunity Act (HEOA) § 110–315 http://ed.gov/policy/highered/leg/hea08/
- PCI Compliance (PCI DSS) https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Suggestions for future topic areas should be emailed to Karen LaMarsh at karen.lamarsh@usg.edu.
In addition to "traditional" audit services, OIAC also performs consulting services. This involves working with senior campus management in jointly developing recommendations and potential action plans on an identified issue or challenge. For instance, we are currently working with an institution in integrating new housing operations in day-to-day campus life. This involves developing the proper organization structure, addressing policy and procedure issues, and accounting for revenue and expenditures. If you are interested, please contact John Fuchko at john.fuchko@usg.edu

Are You PCI Compliant?

by Scott Woodison, Director of Compliance & Enterprise Risk

The Payment Card Industry Data Security Standard (PCI DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. This comprehensive standard is intended to help organizations pro-actively protect customer account data.

Here are some suggestions to help your institution be PCI compliant:

- Do NOT share your IDs and Passwords with others.
- Do NOT store account numbers anywhere unless you absolutely need to. If you need to store, electronic data should be encrypted.
- Do NOT send fully visible account numbers in email.
- Consider truncating (XXXXXXXXXXXX1234) or masking (123456XXXXXX1234) account numbers without the need to encrypt them.
- Do NOT leave printouts that contain fully visible account numbers lying around at your desk, printer, or fax machines.
- Store hardcopies (printouts) that contain fully visible account numbers in locked cabinets or locked desk drawers.
- Consider encrypting all files containing account numbers stored on your computer's hard drive or stored on any network shared drives.
- Restrict access to the files containing account numbers, especially those that are unencrypted.
- Encrypt cardholder data that is to be stored or transported on flash drives, magnetic tapes, CD ROMs, laptop computers, floppy disks, etc.
- Report to your supervisor immediately any situation that you think may not be compliant.
- Follow PCI policies at all times, including during development, testing, and live production.

For more information about PCI Compliance, click here and contact:

For additional information on PCI Compliance and other IT Security issues, please contact USG Chief Information Security Officer Stanton S. Gatewood, infosec@usg.edu, 404-657-0353.

Copier Security by Sterling Roth

Editor's Note: We appreciate Sterling Roth's contribution to our newsletter. He is the Chief Audit Officer for University Auditing and Advisory Services at Georgia State University

A CBS Evening News investigative report (http://www.youtube.com/watch?v=6pIFUOav2xE) last April began: "At a warehouse in New Jersey, 6,000 used copy machines sit ready to be sold . . . [;] almost every one . . . holds a secret. Nearly every digital copier built since 2002 contains a hard drive – like the one on your personal computer – storing an image of every document copied, scanned, or e-mailed by the machine. In the process, it's turned an office staple into a digital time bomb packed with highly personal or sensitive data."

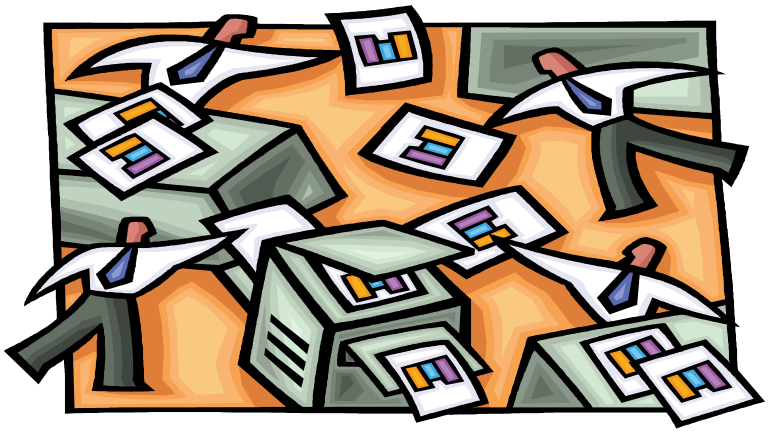
After purchasing four of the machines based on price and pages printed, the investigative team pulled hard drives in half an hour and downloaded tens of thousands of documents in half a day. Police records, medical records, financial records, and even Ground Zero construction plans appeared, courtesy of the previous copier owners. Among them were law enforcement agencies, which did not comment, and a health insurance company, which promised never to let it happen again.

After seeing the investigative report, a college financial officer at Georgia State University (GSU), where I serve as Chief Audit Officer, engaged our office along with campus purchasing, information technology, and risk management officials. The GSU purchasing director contacted the Georgia Department of Administrative Services (DOAS) since DOAS issues the statewide contract for copiers and might already be addressing such issues with vendors. Our campus information security manager, in addition to planning a training/education initiative, noted that risks could be avoided by buying security add-ons from vendors or by ensuring hard drives are erased or destroyed when copiers are returned to vendors or turned in to surplus.

Likewise, professional group listservs and online media soon advanced a multitude of opinions and ideas. Again, vendor security features and actions to remove, sanitize, or destroy hard drives were central. Government also got going. Congressman Ed Markey wrote to the Federal Trade Commission (FTC) on April 29, 2010, urging action. On May 11, 2010, the FTC responded that it "is reaching out to copier manufacturers, resellers, and retail . . . stores to ensure that they are aware of the privacy risks . . . and to determine whether they are warning . . . customers . . . and . . . providing options for secure copying." The FTC assured the congressman that additional guidance would be provided on protecting personal information on digital copier hard drives.

The CBS report closed by amplifying the problem: "The day we visited the New Jersey warehouse, two shipping containers packed with used copiers were headed overseas – loaded with secrets on their way to unknown buyers in Argentina and Singapore." A connection to our institutions' interests was apparent. As our institutions become increasingly high-tech and global, institutional risks do also.

Protecting sensitive data is an important legal and ethical obligation that we all share. Meeting that obligation requires creating awareness and promoting the right actions. In the case of copier security, the need to engage and educate our campuses is evident and essential.



Public Private Venture Program: The Continuing Disclosure Certification Filing

by James F. Winters, III, Public Private Venture Auditor

Overview:

The Continuing Disclosure Certificate filing is for the benefit of the bond holders and is a required annual filing by the foundation. The purpose of the filing is to provide assurance to the bond holders and to comply with the filing requirements as stated in the Official Statement published by the bond underwriter at the time the bond was issued. It is the foundation's management responsibility to insure that the requirements as stated in the Continuing Disclosure Certificate are performed in an accurately and timely manner. It is recommended that these disclosures have an appropriate review by members of the foundation's management team. The Continuing Disclosure Certificate should be filed and records maintained to show proof of delivery and copies of the contents. It is recommended that the annual filing and any reporting of special events be reported to the foundation's board of directors and the event recorded in the board minutes. A notification to the college/university management team should also be evidenced. The Continuing Disclosure Certificate filing is required annually and for the reporting of significant events. This document is signed by the authorized representative of the foundation's real estate LLC.

Procedures for the Annual Filing:

Review the requirements for the Continuing Disclosure Certificate and identify the disclosure requirements including the names and addresses of the receivers. Identify and update the list of names and addresses of the National and State Repositories. This will include the Municipal Securities Rulemaking Board's (MSRB) Electronic Municipal Market Access (EMMA) system. The timing for filing the disclosure annually no later than 150 days after the fiscal year end.

Identify the information that needs to be included with the filing of the annual disclosure certificate. The following are examples of the information that is included.

i. Audited Financial Statements accompanied with the audit report prepared by a CPA.
ii. A notice indicating any accounting principles that changed for the previous fiscal year. If there have been no changes, it is recommended to have a statement confirming that there have been no changes to the accounting principles during the past fiscal year.
iii. A statement indicating that the fiscal year has not changed.
iv. The reportable information for the preceding fiscal year may include; analysis of State General Fund Receipts, summary of appropriation allotments to the Board of Regents, actual to bond pro forma analysis, enrollment numbers, admissions, tuition, fees, and a reference to the official statements of all other debt issues.

Procedures for a Significant Events Filing:

Examples for filing a "Notice to Repositories of the Occurrence of a Significant Event" include:

i. Principal and interest payment delinquencies.
ii. Unscheduled draws on the debt service reserve.
iii. Unscheduled draw on credit enhancements.
iv. Substitution of credit of liquidity providers.
v. Rating changes.

Once a bond is paid in full, identify and perform the requirements for notification for bonds that have been paid in full.

It is recommended that copies of these filings be sent to the Bond Issuer, Underwriter, Trustee, the Chief Business Officer for the college/university and to the foundation's board of directors. This event should be recorded in the foundation's board minutes.

Reminders:

- This document is signed by the authorized representative of the foundation's real estate LLC.
- Review the procedure for document retention for these filings.
- Discuss with the University System Office any communications with Moody's or Standard & Poor's.

HOPE….for Compliance by Beverly A. Boggs

Editor's Note: We appreciate Dr. Beverly Boggs' contribution to our newsletter. She is the Executive Director of Academic Admissions and Student Financial Aid at the Medical College of Georgia.

It is no secret among Student Aid professionals that the convoluted rules associated with HOPE eligibility make the process of ensuring compliance an enormous exercise. I am sure there are seasoned professionals in the state of Georgia who can recite the HOPE eligibility rules in their sleep and possibly even have Banner developed with such sophistication as to answer every challenge. With that being said, there is no replacement for human intelligence and review to ensure full compliance. I can share some lessons learned that have helped us manage this massive program. The actions described here aren't all inclusive, but have provided some much needed management techniques to give us "HOPE" for compliance.

Lesson #1: It really does "take a village" to keep an eye on compliance issues.

HOPE eligibility, determination of awards, and reconciliation has multiple pieces that must be considered. One set of eyes to review eligibility and complete reconciliation just aren't enough. Have you ever written a paper for school or a policy and procedure for your area of responsibility and because you're so familiar with it, even spell check won't catch certain errors? HOPE has the same flavor. What we look at often seems to pass us by when we look at it for the third or fourth time. A new set of eyes can be immediately drawn to an error. We have recently developed a HOPE review process whereby Student Aid Counselors will complete the top portion of an awarding checklist and one month later, a new set of eyes in Student Aid will review the file for errors *before* invoicing. The review occurs a month later than the start to get past the disbursement rush and still remain in the same term in case errors are discovered and adjustments have to be made. The department has to specifically set aside time for all Student Aid personnel to participate, but it will make the reconciliation process smoother.

How many personnel should review HOPE eligibility hours? How many personnel do you have working in Admissions, Student Aid, and Registrar's Office? Seriously, HOPE compliance shouldn't fall on the shoulders of one person or even one department. Students who have prior academic history (which would include all students for us) have a much greater window for error when determining attempted and paid hours for HOPE. The review of attempted and paid hours should be a shared responsibility with a second set of eyes checking the first. We placed our best transcript evaluator on the front line and she has the authority to place holds in Banner if documentation is missing or needs further clarification. Student Aid personnel also review and confirm her decisions by cross referencing school records to SURFER. Student Aid Counselors comparing SURFER to school records also works to identify those students who forgot to list a previous institution on their admissions application but the history appears on SURFER. Student Aid personnel notify the transcript evaluator in Academic Admissions and the hold is placed on the record until all documentation is received. The placement of a hold signals to Student Aid that progress regarding awards should be stopped until the issue has been resolved.

Lesson #2: If there's a chance you may have to ask for the money back, don't award it until you're sure.

Seems like pretty basic stuff, doesn't it? Not so fast! Some schools will allow students to enroll on a provisional basis if they are finishing up a prerequisite the semester before they start their new program. Sure, you can ask for a prediction of what the outcome of the previous semester will be, but you'd be asking for trouble. Of course students are optimistic about their performance and you will be basing your awarding decisions on optimism instead of fact. Consider this: What if the student is on the edge of the GPA threshold and they don't do as well as they had hoped? Opps! Now you have to change hats and become a collector, creative financier, and public relations expert to deal with the overpayment. For Student Aid personnel, becoming the person who both "giveth" and "taketh away" can be poisonous. I can't think of another type of aid that will allow students to receive the funds before eligibility is <u>absolutely</u> confirmed. HOPE should be no exception.

Unfortunately, this proof of eligibility exercise includes students taking transient classes who are riding the wave of eligibility. The Registrar's Office helps us stay on top of these cases. Remember…. you can go back and award the funds in the same year after you have all the facts. Students who know the awarding policies up front won't be alarmed when they realize they need that transcript for those transient hours to determine their HOPE eligibility. Although it may seem harsh to some, the strict enforcement of this policy will prevent your institution from becoming a *savings and loan*.

HOPE….for Compliance cont'd by Beverly A. Boggs

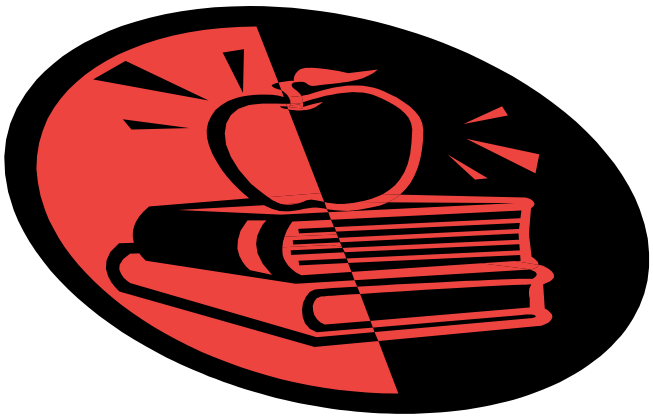
Lesson #3: Review program classifications, hours, and charges annually.

Academic programs constantly review and make changes to their credit hour curriculum, tuition, fees, and method of delivery. The details of changes to each program should be internally logged and shared with multiple personnel for confirmation on an annual basis prior to awarding. A meeting to discuss HOPE eligibility as it relates to each program should occur for all parties that have any impact on the delivery of HOPE. A collaborative effort of all personnel involved in HOPE eligibility determination, awarding, and payment will ensure program changes are clearly understood, adjustments have been discussed among personnel and reflected correctly in Banner. An annual eligibility chart to be included in policy and procedure manuals is recommended and would include:

- Program credit hours allowed for payment,
- Program detail codes, tuition, books, fees, and credit hours that match the list of BOR approved programs and GSFC records.

It seems elementary to even mention this suggestion. However, erroneous assumptions can be made when personnel are busy conducting other business. Since we make time for the things that are important, this process should go on the *list of things to do*. One wrong number here can cost you dearly later.

Eligibility rules associated with HOPE have evolved over time. They have become more complex and difficult to manage. There is no easy process to ensure compliance and many personnel resource hours will have to be dedicated to reviews. If the responsibility for eligibility determination is shared among several departments as a team, the frequency for error and financial liability will be limited.



Preliminary Assessment by Michael J. Foxman

The most successful audit projects are those in which there is a constructive relationship between the audit team and the institution to be audited. One means of achieving such a relationship is to partner upfront, performing a preliminary assessment of operations. Approximately six to eight weeks prior to the start of fieldwork, we arrive on-site for one to two days to meet with the senior management team and perform this preliminary assessment.

What is the purpose of the preliminary assessment?

The goal is to identify areas where OIAC can provide analysis and assistance that will most benefit the area audited or the institution as a whole. The preliminary assessment serves as a tool where we become acquainted with the unique operational issues specific to a campus. The objective is to develop a more complete understanding of the areas which will be audited, prior to the engagement.

Although our risk assessment process identifies areas of potential risk exposure, faculty and staff are most familiar with the daily challenges and opportunities of campus life. Any new developments that may have occurred since the last audit are discussed through interviews with key personnel. Changes in operations and policies and procedures are reviewed. The survey helps to perform an initial assessment of internal controls related to the recording of business transactions, safeguarding assets, compliance with policies and procedures, and promotion of operational efficiency.

The preliminary assessment period is also when institution personnel can convey their areas of concern. We believe that there is benefit to conversation with stakeholders and obtaining their assessment of potential areas of audit focus by asking, "What should we be doing for you?"

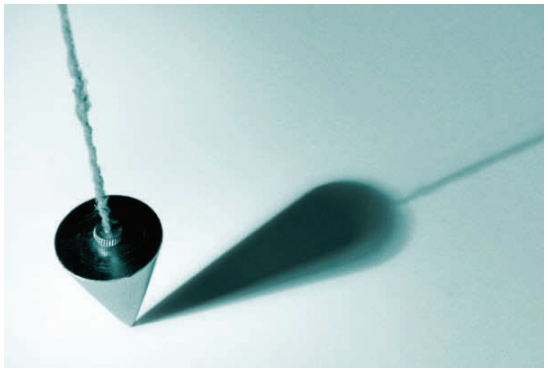
What takes place during the preliminary assessment?

The audit team:

- reviews prior audit reports and other existing information about the institution (much of this is done at our office and will not affect your daily work),
- interviews key employees on how processes work,
- performs initial assessment whether the processes are functioning as described, and
- identifies any additional processes that present risks.

To provide you with the deepest insights, our initial audit plan must remain flexible. The planning of an audit is an iterative, continuous process. We view each audit assignment in the same manner as our audit plan – focus on the high-risk areas that offer the greatest value for resources expended.

At the end of the preliminary assessment stage, the audit team discusses any changes to the planned audit strategy and approach. After reviewing relevant background information and considering the results of this review as a whole, the audit team will identify potential objectives that provide a value-added service to the campus. Where practicable, audit objectives will include items suggested by the management. The audit project manager identifies the final audit objectives and submits these to audit management for approval. Once final objectives are approved, original budgets and timeframes set for the project are adjusted, as needed. The final objectives and information about any changes to the expected duration of the project will be communicated to campus management.



Discussion on Derivative Instruments by Eddy A. Hicks

Editor's Note: We appreciate Eddy Hicks' contribution to our newsletter. He is the Accounting Manager for Statewide Accounting and Reporting in the State Accounting Office of Georgia.

The Government Accounting Standards Board (GASB) has issued Statement No. 53 (Statement), *Accounting and Financial Reporting for Derivative Instruments.* This Statement was issued June 2008 with an implementation date effective for financial statements issued after June 15, 2009.

In preparation for the implementation of this Statement, the State Accounting Office (SAO) distributed a survey to all organizations included in the State of Georgia financial reporting entity. Our objectives for this survey were to introduce the Statement and to create awareness of derivatives and their use.

The SAO has created a policy titled "Derivative Instruments". This policy was distributed for a 30 day solicitation of comment from State organizations on May 12, 2010. A link to the policy will be posted to the Accounting Policy Manual (Revised) index under Derivative Instruments on the SAO's website and should be available by mid June.

As an overview, the objective of Statement No. 53 is to provide the public with more information about the accounting and reporting of derivatives. The number and dollar amount of derivatives entered into by government entities is substantial and has grown rapidly. The complexity and variety of derivatives are also increasing significantly.

The Statement requires that derivative instruments, originally purchased to manage a specific risk, be evaluated for effectiveness. GASB 53 defines effective as "significantly reducing an identified financial risk by providing changes in fair values or cash flows that substantially offset the changes in fair values or cash flows of the associated item being hedged." The Statement requires that derivative instruments be reported in the financial statements at fair value. If the instrument is determined to create an effective hedge, changes in fair value should be deferred. This may require restatement of beginning balance.

Derivative instrument contracts are financial arrangements used to manage specific risks or to produce investment income. Common types of derivative instruments include interest rate and commodity swaps, interest rate locks, options (caps, floors, and collars), swaptions, forward contracts, and futures contracts. A brief description of these derivative instruments can be found toward the end of this article.

Derivative instrument contracts are entered into as investments, as hedges of identified financial risks associated with assets or liabilities, or expected transactions, or to lower the costs of borrowings. Often, they are used to hedge against the risk of rising interest rates or commodity prices that could negatively affect cash flows

A key provision of this Statement is the requirement that derivative instruments be reported at fair value in the financial statements. **State organizations will be required to provide the SAO with the fair value of derivative instruments at 6/30/2010 in addition to supporting documentation required by Statement 53.** Organizations are encouraged to begin planning now to be able to report this information at 6/30/2010.

The following GASB definitions have been included in this article for your convenience. A more complete list can be found in the GASB Statement No. 53 Implementation Guide.

Commodity swaps:
These are contracts that are entered into that have a variable payment based on the price or index of an underlying commodity.

Forward contracts:
This type of contract consist of an agreement to buy or sell a security, commodity, foreign currency, or other financial instrument, at a certain future date for a specific price. One example is an agreement with a supplier to purchase a quantity of heating oil at a certain future time, for a certain price, and a certain quantity.

Futures contracts:
Futures contracts are exchange-traded securities to buy or sell a security, commodity, foreign currency, or other financial instrument at a certain future date for a specific price. This type of contract obligates the buyer to purchase the commodity or financial instrument and the seller to sell it, unless an offsetting contract is entered to offset one's obligation.

Interest rate locks:
An interest rate lock is a type of contract that allow one party to fix an interest rate for a specific period of time much like an individual would lock in an interest rate prior to the purchase of a home.

Discussion on Derivative Instruments cont'd by Eddy A. Hicks

Interest rate swaps:
A rate swap contract is one that has a variable payment based on the price of an underlying interest rate or index. For example, in order to reduce the risk of rising interest rates, and potentially increase interest expense, an agency might enter into an interest rate swap for bonds that have been issued with a variable rate. At the same time, they enter into a contract with a counterparty to pay a fixed rate in exchange for the payment back to the agency an amount based on an index.

Options:
Calls, puts, collars, floors, and swaptions are all examples of Options. They represent contracts or securities that give their holders the right but not the obligation to buy or sell a financial instrument or commodity at a certain price for a certain period of time.

If your agency or organization has an investment/contract that you are unsure as to whether it qualifies as a derivative instrument, please contact the SAO for clarification.

The SAO is aware of the need for guidance relative to this GASB pronouncement. As mentioned above, the derivative instruments policy should be released and available for use on the SAO's website by mid -June. Please refer to this policy for additional information. Any questions may be directed to Eddy Hicks at ehicks@sao.ga.gov. However, organizations are strongly encouraged to review GASB's Implementation Guide on Statement No. 53 immediately if they feel they may have outstanding derivative instruments contracts.

Editor's Note: USG employees with questions about financial reporting issues should contact USG AVC Vikki Williamson at vikki.williamson@usg.edu or 404-657-1011.

Save the Date!!

Co-sponsored by the Association of College and University Auditors

SAVE THE DATE!

Register Today! 100 Seat Capacity!

GEORGIA 2010 CONFERENCE FOR COLLEGE AND UNIVERSITY AUDITORS
Georgia Capitol Hill Campus
August 2-3, 2010

CONFERENCE PROGRAM

16 CPE credits

$110 Registration fee if postmarked on or before July 10, 2010 (personal check)

$125 Late Registration fee received after July 10, 2010 (Only cashier's check or money order)

Registration must be mailed and postmarked on or before 7/26/2010. No registration on day of conference.

Make check payable to "Board of Regents of the University System of Georgia;" indicate for "Georgia 2010 Conference for College and University Auditors" and mail to:

Attn: Tracy Pinnock
Office of Internal Audit and Compliance
Board of Regents of the University System of Georgia
270 Washington Street, SW
Atlanta, Georgia 30334

LODGING

HOLIDAY INN ATLANTA CAPITOL CONFERENCE CENTER

BRAVES VS METS GAME – Aug 2, 7:10 PM

***LIMITED BLOCK SEATING* tickets available in Golden Moon Pavilion @ $14 each**

Email Alex Ingle (Alex.Ingle@braves.com)

Questions? Contact Tracy Pinnock: 404-656-2231 or tracy.pinnock@usg.edu

Save the Date con't

TOPICS AND PRESENTERS

Opening Address
Dr. Susan Herbst, Chief Academic Officer/Executive Vice Chancellor, University System of Georgia
John Fuchko, Chief Audit Officer/Associate Vice Chancellor, University System of Georgia

Current Perspectives on Internal Audit
Dr. Richard Clune, Associate Professor, School of Accountancy; Director, Internal Audit Center; Kennesaw State University

Developing an Antifraud Program
Scott Stevenson, Director of Special Projects, Internal Audit Dept, Emory University
Joe Oringel, Managing Director, Visual Risk IQ

Fraud, Law Enforcement & the Internal Audit Function: A Panel Discussion
Moderator: Michael Foxman, Director of Internal Audit, University System of Georgia
David McLaughlin, Senior Assistant Attorney General, State of Georgia Department of Law, Special Prosecutions Unit
Phil Hurd, Chief Audit Executive/Director of Internal Auditing, Georgia Institute of Technology
Scott Stevenson, Director of Special Projects, Internal Audit Dept, Emory University
Joe Oringel, Managing Director, Visual Risk IQ

Conflicts of Interest in Higher Education
Dr. Thomas E. Creely, Associate Director, The Center for Ethics and Corporate Responsibility, J. Mack Robinson College of Business, Georgia State University

Personality Assessment Skills for Audit Professionals
Julie Crews, Crews Leadership Development

Chief Business Officers, Universities, and Unrelated Business Income
David Carson, Vice President for Business and Finance, Armstrong Atlantic State University

State Auditor's Office: Roles and Responsibilities
Russell Hinton, State Auditor for the State of Georgia

Enterprise Risk Management (ERM) in Higher Education
Scott Woodison, Director, Compliance and Enterprise Risk, University System of Georgia

Developing an Information Technology (IT) Audit Plan
Phil Hurd, Chief Audit Executive/Director of Internal Auditing, Georgia Institute of Technology

Frameworks for Information Systems Security Auditing in Higher Education
Erwin Carrow, IT Director of Internal Auditing, University System of Georgia
Susan Hacker, Internal Auditor, Armstrong Atlantic State University

Software Tools for Data Access and Analysis
Sally Wilson-Smith, Consultant, Audimation Services Inc.

Save the Date cont'd

Continuing Education Credits

Conference participants are eligible to receive a maximum of sixteen (16) CPE credit hours. Association of College and University Auditors is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Suite 700, Nashville, TN 37219-2417 or by visiting the website: www.nasba.org .

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

This program is co-sponsored with the Association of College and University Auditors. (ACUA) is an international professional organization serving institutions of higher education across the globe. Since its establishment in 1958, ACUA has provided its members a collegial forum for exchanging and sharing knowledge and generating new ideas. ACUA is committed to increasing members' knowledge of auditing, regulatory compliance and risk management in higher education. More information about ACUA can be found at www.acua.org .

Board of Regents of the University System of Georgia
Office of Internal Audit & 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:
http://www.usg.edu/audit/

Ask the auditor: If you have a control or ethics question that has been bothering you, it is a good bet someone else in the system is wondering the same thing. We invite you to send your question to Karen.lamarsh@usg.edu and we may feature it in the next or future issues of the Straight & Narrow.

Any other comments or questions?
Contact Karen LaMarsh at Karen.lamarsh@usg.edu

We are looking for suggestions and feedback.