The STRAIGHT and NARROW

Volume 4, Issue 19

May 2012

Internal Audit & Compliance, Board of Regents of the University System of Georgia. 404-962-3020

**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

### Transforming Internal Audit

In their business article *"Creating a World Class Internal Audit Function Reducing risk, identifying efficiencies and driving cost benefits"*, KPMG identified several core attributes of organizations that are able to achieve a world class Internal Audit (IA) function. According to KPMG, a world class IA function requires an optimum balance between positioning, people and processes that can add value across the organization. Excellence is achieved when these key factors work in tandem to create institutional transformation.

Positioning focuses on expanding and focusing the services provided by the IA function, so that institutional business partners view the IA function as providing value across the enterprise and not just evaluating financial compliance. The IA function should employ people who possess a diverse mix of skills, experience and capabilities to expand the ability of the team. Finally, the IA function must employ and integrate formal auditing processes that align with the organizational strategy.

**How does the System Office audit function support this transformation?**
There are currently a few staff resourcing efforts that have been underway for some time. These include:

- Focus audit efforts system-wide and USO

| Category | 2008-2009 | 2012-2013 | 2015-2016 |
|---|---|---|---|
| USO Audit Plan % institutional | 82% | 69% | 40% (projected) |

- Plan USO institutional audits to include special audit requests, consulting engagements and Public Private Venture Audits
- Provide USO audit staff support to campus auditors – data, risk assessment, planning and quality

In addition to staff resourcing efforts, the USO staff has implemented several core IA programs in consonance with the Institutions. These include:

- Compliance and Ethics Program. The USG launched the Compliance, Ethics and Reporting Hotline in 2008. The Hotline has been instrumental in mitigating risks and resolving issues at the institutional level.
- Risk Management. The BOR approved the USG Risk Management Policy in August 2010. Since then, we have organized a leadership task force and we are currently implementing Enterprise Risk Management systemwide.

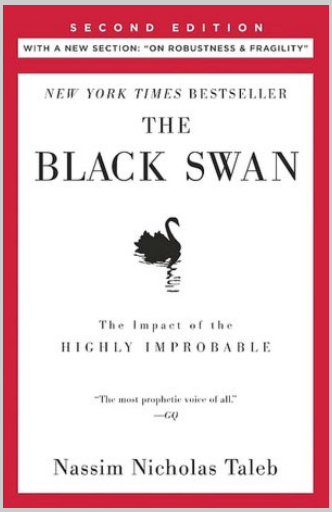
Under the Chancellor's and the Board's leadership, the OIAC's vision is focused on the future. We recognize that relevant risk management, good governance, improved internal controls and efficient financial system support the entire University System of Georgia.

# Embedding "Risk Management" into Your Everyday Decision Making

*by Scott Woodison*

## The Black Swan

*The book is concerned with randomness and uncertainty, and our chronic inability to accurately fathom and measure these phenomena.*




*According to Taleb, a Black Swan event is one that is unpredictable yet has wide-spread ramifications. Not only are Black Swan events difficult to predict, but Taleb also argues that we human beings have certain psychological limitations and biases that prevent us from foreseeing these events, while also thinking that the events were perfectly predictable after they occur.*

Currently one of the hottest topics in the business press is the concept of "*Risk*". Whether it's the collapse of the financial markets, the turmoil in the European Common Market over the Greek debt crisis, or the tsunami and subsequent nuclear reactor failure in Japan, everyone is talking about ***Risk***.

And no, the recent book that everyone is talking about titled *The Black Swan* is not about a ballet dancer. The risk theory known as the Black Swan was developed by Nassim Nicholas Taleb in his book *The Black Swan: The Impact of the Highly Improbable*. His book develops the concept of the disproportionate role of high-impact, hard-to-predict, and rare events beyond the realm of normal expectations, and how to think about these occurrences. Since his writing in 2004, many unexpected, high impact events are now referred to as Black Swan events. But not all of our risks are Black Swan events. In fact, very few risks are Black Swan events. Most risks can be predicted...*or possibly prevented.*

The University System of Georgia is currently implementing a system wide Enterprise Risk Management (ERM) program. The basic tenet of the program is "risk mitigation" through a specific process, which include the following:

- Identifying institutional objectives;
- Identifying and ranking risks.
- Selecting key risks and assigning a key risk owner to each key risk
- Identifying a risk tolerance and mitigating controls for each key risk.

The goal of ERM is to work with each institution to develop a list of key risks, and to subsequently consolidate the key risks of all institutions into a system-wide risk profile. The consolidated list of key risks will then be evaluated to help determine which key risks impact the USG as a whole.

While this creation of a list of key risks for each institution is a major focus of the ERM program, a second focus item of the program is to have each institution embed the concept of risk management into everyday operations. Every major decision made by an institution

Embedding "Risk Management" into Your Everyday Decision Making, ***cont'd***

should be considered in regard to the question, "What is the risk of this decision?"

In order to properly understand risk management, we must understand a new set of terms, processes and questions.

**What occurrence or activity (the risk) will stop us from being successful?**

If we define risk as "something that will stop us from accomplishing our objectives", then we should focus on what environmental risks, (business, legal or otherwise) will prevent us from being successful.

When we evaluate a decision from a risk perspective, we must attempt to answer a number of questions:

What is the impact, likelihood, and the velocity of this risk? The Impact measures the negative outcome if the risk should occur. The Likelihood measures the expectation that something will happen, usually based on prior experience. The Velocity measures how fast the impact can occur. The value of the product of the , impact, likelihood and velocity will provide us with a risk rating.

**What is our tolerance or appetite for risk?**

Risk is inherent in everything we do. In a risk/ reward scenario, to earn a reward requires some level of risk. Our risk tolerance measures how much risk we are willing to accept based on the anticipated reward. Management must decide their tolerance for risk, or how much risk they are willing to accept. For example, management may have a lower tolerance for risk, if that risk could have a major effect on the reputation of an institution or success of a program.

**What controls are currently in place, and what controls should be put in place?**

If there are no controls in place, then we have what is referred to as inherent risk. However, if controls are put in place which will reduce risk, then we will end up with what is called residual risk. As managers, we need to ensure that before starting projects, controls are in place to reduce risk (residual risk) to a level where the risk is below the established risk tolerance.

The purpose of ERM is to evaluate and rate risk. After the risk is identified and rated, controls need to be implemented to reduce the risk to a level commensurate with the institution's risk tolerance.

Risk management is not difficult, but it does often require a new way of thinking. If you can successfully anticipate and control risks, then your project should also be successful.

---

Contact Scott Woodison to learn more about risk management and for assistance with implementing your institution ERM program.

*Scott Woodison*
*Executive Director, Compliance and Enterprise Risk*
*Email: Scott.Woodison@usg.edu*
*Telephone: (404) 962-3027*

# Governance, Risk Management, and Compliance

## *by Jeanne Severns*

Governance. Risk Management. Compliance. These are some of the concepts behind successful organizations. Just like financial institutions and manufacturing businesses, the USG's mission of *Creating a More Educated Georgia* requires a high standard of governance at all institutional levels: administration, faculty, operations, athletics, and the student body.

What does effective governance look like, and how does OIAC play a role in this process? In this Governance column, we will attempt to answer these questions. Each subsequent Governance column will provide more details on governance, as well as address risk management and compliance issues.

The OIAC exists to support the University System of Georgia (USG) in meeting governance, risk management and compliance responsibilities. However, the idea that OIAC alone provides these services to the USG is a misconception. The principles of governance, risk management and compliance are shared responsibilities of leadership, management, faculty, staff and students. Each of us contribute to these principles and are all responsible for minimizing risk, increasing compliance, and strengthening internal controls.

**What is governance?**


Generally, governance refers to the rules, policies, procedures, and laws by which an organization is governed and operated, regulated, and controlled. More specifically, governance includes the following:

**Leadership:** The Tone at the Top; the precedence set within the organization that everyone adheres to legal and ethical behavior, without exception.

*"No matter if you use the term or not – GRC (Governance, Risk Management, & Compliance) is a reality. We are in 2011 and it has been ten years now since I first started using the term GRC in research and interactions with organizations.*

*The truth of the matter is – GRC as an acronym is approximately 10 years old, but GRC as part of business is as old as business itself. "*

*Michael Rassmussen, CCEP, CISSP*

Michael Rasmussen is an internationally recognized pundit on governance, risk management, and compliance (GRC) with specific expertise on the topics of corporate compliance, business ethics, policy management, and corporate culture.
*www.corp-integrity.com*

**Strategy:** The objectives, vision, values, and mission of the institution.

**Policy: T**he guiding principles of the culture that keeps the organization focused on goals and prevents it from going down unintended paths. The Policy defines how an organization meets its obligations and commitments and how it stays within legal, regulatory, and contractual boundaries.

Within an organization with a sound governance structure, we can also expect to find elements of the following:

**A focus on operations,** in that organizational performance is defined, measured, analyzed, improved and controlled.

## Governance, Risk Management and Compliance, *cont'd*

**A focus on human resources** that demonstrates efforts to build and improve an effective and supportive workforce environment by providing training for employees, by engaging employees in the organizational planning, and by ensuring that performance measures are in place and that employees are evaluated against them.

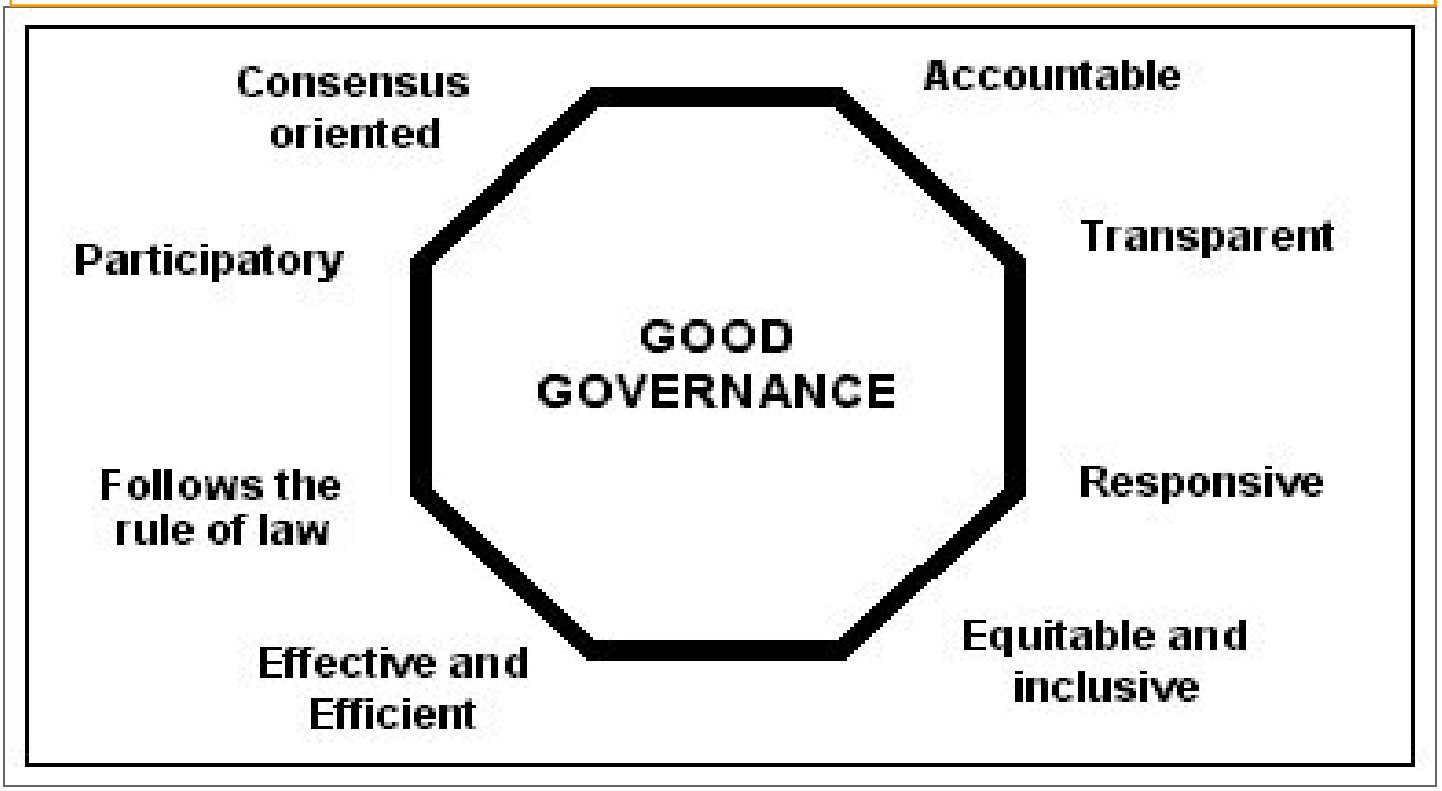
**A focus on results** that provides continual evaluation for effectiveness by looking at productivity, work cycle timelines, and accuracy. A strategy used to measure results is the use of key indicators.

When OIAC performs an internal audit, one of the aspects it considers is the overall governance of the institution. Recommendations are often made based on the assessment of the factors mentioned above. Additionally, in its support role, the OIAC staff is available to consult on what best practices might look like in any of these areas.

We look forward to answering any questions you may have on this topic, and we hope you will look forward to reading more on the topic of governance, risk management and compliance in our next issue.

*Jeanne Severns*
*Interim Executive Director, Internal Audit and Compliance*
*Email: Jeanne.Severns@usg.edu*

### A Model for Good Governance Incorporating Leadership, Policy, Workforce Participation and Results



# Managing Your Grants
## *by Sandy Evans*

If grants are part of the financial and academic fabric of your campus, you are undoubtedly aware of the benefits they provide to faculty, students, and the institution itself. Hopefully, you are also aware of the complexities of managing a grant program and the associated risks. When reporting your grant metrics, there are issues that can complicate an otherwise straightforward compliance requirement if you do not follow directions outlined in the grant reporting guidelines. Below are issues to consider.

**Issue # 1: Reporting of Time and Effort (T&E)**

Time and effort reporting can be a little tricky, especially if there are multiple projects. Following are several issues that warrant closer scrutiny.

- Ensure T&E estimates agree to actual T&E reports for the semester reporting period.
- Verify T&E reports correspond to the payroll calculation used to bill the granting agency.
- Report T&E for the time period the work was done. For example, T&E during Fall or Spring semester cannot be claimed during the Summer semester.
- Follow T&E regulations issued by the granting agency and BoR Policy. For example, National Science Foundation (NSF) policy on funding of summer salaries (known as NSF's two-ninths rule) states, "Proposal budgets submitted should not request, and NSF-approved budgets will not include funding for an individual investigator which exceeds two-ninths of the academic year salary." This limit includes summer salary received from all NSF-funded grants. (NSF Grant Policy Manual, Chapter VI, 611.1 Salaries and Wages)

***Risk:*** Loss of grants, banned from application for future grants, fines, fees, and damage to reputation.

**Issue #2: Submitting Outcomes Reports**

It is important that grant funded programs submit timely outcome reports of work product achieved. Beginning May 2012, NSF will enforce timely submission of Project Outcomes Reports for all awards requiring the report.

***Risk:*** An overdue Project Outcomes Report will delay NSF actions on any other proposal or award related to the Principal Investigator or Co-Principal Investigator.

**Issue #3: Revised National Institute of Health (NIH) Financial Conflict of Interest (FCOI) Reporting Requirements (See NIH 2011 Final Rule)**

Effective August 24, 2012, current and future recipients of NIH grants must comply with stricter Significant Financial Interest (SFI) rules. These rules are designed to provide transparency and financial disclosure on persons/programs receiving NIH grants funds. The new rule requires the institution receiving the grant to publicly disclose financial information on principal investigators, senior researchers, grant managers, their spouses, and their minor children, specifically payment for services or equity interests over $5,000 in a privately held or publicly traded company related to the grant. Expenditures that should be disclosed include reimbursed travel or sponsored travel related to Institutional responsibilities. The disclosure is not required if the reimbursement or teaching fee was sponsored by a government agency, higher education institution, or teaching/research facility. Disclosure must made through Institution website or by written response to any requestor within five business days.

***Risk:*** Institutions who fail to meet the requirements of the NIH deadline, risk NIH sanctions.

# Identifying Potential Fraud Risks

## *By Melissa Hall*

According to the Association of Certified Fraud Examiners' 2010 Report to the Nations on Occupational Fraud and Abuse, approximately 17 percent of frauds in education result from expense reimbursements. In an economy where budget cuts have become a way of life, institutions of higher education simply cannot afford this amount of fraud loss each year. Although the majority of occupational frauds are still discovered by anonymous tips, organizations cannot rely solely on tips. The internal auditors are still expected to search for fraud. Here are a few suggestions to help focus limited resource efforts:

- Expand your reporting channels – not literally, but creatively! We all have a hotline, but sometimes a trusted relationship between you and the major finance managers on campus are more valuable than the hotline. If they trust you, they are more likely to pick up the phone to call you when something doesn't look right, and not fear an audit of their activities. They also hear the unguarded conversations around the water cooler that do not occur when the auditors are around. Unlike us, who only see what actually gets processed, they also see attempted reimbursement requests and have a keen sense of what's really going on in a unit. Across the system, tips from financial unit managers continue to result in a number of major investigations involving fraud, waste and abuse.

- Search travel and expenses for patterns. This may seem like finding a needle in a haystack, right? Focus your efforts on specific time frames when family vacations are likely to occur. For example, pull the records for travel when the campus is closed. *Why would a professor need to be traveling for "research collaboration" to the same University over Christmas break for three years in a row? How about summer conferences in Hawaii?* Approximately 35 percent of all allegations investigated at Georgia Tech in FY 2012 involved travel in some capacity. Almost all valid conferences for which your faculty and staff would need to be traveling can simply be located using a Google search.

- Perform a fraud risk assessment on your IT security policies. The students at your campus are more technically savvy than most professionals on your staff. In order to stay ahead of the students, you should consider hosting a brainstorming session with your IT professionals, and start by asking them "*Could our students gain access to our systems, and change their grades?*" If the answer is "no", think again. In less than three minutes, YouTube can demonstrate "How to obtain someone's password" or "How to change my grades". Studies have shown that 60 percent of freshmen entering college come equipped with three personal internet ready devices, and these devices are getting smarter and faster every day. Investigations involving students and grade changes have been on the rise in the United States. Work with your IT security office to ensure that controls are in place to prevent this from happening, and ask yourself *"Could this be happening on my campus?"*

We would like to hear your thoughts and ideas on identifying potential fraud risks!

*Melissa B. Hall, CPA, CFE*
*Associate Director Forensic Audits*
*Georgia Institute of Technology*
*Email: melissa.hall@business.gatech.edu*

# Desk Audit Results – Compliance and Ethics Reporting Hotline

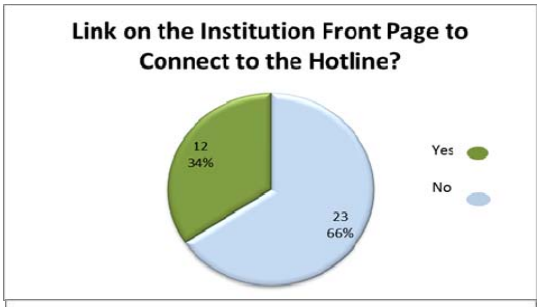
*By Belinda Pedroso*

The OAIC Compliance and Ethics Program launched the Compliance, Ethics and Reporting Hotline in 2008. The Hotline was introduced to reinforce USG's commitment to higher standards of integrity and accountability in respect to governance and financial operations. The Hotline also reinforced the culture established through the USG Ethics Policy, and the administration's goal to increase esteem for higher education.

It's been approximately four years since the launch of the Hotline, so we decided to conduct a brief desk audit of its visibility system-wide. The desk audit entailed a very simple procedure. We identified our objectives: visibility and access. Next, our methodology entailed viewing all USG institution websites and virtual communication portals to find the Hotline link. We asked five very simple questions:

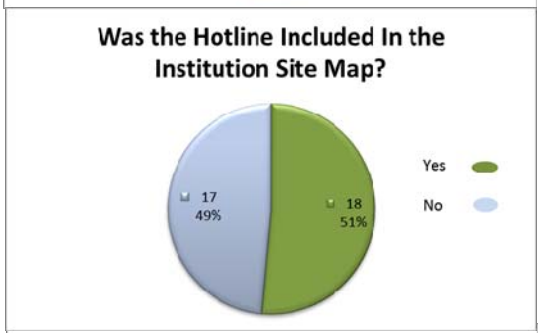
**1. Is there a link on the front page of the Institution's website that connects to the Compliance, Ethics and Reporting Hotline (Hotline)?**

- Approximately one-third of the Institutions had links from the front page of the website directly to the Hotline access portal.



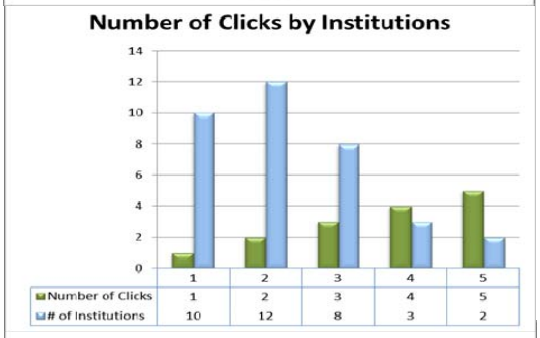

2. **Was the Hotline included in the Institution site map or website index?**

- The results of this question were fairly equal. The Hotline could be accessed by the website index or site page by 18 of the 35 institutions. The other 17 institutions provided access to the Hotline through a "search" mechanism.



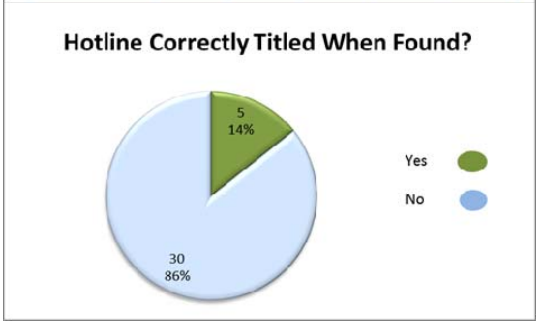

3. **If we could not readily locate the Hotline, how many clicks did it take to locate the Hotline?**

- The results varied. The fewest number of clicks was one and the largest number of clicks was five. Most Institutional websites provided access within two clicks.




4. **When we did locate the Hotline, was it correctly titled as "Compliance, Ethics and Reporting Hotline"?**

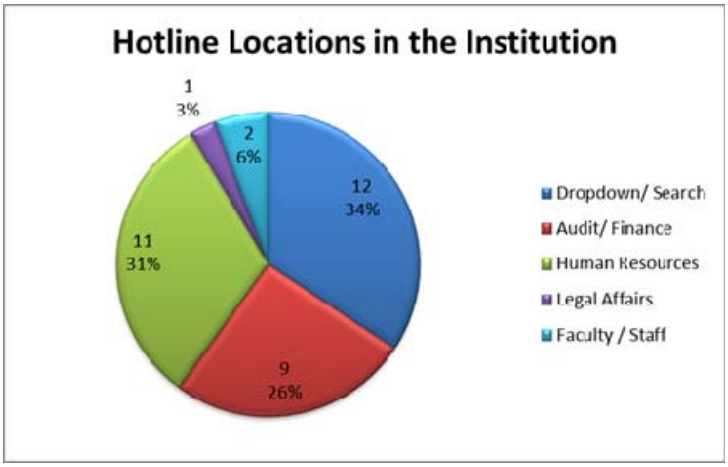
- The greatest difficulty in locating the Hotline was due to inconsistent titling. When we located the Hotline, it was usually titled by another internal or abbreviated name, (Ethics Hotline, Fraud Reporting, Complaint Line, etc.). The Hotline was most often titled "Ethics Hotline".



## Desk Audit - Compliance, Ethics and Reporting Hotline, *cont'd*

5. **Where was the Hotline located on the Institutions' website, as in, what department or division of the Institution?**

- The Hotline was most commonly found through a Search mechanism or located in the Human Resource department. One Institution included the Hotline along with other legal / policy issues. The Hotline was less frequently associated with Audit or Finance.




One way in which we can foster openness of our institutions is for of our constituents to use the Compliance, Ethics and Reporting Hotline not just to report suspected malfeasance or wrongdoing, but to also provide feedback to the institution about employee concerns. Access to the Hotline encourages faculty, staff and students to come forward with information on organizational improvement as well as violations of adopted policies. In our next article about the Compliance, Ethics and Reporting Hotline, we will provide some quick tips on how to improve the visibility of the Hotline and how to increase its usefulness as a tool to achieve organizational goals.

## SAVE THE DATE!

**GEORGIA 2012 CONFERENCE FOR COLLEGE AND UNIVERSITY AUDITORS**
**Georgia Capitol Hill Campus**
**July 30-31, 2012**

**Registration Fee: $150 before 6/30/12 • $175 after 6/30/12**
(Cashier's check, personal checks or money orders only; no personal checks after 6/30/12).
Registration fee must be received by 7/23/12.
**Questions?** Contact Tracy Pinnock, Conference Administrator, tracy.pinnock@usg.edu
**Registration?** EMAIL YOUR: Name, Title, Institution, phone, email, and emergency contact to confirm your attendance. **Send to**: Sandra Evans, Conference Registrar, sandra.evans@usg.edu

**CONFERENCE PROGRAM**
**16 CPE credits (Program info available at:**
**http://www.usg.edu/audit/conference by 5/31/12)**

MAIL REGISTRATION FORM AND CHECK TO
Sandra Evans, Conference Registrar
Board of Regents
Attn: Office of Internal Audit and Compliance, Suite 7074
270 Washington Street, SW • Atlanta, Georgia 30334

*What is John and the OIAC Team Reading*?

**Governance**
*No Nonsense Leadership and Project Management*, The Neal Whitten Group, www.nealwhittengroup.com

*Effective Policy Governance, Oversight and Management* by Michael Rasmussen, Corporate Integrity, www.corp-integrity.com

**Risk Management**
*Who Has or Should Have the Ultimate Responsibility for Managing Risk*? Norman Marks, CRMA, CPA, http://www.theiia.org/blogs/marks/

**Compliance**
*Aligning the Internal Audit Plan and Your Risks*, José Tabuena, Compliance Week, http://www.complianceweek.com


**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:* belinda.pedroso@usg.edu