The STRAIGHT and NARROW

January 2016

Volume 6, Issue 28

Office of Internal Audit & Compliance, BOR — USG, (404) 962-3020

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 Interim Chief Audit Officer, Michael J. Foxman

Happy New Year Colleagues!

Back to Basic! – Turning Our Attention Towards Assurance and Compliance

The OIAC has been hard at work ensuring that we added "value" during 2015. Our work plan included the accomplishment of:

- Presidential Transition Audits
- Systemwide ACA Consulting Engagement
- Systemwide Financial Aid Audit Engagement
- An Assessment of Services Provided to Non-student Minors on Campus
- University System Office Audit including travel, purchase cards, contracts; and Georgia Archives operation
- Systemwide Deferred Compensation

In 2016, we will continue to provide internal audit and consultation services to USG institutions and business units. This year we are turning our attention towards assurance and financial compliance. What's on the horizon? A couple of very significant project worth mentioning include:

- IT Audit and PCI Compliance: 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. Our part in the IT security process is to provide assurance that the USG has implemented proper safeguards to protect vital data. Our IT Audit Director Patrick Jenkins will be visiting each institution to begin these assessment.
- Financial Assurance Reviews

I would also like to acknowledge and welcome Mr. Kwabena J. Boakye to the OIAC. Kwabena joined the staff beginning December 2015. Please welcome him in his new role at the BOR.

I am looking forward to working with each of you during this year as we continue to safeguard USG assets and the USG reputation. Please feel free to contact me at Michael.foxman@usg.edu 404-962-3021.

Michael J. Foxman
Interim Chief Audit Officer

Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards at 2 CFR 200

By Rob Roy

It has been a year since the new Administrative Requirements went into effect. So in short, what is covered by the new Uniform Requirements (UR), frequently referred to as the Uniform Guidance, what is changing and what is not? Starting about 3 years ago the Committee on Financial Assistance Reform (COFAR) addressing President Obama's directive to streamline guidance and increase accountability for federal grants has brought us these changes that went into effect on 26 Dec, 2014. The UR combined circulars A-21, A-110 and A-133 and 5 others into one uniform document that applies to Institutes of Higher Education (IHE), state and local governments and tribal nations. The UR provides guidance to federal agencies on solicitation content and program rule development. This regulation covers how IHEs manage finances, purchasing and property purchased under a federal award. It also governs allowable cost, both direct and indirect. Direct cost such as personal services, travel, material and supplies, contracts and sub-awards as well as how space and utilities costs are used in F&A rate proposals. Under the UR risk management framework, the institutions will rely heavily on their internal controls for administration and research awards.

The UR applies to all federal awards made to the IHE. These rules, agency and program rules as well as special conditions and the notice of award itself will apply to an award. State regulations and IHE policies and procedures will apply to all sponsored research under the doctrine of internal controls. One of the most significant changes in the UR is the use of the word "must" in place of the word "should". COFAR has made it clear that where the word "must" is used, an IHE is required to comply in their administration of sponsored awards. In other words, these are auditable activities of grants management. The word "must" appears over 800 times in the UR. In addition to this change from "should" to "must", researcher's program performance must reflect financial performance, very similar to ARRA reporting. Specifically, the research progress must be mirrored by the financial progress. As indicated above there is an emphasis on internal controls and documentation. This will be reflected in timely expenditures and cost transfers, as well as, the requirement for PI's to certify costs on their projects. When issuing or receiving a sub-award, increased documentation is required.

Office of Management and Budget

Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards

<u>2 CFR 200</u>

- ♦ TITLE 2—Grants and Agreements
- ♦ Subtitle A—Office of Management and Budget Guidance for Grants and Agreements
- ♦ Chapter II—Office of Management and Budget Guidance
- ♦ Part 200—Uniform Requirements

Abbreviations

- ♦ UR—Uniform Requirements
- ♦ COFAR—Committee on Financial Assistance Reform
- ♦ IHE—Institutes of Higher Education
- ♦ ARRA—American Recovery and Reinvestment Act, 2009
- ♦ PI—Principal Investigator
- ♦ F & A Rate—Facilities and Administrative Rate

Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards at 2 CFR 200, Cont'd

There are new limits on fixed price contracts, and changes in payment requirements. Greater financial and programmatic performance monitoring is going to be required by the prime contractor. The changes will necessitate greater planning as contracting will be more constrained, purchasing will require more quotes and bids, and close-out timelines will be more compressed.

Many researchers will want to know what impact the UR will have on their awards. The following are some highlights:

Proposals: The researchers will need to pay very close attention to the solicitation issued by the sponsoring agency. Cost-sharing cannot be considered in proposal review and the requirement of cost share requires agency head approval. In short, do not propose cost-share unless it is required in the solicitation. Awarding agencies are expected to pay the full negotiated F&A rate; any deviations must be approved by agency head and must be stated in the solicitation.

Purchasing: Documentation standards have changed when purchasing equipment and supplies. The threshold level of Micro-purchasing has been reduced from $10,000 to $3,000, with additional documentation required and maintained for any purchase in excess of $3,000.

Materials and Supplies: More attention is will be required when budgeting and purchasing materials and supplies, as there is a new requirement for tracking and documenting residual supplies at the end of a project and for late-term purchases/charges. New limits on the timelines for making cost transfers are included, particularly at the end of a project.

Equipment: Equipment purchased with federal funds must be made available to other federally funded projects and there are disposition requirements that must be adhered to at the end of a project.

So what is not changing? The UR are still built on the foundation of Allowability, Allocability and Reasonableness. All charges to a federal project must adhere to these principles. The dual role of graduate students and post-doctoral trainees has been affirmed. Time and effort will continue to be the standard for documenting personnel charges. Travel regulations will remain consistent with the regulations of the state of Georgia. Computing devices that are essential and allocable, but not solely dedicated to the performance of a federal award, may be allowable as a direct charge, if appropriate and meet the allowable, allocable and reasonable requirements. The expectation to financially and programmatically close awards within 90 days of the term has not changed, what has changed is the process which the IHE must go through in the closeout process and therefore, the timelines are going to be much tighter.

Also not changing are the four cost accounting standards: 1) An institution's practices used in estimating costs in pricing a proposal shall be consistent with the institution's cost accounting practices used in accumulation and reporting costs; 2) like costs in like circumstances must be treated in the same manner; 3) unallowable costs shall be excluded from any billing, claim, or proposal applicable to a sponsored project; 4) an institution shall use their fiscal year as their cost accounting period.

Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards at 2 CFR 200, Cont'd

IHEs should, if they have not already done so, map their policies and procedures to the new UR and conduct information sessions to advise faculty and staff that the new UR are applicable to awards made after 26 December, 2014. IHEs also need to be aware of agency specific requirements and exceptions to the UR that were published by each agency. Also, be aware that procurement requirements have been delayed another 12 months until the beginning the next fiscal year cycle, 1 July 2017 for units of the USG and that DS2 are due within 90 days of the release of the new forms.

The author would like to acknowledge that the above is excerpted from presentations made by Jilda Garton, Vice President for Research and General Manager, GTRC & GTARC .

Robert Roy
Research Associate and Director of Business Operations
rob.roy@usg.edu

Training Opportunity—February 1, 2016

Best Practices for Protecting Minors on Campus

The training conference is designed for campus based personnel to learn important guidelines and procedures an institution can implement to minimize risks when minors participate in camps and programs on college campuses.

This upcoming training conference will cover Best Practices for protecting minors . The conference keynote speaker is Ann Franke, an expert in risk management, employment, student affairs, and governance.

Who would benefit from this experience?
Consider representatives from the following areas:

- Continuing Education
- Conference Services
- Student Affairs
- Facilities / Housing
- Campus Safety
- Legal Counsel
- Athletics
- Human Resources
- Risk Management
- Internal Audit

Register at the conference webpage using the following link:

http://www.cvent.com/d/xfqkth

Please share with staff and administrators at your institution who supervise or work in programs designed for minors.

Effective Management of Scholarship and Fellowship Funding Provided by a University Foundation

By: Mark W. Long, CPA, CGMA; Chief Financial Officer, Georgia Tech Foundation

Georgia Tech is fortunate to receive generous financial support from its alumni and friends to support scholarship and fellowship awards to our students. The contributions received may establish endowments, which provide a perpetual flow of income for student support, or the donor may choose to make a contribution which is fully expendable. This type of private support is critical in advancing an institution's goals in attracting and retaining the best and brightest students and making the institution financially accessible to all qualified students.

Effective management of scholarship and fellowship funds is a vital component in proper stewardship of the funds contributed. At Georgia Tech, three campus offices, the Georgia Tech Foundation, the Controller's Office and the Office of Scholarships and Financial Aid, work collaboratively to ensure the funds are efficiently awarded to our students. In fiscal year 2014, more than $18 million in scholarship support and more than $4 million in fellowship support was provided by the Foundation to Georgia Tech students.

Upon receipt of a contribution, the Foundation establishes an account on its books and records and assigns a unique Foundation account number. The Foundation forwards the information on the gift, including the scholarship criteria and the unit responsible for recipient selection to the Controller's Office and to the Office of Scholarships and Financial Aid. The Accounting Services Department, within the Controller's Office, establishes a sponsored account, or Georgia Tech project number, per the following procedure: http://policies.gatech.edu/business-finance/establishing-scholarship-and-fellowship-projects. The Office of Scholarships and Financial Aid also establishes an account in its Banner system, noting the Foundation account and the Georgia Tech project number. All of the numbers are linked in each system. The unit responsible for selecting the recipients and the criteria for selection are noted and recorded by both offices. As funds are received or made available by the Foundation, the budget is updated on the Georgia Tech records via a daily data feed.

The appropriate campus unit selects the student to receive the scholarship or fellowship award, taking into consideration the institution's goals and the criteria for the award. The award is credited to the student's account and is applied toward his or her tuition and fees. At the end of each month, the Controller's Office prepares a cumulative invoice of all of the scholarship and fellowships paid for the month. The invoice is electronically sent to the Foundation, noting the Foundation account number. The Foundation reimburses Georgia Tech for the monthly awards via a bank transfer. The Controller's Office reconciles the accounts to ensure the accounts are in balance.

At Georgia Tech, proper stewardship of the funds entrusted to us is very important, including informing the donor of the impact of his or her gift. The GThanks program, located on the website at http://www.finaid.gatech.edu/gthanks, encourages students who benefited from the generosity of our donors to thank them for their support. The program encourages interaction between the student and his or her benefactor and has resulted in additional scholarship and fellowship donations. We believe this interaction will motivate our current students, when they become alumni, to give back and help future students.

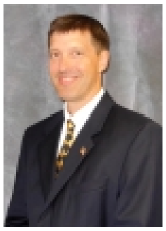
International Fraud Awareness Week – A Success!

Once again, the USG was a proud participant of International Fraud Awareness Week November 15 – 21, 2015. It was great to see all of the system-wide activities that took place at institutions to bring awareness to the importance of an ethical culture. Studies have shown that organizations with an ethical culture are more productive and have higher employee retention rates. No organization is exempt from the potential for fraud and the resulting risk to the reputation of their employees. A recent survey by the Ethics Resource Center revealed that 41% of U.S. workers observed unethical or illegal misconduct on the job.

The USG Awareness programs that took place during International Fraud Awareness Week help to recognize and promote our shared values of ***integrity, excellence, accountability and responsibility.*** Fraud awareness programs are part of the USG's comprehensive ethics and compliance program which includes ethics training, mandatory compliance training, assurance audits, consulting engagements, and an ethics and compliance reporting hotline.

Thanks for all you do to create a more educated Georgia.

Wesley Horne
Director of Ethics & Compliance
404-962-3034
wesley.horne@usg.edu



Bringing Freud to Fraud:
Fraud and Human Behavior
Dr. Sridhar Ramamoorti
School of Accountancy and
Corporate Governance Center
Kennesaw State University

The PCI Monsters under the Bed

By Patrick Jenkins

I recently read an article on University Business' website entitled "PCI Compliance Crackdown" by Pamela Mill-Senn. The article centered on an interview with the founder and president of CampusGuard, Ron King. CampusGuard is a consulting company focusing on special needs of higher education. Several of our USG schools have had engagements with CampusGuard to perform gap assessments related to Payment Card Industry (PCI) Data Security Standards (DSS). The interview with Mr. King went on to highlight some of the challenges that higher education is facing related to PCI compliance. The article has some good, high-level information about PCI and is certainly worth the read

http://www.universitybusiness.com/article/pci-compliance-crackdown

I had the opportunity to have a casual meeting with Mr. King in October of this year and we both agreed that probably the biggest challenge in higher education as it relates to PCI compliance is the fear, uncertainty, and doubt on the part of some administrators, hoping the problem will simply "go away". This approach reminds me of a child fretting about the mean, nasty monsters lurking underneath the bed.

A cause for concern is valid and it won't go away by curling under our blankets, squeezing our eyes shut and wishing for it to disappear. It must be confronted.

A good way to confront the "monster" is to figure out exactly what kind of beast your campus is dealing with. Generically speaking there are only two kinds of monsters that exist in the PCI realm: Merchant and Service Provider.

Understanding your PCI compliance requirements begins with understanding that if any part of your campus infrastructure "stores, processes, or transmits" payment card information it is in scope for PCI-DSS.

I. PCI Monster 1: The Merchant Monster

The first type of monster is the Payment Card Industry (PCI) Merchant.

If your school (or affiliated departments) accepts credit/debit cards as forms of payment, your Institution is required to be compliant with the Payment Card Industry– Data Security Standard (PCI-DSS).

PCI Merchants range in levels from 1 to 4. The Merchant level is determined by the volume of payment card transactions annually. Payment cards are those cards branded with an industry vendor logo, i.e. Visa, MasterCard, Discover, and American Express. Each card brand has their own merchant levels.

How do YOU find out your PCI level? Your acquiring bank determines your merchant level. Your Chief Business Officer (CBO) should know your acquiring bank. Once you have this information, you can find out your PCI-DSS compliance requirements. For example, a PCI Merchant Level 1, for Visa transactions, processes over 6 million Visa transactions annually across all channels of Global Merchants identified as Level 1 by any Visa region. PCI levels 2, 3, 4 each have different annual transaction amounts and criteria. *Source: www.visa.com/cisp*

If your institution is a Merchant Provider, your institution *MUST:*

The PCI Monsters under the Bed, Cont'd

- *Conduct an annual self-assessment.*
- *Have (clean) quarterly network scans by an Approved Scanning Vendor (ASV).*

The PCI Security Standards Council provides tailored guidance for the self-assessment. The self-assessment has two deliverables: the Self-Assessment Questionnaire (SAQ) and the Attestation of Compliance (AOC).

There are:

SAQ – A: This is for card-not-present (e-commerce or mail/telephone order) merchants, and all cardholder data functions are outsourced. This NEVER applies to face-to-face merchants.

SAQ – B: Imprint only merchants with NO electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage.

SAQ – C-VT: Merchants using only web-based virtual terminals, no electronic cardholder data storage

SAQ – C: Merchants with payment application systems connected to the Internet, no electronic card holder data storage.

SAQ – D: All other merchants no included in descriptions for SAQ types A through C and all service providers.

Generic State College (GSC) has decided that its Bursars office will only take payments through online transactions and has outsourced that function to a 3rd party (i.e. TouchNet). Therefore, GSC would need to fill out a SAQ – A for the Bursar's office. However, GSC's Parking Office accepts credit cards for payment of permits and fines in their office using traditional card swipe machines. GSC would need to complete a SAQ – B for the Parking Office. GSC may need to complete multiple SAQs for each area on campus that accepts credit cards.

There is a chance your institution may fall under several SAQ categories, thus you may need to complete multiple SAQs.

GSC will need an AOC for their school covering all areas that accept payment cards. Obtain a template at the Standards Council website: www.pcisecuritystandards.org

II. **PCI Monster 2: The Service Provider**

Chances are, your school has outsourced some of their credit card processing operations to a ***third party***, such as TouchNet, who is considered a Service Provider under PCI-DSS.

As their customer, you have the right to obtain their AOC. This is something the campus CBO or Compliance Officer should be doing on an annual basis as part of compliance efforts.

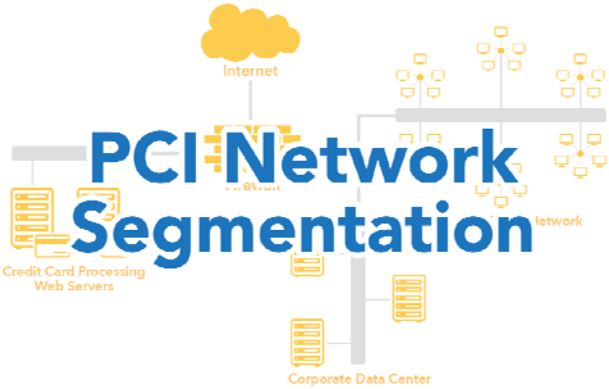
However, some schools have (perhaps unknowingly) put themselves in the roll of a PCI Service Provider. A Service Provider is an entity that is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.

This means that if a school contracts with 3rd Party vendors, such as dining services companies like Sodexo, or food court-type vendors such as Subway, Taco Bell, Chick-fil-A, to provide an ***Internet connection*** via the campus network for credit card processing, then that school is a PCI Service Provider.

The challenge is not all institutions recognize their active role as a service provider, and this lack of awareness puts the institution, the institutions businesses; and customers at risk.

A bigger challenge with unknowingly being a Service Provider is that contract language with the vendors may or may not cover the costs associated with implementing the required security controls of a service provider.

The PCI Monsters under the Bed, Cont'd



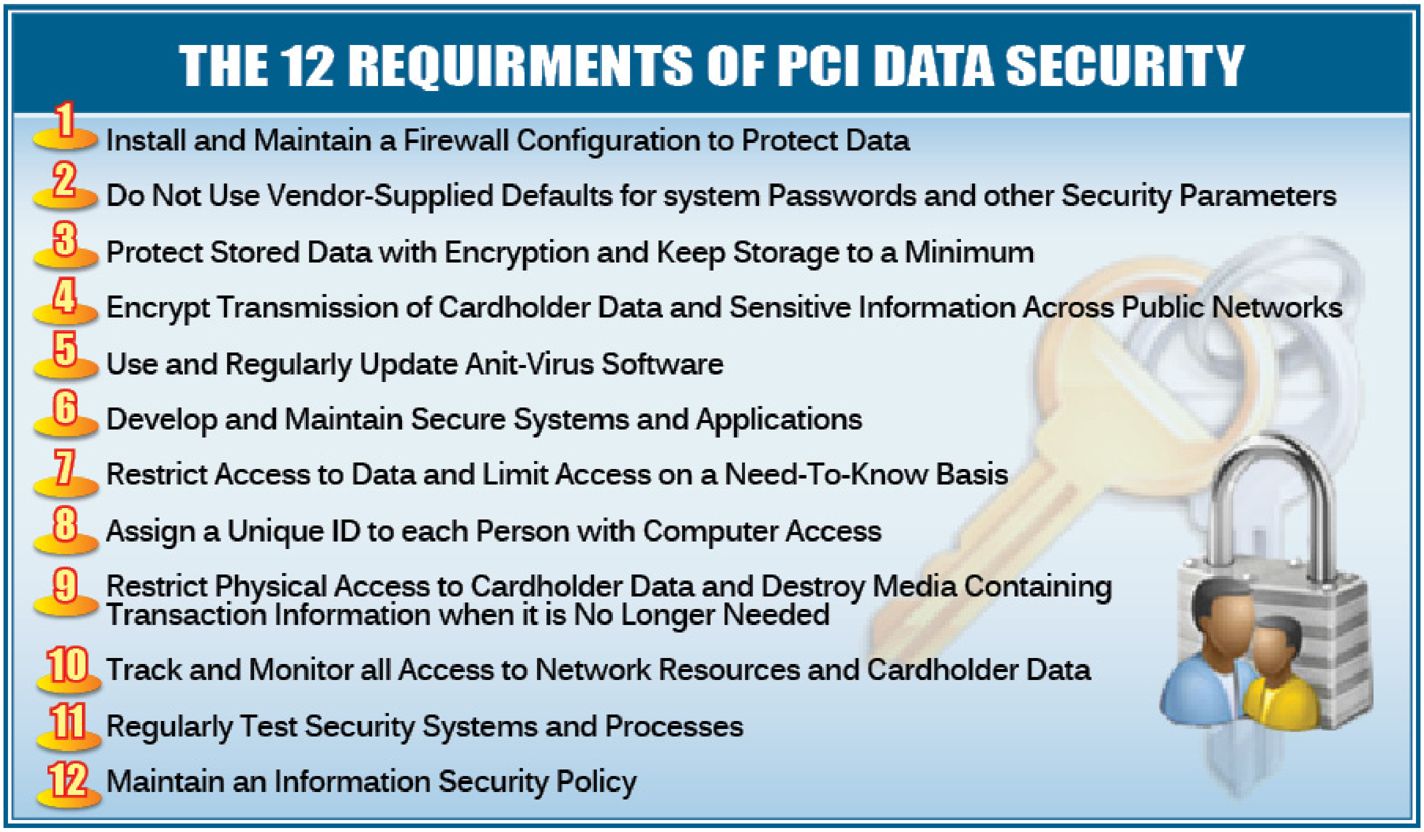
The institution campus network engineering team must properly isolate PCI traffic to certain parts of the network. The value of a properly segmented network to handle PCI traffic cannot be understated.

The service provider must have proper network segmentation, the use of new credit card processing equipment that supports hardware data encryption or data tokenization, and regular security scans of the environment.

An IT security plan will aid in identifying the proper solution. Do not underestimate the need for network segmentation. Improper documentation and network configuration combined with a lack of clear understanding by IT and business administrators may create a costly problem for the institution without adequate safeguards.

Hopefully this article has made you smile and scared you just a little bit. The PCI monsters are indeed under the bed, but with a good flashlight and some clear understanding, we can keep them at bay.

Patrick A. Jenkins
Director of Information
Technology Audit
404-962-3027
Email: Patrick.jenkins@usg.edu



THE 12 REQUIRMENTS OF PCI DATA SECURITY

1. Install and Maintain a Firewall Configuration to Protect Data
2. Do Not Use Vendor-Supplied Defaults for system Passwords and other Security Parameters
3. Protect Stored Data with Encryption and Keep Storage to a Minimum
4. Encrypt Transmission of Cardholder Data and Sensitive Information Across Public Networks
5. Use and Regularly Update Anit-Virus Software
6. Develop and Maintain Secure Systems and Applications
7. Restrict Access to Data and Limit Access on a Need-To-Know Basis
8. Assign a Unique ID to each Person with Computer Access
9. Restrict Physical Access to Cardholder Data and Destroy Media Containing Transaction Information when it is No Longer Needed
10. Track and Monitor all Access to Network Resources and Cardholder Data
11. Regularly Test Security Systems and Processes
12. Maintain an Information Security Policy

Reference Information

2 CFR 200, U.S. Office of Management and Budget
Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards

USG Information Technology Handbook
http://www.usg.edu/information_technology_handbook/

PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, Edition 4, By Brandon L. Williams

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 OIAC Newsletter

"Creating A More Educated Georgia"