The STRAIGHT and NARROW

Volume 3, Issue 15

February 1, 2011

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:

From the Chief Audit Officer - Outside Activities

John M. Fuchko, III

University System of Georgia institutions rightly pride themselves on "doing the right thing" with respect to students, employees, external stakeholders, the community, and all of the many groups impacted by our work of teaching, research, and service. The nature of teaching, research, and service requires ongoing and frequent interaction with outside parties. Additionally, rules with respect to intellectual property may generate legitimate opportunities for employees to financially benefit from some research activities. Unfortunately, an employee may occasionally step outside the bounds of ethical behavior and put the reputation of the institution at risk.

It is not possible to identify every potential instance of inappropriate behavior. However, the following questions and suggestions should assist an institution in ensuring that outside activities are well-managed.

- Do employees comply with Board Policy 8.2.15.1 (http://www.usg.edu/policymanual/section8/policy/8.2_general_policies_for_all_personnel/#p8.2.15_outside_activities) and obtain approval from the President before engaging in regular outside activities?
  - Note: All activities, except single-occasion activities, require an employee to "report in writing through official channels the proposed arrangements and secure the approval of the president or his/her designee" prior to engaging in the activities.
  - Are supervisors occasionally reminding peers and colleagues of these requirements?

- Board Policy 8.2.13.1, #4 (http://www.usg.edu/policymanual/section8/policy/8.2_general_policies_for_all_personnel/#p8.2.13_gratuities) permits an employee to receive "Actual and reasonable expenses for food, beverages, travel, lodging and registration provided to permit participation in a meeting, demonstration, or training related to official or professional duties if participation has been approved in writing by the Chancellor, the President, or his/her designee."
  - When approving travel to a conference, is the approving official confirming the payment arrangements with the employee before travel?
  - Is the approving official ensuring that the employee is obtaining written approval for any payment by an outside party?
  - Is the approving official confirming that the employee is not requesting reimbursement for an expense already paid by an outside party?

- Board Policy 8.2.15.2 (http://www.usg.edu/policymanual/section8/policy/8.2_general_policies_for_all_personnel/#p8.2.15_outside_activities) encourages a faculty member to conduct consulting activities that are professional in nature and based in the appropriate discipline … ." However, the policy also requires an institution to adopt guidelines that minimally address:
  1. "A plan for reimbursing the institution for use of the institution's personnel, facilities, equipment and/or materials consistent with rates charged outside groups or persons.
  2. A procedure for obtaining prior approval of the president or his/her designee.
  3. A procedure for defining and prohibiting conflicts of interest."

The overriding principle in all of these policies is disclosure and oversight by a supervisor. Implementation of these policies does not need to be overly burdensome; however, institutions will be well served to ensure that they are aware of and monitoring outside activities.

Is your Bank Account at Risk from an Illegal ACH Transfer? Could you lose Millions?
by Scott Woodison

A new type of computer fraud has recently emerged which has the capability to cause major harm to businesses and educational institutions. The press recently reported that the University of Virginia's College at Wise, a 4-year public liberal arts college located in the town of Wise in south-western Virginia, had $996,000 stolen from its account at BB&T Bank through an illegal ACH transfer. Thieves were able to compromise a computer belonging to the university's comptroller and transfer the funds from the institution's accounts at BB&T Bank to an account at the Agricultural Bank of China. The attackers used a computer virus to steal the online banking credentials and perform the transfer of funds without the university's knowledge or permission.

This is just one of a number of illegal account takeovers which have been occurring with increasing frequency in the past year. In August, 2010, criminals were able to obtain the on-line banking credentials for the Catholic Diocese of Des Moines and steal $600,000 from the Diocese's accounts at Banker's Trust of Des Moines. Once money is withdrawn from the account it is often moved and quickly dispersed to multiple overseas accounts where it is withdrawn by so-called money mules recruited to retrieve the funds. Once withdrawn, the chance of recovering the funds quickly decreases. The FBI estimates that corporate account takeovers have cost U.S. business more than $100 million over the past two years.

Unlike consumer credit card fraud, current banking regulations do not require a bank to reimburse an account holder if fraudulent ACH transfers are made from their accounts. This can result in an account being drained and the account holder being wiped out with limited recourse.

Institutions which make use of ACH transactions need to take extreme care in protecting their logon credentials; IDs and Passwords. Many ACH credentials are being compromised by use of computer viruses and malware. The Zeus banking Trojan, which is able to identify and store banking information from infected computers, has been involved in many recent account takeovers. Institutions should consider dedicating a single computer for ACH transfers and prohibiting e-mail or other activities on this system. The software should be kept at current patch levels and anti-virus software enabled. If two-factor authentication is available from institution's bank, this increased level of security should be used. (Two-factor authentication involves use of a hardware token along with an ID and password.) Controls such as transaction limits should also be implemented if possible.

Take the time to review your ACH transfer procedures. A malicious exploit in this area could have disastrous results. Please feel free to contact me for additional information.

Scott Woodison, Director, Compliance & Enterprise Risk, scott.woodison@usg.edu, 404-656-2265.

Top Ten Good Management Practices

1. Read all requests to spend University money before you sign them or approve them electronically (*Check Requests*, *Travel Authorizations*, payroll time sheets, etc.). Never sign a document unless you have reviewed at least the most important information on that document. Satisfy yourself it is a wise use of taxpayer and student funds.
2. Develop written procedures for critical operations. These serve as a resource for current employees and a good training tool for new employees.
3. Develop measurable annual department goals based on your department's mission and strategic goals. Create and action plan to achieve goals and communicate to all employees.
4. Make sure each transaction has at least two people involved: one initiator and one approver. Separate two duties to reduce the possibility of errors.
5. Print a detail transaction report from Banner once a month and review it for unusual transactions. Investigate anything that doesn't look right.
6. All cash and checks should be processed through the Cashier's Office. On the rare occasion that you do need to collect cash (this should be rare and exceptional), deposit all cash and checks received to the Cashier's Office daily. If something has to stay in your office overnight, lock it up.
7. Don't be satisfied with "the way we've always done things." Review your processes on a continuous basis for inefficiency and duplication of effort.
8. Ensure all expenditures have a clear business purpose. If the purchase is for something that *could* be construed as personal, clearly document the business purpose on the invoice or receipt.
9. Maintain good supporting documentation for all purchases. Ask yourself, "what would my supervisor or an auditor want to see?"
10. Make sure time sheets are reviewed and signed off by a supervisor or someone who is familiar with the employee's work hours.

Used with Permission of:

Jodi Bailey, CPA/CIA/CCSA | Chief Audit Executive |
Utah State University | jodi.bailey@usu.edu

IT Department Inundated with Problems? GSW has a Solution…

by Dean Crumbley, Tim Faircloth and Royce Hackett

You would have to be in a coma or using a Mac not to have noticed that Internet browsing today comes with increasing attempts to spy on, hijack, or otherwise infect your computer. At Georgia Southwestern State University (GSW) in Americus, Georgia, technicians have been fighting an on-going battle for the last few years, only to see more workstations infected with malware, spyware, adware, and viruses. In an attempt to combat the escalating infections and address recommendations arising from a consulting engagement performed by the Board of Regents, GSW invested in an enterprise firewall to control and manage web users, applications, and content.

In November 2009, the Office of Internal Audit and Compliance (OIAC) visited the campus of Georgia Southwestern to assess the information technology controls in place for mitigating the risks and threats associated with Identity Management, Access Control, and Network Perimeter Security. One recommendation made by the auditor recognized the need for additional technical controls and tools to monitor, identify, and mitigate threats on network segments and computer hosts. The consulting engagement report specifically noted that GSW needed to implement "an appropriate level of network content management to deter abuse or misuse of campus network bandwidth and infrastructure resources."

In order to combat the escalating number of malware infected computers and create a layer of security to mitigate web-borne threats, GSW IT management decided to invest in a web filter which would provide content filtering, application blocking, and malware protection. This web filter was purchased with the goal of supplementing existing firewall capabilities by controlling web applications, users, and content; not just ports, IP addresses, and packets.

The new web firewall was placed in-line at the campus PeachNet handoff in August 2010. Although the device is capable of acting as an "all-in-one" perimeter security solution, GSW deployed it as an additional layer of protection between the existing firewall (which already incorporated intrusion detection and prevention) and the internal network. The device was configured to block websites identified as containing malware and spyware, as well as known phishing sites. It was also set up to manage illegal peer-to-peer traffic and proxy applications.

The reduction in technical support requests concerning malware-infected machines was immediate. A review of help desk tickets revealed 95 workstations infected with malware between August - November 2009 and only 28 infected workstations during the same period in 2010, a significant reversal in the persistent trend of increasing incidents of malware infected workstations. A critical advantage of this reduction in support requests was that technical support staff could concentrate on other tasks.

"It's a huge step forward, enabling a more proactive approach to IT support," said Lynda Shaw, GSW IT support coordinator. "Technicians have been able to change their focus, allowing them to make progress on other ongoing projects, such as our migration to Microsoft Exchange."

The deployment of the network content filter resulted in an increased ability to manage the utilization of GSW computing resources. The removal of offending network activity leaves more bandwidth for legitimate purposes, resulting in better connection speeds for everyone.

IT Department Inundated with Problems? GSW has a Solution… (cont)

In addition to filtering network traffic based on the web content, this device has provided GSW with a tool that logs the traffic associated with threats and vulnerabilities. As this data is collected, computers already infected may be detected in the firewall logs, allowing technicians to seek out and remedy the offending workstations.

In summary, deployment of the network traffic / web content filter at GSW resulted in increased efficiencies of both technical support staff and utilization of computing resources. It was a successful example of a technical control that not only mitigated risk, but also reduced the technical workload.

Author Bio: **Royce Hackett**, Director of Information and Instruction Technology Department, Georgia Southwestern, has been with the University for 14 years. He can be reached at the following:
Phone: (229) 931-2641
Email: royce.hackett@gsw.edu

Author Bio: **Dean Crumbley**, Network Administrator and Information Security Officer, has ten years of network experience and six years as network administrator, with twelve of those years at Georgia Southwestern. He can be contacted as follows:
Phone: (229) 931-2074
Email: dean.crumbley@gsw.edu

Author Bio: **Timothy Faircloth**, System Administrator, has been with Georgia Southwestern University for five years. He can be contacted as follows:
Phone: Phone: (229) 931-5076
Email: tim.faircloth@gsw.edu

Reminder: Acceptable Methods of Federal Effort Reporting
By Chuck Fell

Time and effort reporting is the federally mandated method of certifying that the salary and benefits charged to a Federal grant are reasonably accurate. An acceptable effort reporting system requires a signature of a responsible official with a suitable means of verification that work was performed. Because the federal government mandates effort reporting, it is incumbent upon institutions receiving federal funding to maintain accurate and auditable systems and records.

2 CFR 220, Section J.10 (OMB Circular A-21) describes three acceptable effort reporting systems:

1. After-the-Fact Activity Report System
2. Plan-Confirmation System
3. Multiple Confirmation System

Note: After-the-Fact Activity Reporting System **must** be used by classified employees. Professional and professorial employees may use any of the three reporting systems.

After-the-Fact Activity Report System

Under this system, the distribution of salaries and wages by the institution will be supported by activity reports, reflecting the percentage distribution of activity of employees. Charges may be made initially on the basis of estimates made before the services are performed.

For professorial and professional staff, the reports will be prepared each academic term, but no less frequently than every six months. For other employees, unless alternate arrangements are agreed to, the reports will be prepared no less frequently than monthly and will coincide with one or more pay periods.

Plan-Confirmation System

Under this method, the distribution of salaries and wages of professorial and professional staff applicable to sponsored agreements is based on budgeted, planned, or assigned work activity, updated to reflect any significant changes in work distribution.

Multiple Confirmation System

Under this system, the distribution of salaries and wages of professorial and professional staff will be supported by direct cost records to reflect the distribution of activity expended which is to be allocable as direct cost to each sponsored agreement. There will also be F&A cost records to reflect the distribution of activity to F&A costs. These records may be kept jointly or separately; however, they are to be certified separately.

For additional requirements and details, please refer to OMB A-21.

Tips On Spending Federal Grant Money
by Sandy Evans

Recent announcements from USG institutions have elevated community awareness and pride. Significant grants totaling millions of dollars in technical, medical, environmental, and biofuel research place Georgia in the forefront of many aspects of innovation.

Along with the grants, collaborative partnerships, and resulting recognition, the institutions need to be ready for the challenges of administrative precision in adhering to regulations, timelines, and other requirements. Amidst the euphoria of forming a technology company or winning a biomedical grant, the institutions need to ask, "Are we ready to maximize the impact of this grant/ opportunity, track the costs of the research, and accurately report to the funding entity?"

If a grant or budget was designed carefully and realistically, the research project should be able to spend exactly the amount received and accomplish the objectives. In order to do this and stay within the regulations, recipients should have an understanding of basic terms and procedures in spending grant or contract money. For instance, recipients should be familiar with:

- **Allowable Costs:**

Every funding agency has categories of items for which grant recipients may spend money, and categories for which they may not. For federal grants, for instance, funds may not be used for "entertainment." As an example, principal investigators (P.I.) may not know that refreshments served at a project-related meeting may be classified by the funding agency as entertainment and, therefore, may not be allowable. For other funding agencies, the award notice or the grant application materials will often list allowable and unallowable costs. What happens if grant funds are spent on an unallowable item? The money will have to be given back, usually accomplished by cutting another expense in the grant budget.

- **Cost Reimbursable Awards:**

Federal awards received can be on a "cost reimbursable" basis. As a result, the money must be spent first, and then reimbursed. In order to be reimbursed, documentation must be presented to substantiate that the funds were spent on allowable expenses. Without documentation or if an expense was not allowable, the money cannot be recovered.

Since account balances for cost reimbursable awards always run a deficit, the P.I. should to do more than just check their account balance to make sure spending is consistent with the budget. The P.I. should also be aware that it is not possible to have "leftover" money from a cost reimbursable award. Without documentation of actual spending of the whole award, the unexpended funds go back to the funding agency at the end of the grant period.

- **Other Payment Structures:**

Certain funding agencies will pay lump sum installments every quarter, or may even award the entire amount up front. With installment plans, release of the funds for the next quarter is often contingent on submitting a report of activities completed for the quarter just ending. This is probably the most common for state-administered grants. Extra money at the end of the grant period usually must be returned to the funder.

Tips On Spending Federal Grant Money, (cont.)

- **Documenting Expenditures:**

Undocumented expenditures are considered not includable. There must be documentation to show that money was spent properly, or the funds cannot be recovered. Generally, the documentation is via invoices, receipts, payroll records, etc. Hence, if the receipt is lost, the expense cannot be reimbursed.

- **Documenting Time and Effort:**

The biggest single budget category for most grants is personnel. The funding agency is essentially buying the time of the persons named in the grant budget and paying them to execute the project. It is important to document that the time was spent as agreed and the money was spent appropriately.

- **Tracking Expenditures:**

Although there are usually reports that show budgeted funds compared to what has been expended to-date, a P.I. should not depend solely on these statements to track expenditures. Statements can be a month or more behind; moreover, they occasionally contain mistakes. If the P.I. is seriously over spending or under spending funds, he or she may not know until it's too late. Expenditure reports should be reviewed on a timely basis. Most costs are typically in the personnel line; therefore, the review should not require extensive time.

- **Rollover of Unexpended Funds/No Cost Extensions:**

Occasionally, money may remain at the end of an award year. Perhaps, equipment or services cost less than anticipated or delays pushed cost into the next year. If there is a good project-related use for the extra funds, the P.I. ***may*** be able to re-budget them. The P.I. must be careful to avoid the appearance of trying to spend the extra funds before time runs out. For instance, buying a computer in the last month of a project usually is difficult to justify.

If the P.I. needs to have funds available in the next year of the project, he or she must request permission from the funding agency to roll funds over into the next award year. The P.I. typically must request the roll-over, since it is not done automatically. The request should be submitted as soon as the need is apparent. Funding agencies are not sympathetic to last minute roll-over requests, especially if they have published time limits after which requests are not accepted.

When nearing the end of the whole grant period with excess funds, the P.I. can request a no-cost extension. This basically extends the end date of the award, allowing remaining funds to be spent as the project is completed. As with rolling over funds, the P.I. must get permission and the earlier the better.

- **Closing Out:**

Depending on the funding source, a final report of expenditures may be required at the end of the grant period. Because these reports are required, all expenditures must be finalized and the account closed within the specified time. Most funded projects do not allow the institution to retain residual funds. Therefore, when the time is up the funds must be spent or returned.

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 sandra.evans@usg.edu *and we may feature it in the next or future issues of the Straight & Narrow.*

Any other comments or questions?
Contact Sandra Evans at sandra.evans@usg.edu

We are looking for suggestions and feedback.