R·I·T

Institute Audit, Compliance & Advisement
Achieving Excellence Through Collaboration

the Quaestor Quarterly

Volume 7, Issue 1 Summer 2012

Cash, Checks, and Credit Card Receipts, Oh My…

Many RIT colleges and divisions sponsor events (i.e., alumni functions, club or charity fundraisers) or perform services which require the collection of event fees, donations and other related funds. This revenue may be in the form of cash, checks, credit card receipts or even Tiger Bucks. Even in situations where the amount of funds being collected is small, it is important to ensure that there are adequate processes in place to verify that all receipts have been accounted for and deposited completely, accurately, and in a timely manner.

Following are some simple practices that can be implemented to enhance the funds collection function:

Physical Security

Did you know that Public Safety offers a Cash Handling Safety Procedures workshop through the Center for Professional Development?

- All cash and check receipts should be kept secured in a locked drawer or safe and deposited with Student Financial Services on a timely basis (within a day or two of receipt).
- All checks should be endorsed "For Deposit Only" immediately when received.
- Customer credit card numbers should be kept secured. Any payment slips with credit card numbers should be shredded or if there is a legitimate business need to retain them, then the number should be redacted (blacked out) after the transaction is processed.

Segregation of Duties

- There should be a proper segregation of duties in the cash handling function so that the collection, deposit, and reconciliation of funds to source documentation are performed by different employees.

(continued on p. 2)

IACA's Mission

Institute Audit, Compliance & Advisement promotes a strong internal control environment by objectively and independently assessing risks and controls; evaluating business processes for efficiency, effectiveness, and compliance; providing management advisory services; and offering training to the university community. We focus on preserving the resources of the university for use by our students as they prepare for successful careers in a global society.

Inside This Issue **Page**

IACA
Institute Audit, Compliance & Advisement

Cash, Checks, and...

(continued from p. 1)

Segregation of Duties (continued)

- In situations where due to limited resources, all of the cash handling functions cannot be properly segregated, at a minimum, an individual independent of the cash collection function should reconcile the funds collected to source documentation on a timely basis.
- Keep in mind that although an individual may not be responsible for collecting funds, if that individual has access to these funds then although there may be a functional segregation of duties in place, a true operational segregation of duties does not exist.
- No one individual should have the ability to access funds without anyone else knowing or having the ability to detect an error or irregularity (always use the "buddy system").

Supporting Documentation

- Source documentation should be maintained which supports the amount of funds that should have been collected. Examples include:
    - The number of tickets sold for an event
    - The number of items purchased for sale (i.e., t-shirts) and the number of items remaining after the sale (the difference will be the number of items sold)
    - Pre-numbered invoices
    - Pre-numbered customer receipts
    - Appropriate approval for any complimentary tickets/items distributed
- If multiple individuals are responsible for the collection of funds, then reference information should be available which makes it possible to trace who was responsible for the collection of each receipt (i.e., initial on pre-numbered customer receipt) in case a question later arises.

Reconciliation

- On at least a monthly basis, an individual independent of the funds collection function should reconcile the amount of funds recorded in the appropriate Oracle general ledger account back to relevant supporting documentation (see examples given above) to verify that all of the funds (cash, checks, credit card charges and Tiger bucks) were recorded completely, accurately and on a timely basis.

~~ Contributed by Nancy A. Nasca
IACA Senior Internal Auditor

~ Ask the Auditor ~

Submit a question to the IACA webpage http://finweb.rit.edu/iaca/forms/ask/ by August 15, 2012. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

Inform RIT

Inform RIT is a recurring column provided by the RIT Information Security Office. The column highlights current issues and initiatives that impact the RIT community. In this issue, we'll talk about avoiding identity theft online.

INFORMATION SECURITY

Avoiding Identity Theft Online: Detecting Online Scams & Phishing

Dear Webmail User,
You've recently exceeded your e-mail quota. Please provide your login name and password within 24 hours or you will no longer be able to login to your account.
Thank you,
The Webmail Team

Have you received an email like this? Did you click on the link and enter login information?

If you did, you've been phished!

Phishing is a common technique for identity theft. We've all received phishing emails or instant messages that appear to link to a legitimate site. These emails and websites are designed to capture private information, such as bank account passwords, social security numbers and credit card numbers.

RIT receives many phishing attacks each year. Some phishing attempts have targeted RIT Computer Account passwords. After the accounts were compromised, the attacker used them to send out thousands of pieces of spam.

Phishing is also used to trick employees into providing login information. Attackers often use this technique to gain access to corporate "secrets" and other confidential information.

This column provides tips on identifying phishing attempts and suggests a number of tools and techniques you can use to defend yourself and others from them.

How Phishing Works

- Phishers send out millions of emails disguised as official correspondence from a financial institution, e-tailer, ISP, etc.
- You receive the phish in your email.
- After opening the email, you click on the link to access your account.
- Clicking on the link takes you to a web site that looks just like a legitimate site.
- At this point, you enter your account and password information, which is captured by the person who sent out the phish.
- Some phishers will actually log you into the real site after capturing your information, so that you don't even realize you were on a forged ("spoofed") site.
- Phishing sites are also used to deliver malware. You may find that you've both compromised your private information and installed malware on your computer by responding to the phish.

(continued on p. 4)

"I believe in evidence. I believe in observation, measurement, and reasoning, confirmed by independent observers.

I'll believe anything, no matter how wild and ridiculous, if there is evidence for it.

The wilder and more ridiculous something is, however, the firmer and more solid the evidence will have to be."

- Isaac Asimov, scientist and writer (1920-1992)

(continued from p. 3)

Detecting a Phish

Phishing emails used to be easy to recognize because of their poor spelling and grammar. Now, phishing emails are often indistinguishable from official correspondence. Most phishing attempts try to create a sense of urgency to provoke a quick response. For example, many phishing emails threaten negative consequences unless there's a quick reply. Phishing sites may also be difficult to distinguish from legitimate sites because of their use of these techniques:

- URL masking/cloaking—phishing emails may display a link that appears to go to one site, but in reality goes to another.
- Modifying a legitimate email—phishers may simply copy an official email from a bank or retailer, and edit that email for their own purposes before sending it to you.
- Cybersquatting—phishing sites may rely on similar URLs, such as googkle.com, ebay-secure.com, upgrade-hsbc.com to fool users.
- Use of the @ symbol—the phishing URL may include the @ symbol somewhere within the address. When reading an Internet address, browsers ignore everything to the left of the @ symbol, so the address "ebay.com@fake-auction.com" would actually be "fake-auction.com."

Safe Practices

It's not always safe to just click on a link! Enter or copy the link into the address bar or go to the institution's website and navigate to the correct location as you normally would.

Check the properties of websites before entering information. You can check the properties from the file menu or by right-clicking on the web page and selecting properties.

Secure web sites use a technique called SSL (Secure Socket Layer) that ensures the connection between you and the website is private. The use of SSL is indicated by "https://" (instead of "http://") at the beginning of the address AND by a padlock icon, which must be found either at the right end of the address bar or in the bottom right-hand corner of your browser window. (A padlock appearing anywhere else on the page does not represent a secure site.)

Anti-phishing Tools

There are a number of tools available to help warn you of suspicious websites. Use one or more for your protection. For an updated list of anti-phishing tools, visit the RIT Information Security Phishing page at http://security.rit.edu/dsd/bestpractices/phishing.html.

Take a Phishing Quiz

Do you think you can identify a phishing attempt successfully? Find out by taking the SonicWall phishing quiz at http://www.sonicwall.com/furl/phishing/.

~~ Contributed by Ben Woelk
Policy and Awareness Analyst
Information Security Office

Word on the Street

The word 'audit' comes from the Latin root audi, which means 'to hear'. So why does the word 'audit' strike fear and loathing into so many of us? No doubt the fear results from the perception that when we are audited, the auditors will find something less than perfect. In truth, this perception is well founded! A good audit will find errors in processing, policy, and documentation because an audit is meant to root out these process errors so they can be corrected before they become real problems.

Now the good folks at Institute Audit, Compliance, and Advisement (IACA) know all about the reaction people have when they hear they are to be audited. In response, they make their first priority to put you at ease by demystifying the audit purpose. Steve Morse and his staff at IACA do an excellent job at explaining the purpose of an audit and the reason for policies. In doing so, the tension of an audit is eased and people can rest a bit easier.

We know when it comes to audits, IACA takes a collaborative partnership approach. But what about the other 'A' in IACA? Another service that IACA provides is advisement, which means IACA can help determine what processes are needed and how they can be structured. Recently Academic Affairs took advantage of this service by asking IACA to become involved with our work to review policy at RIT for the calendar conversion. IACA gave our team some great insight, and the staff was very willing to roll up their sleeves and assist in the process. So the next time you find yourself or your project being audited, don't panic; IACA is there to help.

~~ Contributed by Jeremy Haefner
Provost and Senior Vice President for
Academic Affairs

What about ethics in the workplace?

To learn more about RIT's Code of Conduct and the RIT Ethics Hotline, check out

http://finweb.rit.edu/svp/ethics/

Training Opportunities Provided by IACA

IACA's Internal Controls and Fraud in the Workplace class is two and one half hours in length and is required to receive the RIT Accounting Practices, Procedures and Protocol Certificate of Completion. However, anyone interested in learning about internal controls and fraud prevention is welcome to attend.

To learn more about these important topics, sign up for IACA's Internal Controls and Fraud in the Workplace class at the CPD website:
http://finweb.rit.edu/cpd/leadership/internalcontrolsandfraud.html

Upcoming Sessions:

July 17, 2012 9:00 - 11:30 am	October 17, 2012 9:00 - 11:30 am	January 15, 2013 1:30 - 4:00 pm

Institute Audit, Compliance & Advisement
Achieving Excellence Through Collaboration

IACA TEAM:

Steven M. Morse '86, CPA
assistant vice president
475-7943

Patrick M. Didas '90, CPA, CFE, CCA
associate director
475-6826

Wendy J. Roy, CPA
senior internal auditor
475-7011

Nancy A. Nasca, CPA, CIA
senior internal auditor
475-5293

Christine M. VanHemel '12
staff & audit assistant
475-7647

Grace G. Denny
co-op student internal auditor
475-4318

Pop Quiz Challenge

Take the Pop Quiz Challenge! Correctly answer the question below and you will be entered in a drawing to win a prize valued at $15. One lucky winner will be chosen randomly and notified by email.

Question: On average, the most expensive corruption scheme committed by employees is ...

A. Accepting illegal gratuities

B. Economic extortion

C. Undisclosed conflicts of interest

D. Bribes and kickbacks

Post your answer to our Quiz webpage at:
https://finweb.rit.edu/iaca/forms/quiz/

The winner's name and answer will be included in the Fall '12 Quaestor Quarterly Newsletter.

****

Congratulations to Kristine Shamp from Student Affairs for correctly answering the previous issue's Pop Quiz question.

The question and the correct answer was:

How often do employees of RIT need to complete an RIT Individual Conflict of Interest and Commitment questionnaire?

A. Upon hire

B. Annually

C. Whenever circumstances change that might give rise to an actual or potential conflict

Correct

D. All of the above

R·I·T