



AUDIT Newscast

University Internal Audit

Fall 2010

Audit and Management Advisory Services

In This Issue

- Welcome!
- Who We Are...
- Meet an Auditor
- Audit Query
- Today's Best Practice
- Responsibility: We're in this Together!
- Suspect Financial Fraud?

Visit us Online!

Our web site has a lot more detailed information, articles and resources.

Visit us at:

www.massachusetts.edu/audit/

Contact Us:

General Inquires

InternalAudit@umassp.edu

rharrison@umassp.edu

774-455-7551

774-455-7550 Fax

Welcome!

Welcome to the third edition of **Audit Newscast!** In each issue, we hope to provide answers to your specific questions from our "Audit Query" Q&A section, provide tips on 'best practices', and share events highlighting control issues and successes throughout the University. In this issue look for articles about "Phishing Emails" and "Tips for Credit Card Users". Our hope is that by providing this information we can increase awareness of responsibility and assist you in implementing effective controls in your areas of operations.

A Note About Our Audit Committee Trustees -

Two UMass Board of Trustee members have recently taken over the helm of the Audit Committee: Chair Maria D. Furman (Wellesley, MA), and Vice-Chair Victor Woolridge (Springfield, MA). Both have close ties to individual campuses and support the University's mission of affordable education for all. They believe a proactive Internal Audit function can help sustain that goal. "We wish to strengthen system-wide efficiencies and encourage our auditors to research and advise on best practices," asserts Maria. Likewise, Victor states that we "depend on our internal auditors to identify business risks and recommend ways of controlling risks." We welcome the leadership, guidance, and new ideas that Maria and Victor bring to the Audit Committee.

Thank You - Bob Harrison, Associate Vice President & Director

Who We Are...

While many of you are familiar with our office and some may even have been visited by one or more Internal Audit staff, you may not know us,

Robert Harrison, Director, CIA, CPA, CFE: rharrison@umassp.edu – 774-455-7560

Brian McCormick, Manager, CISA: bmccormick@umassp.edu – 774-455-7556

Chris Galica, Senior Auditor, CIA, CPA: cgalica@umassp.edu – 774-455-7557

Derek Scano, Senior Auditor, CIA, CFE: dscano@umassp.edu – 774-455-7552

Lance Watkins, Senior Auditor, CFE: lwatkins@umassp.edu – 774-455-7553

Sarah Mongeau, Senior Auditor, CPA: smongeau@umassp.edu – 774-455-7554

Dan Sarazen, Senior IT Auditor, CISSP, CISA: dsarazen@umassp.edu – 774-455-7558

Deborah Fisher, Administrative Assistant, dfisher@umassp.edu – 774-455-7551

Meet an Auditor - Sarah Mongeau

Sarah, a Senior Internal Auditor, joined us in February of 2008.

Sarah has over twenty years of diversified experience in both public and private accounting, business support, performance reporting and financial analysis. Sarah holds a Master of Science Degree in Accountancy from Bentley College and is a CPA in Massachusetts. She also enjoys running and playing soccer. She coaches her daughter's soccer team and is the treasurer of the Grafton/Wachusett Lakers Youth Hockey Association.

May Internal Audit Services be Requested?

Senior management may contact the Audit Director to request our services. The request will be reviewed to determine how we can best serve your needs and coordinate a review within our schedule. We also rely on an extensive Campus Audit Liaison network to help us manage all audit activity of the University.

The Audit Liaisons for each campus are:

Amherst:	Andrew Mangels	413-545-1675	amangels@admin.umass.edu
Boston:	Leanne Marden	617-287-5196	leanne.marden@umb.edu
Dartmouth:	Suzanne Audet	508-999-8076	saudet@umassd.edu
Lowell:	Steve O'Riordan	978-934-3450	steven_ORiordan@uml.edu
Worcester:	Nancy Vasil	508-856-8606	nancy.vasil@umassmed.edu
President's Office:	Christine Wilda	774-455-7549	cwilda@umassp.edu

Audit Query



If you have a question, most likely someone else is wondering the same thing. The Internal Audit staff will do our best to give you good advice. Send your questions to:

InternalAudit@umassp.edu

Submit the most meaningful "Audit Query" for the next Audit Newscast issue and you may win a sweatshirt emblazoned with the UMass logo.

Phishing Emails

External fraud and phishing attempts are always increasing. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Cyber Crime surpassed drug trafficking as the number one criminal money maker in 2008. Internal Audit has received notification of numerous phishing emails that attempted to fraudulently obtain secure financial information.

Here are some tips to avoid being a victim of a phishing scam:

- Be suspicious of any email with urgent requests for university or personal financial information
- Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don't know the sender or user's handle
- Avoid filling out forms in email messages that ask for personal financial information
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser

Remember not all scam sites will try to show the "https://" and/or the security lock. Also get in the habit of looking at the address line. Were you directed to PayPal? Does the address line display something different like "<http://www.gotyouscammed.com/paypal/login.htm?>"

Always know where your web address is directing you. Ensure that your browser is up to date and security patches are applied.

Today's Best Practice

Tips for Credit Card Users

Credit card scams are always increasing, especially in today's economic climate. We spend a lot of time reviewing business practices and wanted to offer some suggestions to keep your cards and your credit history safe:

- Be sure to secure your credit cards when not in use, and keep university cards separate from personal cards to prevent accidental personal purchases on the business cards.
- Be alert to credit card scams. A thief can steal your card number and purchase thousands of dollars of merchandise in a short period of time.
- Your campus ProCard and Travel Card offices, as well as your credit card banks, are reviewing your transactions for unusual activity. Please be sure that your bank has your up-to-date phone numbers.
- If a vendor offers to split a transaction to complete a ProCard purchase above your dollar limit, please report the vendor to your Campus ProCard Manager. Instead, the Manager can temporarily increase your limit.
- If you are changing departments, contact your campus ProCard Manager to close cards that you will no longer use. It is not a good idea to keep them open after you leave the department.
- Everyone must be attentive to their credit card activity. For ProCard users, this means keeping all receipts, avoiding sales tax, and obtaining your supervisor's approval.

Following these practices will help to ensure that your credit cards and credit history remain safe.

Responsibility: We're in this Together!



Wondering what internal control has to do with you? Everyone at the University has some level of responsibility for internal control. The level will vary depending on your role. All employees are responsible for communicating operational deficiencies, deviations from established procedures, and violations of law or policy. You can report these to your supervisor and /or the Internal Audit department.

Suspect Fraud?

If you suspect, or discover financial fraud in your department, either follow the Guidelines on our website below, or your Campus Controller's website, or call Internal Audit. All calls are handled confidentially when possible.

www.massachusetts.edu/audit/fraud



Report by Phone

1-774-455-7555



Report by Email

AuditLine@umassp.edu

Suspect Financial Fraud?



Fraud is defined generally as a willful or deliberate act with the intention of obtaining an unauthorized benefit, such as money or property by deception or other unethical means. Fraudulent acts may include: embezzlement; forgery or alteration of documents; misappropriation of funds, supplies, inventory and equipment; authorizing or receiving payment for goods or services not performed; and receiving payment for time not worked.

Many of you have never encountered fraud issues at the work place; however, the fact is that ***Fraud Happens***.

The University has a Financial Fraud policy in place that provides information on how to report known or suspected fraudulent financial activity. Please see:

[University Fraud Policy and Guidelines](#) by using this link or viewing our web site at www.massachusetts.edu/audit.

You may also email us at AuditLine@umassp.edu or leave us a message on a confidential phone line at 774-455-7555.

Why do people commit fraud?

The answer to this question may help us understand that a fraud can be committed by anyone given the right environment. There are three elements common within all frauds: opportunity, need and rationalization. These three items make up what is commonly known as the "***fraud triangle***."

Opportunity Many organizations unknowingly provide their employees with opportunities to commit fraud. How? By not having appropriate controls in place to either prevent or detect misappropriation. In some departments, a small staff may make adequate segregation of duties unrealistic; however, appropriate management oversight and monthly review of accounting reports can be effective controls against fraud or theft.

Need What is it that causes one employee to commit a fraudulent act, while another remains honest? Financial need is the second element of the fraud triangle and can come from a variety of sources: the need to maintain a certain lifestyle, personal debts and financial losses caused by a poor economy, gambling losses, substance abuse or bad investments.

Rationalization This is the third and final element and the means by which a perpetrator "justifies" the fraud or theft. Some common rationalizations include:

- "I'm only borrowing it and I'll pay it back."
- "The department can afford it. Nobody is going to miss it."
- "They don't pay me enough; they owe it to me."

In this current economic environment, where need and rationalization may be more likely, it is more important than ever for everyone to keep a close eye on their departments so that an opportunity for fraud does not exist.