NEWSLETTER

Office of Internal Audit

Issue 3

CONTENTS

INTERNAL CONTROLS – A TOP TEN LIST

Internal controls, in their simplest form, are anything we do to help us achieve our objective. In your everyday life you use controls to some extent, including locking up your car before walking into work, committing passwords to memory, and keeping credit cards in a safe place. These controls are protecting your assets, limiting access to your data and preventing identity theft. So how can these simple concepts be applied to your job?

During the past year of performing audits and reviews on campus, I found myself continuing to provide a short list of things that would help alleviate risks within a certain area that I was working. I began to research best practices for internal controls and began comparing my list of controls to other resources.

Based on research I performed, I confirmed that my short list could be part of something bigger. The following is a list of controls that you can begin to implement in your area, if applicable. Keep in mind that the order of the list does not dictate the importance of the control because all are equally important.

I like to call this list The TOPS Ten List – Internal Controls (Late Show style).

10. **Identify Risk in Your Office** – risks are difficult to manage if you do not know what they are.

9. **Protect Data and Physical Assets** – lockup procurement cards, secure your offices/workspaces, and perform daily deposit procedures (if applicable).

8. **Maintain Adequate Supporting Documentation** – provide hard evidence to adequately verify that appropriate processes, policies and controls are being followed.

7. **Implement a Review and Approve Process** – an independent reviewer/approver should be involved with significant processes or transactions, especially if it's required per University policy. The review and approval should be DOCUMENTED to verify that those tasks were performed.

6. **Regularly Perform Reconciliations** – reconciliations bring two information points together to verify that those two points agree, which in my opinion is an underappreciated internal control. Reconciliations should be reviewed and approved by someone outside of the reconciliation process.

5. **Communicate** – share concerns timely so those concerns can be addressed and know where to go for assistance. Become familiar with University policies. Reach out to a supervisor, internal audit, the Ethics & Compliance hotline, etc.

4. **Segregate Duties** – ensure that errors and irregularities are prevented or detected on a timely basis. No single individual should have control over two or more phases of a transaction or operation (e.g. a reconciliation should not be reviewed and approved by the same person that performed the reconciliation).

3. **Practice Safe Computing** – never share your password with anyone under any circumstances.

2. **Promptly Correct Errors** – sometimes controls can break down due to misunderstanding or innocent human error. Errors detected at any given stage in a process should be corrected and reported to the appropriate individuals.

1. **Develop Written Policies and Procedures** – Although the University has centralized policies that all of the campus should be adhering to, sometimes the policies do not dive into the details. Also, there may not be a written University policy or procedure at all. Each area should develop its own comprehensive procedures manual or a Standard Operating Procedures manual. The manual will provide expectations, guidelines, and references to all employees in that area and can also be used as a training tool for new employees. The manual will be the base for providing consistency and continuity in its related area.

WHO STOLE MY IDENTITY?

According to the Identity Theft Resource Center, a cybercrime research and education group, data breaches are up approximately 20% from July 2013 to July 2014. Data breaches can vary from simple to highly sophisticated. The culprit can be a single individual or a group of people. The number of personal records exposed during the same period was over 10 million. Based on these factors, the question of, "who stole my identity?" may be a difficult one to answer.

Personal records can include personally identifiable information or PII, a legal concept that is the name given to a group of data used to distinguish an individual's identity. For example, PII includes a person's full name, home address, driver's license number, date of birth, SSN, etc. If PII is obtained by the criminals of the cyber world or the real world for that matter, it can assist them in stealing identities. They can open bank accounts and credit cards, and even file tax returns in your name while you are at work, at home or on vacation.

There are some practices that you can implement to deter you from becoming a victim. The first rule of protecting your PII – don't give it out to just anyone. If you **receive** a phone call and the person on the other end asks you to verify your information, say "No, I'm unable to do that at this time." The second rule, keep your passwords private and, when creating a password, consider substituting letters with numbers or varying the capitalization of the letters. Third rule, and this may be a difficult one for some, don't overshare on social networking sites. You can find out more by going to www.consumer.ftc.gov.

ETHICS & COMPLIANCE HOTLINE AND WEB SITE INFORMATION

In regards to internal controls, communicating gaps in those controls can make a difference and add value to the University. Please remember that you can remain anonymous when reporting to the WKU Ethics & Compliance Hotline. To report a concern or an issue, see the following:

Toll free: 1-877-318-9178

Web site: www.wku.ethicspoint.com

Please share this information with your faculty and staff.

Contact Us

Office of Internal Audit
WAB, G-18
1906 College Heights Blvd, #11002
270.745.4250
jennifer.miller@wku.edu
http://www.wku.edu/finadmin/ia/