Quaestor Quarterly

the

Volume 11, Issue 3

Fall 2016

revolution with the Changes....

Quaes·tor [kwes'tôr] ‘one who asks questions’

Rolling with the Changes....

We wanted to take this opportunity to allow a few new RIT employees to introduce themselves...

Aldwin B. Maloto

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
Inform RIT 3
Training Opportunities 5
Provided by IACA
COSO Corner 6
Pop Quiz Challenge 7

From Global Risk Management Services
Information Security Office

Aldwin B. Maloto recently joined RIT as the Information Security Officer (ISO) on July 1, 2016. He is a graduate of the Management Information Systems (MIS) program and the Executive Masters of Business Administration (EMBA) program at the E. Philip Saunders College of Business. Aldwin is also a Certified Information Security Manager (CISM) and a Certified Information Systems Auditor (CISA). He brings over 18 years of experience in Information Security and Information Technology. He has a high level of technical and security expertise with expert level knowledge of current data protection best practices, standards and applicable legislation, and is well versed with principles and techniques of security risk analysis, disaster recovery planning, and business continuity processes. Aldwin has a comprehensive understanding of industry frameworks, approaches, and standards such as COBIT, ITIL, NIST 8000, European Union Safe Harbor Framework, Payment Card Industry Data Security Standards (PCI-DSS), and SSAE 16. He also has regulatory expertise in the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, 42CFR, Gramm Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), US Patriot Act, and EU Privacy Directive.

Aldwin is excited to be part of RIT’s ISO. The ISO partners with the university community to achieve the university’s mission by maintaining an appropriate level of information security risk that is in alignment with our academic portfolio, research agenda and educational model. As a community, we strongly endeavor to appropriately preserve the confidentiality, integrity and availability of university information assets through the innovative use of the
Aldwin will chair the Information Security Council. The council is comprised of technical and senior management representatives from each College, Division and operating units across campus. The Information Security Council is the body responsible for the creation of Information Security Standards at RIT.

“I am thrilled to be back at my Alma mater, doing work that I am really passionate about. I am deeply honored to be working amongst some of the best minds in the industry and academia. The level of talent and diversity that you see on campus is really second to none, and I am very proud to be part of the RIT team.”

From Institute Audit, Compliance & Advisement

My name is Jeffrey Butler, and I’m the new Associate Internal Auditor in IACA. I attended St. Bonaventure University, where I received my BBA and MBA, both with a focus in Accounting. Since graduating, I’ve worked at both a Big 4 and a regional accounting firm, PwC and Insero & Co. CPAs, respectively. I’ve worked in consulting; audited for-profits, not-for-profits, and universities; and now I’ve found my way into internal audit and I couldn’t be happier to call myself a Tiger!

Jeffrey W. Butler

My name is Ginger Howe, and I recently became the Staff and Audit Assistant for the IACA Department. I am an alumni, so coming back to RIT was an opportunity for me to reconnect with the environment that motivated me to make a difference. I’ve worked in the hospitality, insurance, and healthcare fields. This background has helped me to achieve excellence in problem solving and customer satisfaction.

Ginger Howe

~~ Contributed by: Aldwin B. Maloto, Jeffrey W. Butler, Ginger Howe
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 the benefits of using a password manager. A special thank you to Eilysh Haeger, Information Security Communications Associate for drafting the original article.

**Why Use a Password Manager?**

Using a password manager is the easiest way to keep your personal and private information safe. A password vault stores your passwords securely, allowing you to save the information in the cloud or on your personal computer. This allows you to use truly random combinations in all of your passwords, making them much harder for malicious users or bots to crack. Password managers also protect you from giving away private information inadvertently. In fact, there are multiple reasons you should be using a password manager right now.

**Remember Only One Password**

A password manager stores all of your passwords in a single account. The master password to your safe is the only password you’ll ever need to remember.

**Generate Random Passwords**

Password managers can generate random passwords for each of your accounts. Password cracking programs are designed to guess the most common passwords first so completely random passwords are far stronger than those you come up with off the top of your head.

**Login to Accounts Simply**

You can login to accounts the easy way. Once you sign up for a password manager, you can install a browser extension that will autofill logins for you while still storing them securely.

**Easily Change Your Passwords**

Password managers make it easy to change or reset passwords. If a website you have an account with has been hacked, you can stay secure by using a built-in password generator to create a new password. Some password managers can even reset your passwords with the click of a button. You can also choose to change all of your passwords periodically for optimal security.
Inform RIT

(continued from p. 3)

Use the Convenient Autofill Feature

You can still use the form autofill feature when you have a password safe. Instead of letting your web browser save your form information, entrust your password manager to store your personal information safely.

Share Passwords Securely

You can share passwords to joint accounts with family or coworkers. Of course, it’s generally not recommended you give away your personal passwords, but for shared accounts, a password manager gives you the option to control who has access to passwords.

Store More Than Just Passwords

Answers to security questions, shopping profiles, memberships, and medical prescriptions are just a few examples of additional information that can be stored securely in a password safe.

Use the Same Password Manager Across Multiple Devices

Many password managers provide access across multiple devices. As we use our mobile devices more often (and as more websites provide optimized mobile experiences), this is increasingly important. Many of the password managers also provide support for passwords for apps.

Right now, several popular password managers are: LastPass, 1Password, KeePass, Dashlane, and RoboForm. If using a password manager at RIT, we recommend LastPass or KeePass.

Keep your personal information and accounts safe by switching to a password manager today!

Sign up for our DSD101 course, Introduction to Digital Self Defense, through CPD. Contact Ben if you’d like us to present DSD101 or provide information on other security topics to your department.

http://www.rit.edu/security/
Like RIT Information Security at www.facebook.com/RITInfosec
Follow us on Twitter: @rit_infosec
Image: https://checksum.biz/wp-content/uploads/2015/05/PasswordKeeper.png
This article was previously posted in May 2016 on the RIT Information Security website.

~~ Contributed by Ben Woelk
Program Manager
RIT Information Security Office
infosec@rit.edu

What about ethics in the workplace?

Learn about the RIT Ethics and Compliance Hotline
Internal Controls and Fraud in the Workplace

During the 2.5 hour Internal Controls and Fraud in the Workplace class, the importance of, components of, and the responsibility for establishing and maintaining effective internal controls are discussed. Various examples of what can happen when controls are non-existent or break down (i.e., fraud) are shared throughout the class. The session 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 a session at the CPD website.

Unit Level Risk Assessment—How to Advance Your Organization’s Agility

The first step towards successfully managing risks is to implement an effective risk assessment methodology. Risk assessment is a systematic process for identifying and evaluating both external and internal events (risks) that could affect the achievement of objectives, positively or negatively. During this two hour class, we will discuss the key components of an effective risk assessment process and how to integrate it into the business process to provide timely and relevant risk information to management. To learn more about this offering, see the corresponding CPD website.

Upcoming Internal Controls & Fraud in the Workplace Training Sessions:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday, October 12, 2016</td>
<td>9:00am to 11:30am</td>
<td>Louise Slaughter Hall</td>
</tr>
<tr>
<td>Tuesday, January 17, 2017</td>
<td>1:30pm to 4:00 PM</td>
<td>Louise Slaughter Hall</td>
</tr>
<tr>
<td>Thursday, April 13, 2017</td>
<td>9:00AM to 11:30AM</td>
<td>Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

Upcoming Unit Level Risk Assessment—How to Advance Your Organization’s Agility Training Sessions:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, December 13, 2016</td>
<td>10:00am to 12:00pm</td>
<td>Louise Slaughter Hall</td>
</tr>
<tr>
<td>Wednesday, April 5, 2017</td>
<td>10:00am to 12:00pm</td>
<td>Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

“Tell me and I forget, teach me and I may remember, involve me and I learn.”

— Benjamin Franklin
COSO Corner

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

As explained in previous editions of the Quaestor Quarterly, the COSO Framework (internationally recognized standard against which the adequacy and effectiveness of an organization’s internal controls are evaluated) was updated in May 2013 to further define the principles underlying the five components of internal control (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring). According to the Framework, these principles are fundamental concepts that must be present and functioning in order to achieve an effective system of internal control. In addition, the Framework includes points of focus or characteristics that are examples of behaviors or processes that would be expected to be in place to demonstrate that the related principle is in fact present and functioning. This edition of the COSO Corner will summarize the ninth COSO principle which is the fourth and final principle related to the Risk Assessment component of the COSO Framework, as well as the related points of focus.

Principle 9 – The university identifies and assesses changes that could significantly impact the system of internal control. The three key areas where the university should consider changes include:

- The External Environment – As economic, industry, and regulatory environments change, the university should consider the need to adapt and evolve. For example, as a result of recent revisions to the U.S. Department of Labor regulations governing exemptions to the Fair Labor Standards Act, Human Resources is working with senior leadership of the university to determine what actions are required in order for RIT to remain in compliance with the new regulations.

- The Business Model – The university should consider the potential impact of new business models on the system of internal control, changing reliance on foreign geographies, and new technologies. As opportunities arise to enter into new joint ventures or affiliation agreements to advance RIT’s Strategic Plan (e.g., to facilitate the expansion of global engagement), senior leaders should evaluate if revisions to current university policies and procedures will be necessary to support these new ventures.

- Leadership – The university community should consider changes in management and respective attitudes and philosophies on the system of internal control. This is particularly relevant for RIT with some of the recent changes in College leadership, and as we begin the search for a new president.

In the next Quaestor Quarterly, we will review Principle 10, the first principal related to the Control Activities component of the COSO Framework. Control activities are the actions established through policies and procedures to assist with the mitigation of risks which threaten the achievement of the university’s key objectives.

Reference

~~ Contributed by Nancy A. Nasca
Manager
Institute Audit, Compliance & Advisement
Watch IACA’s Monday Minute video series here!

This video series focuses on opportunities for improving internal controls and increasing awareness of various university processes, policies, and protocols. If you have questions, feel free to contact anyone in the IACA office using information on our webpage.

Past topics include: Information Security Standards, Lenel Card Swipe Access Management, Conflict of Interest & Commitment Disclosures, Records Management Policy, Risk Assessment, Giving Gifts to Individuals, and many others.

IACA TEAM:

Patrick M. Didas ’90, CPA, CFE, CCA
assistant vice president
475-6826

Wendy J. Roy, CPA
manager
475-7011

Nancy A. Nasca, CPA, CIA, CRMA
manager
475-5293

Jeffrey W. Butler, CPA
associate internal auditor
475-7849

Vernice M. Stefano, MBA, CISA
senior IT internal auditor
475-4318

Virginia Howe ’97
staff and audit assistant
475-7647

Matthew D. Hadorn
student internal auditor
475-6242

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:

According to the Inform RIT article, the reason(s) for using a password manager include:

A. The master password to your safe is the only one that you will need to remember for the password manager.

B. As we use multiple and mobile devices more often, a password manager becomes increasingly important.

C. Both A and B

D. None of the above

Post your answer to our Quiz webpage at:

https://www.rit.edu/fa/iaca/content/quiz

- Ask the Auditor -

Submit a question to the IACA webpage https://www.rit.edu/fa/iaca/forms/ask by December 30, 2016. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.