What’s New in IACA? (Part 2)

As reported in the last edition of Quaestor Quarterly, there were many changes in IACA over the past year. For this edition, I would like to introduce another change to the IACA team, me. My name is Vernice Stefano, and I’m the new Senior IT Auditor as of August of this year. My audit experience started at Bausch & Lomb (B&L) where, as a member of the PeopleSoft finance team, I assisted audit with data extraction and analysis, and later joined the audit team as an IT auditor. Then, I transitioned to the internal audit department at Xerox. I have also worked in a variety of industries including pharmaceutical, manufacturing, services outsourcing, government, hospitality, and insurance.

So what does an IT internal auditor do? Like any auditor, we help an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes; we provide management with a level of assurance that financial, operational, and system controls are adequate and effective. Providing assurance on various aspects of the university’s system controls is where you will find me.

Most IT audits center around IT general controls and how effective they are in preventing, detecting, or mitigating risk. There are many frameworks and standards by which IT general controls are evaluated including the International Organization for Standards or ISO (not to be confused with RIT’s Information Security Office), Information Technology Infrastructure Library (ITIL), the SANS Institute, Higher Education Information Security Council (HEISC), Control Objective for Information and Technology (COBIT), National Institute of Standards and Technology (NIST), and Payment Card Industry Data Security Standards (PCI DSS); this is not an exhaustive list.

The frameworks and standards identify hundreds of IT control activities that an organization can employ. However, most can be grouped into the following categories:

- **IT Governance** - or Tone at the Top.
- **Access Management** - management of data and system access, as well as physical and logical access. It includes password configurations as well as data, information, and system security.

(continued on p. 2)
IT control activities, continued

- Change Management – management of information and technology system changes. It includes system development life cycle management (although sometimes this is separated out as its own category) and configuration management.

- Operations – management of IT operations. It includes business continuity planning/disaster recovery planning, data center operations, system administration and support, and patch management.

- Vendor Management – management of third parties. It includes service level agreement (SLA) monitoring, third-party assurance reviews, and vendor life cycle management.

My work at the university will be to explore the nature of the system controls in place and the extent to which they are operating to promote an effective and secure IT environment. I am excited to begin my journey here at RIT and look forward to working with you along the way.

~~ Contributed by Vernice M. Stefano
Senior IT Internal Auditor
Institute Audit, Compliance & Advisement

Word on the Street

Normally when you hear the word “Audit,” it conjures up a major inquisition which might not result in a physical injury, but an injury to one’s self esteem that might be subject to ridicule. That was not the case at all with the IACA team who performed our most recent audit.

From the beginning to completion, the IACA team treated our Student Auxiliary Services team with the utmost respect and kindness as we progressed through our 2015 Housing Operations Audit. Now keep in mind that my operations in Student Auxiliary Services have thousands of moving parts, touch points, and yes—even opportunities for risk and failure on a daily basis. Over 7,000 students in our housing program can be a nightmare on its own, never mind having the peering eyes of those whose jobs are to identify areas needing improvement in our operations, which can create unwanted stress.

The IACA team never made us feel like we were “dead in the water;” instead they walked us through the process in a thoughtful and respectful manner while also honoring our difficult operational timelines. This was especially important this summer as a result of the 230-plus unexpected students we now have in housing due to a 10% increase in the freshman class. Additionally, IACA’s final report for the audit was thorough.

I never thought that I would say this, but after this painless experience with the IACA team, I’m looking forward to our next Student Auxiliary Services Audit.

~~ Contributed by Howard Ward, PhD
Associate Vice President
Student Auxiliary Services
Online Shopping Safety
The time of year spent with family, traveling, and shopping is upon us once again. With the holidays right around the corner, over 60% of Americans will be hopping online to buy and send their gifts. In the past five years alone, online shopping has grown nearly 30% with projections suggesting it may rise another 14% in the next few years.

With more people relying on the convenience of online shopping for their purchases, it’s important to remember safe shopping practices and tips so that you don’t succumb to identity theft, fraud, or scams that are in abundance online. Follow these tips to protect your privacy and information, and increase purchasing security.

1. **Use a Secure Computer**
   Make sure you are using a secure internet connection and not sending private information out on public computers that could contain malware. Additionally, make sure that your anti-virus, operating system, and web browser have the latest versions and security patches installed.

2. **Research the Company/Website**
   Investigate any retailer before you make a purchase from them. With sites like Amazon that have many different users selling products on their site, be sure to check the sellers feedback and rating to make sure they’re legitimate and have left other customers with good experiences.

3. **Research the Product/Service**
   Do the prices seem amazing or too good to pass up? Oftentimes, insane deals can indicate a counterfeit product or may contain links to a malicious website. Bottom line: if it seems too good to be true, it probably is.

4. **Use Strong Passwords**
   When creating an account on a site, make sure to use a strong password to help protect your private information. Remember to never use the same password twice and to add special characters, upper and lower case letters, and numbers to create a secure password!

5. **Make Sure Purchases are made on Encrypted Sites**
   You’re ready to create your account or submit a payment, but does the website’s address bar contain "shttp," "https," or a padlock in the web browser (typically in the address bar at the top or status bar at the bottom, depending on the site)? If not, the site might not be secure and it’s best to back away.

6. **Use a Secure Payment Method**
   Credit cards are one of the safest options when submitting online payments because of the federal laws in place to protect your liability against credit card fraud. Be wary of anyone who insists upon cash or wire transfers only.

   Extra Tip: Want to take it one step further? Find out if your bank or credit card issuer offers one-time use virtual card numbers!

(continued on p. 4)
7. **Monitor Your Accounts**

   Make sure to keep track of all your purchases and account histories. Print out orders, receipts, email confirmations, and product descriptions to keep on hand if anything goes awry. Follow up on purchases by monitoring your bank account and credit card statements to ensure unauthorized transactions don’t occur.

**For more information**

- RIT Information Security Safe Online Shopping & Banking
  [https://www.rit.edu/security/content/safe-online-shopping-banking](https://www.rit.edu/security/content/safe-online-shopping-banking)

- RIT Information Security How to Create a Secure Password
  [https://www.rit.edu/security/content/creating-strong-passwords](https://www.rit.edu/security/content/creating-strong-passwords)

- 11 Tips for Safe Online Shopping
  [http://www.pcmag.com/article2/0,2817,2373130,00.asp](http://www.pcmag.com/article2/0,2817,2373130,00.asp)

- Online Shopping Scams

- Fake Order Confirmations

- I’ll Never Fall for an Online Shopping Scam Ever Again

**Sign up for our new DSD101 course**, *Introduction to Digital Self Defense* through CPD.

**Contact Ben** if you’d like us to present DSD101 to your department.

http://www.rit.edu/security/

Like RIT Information Security at www.facebook.com/RITInfosec

Follow us on Twitter: @rit_infosec

~~ Contributed by Ben Woelk
Program Manager
RIT Information Security Office

---

**What about ethics in the workplace?**

Learn about the [RIT Ethics and Compliance Hotline](https://www.rit.edu/security/content/ethics-and-compliance-hoteline)
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: http://www.rit.edu/fa/cpd/leadership/internalcontrolsandfraud.html

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 webpage: https://www.rit.edu/fa/cpd/unit-level-risk-assessment-how.advance-your-organization%E2%80%99s-agility

<table>
<thead>
<tr>
<th>Upcoming Internal Controls &amp; Fraud in the Workplace Training Sessions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, January 12, 2016</td>
</tr>
<tr>
<td>1:30pm to 4:00pm; 2140 Louise Slaughter Hall</td>
</tr>
<tr>
<td>Tuesday, April 12, 2016</td>
</tr>
<tr>
<td>1:30pm to 4:00pm; 2140 Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upcoming Unit Level Risk Assessment—How to Advance Your Organization’s Agility Training Sessions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday, March 23, 2016</td>
</tr>
<tr>
<td>2:00pm to 4:00pm; 2140 Louise Slaughter Hall</td>
</tr>
<tr>
<td>Tuesday, August 2, 2016</td>
</tr>
<tr>
<td>10:00am to 12:00pm; 2140 Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

Watch IACA’s Monday Minute video series here!

Our monthly 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: Travel Policy changes, FERPA Regulations, RIT’s Ethics & Compliance Hotline, Records Management Policy, Risk Assessment and many others.
COSO Corner

As explained in previous editions of the Quaestor Quarterly, the COSO Framework (an 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 sixth COSO principle, which is the first principle related to the Risk Assessment component of the COSO Framework, as well as the related points of focus.

Principle 6 – The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. These objectives align with and support the university in the pursuit of its strategic direction. As part of internal control, management objectives should be grouped within relevant categories (i.e., operations, reporting, compliance) at all levels of the university to allow for the identification and assessment of the risks that could compromise the achievement of these objectives. The related points of focus for this principle and how they are relevant to RIT operations include:

- Organizational objectives reflect management’s choices about structure, industry considerations and performance of the university and consider acceptable levels of variation relative to the achievement of these goals. RIT’s mission, vision, and most recent strategic plan establish the university’s key objectives and goals.

- External financial reporting objectives should be consistent with applicable accounting principles and reflect the underlying university transactions and events. RIT publishes audited financial statements on an annual basis which are available on the Controller’s Office website: [https://www.rit.edu/fa/controller/accounting/auditstatements.html](https://www.rit.edu/fa/controller/accounting/auditstatements.html).

- External non-financial reporting objectives should be consistent with laws and regulations or standards and frameworks of recognized external organizations. RIT has multiple external non-financial reporting requirements (i.e., accreditation organizations, sponsoring organizations, federal and state agencies) with which it must comply.

- Internal reporting should provide management with accurate and complete information to assist in assessing whether objectives have been met. Outcomes assessment reporting is an integral part of RIT’s commitment to measuring success and guiding improvements towards the accomplishment of objectives.

- Compliance objectives should be consistent with standards of conduct established by applicable laws and regulations. RIT has demonstrated a commitment to compliance as documented in RIT’s Compliance Policy and Code of Ethical Conduct and with the recent appointment of the newly created Assistant Vice President for Compliance & Ethics position.

Reference
Committee of Sponsoring Organizations of the Treadway Commission (May 2013). "Internal Control – Integrated Framework – Framework and Appendices"

~~ Contributed by Nancy A. Nasca
Manager
Institute Audit, Compliance & Advisement
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:**
According to *Inform RIT*, safe online shopping practices include:

A. Making purchases on encrypted sites only  
B. Using a secure internet connection  
C. Using a secure payment method  
D. All of the above

**Post your answer to our Quiz webpage at:**
[https://www.rit.edu/fa/iaca/content/quiz](https://www.rit.edu/fa/iaca/content/quiz)

****************************************************************************

**Congratulations to Paula Grcevic from NTID for correctly answering the Spring issue’s Pop Quiz question.**

The question and the correct answer were:

According to *Inform RIT*, malware “signatures” are also known as which of the following?

**Correct**
A. DAT files  
B. Heuristic detection  
C. Malware  
D. Anti-virus software

- Ask the Auditor -

Submit a question to the IACA webpage [https://www.rit.edu/fa/iaca/forms/ask](https://www.rit.edu/fa/iaca/forms/ask) by January 21, 2016. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

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**  
manager  
475-5293

**Alissa Jatsenti, CPA**  
associate internal auditor  
475-7849

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

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

**Matthew D. Hadorn**  
co-op student internal auditor  
475-6242