Whether you handle Private student information and are bound by FERPA requirements, work with chemicals in the labs and are required to comply with OSHA regulations, or perform research internationally and must be cognizant of Export Control rules, there is a high likelihood that your responsibilities at RIT are affected by multiple Federal and State regulations. In addition to performing financial and operational audits, Institute Audit, Compliance & Advisement (IACA) also performs regulatory compliance audits. The objective of these audits is not only to evaluate whether RIT is in compliance with relevant Federal and State regulations, but to evaluate whether there are adequate procedures in place at RIT to promote and monitor compliance with these regulations.

(continued on p. 2)
To promote compliance with Federal and State regulations, RIT has multiple policies in place which specifically address procedures which must be followed in order to comply with these laws such as: RIT’s Educational Records Policy which addresses FERPA; Policy Prohibiting Discrimination and Harassment which addresses key requirements of both Title IX and the Americans with Disabilities Act; and the Foreign Corrupt Practices Act (FCPA), the policy which addresses the law with the same name, to name a few. In addition, at the college and departmental level, additional policies and procedures have been created in order to promote compliance with relevant regulations. For example, The Department of Environmental, Health and Safety (EH&S) has created laboratory standard operating procedures which address proper chemical storage, proper handling of particularly hazardous chemicals, and use of proper personal protective equipment consistent with OSHA requirements.

Another important aspect of promoting compliance with Federal and State regulations is providing training to faculty, staff and students. RIT’s Center for Professional Development offers many courses both in a classroom or e-learning setting which include information to educate faculty, staff, and students regarding relevant Federal and State requirements such as lab safety training, compliance and conflict of interest programs, and RIT’s Policy on Prohibiting Harassment and Discrimination. In addition, there are numerous external resources available (i.e., conferences, webinars, governmental websites) to educate RIT faculty, staff, and students on regulatory requirements. The Higher Education Compliance Alliance is a great website to obtain information regarding laws and regulations relevant to universities.

Subsequent to verifying that there are adequate procedures in place to promote compliance with a particular Federal or State regulation, IACA will assess whether there is adequate monitoring and oversight by department management in place to evaluate the effectiveness of these procedures. For example, EH&S performs periodic inspections of RIT labs to verify compliance with RIT policies and procedures (which are consistent with Federal and State regulatory requirements). IACA’s compliance audits also serve as a process employed by RIT senior management to monitor whether RIT has adequate procedures in place to ensure compliance with Federal and State laws and regulations which could have a significant impact on operations.

Ultimately, it is each employee’s responsibility to ensure that you are aware of the key regulations which affect your area of operations and to discuss any questions or concerns regarding compliance with these laws with your supervisor or other knowledgeable resource (i.e., Office of Legal Affairs, EH&S, Information Security Office, Human Resources Department).

~~ Contributed by Nancy A. Nasca
Manager
Institute Audit, Compliance & Advisement

- Ask the Auditor -

Submit a question to the IACA webpage
https://www.rit.edu/fa/iaca/forms/ask
by April 1, 2015.
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.

Changes to the Desktop and Password Security Standards and How They Will Affect You

After a lengthy review process, a number of new and revised security standards were approved for the RIT community this past summer. Most of the new and revised standards are effective January 23, 2015, although their implementation will occur over the next several months. In this issue, we’ll talk about changes to the Desktop and Portable Computer and Password Standards and how they affect you. You can access all of the information security standards on the RIT Information Security website.

Desktop and Portable Computer Security Standard (revised)

The Desktop and Portable Computer Security Standard provides requirements for all computers that connect to the RIT network, excluding computers that connect only through their web browsers.

What’s new?

The key changes that impact end users are around encryption and managing Private Information. All systems (laptop or desktop) that access Private Information will be encrypted. (Previously, all laptop computers were encrypted, regardless of whether or not they accessed Private Information.) At the discretion of your deans and vice presidents, any systems (laptop or desktop) that do not access Private Information and that report no unprotected matches in the Identity Finder scan reports may have encryption removed. (You will still need to run monthly Identity Finder scans and remediate any unprotected matches.)

Note that lab computers and grant-funded computers that don’t access Private Information are not required to run Identity Finder. If you have any questions about whether a computer is required to run Identity Finder or about encryption requirements in your area, contact your PIMI rep.

What remains the same?

The standard requires appropriate security software and settings on each computer. For most RIT computers, that includes centralized management, anti-virus or a host-based intrusion prevention system, an endpoint firewall, software with up-to-date patches, and automatic log out/lockout. Note that implementation of the requirement for host-based vulnerability management is pending product selection.

Visit the Desktop and Portable Computer page for more information.

To read about how RIT is helping protect you and others by reducing the locations and quantity of Private Information, visit our Private Information Management Initiative page.

(continued on p. 4)
**Password/Passphrase (revised)**
The Password/Passphrase Standard provides requirements around password length and complexity, change frequency, and storage of passwords.

**Length and complexity**
The standard requires passwords of at least 8 characters. The passwords should include an upper case letter, a lower case letter, a number, and a symbol. (Requiring a symbol is the new part.)

We encourage you to start using a passphrase instead of a jumble of letters, numbers, and symbols. A long passphrase is easier to remember and harder for a hacker to break than a short jumble. (An example of a long passphrase is It was&theBestof45Times.)

**Change frequency**
Another change is that we’ve lengthened the time a password can be used from 120 days to one year. That change will make it easier to keep your passwords on your mobile devices in synch. You’ll still need to change passwords if you’ve shared the password, if there’s a possible compromise, or if you’re using a default/temporary password.

**Storage**
We don’t want you to write down your passwords. However, if you do, you should secure them physically. If you’re storing them digitally, they must be encrypted. It’s not a good practice to store them in a spreadsheet on your desktop. (You may find a password safe/vault helpful. There are a number of good choices, including KeePass, Password Gorilla, and LastPass.)

Visit our [Passwords](#) page for more information. For tips on creating a strong easy-to-remember passphrase, visit [How to Create a Strong Password](#).

**Get informed**
Visit the [RIT Information Security](#) website to read the security standards, access security tools and software, and find out more ways to protect yourself.


*Follow us on Twitter: [http://twitter.com/RIT_InfoSec](http://twitter.com/RIT_InfoSec)*

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

---

**Watch IACA’s Monday Minute video series [here!](#)**

Our monthly one-minute video series focuses on opportunities for improving internal controls; we hope that you find the information beneficial. If you have questions, feel free to contact anyone in the IACA office using information on our [webpage](#).
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 fourth principle relating to the Control Environment component of the COSO Framework, as well as the related points of focus.

Principle 4 – The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives:

- Policies and procedures are developed to reflect expectations of competence necessary to achieve the organization’s objectives. These policies and procedures provide accountability and support effective decision making by providing guidance on acceptable employee conduct.

- Competence requirements such as knowledge, skills, and experience are defined to support the achievement of the organization’s objectives. The Board of Trustees and senior management evaluate competence across the organization and act as necessary to address any shortcomings or excesses.

- Sufficient and competent personnel are attracted, developed (mentored and trained), and retained in support of the organization’s business objectives and strategic plan.

- Management identifies and assesses those functions that are deemed essential to achieving the organization’s objectives and develops contingency and/or succession plans for assigning key responsibilities in the absence of the individuals filling those functions.

~~ Contributed by Nancy A. Nasca
Manager
Institute Audit Compliance & Advisement

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://www.rit.edu/fa/cpd/leadership/internalcontrolsandfraud.html

<table>
<thead>
<tr>
<th>Upcoming Internal Controls and Fraud in the Workplace Training Sessions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, April 21, 2015</td>
</tr>
<tr>
<td>9:00am to 11:30am</td>
</tr>
<tr>
<td>2140 Louise Slaughter Hall</td>
</tr>
<tr>
<td>Tuesday, July 21, 2015</td>
</tr>
<tr>
<td>9:00am to 11:30am</td>
</tr>
<tr>
<td>2140 Louise Slaughter Hall</td>
</tr>
</tbody>
</table>
"This past year, I was asked to step into the role of Interim Director of IACA. I was able to experience firsthand the internal audit process from the planning phase to the issuance of an audit report. I was so impressed with the quality of service performed by each member of the team. Each audit is approached thoughtfully, balancing the business needs of the clients with the university’s goal to maintain effective and consistent processes. IACA reviews each of its clients’ operations against the backdrop of the highly regulated environment in which colleges and universities operate and provides unbiased suggestions aimed at helping its clients succeed by improving and maximizing operational efficiencies. In addition to providing competent services, the IACA team is approachable and friendly. I am very fortunate to have worked so closely with consummate professionals and I look forward to continued collaboration with IACA."

~~ Erika J. Duthiers, Esq.  
Deputy General Counsel  
Office of Legal Affairs

**Ask the Auditor**

**Robin Amico from Campus Life asked:**
What year was IACA formed at RIT and was it in response to the Sarbanes-Oxley Act? (even though it was not designed for higher education - or was it in response to NACUBO’s recommendation report in 2003?)

**Answer:**
IACA records show that we were accepted into the Association of College and University Auditors (ACUA) in September 1963. ACUA was founded in 1958, in order to provide an arena to discuss mutual professional issues and to generate new ideas and methods concerning the higher education internal audit profession. So our best guess would be that IACA has existed (under various departmental names) since at least 1963 -- that is greater than 50 years!

Here is a bit more history on the internal audit profession. IACA also belongs to the Institute of Internal Auditors (IIA), specifically, the Rochester Chapter IIA. Established in 1941, the IIA is an international professional association with world headquarters in Altamonte Springs, Florida. The IIA has more than 100,000 members in internal auditing, risk management, governance, internal control, IT audit, education, and security. The Rochester Chapter IIA joined the IIA as its 20th affiliate on September 25, 1947, and offers local training, education, and networking.

**What about ethics in the workplace?**

To learn more about the RIT Ethics Hotline, check out [http://www.rit.edu/fa/svp/content/ethics-and-compliance-hotline-whistleblower](http://www.rit.edu/fa/svp/content/ethics-and-compliance-hotline-whistleblower)
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 the lead article, RIT's Educational Records Policy addresses key requirements of which Federal or State laws?

- A. FCPA
- B. Title IX
- C. EH&S
- D. FERPA

Post your answer to our Quiz webpage at:

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

====================================================================================

Congratulations to Anna Fiorucci from the College of Science for correctly answering the Fall issue's Pop Quiz question.

The question and the correct answer were:

According to the lead article, what has IACA done to efficiently manage finite auditing resources?

Correct: A. Implemented a risk-based strategy to build an annual audit plan

- B. Transferred risk to another party
- C. Modeled risk concerns
- D. Reduced probability of negative risks

- Ask the Auditor -

Submit a question to the IACA webpage
https://www.rit.edu/fa/iaca/forms/ask
by April 1, 2015.
If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.