R·I·T

Institute Audit, Compliance & Advisement
Achieving Excellence Through Collaboration

the Quaestor Quarterly

Volume 9, Issue 2 Spring 2014

quaes·tor [kwes'tôr] 'one who asks questions'

How Strong is the Control Environment in your Area?

By now you have noticed the regular column in the Quaestor Quarterly called COSO Corner. Look for it in this issue on page 7. COSO Corner is written by IACA Senior Internal Auditor Nancy Nasca and highlights the new COSO framework which was redesigned last year in light of many changes in business and operating environments since the issuance of the original COSO framework in 1992.

This article focuses on the bedrock of a well-controlled operation, the control environment. Also referred to as the internal environment, the control environment is the foundation for a solid internal control structure in any entity and establishes the business risk culture. Every layer of an entity – a division, a department, or an operating unit within a department, has its own control environment. You have likely heard of it referred to as the "tone at the top." Keep in mind the tone at the top is not just senior management's responsibility, but that of all leaders. It could be said that all employees, regardless of job title, function as leaders if they embody the key values of stewardship, trustworthiness, insight, humility and enthusiasm.

The control environment sets the basis of how risk and control are viewed by an entity's people. You will agree that the core of any business is its people – their attributes, integrity, ethical values, competence - influence the environment in which they operate. Other control environment factors include management's philosophy and operating style, the way management assigns authority and responsibility, and organizes and develops its people.

Other signs of a solid control environment include:

Leading by Example:

Managers should demonstrate through their own actions their commitment to honesty, ethical strength, reliability, and fairness.

Communicating and Promoting Ethics and Values:

Management should clearly communicate its ethics and values throughout their area of responsibility. These values could be communicated through formal methods (written codes of conduct, policies, staff meetings, memos, etc.), or informally, during day-to-day interaction and operations.

(continued on p. 2)

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**

What Were They Thinking?!	2
Inform RIT	3
Word on the Street	6
Ask the Auditor	6
COSO Corner	7
RIT Ethics Hotline	7
Pop Quiz Challenge	8
Training Opportunities Provided by IACA	8

IACA
Institute Audit, Compliance & Advisement

How Strong is the Control…

(continued from p. 1)

Reporting:

RIT has a method for employees who are witnessing unethical behavior to report such behavior anonymously (the RIT Ethics Hotline). Employees are responsible to report such activity and should feel safe from retaliation. Managers should be familiar with, and make their employees aware of, the RIT Ethics Hotline and RIT Policy C0.0, which contains within it Standards of Ethical Conduct including *Whistleblower Protection Against Retaliation*.

Rewarding Integrity:

Management should acknowledge employees who demonstrate honesty and integrity. Doing so will help communicate management's commitment to this behavior and will encourage others to act likewise. This will promote integrity within the university and have a positive influence on others.

To summarize, while every employee in the RIT community has a personal and professional obligation to be a good steward of university assets and resources, a manager has a particular responsibility to ensure that the control environment in their area of responsibility is aligned with the expectations of senior management and the Board of Trustees and promotes ethical behavior.

How strong is the control environment in your area?

The RIT Ethics Hotline is a great option for employees to utilize when they are uncomfortable about bringing a concern forward in person. Every report is taken seriously and is appropriately investigated. If you have any questions about the Hotline, please contact Steve Morse at smmiaca@rit.edu.

~~ Contributed by Patrick Didas
Associate Director
Institute Audit Compliance & Advisement

What Were They Thinking?!

A woman faces charges after extorting a former employee of Bethany College, Shelly Lough. Rachelle Weese, 26, allegedly used fear and violence to bully Lough into stealing a large sum of money from the college after learning about Lough's extra-marital affair. Lough, in an attempt to keep Weese quiet, stole nearly $500,000 from the college's cash window where employees and students can cash checks. This cash was then given to Weese for her personal use.

Weese used the substantial amount of money to buy luxurious jewelry totaling over $25,000 and to purchase a new SUV; a search of Weese's home also uncovered over $250,000 in cash.

"A lot of money was taken from Bethany… We may never account for all of it." William Ihlenfeld II, US Attorney for the Northern District of West Virginia, said regarding the case.

Weese had a preliminary hearing on February 28th, 2014, and was released on bond. The director of finance of the college, who was responsible for oversight of the account in question, was also terminated. For more information, follow the link here.

Lesson Learned: There was an apparent lack of oversight of the reconciliation of the daily cash activity which allowed this to occur. Reconciliations are a critical control.

Reference: "Bethany College Employee Fired Stealing $500,000 - WTRF 7 News." *Bethany College Employee Fired Stealing $500,000*. N.p., 1 Oct. 2013. Web. 07 Apr. 2014.

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.

Information Handling and You

Did you know that all information you handle in the course of your work at RIT has one of four classifications? Did you know that RIT has specific policies governing how you handle these different types of information?

We handle many types of information at RIT. Much of it is relatively innocuous and not anything we need to worry about. However, some of the information you handle may be useful for identity theft or be RIT business-related and confidential. There are also federal and state laws governing the handling of specific types of information.

Information is classified by its degree of confidentiality by the Information Access and Protection Standard. Here are the four classification levels and related handling information:

Private Information

Private information is information that is confidential and which could be used for identity theft. Private information also has additional requirements associated with its protection (e.g., state and federal mandates). Examples include:

- Social Security Numbers (SSNs) or other national identification numbers
- Driver's license numbers
- Financial account information (bank account numbers, checks, credit or debit card numbers), etc.

Use alternatives to Private information whenever possible. Unless required by RIT business processes, files should not contain Private information. Sanitize all unnecessary Private information by redacting (removing) the Private information. Redaction should be done in such a manner that the Private information is completely removed from the files—masking of Private information is insufficient. Approved sanitization, redaction, and disposal practices may be found at https://www.rit.edu/security/content/information-access-protection-standard.

Stored Private information should be protected with documented technical and process controls that limit access in both physical and electronic environments. Private information in electronic form should be stored in secure ISO-approved servers or another ISO-authorized, encrypted form. Transfer or sharing of Private information is prohibited unless it is essential to RIT business practices, and should be done using an ISO-approved transfer method such as the Tiger File exchanger, encrypted e-mail, or file-based encryption. Avoid printing Private information unless necessary for business operations, and implement the ISO-recommended printer best practices where possible.

(continued on p. 4)

"I believe in evidence. I believe in observation, measurement, and reasoning, confirmed by independent observers.

I'll believe anything, no matter how wild and ridiculous, if there is evidence for it.

The wilder and more ridiculous something is, however, the firmer and more solid the evidence will have to be."

- Isaac Asimov, scientist and writer (1920-1992)

(continued from p. 3)

Confidential Information
Confidential information is information that is restricted to a need-to-know basis and due to legal, contractual, ethical, or other constraints may not be accessed or communicated without specific authorization. Examples include:

- University Identification Numbers
- Educational records governed by FERPA that are not defined as directory information (see RIT Educational Records Policy D15.0)
- Employee health information as defined by the Health Insurance Portability and Accountability Act (HIPAA)
- Management information, including communications or records of the Board of Trustees and senior administrators, designated as Confidential
- Faculty research or writing before publication or during the intellectual property period (see RIT Intellectual Property Policy 3.0)
- Third party information that RIT has agreed by contract to handle as confidential

Confidential information should only be used and disclosed to others on a need-to-know basis in order to perform RIT business operations. Any transfer or sharing of Confidential information should include an annotation labeling the document or file as "Confidential" (education records governed by FERPA that are not defined as directory information are excluded from the marking requirement).

Confidential information in paper form should be stored in locked areas; in electronic form, it should be protected using secure information technology resources and access controls. Confidential information should not be stored or posted in blogs, wikis, or other digital locations/repositories that do not use ISO-approved authentication and authorization.

Internal Information
Internal information is restricted to RIT faculty, staff, students, alumni, contractors, volunteers, and business associates for the conduct of university business. Examples include online building floor plans, specific library collections, etc.

Use secure information technology resources and access controls whenever storing, transferring, or sharing Internal information.

(continued on p. 5)

Watch IACA's Monday Minute video series here!

This 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 located on our webpage.

(continued from p. 4)

Public Information
Public information may be accessed or communicated by anyone without restriction and has no special handling requirements associated with it.

Private Information Management Initiative
The Private Information Management Initiative focuses on helping RIT employees identify and reduce or eliminate Private Information not needed for business processes. Most of you are familiar with the Identity Finder software that runs monthly on your RIT computer. The Identity Finder software searches your system for data patterns that look like Private Information. Identity Finder provides a search results window that enables you to examine the suspected Private Information found and shred (delete) or scrub (redact) the information. It also allows you to choose "Ignore" for information that is a false positive. (A false positive matches the data pattern of Private Information, but is not actually Private Information. We typically see false positives in various statistical packages and in spreadsheets that contain entries that are nine-digit numbers or otherwise appear to be account numbers.)

We appreciate your diligence in handling information properly. It increases the safety of both RIT's and your information.

Courses Available to Employees Include:

DSD 103 Information Handling
RIT employees handle or are exposed to Private and Confidential information every week. It is important to use appropriate and secure information handling practices to protect these types of information. Inadvertent loss or disclosure of Private information may result in a Notification event under the NYS Information Security Breach and Notification Act.

Course Objectives
Attendees of the Digital Self Defense (DSD) 103—Information Handling course will learn new and improve existing information handling skills. Specifically, the course explains the different classes of information at RIT, how these types of information should be treated, and the correct means of storage, transfer, and destruction to be used. Completion of the course should provide the user with the necessary knowledge to be in compliance with the Information Access & Protection (IAP) Standard.

DSD 103 Online Course
DSD 103 Information Handling is now available as a self-paced online class through the RIT E-Learning Zone.

Access DSD 103 Information Handling Web-based training on the RIT E-Learning Zone
Login with your RIT credentials

- Open the course.
- Click the blue triangle to launch the course. (You may want to perform a Browser Check to ensure your computer is configured correctly.)
- Take the course and complete the post-course assessment.

For More Information
https://www.rit.edu/security/content/information-access-protection-standard

https://www.rit.edu/security/sites/rit.edu.security/files/PlainEnglishGuideAccessProtection2009_0.pdf

~~ Contributed by Ben Woelk
Program Manager
Information Security Office

Word on the Street

As the Administrative Chair of the School of Design, I recently completed my first experience working with IACA in conducting an audit of our School. The School of Design serves over 800 students, has over 30 full-time faculty and 30 adjuncts. We have several nationally ranked programs and we are located in the College of Imaging Arts and Sciences. As a School, we are all very dedicated to a continuous improvement approach. Going through my first audit assisted me in seeing the mechanics of the day-to-day workings of the unit even more clearly. With the guidance and support of the Audit team we are now able to successfully demonstrate with evidence how we manage and how we can improve.

The Auditors that we worked with are highly experienced and as experts in their field, they could pinpoint queries that would help us to clarify our procedures and processes. An important part of the process was the accessibility of the Audit team. They gave us time, asked key questions and supported our process of inquiry. Beneficial to us was the fact that they were also open to learning more about us as a unit to better understand our context as a Design school. It was all very enlightening to a recently appointed Chair! Now that it is complete, I can say that we as a School have gained a valuable insight into our management systems and we are already making daily improvements to make the work environment supportive of the excellent teaching and learning that takes place in the School of Design.

~~ Contributed by Peter Byrne
Administrative Chair
School of Design

Ask the Auditor

Question:
How do internal and external auditors differ?

Answer:
Although they are both independent of the activities they audit, internal auditors are generally employed by the organization and provide ongoing monitoring and assessment of all activities in that organization. External auditors are independent of the organization, and provide an annual opinion on the financial statements.

Both professions adhere to codes of ethics and professional standards set by their respective professional associations. There are, however, major differences with regard to their relationships to the organization, and to their scope of work and objectives.

The internal auditor's scope of work is comprehensive. It serves the organization by helping it accomplish its objectives and improve operations, risk management, internal controls, and governance processes. Concerned with all aspects of the organization — both financial and non-financial — the internal auditors focus on reducing risk to the organization. They also are concerned with the prevention of fraud in any form.

The primary mission of external auditors is to provide an independent opinion on the organization's financial statements, annually. Their approach is historical in nature, as they assess whether the statements conform with generally accepted accounting principles, whether they fairly present the financial position of the organization, whether the results of operations for a given period of time are accurately represented, and whether the financial statements have been materially affected.

~ Ask the Auditor ~

Submit a question to the IACA webpage https://www.rit.edu/fa/iaca/forms/ask by June 30, 2014. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

COSO Corner

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

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 second principle relating to the Control Environment component of the COSO Framework, as well as the related points of focus.

Principle 2 – The Board of Trustees (BOT) demonstrates independence from management and exercises oversight of the development and performance of internal control. Key characteristics (points of focus) relating to this principle include:

- The BOT identifies and accepts its oversight responsibilities in relation to established requirements and expectations. The Board is responsible for providing oversight and constructive feedback to management.
- The BOT, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate actions.
- The BOT has sufficient members who are independent from management and objective in evaluations and decision making.
- The BOT retains oversight responsibility for management's design, implementation, and conduct of internal control. The President and senior management bear direct responsibility for developing and implementing the internal control system. Board oversight is supported by structures and processes that management establishes at a business-execution level.

Follow this link to learn more about RIT's BOT:
https://www.rit.edu/president/trustees/trustee-home.

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

~~ Contributed by Nancy A. Nasca
Senior Internal Auditor
Institute Audit Compliance & Advisement

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

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, what is often referred to as the "internal environment"?

A. RIT Ethics Hotline
B. Control environment
C. A department or other entity
D. RIT's Whistleblower Policy

Post your answer to our Quiz webpage at:
https://www.rit.edu/fa/iaca/content/quiz

****

Congratulations to Charles Gruener from the Golisano College of Computing & Information Sciences for correctly answering the Winter issue's Pop Quiz question.

The question and the correct answer were:

According to the article, *Another Way to Share Your Financial, Compliance, and Ethical Concerns-The RIT Ethics Hotline*, what happens first after a report is made?

A. A department investigation occurs immediately following the report.
B. A general receipt acknowledgement is posted in the system.
Correct C. A small group of senior RIT managers receive the report and dispatch it to the appropriate department(s) for investigation.
D. Additional questions are immediately asked of the reporter.

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 in order 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

Upcoming Sessions:

April 29, 2014 - 1:30pm - 4:00pm 2140 Louise Slaughter Hall	July 16, 2014 - 9:00am - 11:30am 2140 Louise Slaughter Hall	October 15, 2014 - 9:00am - 11:30am 2140 Louise Slaughter Hall

IACA
Institute Audit, Compliance & Advisement

Achieving Excellence Through Collaboration

IACA TEAM:

Steven M. Morse '86, CPA
assistant vice president
475-7943

Patrick M. Didas '90, CPA, CFE, CCA
associate director
475-6826

Wendy J. Roy, CPA
senior internal auditor &
professional development coordinator
475-7011

Nancy A. Nasca, CPA, CIA
senior internal auditor
475-5293

Gregg S. Despard, CISA
senior IT internal auditor
475-7849

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

Hannah B. Miller
co-op student internal auditor
475-4318

R·I·T