R·I·T

Institute Audit, Compliance & Advisement Newsletter

the Quaestor Quarterly

Volume 3, Issue 1 January 2008

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

Protecting and Handling Information at RIT

Do you know if you handle RIT Confidential or Operationally Critical information? Do you know that there are both external and internal requirements for protecting sensitive information at RIT? Do you know that each department is required to have an Information Access and Protection Plan?

There are a number of requirements for handling information and general computing at RIT. These requirements (standards) are components of the Information Security Policy (C8.1).

The Information Access and Protection Standard (IAP) requires that RIT departments determine appropriate handling of RIT information to protect its confidentiality, integrity, and availability (these requirements vary according to the information's classification).

All information at RIT belongs to one of the following categories*:

- *RIT Confidential*
- *RIT Internal Use Only*
- *Public Information*

Some of this information may also be needed to ensure the successful operation of the university. This type of information has an additional classification of *RIT Operationally Critical*.

Departmental IAP Plans

Department-specific information handling requirements are specified in your department's Information Access and Protection Plan (IAP Plan). This plan provides the requirements you need to follow when handling RIT information through its lifecycle of creation, transfer, storage, and disposal.

In addition to helping departments comply with external and internal information protection mandates, the IAP Plan provides additional benefits:

- The *information inventory* process can help you prepare better business continuity plans by documenting the information that your department needs to operate, and the sources and destinations of said information. Identifying information for which your department is the authoritative source (authoritative source meaning you hold the highest level of information verification/data integrity) will serve not only your IAP Plan, but your business continuity plan as well.

*A fourth category, *3rd-Party Confidential*, is used for confidential information not belonging to RIT. Information about RIT information classifications can be found at http://security.rit.edu/iap.html.

(*continued on p. 2*)

Inside This Issue

ACA Institute Audit, Compliance & Advisement

Protecting and Handling Information at RIT (continued from p. 1)

- The *information inventory* process can help departments identify outdated confidential information. Obsolete data can be a security risk. During the inventory process, you may uncover old CDs or floppy disks with data that is no longer current but still confidential (for example, student Social Security numbers). In most cases, older data was collected and stored prior to the implementation of RIT security standards and during a time when the threat of identity theft was considerably lower. The inventory process provides an opportunity to sanitize or dispose of outdated information.

Next Steps

In February 2008, the Information Security Office will begin inspecting IAP plans. We will evaluate plans for opportunities to improve information handling at RIT. If you have questions about the IAP plan requirements, visit the IAP Resource page (http://security.rit.edu/iap.html) and read the Plain English Guide. We've provided a number of job aids, including an FAQ section and an IAP Plan template.

Additional Resources

The Information Security Office web site (http://security.rit.edu) provides information on security requirements at RIT, general awareness information, user guides, and how to practice digital self defense. Our *Digital Self Defense 103—Information Handling* course provides an introduction to the information lifecycle and appropriate methods of handling sensitive information. You can access this self-paced online course through the Center for Professional Development (http://finweb.rit.edu/cpd/).

The ITS Help Desk is available to provide assistance on safe information handling practices. If you need to dispose of sensitive information, the ITS HelpDesk provides access to a media shredder and a hard drive degausser.

For more information, contact RIT Information Security at Infosec@rit.edu or 585-475-4122.

~ RIT's Information Security Office

Control of the Quarter

In the last newsletter, we continued our internal control discussion focusing on the 3rd component, "control activities." Control activities, which are designed to help ensure that necessary actions are taken to address risks to achieving the objectives of the University, occur at all levels and in all functions of the organization. These activities include:

- Approvals
- Authorizations
- Verifications
- Reconciliations
- Reviews of operating performance
- Security of assets
- Segregation of duties

The 4th internal control component is "information and communication."

Information

Information involves identifying, capturing, and communicating pertinent information in a format and timeframe that enables individuals internal and external to the organization to carry out their responsibilities. Information enables the organization to move towards or meet its operating, financial reporting, and compliance objectives.

(*continued on p. 3*)

Occupational fraud can be found in any workplace. Whether an organization is a non-profit entity such as a university or a large for-profit corporation, fraud has occurred and continues to occur.

To learn more about occupational fraud, sign up for Fraud in the Workplace Training.

Upcoming Sessions:

March 13, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

May 29, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

August 21, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

Sign up at the CPD website https://finweb.rit.edu/cpd/leadership/fraud.html

Control of the Quarter

(continued from p. 2)

For example, financial information available from the University's financial systems is used in a variety of ways including:

- For the development of financial statements for use by vendors, sponsors, creditors, donors, and others with an interest in RIT.
- By senior management to make operating decisions such as monitoring performance and allocating resources.

System-generated reports must contain information necessary to support effective controls including:

- Appropriate content – Is the required information available?
- Timeliness – Is it available when needed?
- Current – Is it the latest available information?
- Accurate – Is the information correct?
- Accessible – Can the information be obtained easily by those who need it?

Communication

In order for employees to understand their role in the control system, as well as how their work activities relate to the work of others, effective communication must occur throughout the organization (e.g., down, across, and up). Senior management is responsible for communicating to all employees that control activities must be taken seriously and there must be a mechanism in place to ensure that significant information flows upwards in the organization. An example of upward flow of information at RIT is the Ethics Hotline, an anonymous whistleblower system designed to augment existing campus options for reporting possible financial, accounting, and compliance related irregularities (see "My Two Cents" section of this newsletter). Effective communication is also required with external parties including students, parents, vendors, donors, etc. Another critical component of effective communication is timely and appropriate follow-up action by management.

In summary, organizations must capture pertinent information relevant to managing their business and it must be delivered to those who need it in a format and timeline that allows them to carry out their control (and other) responsibilities.

In the next newsletter, we'll review "monitoring," the 5th and final control component."

~ Controller's Office

Word on the Street

The Institute Audit, Compliance & Advisement (IACA) group recently completed their audit of our Information Technology Department within the Golisano College of Computing and Information Sciences. The term "audit" is defined by the American Heritage dictionary as "an examination of records or financial accounts to check their accuracy." To most of us, however, the word means "dread."

We waited in anxious anticipation for months, only to discover that the entire process was actually quite invigorating. Organizations frequently get caught up in their day-to-day operations and don't take the time to reflect about current processes. The audit forced us to examine the department; it reinforced what we are doing well and provided us with ideas on where to make enhancements. In fact, we were so impressed with the entire audit that we will be using the information to provide a training session for the other GCCIS departments in mid-December. The goal is to familiarize the managers and staff with the audit process, to share the issues that were found in IT, and to insure compliance with RIT's policies and procedures. The departments will then use this information to enhance their operations.

What presented itself as a dreadful task in the beginning, actually turned out to be quite invaluable. Wendy Roy, Pat Didas, and Steve Morse are commended for the professional and non-intrusive manner in which they accomplished their task.

~ Kimeley Shearer, Director of Operations, GCCIS

Ensure that your department has established and is maintaining good internal controls.

To learn more about internal controls, sign up for Internal Controls Training.

Upcoming sessions:

February 28, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

April 29, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

June 24, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

August 19, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

October 14, 2008
9:00 AM - 11:00 AM
Location: CIMS 2140

Sign up at the CPD website
https://finweb.rit.edu/cpd/leadership/cares.html

Ask the Auditor ~

Submit a question to the IACA webpage **http://finweb.rit.edu/iaca/forms/ask/** by 2/29/08. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

IACA TEAM:

Steven M. Morse '86, CPA
executive director
475-7943

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

Wendy J. Roy, CPA
senior internal auditor
475-7011

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

Elisa M. Cockburn, CPA
senior internal auditor
475-7849

Christine M. VanHemel
staff & audit assistant
475-7647

R·I·T

My Two Cents

All employees play an important role in the identification of improper behavior or activity on campus. We all have a vested interest in making sure that RIT is operating effectively. The RIT Ethics Hotline provides employees with the ability to report on a variety of improper activities anonymously.

In November, all RIT employees received a "Taking Responsibility" brochure that describes the RIT Ethics Hotline. The RIT Ethics Hotline was introduced to the campus two years ago as whistleblower hotlines became a best practice for organizations. The RIT Ethics Hotline is administered by EthicsPoint, a third party service provider. EthicsPoint has a commitment to the Higher Education industry and serves many colleges and universities.

Before utilizing the RIT Ethics Hotline, employees are encouraged to first explore existing means by which to report situations of concern or impropriety such as discussing them with a supervisor or contacting an appropriate RIT department such as Human Resources; Institute Audit, Compliance & Advisement; Public Safety; or the Controller's office. These pre-existing channels for dealing with situations of concern or impropriety are well established and are proven means by which to report such instances. However, if you are not comfortable discussing a situation in person, be sure to contact the RIT Ethics Hotline which will enable you to maintain your anonymity.

As detailed in the "Taking Responsibility" brochure, a "reporter" may access the RIT Ethics Hotline via telephone, TTY, or internet to anonymously and confidentially report financial reporting, accounting, internal control, regulatory compliances, and RIT resource violations.

Here is that contact information:
Web: http://finweb.rit.edu/svp/ethics or
http://www.ethicspoint.com
Toll-free: 1 - 866 - 294 - 9358
1 - 866 - 294 - 9572 (TTY)

~ Steven M. Morse, Executive Director

Pop Quiz

The first reader to correctly answer the question below will win a prize worth $10.

Question: Executives in organizations are more honest than rank-and-file employees and are therefore less likely to commit fraud.

A. True
B. False

See our Quiz webpage to post your answer:

https://finweb.rit.edu/iaca/forms/quiz/

The winner's name and answer will be included in the next newsletter.

Congratulations to Jan Cope, CIAS Dean's Office, for being the first reader to correctly answer the October issue Pop Quiz question.

The question and the correct answer for October:
"On average the most expensive corruption scheme committed by employees of an organization is…"

A. Bribes and kickbacks