R·I·T

Institute Audit, Compliance & Advisement

the Quaestor Quarterly

Volume 5, Issue 2 Spring 2010

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

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**

IACA Institute Audit, Compliance & Advisement

Risk Considerations for Outsourced Operations

Organizations may choose to outsource specific business functions to assist with the effective and efficient accomplishment of operational objectives. Key criteria to consider when making outsourcing decisions include the entity's core competencies, specialized training needs, system requirements, and the cost benefit of obtaining external resources as compared to providing these services internally. Examples of services which are currently outsourced by RIT include benefit administration (health care, retirement plans) and off-site data retention.

One of the key risks associated with the outsourcing of services is that RIT employees do not directly control the processes that are being outsourced. The vendor is responsible for the day-to-day operation of the process. So how do we ensure that the vendor's operations are running effectively and that the services being provided to RIT meet management's expectations? In addition, depending on the services that will be provided by the vendor, other risks should also be considered, such as:

- Could RIT Private or Confidential data be comprised?
- Is data being processed completely, accurately, and on a timely basis?
- Will access to RIT resources result in the misappropriation of these assets?

The first step in minimizing the risks when outsourcing services is to understand and document these risks and determine whether the benefits of obtaining these services outweigh the potential costs associated with the risks. Next, management must ensure that the best vendor is selected to perform these services. Considerations in the vendor selection process should include utilizing a request for proposal process that clearly explains the services desired and defines management's expectations, evaluating the long-term financial and operational viability of the vendor, and evaluating whether the vendor has the expertise and systems (if applicable) necessary to perform the service.

continued on p. 2

Outsourcing Risk Considerations

(continued from p. 1)

Once a vendor is selected, the next step in minimizing the risks inherent in outsourced relationships is to ensure that a comprehensive vendor contract is executed. The contract should clearly document the services that are to be provided by the vendor and also include performance standards and service level agreements, regulatory compliance requirements, confidentiality and data security expectations, compensation and payment terms, reporting expectations, and a right to audit clause.

In addition, management must consider what internal processes (monitoring controls) must be developed in order to support the vendor services and mitigate the risks identified during management's initial risk assessment process as described above. Examples of processes that need to be developed in support of these relationships may include reconciliation controls such as the reconciliation of batch totals to ensure that data is transmitted completely and accurately, logical access controls, and monitoring controls such as the review of vendor fee calculations or service level agreement metrics.

For vendors who perform higher risk operations for RIT, SAS 70, SysTrust or WebTrust reports are additional tools that can assist RIT managers in evaluating whether the operations of these vendors are adequately controlled to achieve the desired objectives. Service vendors may engage a CPA to perform a SAS 70 review of the key controls (as identified by the service organization) over significant processes and to evaluate whether these controls are suitably designed to achieve the control objectives specified by the service organization. A SAS 70 Type II report also evaluates whether these controls are operating effectively. SysTrust and WebTrust services are typically utilized for information technology services and specifically address security, online privacy, availability, confidentiality, and processing integrity.

Similar to any key internal process that is performed at RIT, key RIT processes performed by external vendors must be well controlled to ensure the integrity and effectiveness of that process. These controls should include a combination of preventive (i.e., vendor selection, contracting, SAS 70 verification) and monitoring (i.e., review of vendor performance indicators and reporting) procedures to effectively mitigate the risks identified relating to the processes being performed by the vendor.

Reference

Benvenuto, Nicholas A (2005). "Outsourcing – A Risk Management Perspective," *Information Systems Control Journal*, Volume 5

~~ Contributed by Nancy Nasca
Sr. Internal Auditor
Institute Audit, Compliance, & Advisement

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

To learn more about internal controls, sign up for Internal Controls Training. This is now a required course to receive the RIT Accounting Practices, Procedures, and Protocol Certificate of Completion.

Upcoming Session:

July 20, 2010
9:00 am - 11:00 am
Location: CIMS 2130

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

Control of the Quarter

In the last several Newsletters, we've reviewed the five interrelated components of internal control, including control environment, risk assessment, control activities, information and communication, and monitoring. We've also talked about who in the organization is responsible for internal control (to some degree, it's everyone's responsibility). Now we're providing real-life examples of how a system of internal control is built into the University's infrastructure; it's a fundamental part of our operation.

First, here's a quick refresher about controls. They can be either preventive or detective, but it's important to note that the intent of each is different.

- ✓ Preventive controls are designed to deter or prevent undesirable events from occurring; they are proactive controls that help to prevent a loss. Examples of preventive controls are segregation of duties, proper authorization of financial transactions, adequate documentation, and physical control over assets.

- ✓ Detective controls, on the other hand, attempt to detect errors and irregularities which have already occurred and ensure their prompt correction. Detective controls supply the means with which to correct data errors, modify controls or recover missing assets. Examples of detective controls are reviews, analyses, variance analyses, account reconciliations, physical inventories, and audits.

Both types of controls are essential to an effective internal control system. Preventive controls are important because, by design, they are proactive and emphasize sound business practices. Detective controls also play a critical role by providing evidence that the preventive controls are functioning correctly and preventing losses.

Let's take a look at one critical preventive control activity in place at RIT designed to ensure that procurement transactions are approved by authorized individuals prior to orders being placed.

- ✓ Purchase Requisition Approvals – According to the University's signatory authority policy, officers of RIT (e.g., the vice presidents) have delegated authority to certain employees to approve the procurement of goods and services from third-party suppliers. When a requisition is created in the Oracle purchasing application, the requisitioner forwards it to an authorized approver (i.e., an employee who is able to approve a purchase for the specific department up to a specified dollar amount). Such approval must be explicitly granted by the division vice president and it can't exceed the amount delegated to the more senior manager. When a transaction exceeds the approver's authorized limit, it will automatically be forwarded to the next level of management for approval.

Continued on p. 4

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. This is now a required course to receive the RIT Accounting Practices, Procedures, and Protocol Certificate of Completion.

Upcoming Session:

July 13, 2010
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. 3)

- ✓ Approver's Responsibilities – The individual who approves a transaction which constitutes a commitment between the University and the supplier is responsible to ensure that:
  - All procurement policies of the University have been followed including the requirement to obtain three competitive quotes for orders of $5,000 or more.
  - The transaction, proposal or agreement includes the appropriate standard provisions recommended by RIT legal counsel.
  - Funds for the transaction have been allocated or are available within regularly approved budgets or other University accounts.
  - There is no real or apparent conflict of interest on the part of the approver or other individual in the organization involved in the transaction.

This preventive control is designed to ensure that only authorized personnel who have knowledge of the University's policies (e.g., procurement, conflict of interest, etc.) are able to commit or expend assets of the University. Management periodically reviews/monitors the approval system to ensure that it is functioning as intended and that approval authority has been delegated in a way that allows for efficient, but controlled, operation of the business of the University.

~~ Contributed by Lyn Kelly
Controller and Assistant Treasurer
Controller's Office

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

To learn more about internal controls, sign up for Internal Controls Training. This is now a required course to receive the RIT Accounting Practices, Procedures, and Protocol Certificate of Completion.

Upcoming Session:

July 20, 2010
9:00 am - 11:00 am
Location: CIMS 2130

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

What about *ethics* in the workplace?

To learn more about RIT's Code of Conduct and the Ethics Hotline, check out http://finweb.rit.edu/svp/ethics/

Word on the Street

When you receive word that a department in your college is being audited, initial thoughts turn to "what's wrong" or "why us." In actuality, Institute Audit, Compliance & Advisement (IACA) selects several departments each year to audit. Although the department chosen to be audited in our College offers multiple sections of courses that include hands on activities and unique types of purchases, the audit turned out to be a very positive learning experience that will benefit the entire College.

The process began with a review of the audit planning document, identifying and discussing the 15 key processes that would be reviewed. These processes were not unique to the department being audited, although we certainly tailored the discussion to meet the uniqueness of the area; they represent processes used across the university. Throughout the exercise, the IACA team focused on compliance with university practices, compliance with regulatory requirements, and sound managerial structure that would provide proper internal controls. The senior auditor reviewed documents, talked to employees within the dean's office and department, and asked questions that helped to identify the details of how and why we handle our business operations as we do. They were not threatening questions, but very insightful questions that allowed us to think through operations that occur on a daily basis.

As IACA created a list of findings, they worked with CAST to develop actionable responses to those findings, giving us guidance but not dictating a solution. This allowed us to consider, in some cases, how our proposed response could benefit the entire college, beyond this one department, eventually resulting in some standard operating procedures.

We are not done. Although we have initiated changes to our practices in response to the audit findings, IACA will work with us to monitor our progress. Like our approach to academic quality, this is a continuous improvement process.

~~ Contributed by Maureen S. Valentine, PE
Associate Dean and Miller Professor
College of Applied Science and Technology

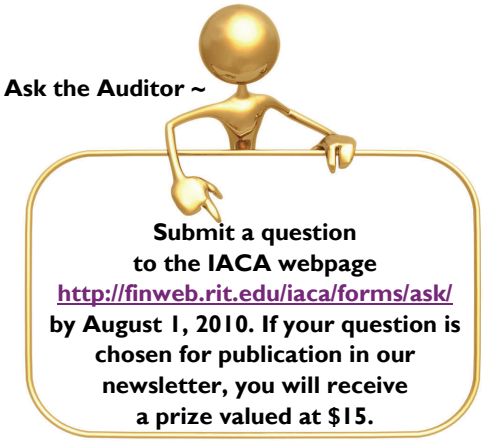
Occupational fraud can be found in any workplace. Whether an organization is a non-profit entity such as a university or a large for-profit corporation, fraud has occurred and continues to occur.

To learn more about occupational fraud, sign up for Fraud in the Workplace Training. This is now a required course to receive the RIT Accounting Practices, Procedures, and Protocol Certificate of Completion.

Upcoming Session:

July 13, 2010
9:00 am - 11:00 am
Location: CIMS 2140

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



IACA TEAM:

Steven M. Morse '86, CPA
assistant vice president
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

Daniel R. Dellaquila
co-op student internal auditor
475-4318

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: The goal of information security is to protect the:

A. Confidentiality of information
B. Availability of information
C. Integrity of information
D. All of the above

Post your answer to our Quiz webpage at:
https://finweb.rit.edu/iaca/forms/quiz/

The winner's name and answer will be included in the Fall '10 Quaestor Quarterly Newsletter.

****

Congratulations to Julie Magnuson, Osher Lifelong Learning Institute at RIT/ Athenaeum, for correctly answering the Winter issue's Pop Quiz question.

The question and the correct answer was:

"Tone at the Top" is a term everyone has likely heard. It can be defined or characterized by:

A. A culture in which managers are aware of the risks in their areas of responsibility, monitor the internal controls to mitigate those risks, and take action if the controls are not working.
B. How an organization should relate to all of its stakeholders – employees, vendors, customers, and the community as a whole.
C. One of the most important things that allows an organization to be aligned and steered in the right way.
D. How organizational processes and structures, such as targets and incentives, drive people's behavior.

Correct E. All of the above.

R·I·T