What is the Standard by Which Internal Controls are Evaluated?

In 1992, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission published an Internal Control – Integrated Framework (the COSO Framework). Since 1992, the COSO Framework has become an internationally recognized standard against which the adequacy and effectiveness of an organization’s internal controls are evaluated. The COSO framework defines an internal control as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and, compliance with applicable laws and regulations.” The framework further goes on to define the following five components that are an integral part of an effective overall internal control system:

- **Control Environment** – The control environment of an organization is often referred to as the “Tone at the Top” and refers to the ethical values promulgated by senior management and demonstrated through their management philosophy and operating style. Examples of practices which would indicate that a strong control environment exists include, but are not limited to, an employee code of conduct, well-defined roles and responsibilities, published authorization hierarchies, conflict of interest policies, and adequate employee training.

- **Risk Assessment** – Risks can be both external (i.e., economic changes, competition, regulatory changes) and internal (i.e., misappropriation of assets, change in management, data corruption/inaccuracies) and must be identified and effectively managed in order to reduce the possibility of an organization failing to meet its strategic objectives (both at the entity-wide and activity level).

- **Control Activities** – Control activities are the specific processes designed to mitigate the risks which would prevent an organization from achieving its objectives. Examples of common control activities found within successful organizations include, but are not limited to, segregation of duties, reconciliations, use of performance indicators, and policies and procedures.

(continued on p. 2)
Information and Communication – Communication of an organization’s objectives and the dissemination of relevant and timely information necessary for effective decision making are crucial components of an effective internal control system enabling management to successfully conduct, manage, and control its operations.

Monitoring – Although an organization may design an adequate internal control system to facilitate the achievement of its goals and objectives, this system must be regularly monitored and evaluated to ensure that the controls are effectively functioning as intended.

In 2013, the COSO Framework was updated to provide additional guidance on the evaluation of internal controls. Although the revised framework retained the five components of internal control as described above, it further defines 17 principles associated within these five components which are necessary for effective internal control. In addition, it provides 81 points of focus to help assess whether the 17 principles are present and functioning. IACA will further expand upon the principles included in the new 2013 COSO framework (which will replace the original framework as the standard for internal control assessment effective December 15, 2014) in future Quaestor Quarterly Issues. Look for this information in our new “COSO Corner.”

Reference

~~ Contributed by Nancy Nasca
IACA Senior Internal Auditor

What is the Standard...
(continued from p. 1)

Submit a question to the IACA webpage https://www.rit.edu/fa/iaca/content/quiz by October 30, 2013 If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

Question:
I recently heard RIT has some sort of hotline. I have been here 12 years and have never heard of this. What is it for and how do I utilize it if necessary?

Answer:
RIT’s Ethics and Compliance Hotline, an anonymous whistleblower system hosted by EthicsPoint, is a way for RIT’s community members to anonymously report financial reporting, accounting, internal control, regulatory compliance, and university resource violation concerns.

To report any suspicious activity anonymously, you can go to www.ethicspoint.com and file a report, or you can call 866-294-9358 or 866-294-9572 TTY. To learn more about the hotline and RIT’s Code of Conduct, visit http://www.rit.edu/fa/svp/content/ethics-and-compliance-hotline-whistleblower.
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. In this issue, we’ll talk about secure use of wireless networks.

Accessing wireless networks safely

Wireless networking allows you to connect to a network or the Internet without a cable. Some of the networks you may connect to wirelessly include:

- The RIT public network and encrypted WPA and WPA2 networks through campus-wide wireless access points
- A wireless router connected to your home Internet connection
- A wireless “hotspot” at an airport, hotel, coffee shop, or rest area

As more people purchase laptops, smartphones and other mobile devices, wireless network access has become increasingly popular and convenient. Unfortunately, most wireless access points are set up in a manner that is insecure; placing your privacy, your data and your computer at significant risk.

Network security:

Secure networks
Secure wireless networks use WPA2 encryption protocols, and should prompt you for a passcode or key in order to gain access. Some protocols, such as WEP and WPA, will require a password but do not provide adequate security. Make sure to identify what protocol the network is using by checking your wireless settings.

Insecure networks
If the wireless network you are trying to access uses WEP or WPA encryption or does not require a passcode at all, then it is probably insecure.

Insecure wireless networks are susceptible to “sniffing.” Anyone with a laptop or mobile device in range of your computer can read your network traffic, including unencrypted websites, e-mails, instant messages and any file you download. It’s similar to a home phone line—someone in another room can pick up a different receiver and listen to your entire conversation.

Piggybacking
If you are hosting your own wireless network and have not enabled encryption, anyone within range will be able to access your Internet connection. If an unauthorized person uses your network to commit a crime or send spam, the activity can be traced back to your account.

Protect your privacy
Accessing an insecure wireless network is inherently risky, but there are some things you can do to help protect yourself (and your private information):

(continued on p. 4)
Use a VPN
A Virtual Private Network, or VPN, is a private network that uses the Internet to connect remote sites or users together. In doing so, it encrypts all network traffic at the sending and receiving ends, and uses authentication to deny access to unauthorized users. If you have VPN access through RIT or another service, use it whenever you access a wireless network.

Stay on “secure” sites
Some “secure” websites encrypt traffic to and from them automatically. You can recognize these sites by checking for “https://” (note the “s”) and a lock icon either in the address bar or the lower right-hand corner of your browser.

Encrypt your traffic
Encrypting your Internet traffic makes it much harder for others to “listen in” on what you’re doing. Check the settings on your e-mail and instant messaging software for some method of encrypting your traffic. Enable settings for “Secure Socket Layer” or “SSL.”

Disable ad-hoc networking
Ad-hoc networking allows computers to connect directly to one another without an access point between them. These types of networks can pose a security threat because they usually have little protection. Disable this feature unless you need it.

Get connected
Running your own wireless network is easy, but it’s critical to secure it properly. The steps that you need to take vary by device so make sure you check your manual.

Make sure you configure the following settings on your router/access point:

- **Enable WPA2 encryption.** Enabling encryption helps prevent attackers from sniffing your traffic and forces anyone attempting to access your wireless network to enter in a passcode. Without the right passcode, they can’t “piggyback” on your network.

- **Change the default SSID and administrative password.** The SSID (Service Set Identifier) is essentially the “name” of your network. Beware of using the default router name and password – hackers can easily find the default login information from the vendor.

- **Disable SSID broadcasting.** Many public networks broadcast their SSID to make the network easy to find. Disabling SSID broadcasting hides your wireless network from the casual observer. Anyone attempting to connect must know the SSID.

- **Enable MAC filtering.** Each wireless network card has a unique identification number known as a Media Access Control (MAC) address. Set your network to only allow approved MAC addresses to prevent network break-ins.

- **Keep your router software and drivers up to date.** A driver is just a piece of software, and like any software, is not immune to bugs. Keeping the drivers up to date ensures that your wireless device has the latest protection and support from product vendors.
Using wireless at RIT
All wireless users at RIT are strongly urged to use the encrypted WPA2 network. The use of wireless routers is prohibited in residential areas on campus.

Get informed
Visit the RIT Information Security website <www.rit.edu/security> to read the security standards, access security tools and software, or find out more ways to protect yourself.

For more information about the Private Information Management Initiative or if you have any other questions about Information Security at RIT, visit the RIT Information Security Webpage at http://security.rit.edu, contact us at infosec@rit.edu, or call 585-475-4123.

~~ Contributed by Ben Woelk
Program Manager
Information Security Office

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

Upcoming Sessions:

<table>
<thead>
<tr>
<th>October 9, 2013</th>
<th>January 14, 2014</th>
<th>April 29, 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 - 11:30 am</td>
<td>1:30 - 4:00 pm</td>
<td>1:30 - 4:00 pm</td>
</tr>
<tr>
<td>2140 Louise Slaughter Hall</td>
<td>2140 Louise Slaughter Hall</td>
<td>2140 Louise Slaughter Hall</td>
</tr>
</tbody>
</table>

What about ethics in the workplace?

To learn more about RIT’s Code of Conduct and the RIT Ethics Hotline, check out http://www.rit.edu/fa/svp/content/ethics-and-compliance-hotline-whistleblower
Internal Audit…it does not sound like something anyone would request or want, for a variety of obvious reasons, but after going through the process with my office, I have a different opinion. The key is that it is an "internal" audit. It is like getting free advice from an independent and objective advisor that has the best interest of the University as the top priority. Now it sounds like something you would ask for, right?

It is sometimes difficult to identify issues in your own unit because you are too close to the processes and procedures and in some cases because you may not be up-to-date on new guidelines. The internal audit process helps you overcome these "blind spots." In addition, the staff of IACA did an excellent job explaining the process, managing the process and keeping everyone informed about the progress throughout. Further, the work was accomplished with virtually no disruption to daily office activities.

What Were They Thinking?!

A fraud investigation took place back in December of 2009 on the New York University campus after a student became suspicious of the expense reports he was delivering. What started as an initial report from one student worker became a lesson to be learned for NYU and its employees as hundreds of thousands of dollars worth of fraudulent claims were uncovered.

Digging through the trash to find receipts, John Runowicz, a former NYU budget coordinator in the chemistry department, allegedly submitted over 13,000 slips of paper for fraudulent reimbursement claims. The receipts, all having come from a local wine and spirits shop, totaled to over $400,000 in expenses; that were ultimately paid out to John Runowicz in the form of expense reimbursements.

Runowicz spent a number of years collecting the ordinary-looking receipts, with the wine shop’s name on them, and sending them with expense reports, unbeknownst to the other accountants.

NYU Spokesman John Beckman had this to say when reports of the fraud went public: "The university is deeply disappointed that one of its employees would abuse the trust of our students, faculty, administrators and staff in this way."

Read more by clicking [here](#).

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 article, What is the Standard by Which Internal Controls are Evaluated?, “Control Activities” are...

A. ...often known as “Tone at the Top” and refer to the ethical values of senior management
B. ...specific processes designed to mitigate the risks which would prevent an organization from achieving its objectives
C. ...both external and internal and must be identified
D. ...crucial components of an effective internal control system enabling management to successfully conduct, manage, and control its operations

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

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

Congratulations to Ulrike Stroszeck from the College of Liberal Arts for correctly answering the Spring issue’s Pop Quiz question.

The question and the correct answer were:

One component of a strong internal control environment is having an appropriate segregation of duties. Which statement below is consistent with this concept?

A. Employees collecting cash should also perform the cash reconciliations and deposit the funds.
B. Account reconciliations should be completed by the individuals responsible for transacting the purchases.
C. No one employee should handle all aspects of a transaction.
D. Employees with custody of assets should maintain the accounting records related to those assets.

Correct