AuditNews

Produced by: Internal Audit (617) 552-8689 **Fall 2005** Volume XXXIX

Save the Date.....

Thursday, November 10th 10-11:30
Business Ethics and Controls Workshop
(McElroy Conference Room)

"Ethics is a "hot" topic in today's business world. How can we be proactive to prevent theft or fraud? In this interactive session, you will learn (1) ways to identify risks, (2) how to implement procedures to improve your controls, and (3) appropriate actions to resolve ethical issues and maintain the University's integrity.

Who Should Attend?
Anyone who wants to learn more to maintain high professional and ethical standards in their work environment.

To register, email employee.development@bc.edu or call

The purpose of this newsletter is to provide the BC community with articles on good business practices, internal controls and responsibilities. Each issue will provide insights to internal control techniques. We have also included an "Ask the Auditor" section to give you an opportunity to obtain answers to specific questions. Additionally, we will provide information on recent items in the news.

We hope that by providing this array of information, we can help you implement effective controls in your area of operations.

Contents

Evaluating Risk	2
Risks and Controls	2
In the News	3
Ask the Auditor!	3
Internet Security	4
More News.....	4

The Human Resources Benefits Office Receives Boston College 2005 Internal Control Best Practices Award

The Benefits Director in the Department of Human Resources is responsible for the administration of all benefits programs including (1) Health Benefits, (2) Flexible Spending Accounts, (3) Life Insurance, (4) Group Automobile and Homeowners Insurance Plans, (5) Sick Leave and Disability Policies, (6) Workers Compensation, and (7) Retirement Programs. Internal Audit reviewed the Benefits Office to evaluate procedures and controls designed to ensure the effective and efficient administration of operations. Under the direction of Jack Burke, Director, financial controls are in place and effectively managed. The cooperation of the entire staff made for a very smooth audit of this area.

Ann Crowley, Kelly Fitzgerald, Jack Burke, Anabelle Murphy, and Devon Celic

Evaluating Risk

One primary activity of the Internal Audit Department is to assist the organization by identifying and evaluating significant exposures to risk and recommending controls to mitigate risk.

Managing risk is a key responsibility of Management. Managers should (1) ensure that adequate and effective processes are in place to control risk exposures and (2) develop ongoing monitoring processes to periodically reassess risk and the effectiveness of controls.

The results of a risk assessment should identify the adequacy and effectiveness of controls that encompass:

- reliability and integrity of financial and operational information.
- effectiveness and efficiency of operations.
- safeguarding of assets.
- compliance with laws, regulations, and contracts.

Control Self Assessment (CSA) methodology is a useful and efficient approach for managers in assessing and evaluating control procedures. A self-assessment allows management to:

- identify risks and exposures,
- assess control processes that mitigate or manage those risks,
- develop action plans to reduce risks to acceptable levels, and
- determine the likelihood of achieving business objectives.

Positive outcomes of a self-assessment include (1) staff being trained to assess and manage risks, and (2) staff taking ownership of control processes in their units and taking responsibility for corrective actions.

More information including a questionnaire can be found at: http://www.bc.edu/offices/audit/controls/selfassess/

Listed below are examples of potential risks and mitigating controls.

Risks and Controls

RISK	CONTROL
Purchases may be inappropriate.	Step-up level of approving expenses and reviewing budget reports.
Private information might be disclosed to unauthorized individuals.	Properly securing offices from unauthorized access.
Incorrect data may be erroneously reported.	Reviewing reports and performing reconciliations to source documents or systems.
Funds could be misappropriated.	The same person does not initiating, authorizing, and processing a transaction.
Critical operations could be seriously interrupted if key individuals were not available because of illness or a decision to leave the University.	Employees receiving timely and effective training.
The University may be liable for unforeseen risks for improper contract negotiations.	Appropriately monitoring vendor contracts and reviewing by General Counsel if necessary.
The reputation of the University could be at risk.	Monitoring changes in accounting methodologies and regulatory requirements and determining applicability to business functions.
A major business disruption because of loss of critical data.	Backing up critical data and software daily and rotating offsite.

In the News: PHISHING

New Scam Asks People to Fax Away Data

From Cnet News
Published: August 11, 2005
http://news.com. com/

Phishers have added a new scam to their bag of tricks to get you to fax sensitive data to phony security investigators.

Cnet reports that "E-mail warnings that appear to come from PayPal, say that someone tried to reset your password and asks you to participate in an investigation. The e-mails direct you to download a form, fill it out, include credit card information, and fax the form to a toll-free number."

Cnet states that phishers are hoping that people will feel it's safer to fax back a form rather than sending data over the Internet.

The good news is that e-mail-based phising attempts may be getting less effective as individuals become more educated about phising. "Trojans and worms are becoming more popular, because the information can be gleaned surreptitiously."

On-Line Scammers Pose as Execs in "Spear-Phishing"

From Yahoo News
Published: August 17, 2005
http://news.yahoo.com

Another reported powerful phishir scam is when "spear phishers" send e-mail to employees at a company or government agency, making it appear that the e-mail comes from a powerful person within the organization.

"Spear phishers target only one organization at a time. Once they trick employees into giving up passwords, they can install 'Troja Horses' or other malicious softwa programs that ferret out corporate or government secrets. Spear phishing has emerged as one of several kinds of 'targeted attacks' that experts say have grown more common in 2005."

Protect yourself against these attacks by never giving out personal information. Read more about e-mail scams from the BC ITS Help Center:
http://www.bc.edu/helpdocs/EM-spam002.shtml

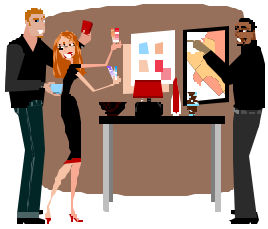
Useful Websites:

ID Theft Resource Center:
http://www.idtheftcenter.org

ID Theft Prevention & Survival:
http://www.identitytheft.org/

Office of Privacy Protection:
http://www.privacy.ca.gov/cover/identitytheft.htm

Ask the Auditor!



How do I ensure that duties performed in my department are properly segregated if there are only two employees in the department?

It is difficult for small departments to properly segregate specific functions that it performs. For example, if a department only has three individuals and it bills, collects, records, and deposits revenue, it can be a challenge to ensure proper controls over these procedures. In situations such as these, management oversight becomes very important. Management should review all invoices and thoroughly review monthly financial reports and reconciliations. Management should also sign off on any documents they review.

How does internal control affect people?

Internal control influences people's actions. Internal control recognizes that people do not understand, communicate or perform the same way. Each individual brings to the workplace a unique background and technical ability and has different personal needs and priorities. These realities affect, and are affected by, internal control. People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's responsibilities and the way in which they are carried out and the entity's objectives.

Is internal control infallible?

Internal control, no matter how well designed and operated, can provide only reasonable assurance to management and the board of directors/trustees regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that

- human judgment in decision-making can be faulty.
- persons responsible for establishing controls need to consider their relative costs and benefits.
- breakdowns can occur because of human failures such as simple error or mistake.
- controls can be circumvented by collusion of two or more people.
- management has the ability to override the internal control system.

Internet Security: Protect Yourself at Home

Contact the ITS Help Center for any questions concerning protection of your systems.

http://www.bc.edu/offices/help/

Computer security is the process of preventing and detecting unauthorized use of your computer—even at home. Hackers often want to gain control of your computer so they can use it to launch attacks on other computer systems.

Having control of your computer gives hackers the ability to hide their true location as they launch attacks. Even if your computer is connected to the Internet only to play games or to send email to friends and family, your computer may be a target.

Intruders may be able to watch actions on your computer, or cause damage to your computer by reformatting your hard drive or changing your data. Unfortunately, intruders are always discovering new vulnerabilities to exploit in computer software.

To protect your system, the CERT® Coordination Center, http://www.cert.org makes the following recommendations:

- If you use your broadband access to connect to your employer's network use a Virtual Private Network (VPN).
- Use anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions.
- Use a firewall.
- Make regular backups of critical data.
- Never run a program unless you know it to be authored by a someone you trust.
- Before opening any email attachments, be sure you know the source of the attachment. If you must open an attachment before you can verify the source, save the file to your hard disk and scan the file using your antivirus software before opening the file.
- Keep all applications, including your operating system, patched. Vendors will usually release patches for their software when vulnerability has been discovered.
- Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

From InformationWeek, Sept 5, 2005:

"Katrina scams are on the horizon.. there are more than 100 registered domain names using combinations of 'katrina,' 'donate' or 'disaster'...some are legit, but most will end up with scammers". Be very careful about giving out personal information.

More News.....

The SANS Institute and experts from the US, UK and Canadian governments and four private groups have identified the most critical new **Internet security vulnerabilities** discovered during the 2nd quarter of 2005. Read more at: http://www.sans.org/top20/q2-2005update/

Report: Spyware Eyes Bigger Bucks, August 24, 2005. From ComputerWorld.com: "Spyware is getting more dangerous and has become a greater threat for the enterprise."
http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,104135,00.html?SKC=cybercrime-104135

Is VoIP Secure Enough For Prime Time? August 1, 2005. From InformationWeek.com: "VoIP is hot, but VoIP security is not. Security risks abound in current commercial VoIP solutions, including Denial of Service (DoS) attacks, eavesdropping, and a host of new vectors for intrusion and malware propagation."
http://www.informationweek.com/showArticle.jhtml;jsessionid=2F22EWRFC1ETYQSNDBCCKHSCJUMEKJVN?articleID=166404306