

In this issue:

- Introduction **1**
- Top 10 Good Management Practices **1**
- Quick Tips & Tricks **2**
- Tips On Spending Federal Grant Money **3**

Our three strategic priorities are to:

1. anticipate and help prevent compliance and control issues and to mitigate the risk.
2. foster enduring cultural change that results in consistent and quality management of College operations.
3. serve the College's needs related to risk management and internal controls. Our mission is to support the College management in meeting its responsibilities while helping to improve organizational and operational effectiveness and efficiency.

Message from the Associate Vice President of Auditing Services and Reporting

Brenda Leonard

Welcome to the first edition of our Audit Newsletter. We believe vital internal control for any organization is communication, the flow of information, correct interpretation of policies and procedures, and guidance.

Our mission is to provide quality internal auditing services and business advice, consistent with professional standards,

to senior management, faculty, and staff to help improve efficiency, compliance with applicable laws, regulations and College's policies and accountability of College's asset. Our goal is to have positive influence on the internal control environment throughout the many and varied operations of the College.

This newsletter will continue to provide you with articles that demonstrate why internal controls are important to help prevent fraud, as well as articles offering internal control principles and recommendations, best business practice guidelines, and other tidbits that may assist you or your office to establish good internal controls.

Top 10 Good Management Practices

1. Read all requests to spend the College's money before you sign them or approve them electronically (Check Requests, Travel Authorizations, payroll time sheets, etc.). Never sign a document unless you have reviewed at least the most important information on that document.
2. Develop written procedures for critical operations. These serve as a resource for current employees and a good training tool for new employees.
3. Develop measurable annual department goals based on your department's mission and strategic goals. Create an action plan to achieve goals and communicate to all employees.
4. Make sure each transaction has at least two people involved: one initiator and one approver. Separate two duties to reduce the possibility of errors.
5. Review the General Ledger Browse Report (GLBR) screen once a month or periodically. This screen shows available budgets, encumbrances, MTD and YTD expenses, and allocated budgets. Investigate anything that doesn't look right.
6. All cash and checks should be processed through the Cashier's Office. On the rare occasion that you do need to collect cash (this should be rare and exceptional), deposit all cash and checks received to the Cashier's Office daily. If something has to stay in your office overnight, lock it up.
7. Don't be satisfied with "the way we've always done things." Review your processes on a continuous basis for inefficiency and duplication of effort.
8. Ensure all expenditures have a clear business purpose. If the purchase is for something that could be construed as personal, clearly document the business purpose on the invoice or receipt.
9. Maintain good supporting documentation for all purchases. Ask yourself, "What would my supervisor or an auditor want to see?"
10. Make sure time sheets are reviewed and signed off by a supervisor or someone who is familiar with the employee's work hours.

Used with permission of: Jodi Bailey, chief audit executive, Utah State University; Updates by Elena Randolph, executive director, Budgets and Payroll, and Brenda Leonard, associate vice president, Auditing Services and Reporting, CPCC



Phishing Emails

External fraud and phishing attempts are always increasing. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Cyber crime surpassed drug trafficking as the number one criminal money maker in 2008.

Here are some tips to avoid being a victim of a phishing scam:

- Never provide personal information (Social Security Number, birth date, password, credit card number) to anyone through email. No legitimate entity will ask you for such information via email.
- Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or if you don't know the sender or user's identity.
- Avoid filling out forms in email messages that ask for personal information.
- Always ensure that you're using a secure (https) website when submitting credit card or other sensitive information via your Web browser.
- Please forward any suspicious emails as an attachment to spam@cpcc.edu for analysis and corrective measures.

Remember some scam sites will try to show the "https://" and/or the security lock to look legitimate. Get in the habit of looking at the address line, and make sure you are visiting the correct URL. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?"

Always know where your web address is directing you. Ensure that your browser is up to date and security patches are applied.

Password and Malware

Use a passphrase (e.g., TheCatInTheHat) instead of a password. The more numbers, special characters, and punctuation in your passphrase the better (e.g., Let\$GOP@nther\$). Never share your password with ANYONE, including the helpdesk or your supervisor. Use different passphrases for different purposes, in case one is compromised, and never use your CPCC login or password on a non-CPCC website or application. If you feel your passphrase has been compromised, change it immediately. Also, ALWAYS lock your computer anytime you are away from your desk.

1. HTTP/HTTPS: **http**, or hypertext transfer protocol, is the standard prefix used for website addresses. **https** (hypertext transfer protocol secure) on the other hand, signals that the website you are visiting is secure. When browsing bank, credit card, or shopping websites on line, for example, look for "https" before entering any sensitive information.
2. Always keep your software and anti-virus updated. In the event you do click on a malicious link, having a properly patched system can reduce your chances of infection. Also, an updated anti-virus can detect and prevent known malware.
3. Never store sensitive information on your computer or mobile device. Delete it as soon as it is no longer needed.

For additional best practices, alerts and resources, please visit the ITS Security site at www.cpcc.edu/its/faculty-staff/its-security.

Top three Internet scams to avoid in 2011

Sophisticated scams developed by cyber-criminals to target smartphones and social networks means businesses must increase awareness of Internet scams, according to security firm KnowTheNet.

You can visit the link provided to find more information about the top three scams in 2011:

1. Smartphone app scam
2. Facebook wall virus
3. The phone support switch

www.infosecurity-magazine.com/view/15163/top-three-internet-scams-to-avoid-in-2011



High tech pick-pocketing

Most of you might have already heard about it or seen a segment on the evening news that someone can easily get your credit card information without ever touching your credit card. We have provided a few Web links below that discuss this topic if you want to know more.

- www.nbc-2.com/Global/story.asp?S=13463897
- www.abcactionnews.com/dpp/news/region_tampa/downtown_tampa/New-technology-allows-credit-card-numbers-to-be-stolen-by-just-walking-by
- www.connectmidmissouri.com/news/story.aspx?list=~%5Chome%5Clists%5Csearch&id=578478

Used with permission of: Syracuse University Audit Insights Newsletter from Stephen G. Colicci, director, Office of Audit and Management Advisory Services, Syracuse University; Updated by CPCC ITS Team

IMPACT

Tips On Spending Federal Grant Money

Institutions need to be ready for the challenges of administrative precision in adhering to regulations, timelines and other requirements attached to billions of dollars in grants that have been awarded in recent years. Amidst the euphoria of building a state-of-the-art teaching laboratory or receiving a training grant, the institutions need to ask, "Are we ready to maximize the impact of this grant, track the costs of the program and provide accurate and timely reports to the funding entity?" If a grant proposal and budget is carefully and realistically designed, the project team should spend exactly the amount received and successfully accomplish the stated objectives while achieving the project's outcomes. In order to do this and adhere to funding agency regulations, recipients should have an understanding of the basic terms and procedures regarding grant or contract money.

Allowable Costs

Every funding agency has categories of items for which grant recipients may spend money, and categories for which they may not. For instance, federal grant funds may not be used for "entertainment." It is important for project directors to know that refreshments served at a project-related meeting may be classified by the funding agency as entertainment, and therefore may not be allowable. What happens if grant funds are spent on an unallowable item? The money will have to be given back, and another funding source will need to be used to pay for that expense. Project directors at CPCC can work with the Grants and Contracts Accounting Office and the Office of Government Relations and Grants to ask questions regarding allowable and unallowable costs.

Documenting Expenditures

Institutions must provide documentation to show that money was spent properly, or the funds cannot be recovered. Generally, the documentation is sent via invoices, receipts, payroll records, etc.

Documenting Time and Effort

The biggest single budget category for most grants is personnel. Funding agencies are supporting the individuals who will be executing the project activities and accomplishing the project objectives and outcomes. It is important to document that the time was spent as agreed and the money was spent appropriately. CPCC tracks personnel time through Time and Effort reports and monthly timesheets.



Tracking Expenditures

Project directors should carefully review the monthly financial reports prepared by the Grants and Contracts Accounting Office. However, project directors should not depend solely on these reports to track expenditures. Statements can be a month or more behind; moreover, they occasionally contain mistakes.

Cost Reimbursable Awards

Federal awards received can be on a "cost reimbursable" basis. This means that the institution must cover the initial cost and then request reimbursement from the funding agency. In order to be reimbursed, documentation must be presented to substantiate that the funds were spent on allowable expenses. The Grants and Contracts Accounting Office works closely with project directors to track project-related expenses and request reimbursements from funding agencies. At the end of the grant period, any unexpended funds remain with the funding agency.

Other Payment Structures

Some funding agencies will pay lump sum installments every quarter or based on the receipt of project deliverables. Others may even award the entire amount up front. With installment plans, the release of the funds is often contingent on the institution submitting an activity report detailing project accomplishments. At the end of the grant period, unexpended funds usually must be returned to the funding agency.

continued on next page

IMPACT



Rollover of Unexpended Funds/No Cost Extensions

Occasionally, an institution may find that they are not able to expend grant funds exactly as expected. Perhaps, equipment or services cost less than anticipated or hiring project personnel delayed the project's timeline. It is important that project directors do not rush to expend a large amount of funds immediately before a grant ends. Instead, institutions can request a No Cost Extension and ask for permission to extend the project period to enable grant funds to be expended and project goals to be accomplished. The Government Relations and Grants Office works closely with project directors and funding agencies to submit requests for No Cost Extensions when they are needed.

Closing Out

Many funding agencies require a final report of expenditures at the end of the grant period. All expenditures must be finalized and the account closed within the specified time. Most funding agencies do not allow the institution to retain residual funds. Therefore, at the end of the grant period, funds must be spent or returned.

CPCC receives numerous grants each year from a variety of funding agencies, and has a dedicated team of staff in the Offices of Government Relations and Grants, and Grants and Contracts Accounting committed to helping project directors comply with the administrative requirements associated with receiving grant funds.

Used with permission of: Lisa M. Kedigh, administrative assistant, Office of Internal Audit, Georgia Health Sciences University; Updates by CPCC's Government Relations, Grants Team and Grants & Contracts Accounting Team

Requesting Internal Audit Services

The CPCC Internal Audit staff is committed to assisting college management by providing an independent appraisal within Central Piedmont Community College to determine the appropriateness, soundness and adequacy of the College's accounting, financial and operational controls. These appraisals provide information and recommendations to the College's administrators.

In addition to the formal audits, we are available to answer questions and give advice regarding specific policies and procedures and act as consultants on internal controls.

For more information, please visit us at our website at www.cpcc.edu/audit/internal-audit-office or contact one of the staff members.

- Brenda Leonard, associate vice president of auditing, brenda.leonard@cpcc.edu
- Janice Hill, director of internal audit, janice.hill@cpcc.edu
- Meera Vora, assistant director of internal audit, meera.vora@cpcc.edu



IMPACT