Chief Information Officer Managers' Internal Control Program

INFORMATION BULLETIN

Volume 5, Issue 4 October 3, 2008

Special Message:

The start of a new fiscal year is a great time to update policies and procedures with lessons learned from the previous year. The MIC Program Office would like to encourage offices to take this time to review their internal controls to ensure they are accurate and up-to-date.

"Purchase card reviews will help to ensure that agencies establish and maintain internal controls to provide reasonable assurance that: goals and objectives of the purchase card program are being met and safeguards against fraudulent, improper, and abusive purchases are adequate."

Annual Purchase Card Reviews

According to the Contracting Center of Excellence (CCE), Purchase Card Reviews will be performed **once each fiscal year** on all purchase card accounts. These reviews will focus on transactional activity and overall adherence to the purchase card program requirements, as well as responses to previous findings and corrective actions.

There are two types of purchase card reviews:

1) **Billing Official (BO) Review** - **BOs are required to perform an annual review of their accounts** using the checklist in Chapter 9 of the CCE Purchase Card Operating Procedures. BOs must also document any deficiencies identified during the review and have a copy available when CCE performs its review. **Review reports must be maintained on file for six years and three months.**

Repeat findings from the previous fiscal year review report may result in suspension of accounts.

2) **CCE Purchase Card Review** - A review by the CCE conducted with the BO on all cardholder accounts under their authority. During the review, the CCE will obtain and review the written policies and procedures, which describe and control the purchase card program. They will also review the key elements of the transaction and control environment, as well as other internal control activities listed in Chapter 9 of the CCE Purchase Card Operating Procedures.

The CCE will issue a report approximately 30 days after the review to communicate findings, discrepancies, and issues. Upon receipt of the review report, BOs may respond in writing within 30 days to any of the findings, discrepancies, issues or recommendations. CCE's review findings will be documented in writing and forwarded to the BO for corrective action. A copy of this review will be forwarded to the BO's supervisor.

For a copy of the CCE Purchase Card Operating Procedures visit http://cce.hqda.pentagon.mil/services/docs/FY08%20PCOP%20web%20version.pdf.

Positive Purchase Card Reviews

According to the FY 2008 CCE Purchase Card Operating Procedures, **agencies will generally receive a positive report** if they adhere to the following:

a) Written procedures outlining areas such as property accountability for non-expendable items and coordination with an Information Management Officer when buying information technology items.

b) Written guidance to Cardholders (CHs) advising of office limits, and when and how funding will be managed for each purchase card account.

c) Adequate separation of duties between the BO, CHs, Resource Manager, and the Property Book Officer.

d) Records are well organized, and purchase files are properly documented with receipts.

Continued next page

Positive Purchase Card Reviews *Cont'd*

e) Documentation in the file explaining any unusual situations, such as a buy that appears to have been a "split" but wasn't, or unusual purchases, such as items that are infrequently purchased.

f) Active consideration of mandatory sources consistent with Federal Acquisition Regulation Part 8.

g) Rotation of vendors to promote competition, as well as seeking fair and reasonable pricing for open market buys.

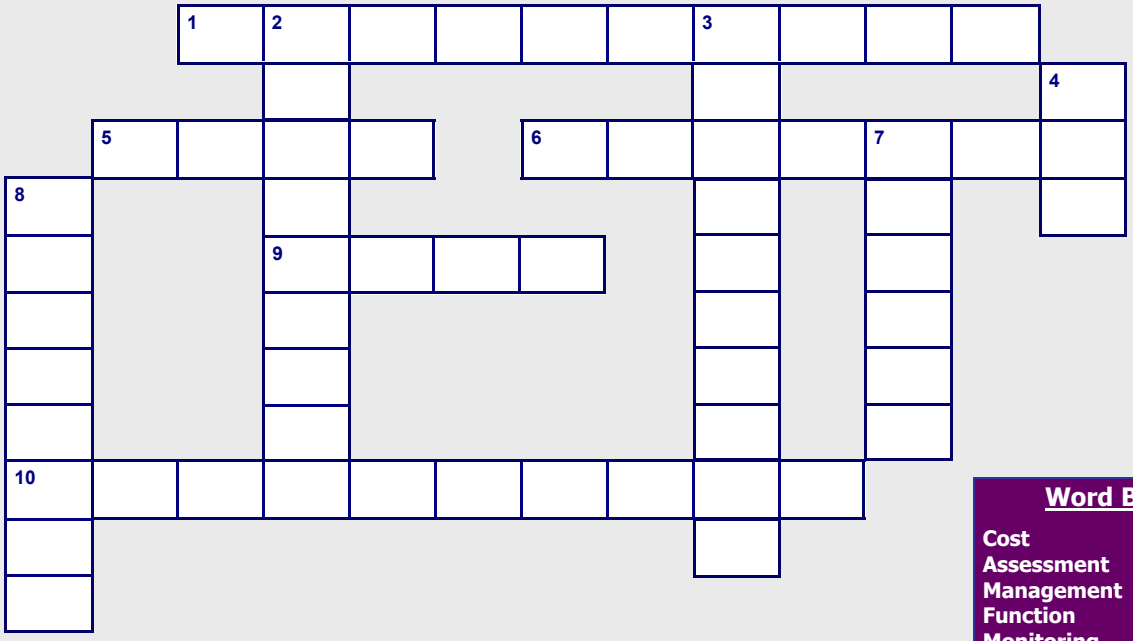
h) No unauthorized purchases.

i) Proper span of control, i.e., a BO having no more than seven CH accounts.

j) Closing accounts with no activity for six months or longer.

Complying with these guidelines will not only help agencies receive positive reports, but it will also help BOs maintain proper control of their purchase card accounts.

Internal Control Crossword Puzzle



Word Bank

Cost	Risk
Assessment	Control
Management	Mitigate
Function	Review
Monitoring	All
Assurance	Manager

ACROSS

1. _____ sets the tone for all aspects of an organizations internal control activities.
5. The _____ of control should not exceed the benefits likely to be derived.
6. Internal _____ is a continuous built-in component of operations.
9. The possibility an event will occur and adversely effect the achievement of internal control objectives and may result in the loss of Government resources due to fraud, waste, or mismanagement.
10. A Risk _____ is an evaluation of the susceptibility of an activity to fraud, waste, and mismanagement.

DOWN

2. The Annual Statement of _____ is an annual report stating that an evaluation of the CIO Managers' Internal Control Program was conducted and taken as a whole, it provides reasonable assurance that controls are in place and operating effectively.
3. Internal control _____ should assess the quality of performance over time and ensure that the findings from audits and reviews are promptly resolved.
4. _____ personnel play an important role in making controls happen.
7. An internal control _____ is the evaluation and testing of internal controls to determine whether necessary controls are in place and producing the intended results.
8. Internal controls are policies, procedures, guidance, instructions, and techniques that help _____ or prevent risks.

Government Employees Facing Prison Time

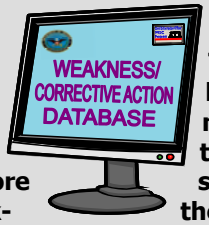
Constance Walton, a former Defense Logistics Agency employee, is facing up to 5 years in prison for failing to disclose income she earned from a company that she owned. Walton's company received work assignments from contractors of the Army Information Technology Agency with the help of one of their employees, Robert Johnson. Johnson used his position as the Chief of Quality Assurance and the Contracting Officer's Technical Representative to direct two contracting companies to subcontract with two companies where he secretly held a financial interest, one of which was Walton's.

From 2000 - 2006, Walton received more than $100,000 from the contractors while Johnson obtained over $150,000. Johnson pleaded guilty to wire fraud and was sentenced to 2 years in prison, 3 years supervised release, and ordered to pay over $150,000 in restitution. Walton pleaded guilty to 1 count of making a false statement and is awaiting sentencing. In addition to jail time, she faces 3 years of supervised release and a fine of $250,000.

Source: US Department of Justice

Assessable Unit Managers' Corner

The CIO MIC Program Office has developed two new multi-user management tools to assist offices with their internal control responsibilities: 1) the Weakness/Corrective Action Database and 2) the Risk Assessment Database.

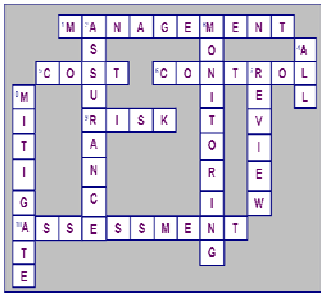


The Weakness/ Corrective Action Database allows offices to more effectively manage weaknesses from internal and external reviews and the actions taken to correct these weaknesses. Offices now have the ability to produce and submit their corrective action plans through the database.

The Risk Assessment Database allows offices to enter new or edit existing functions, activities, and risk assessments. Offices now have the ability to produce and submit their Functions & Activities and Risk Assessment Reports.

In addition to being valuable tools for managing corrective actions and risks, these databases will provide offices with more control over their internal control data.

Audit Reviews Highlight Internal Control

During their review of IT project rebaselining, the GAO determined that approximately 48% of the government's IT projects have been rebaselined, several of which were rebaselined twice or more. The frequency of which these projects are being rebaselined highlights the importance of sound policies to guide agencies in these efforts. However, agencies' policies lack the important elements of a comprehensive policy, such as being consistent with best practices. Without comprehensive policies to guide them, agencies may not be optimizing the effectiveness of rebaselining as a tool to improve performance management. In addition, their rebaselining processes may not have the transparency needed to ensure effective oversight. To help agencies improve their policies, the GAO recommended that OMB issue guidance for rebaselining policies that would specify a minimum set of key elements. To read more about this report (GAO-08-925), please visit http://www.gao.gov/new.items/d08925.pdf.

When the Defense Security Service (DSS) transferred its personnel security investigation function to the Office of Personnel Management, they put the personally identifiable information (PII) of employees who were investigated for security clearances at undue risk of being compromised. DSS management, in place during the transfer, failed to account for approximately 501 laptops and an undetermined number of safes and auxiliary hard drives. DSS also deviated from internal guidance when it allowed 48 employees to leave without collecting, deactivating, and disposing of their Common Access Cards. This lack of accountability led the DoD IG to identify DSS property accountability as a material weakness. To prevent recurrence, the DoD IG recommended that DSS implement controls over property that contains sensitive or classified information or PII, conduct periodic physical inventories of assets, and track assets containing PII by unique identifier. To read more about this report (D-2008-114), please visit http://www.dodig.mil/Audit/reports/fy08/08-114.pdf.