



Chief Information Officer Managers' Internal Control Program



INFORMATION BULLETIN

Volume 6, Issue 2

March 31, 2009

Special Reminder:

The goal is not to establish the greatest possible number of internal controls; instead, it is to establish those that will be the most effective in meeting mission objectives.



When Things Go Wrong — What Then?

The primary purpose of internal controls is to provide reasonable assurance that nothing will go wrong. However, sometimes despite good intentions and well designed controls things do go wrong. If that happens, what then?

1. Take action to rectify or resolve the problem and/or mitigate the consequences and turn the event into an opportunity to reduce the likelihood of a repeat occurrence.

2. Discuss what went wrong with those directly involved. Research the “how” and “why” of the event. Discovery of the conditions that led to the problem is the first step in prevention. Among the

questions to ask are: Is there a knowledge gap? Does everyone clearly understand their duties and responsibilities? Is additional training needed? Are there controls that are inadequate or missing? Encourage feedback and recommendations on how the process may be improved.

3. Evaluate the likelihood and impact of the same or a similar event occurring in the future. In evaluating the likelihood of recurrence, use past history. Also, consider changes in the current operating environment (e.g. staffing, systems, processes, etc.) In evaluating the impact or seriousness of consequences, some criteria to consider are:

threats to health and safety, violations of laws and regulations, loss of assets or revenue, disruption of the mission, and impairment of public trust or confidence.

4. Develop corrective actions based on the information derived from the first three steps.

5. Discuss the event and the corrective actions with all staff. Raise awareness of what could go wrong and attach importance to the tasks performed. Through timely and constructive feedback, encourage a commitment to competence and a job well done.

Performing these steps will help reduce the risk of a repeat occurrence of “things going wrong.”



***"Risk is not a problem.
A problem is a risk whose time has come."***

Revision to OMB Circular A-123 Appendix B

The January 15, 2009, revision to the Office of Management & Budget Circular A-123, Appendix B has established additional internal control guidance regarding purchase cards, travel cards, convenience checks, and the management of any property purchased with them. This guidance is con-

tained in two newly added chapters.

Chapter 12 contains specific guidance concerning convenience checks:

- When they may and may not be used, and other limitations and restrictions;

- Reporting and management requirements, in addition to those included in previous guidance, on purchase cards; and

- Guidance on obtaining waivers for exceptions to the policy.



Continued on page 2

Revision to OMB Circular A-123 Appendix B *cont.*

Chapter 13 addresses the importance of appropriate management of property. Citing the enormous amounts of money that are spent each year using purchase cards and convenience checks, the guidance states: **“Agencies must have reasonable, effective internal controls so that this property can be accounted for, and so that use of this property is limited to official purposes.”** Cardholders/custodians should be familiar

with the agency policies on property management, which should be compliant with Federal government-wide policies.

Because property is frequently delivered directly to the cardholder, each agency is charged with developing internal controls for effective management of this property.



Revisions in other chapters include guidance regarding reimbursement to the government and disciplinary action in the event of misuse, fraud or erroneous charges.

For details, please see the complete revision package at: http://www.whitehouse.gov/omb/circulars/a123/a123_appendix_b.pdf.

Internal Control Best Practices for Purchase Cards

- ★ Ensure that all Billing Officials have received appropriate training.
- ★ Ensure that the cardholder has received appropriate training prior to issuance of a charge card.
- ★ Apply policies and procedures to ensure high-risk property is included in the organization’s property control system.
- ★ Use available authorization controls to mitigate risk of misuse or fraud.
- ★ Conduct periodic reviews of cardholder records.

Internal Controls: Preventive, Detective, Corrective

Internal controls can be categorized in a number of ways. When defined by the function they perform, internal controls can be divided into three types:

1. Preventive Controls - designed to keep risks from occurring in the first place. Preventive controls are the most common type of internal control.



Determining risk factors associated with an activity is the key to developing preventive controls. This type of control is extremely important. Prevention is always preferred over recovery from the consequences of something going wrong. Prevention is usually the most “cost effective” type of control. To quote Benjamin

Franklin, “An ounce of prevention is worth a pound of cure.” Policies, procedures, and even job descriptions fall under this type of control.

2. Detective Controls - designed to detect an error or a newly developed weakness, preferably before it becomes a serious problem.



The control environment, as a whole, is dynamic. Some risks may disappear and new risks/weaknesses may appear because of changes in operations. Detective controls help detect risks/weaknesses early.

3. Corrective Controls - usually developed because a weakness has been identified. This type

may also be in response to a breach, or because a problem has been detected early enough to avoid a breach. A corrective control may share aspects of the first two types.



When developing internal controls to fit a specific activity, knowledge is key. Understanding the purpose and goals of the activity and analyzing the processes and risks involved will make selecting the appropriate type of control relatively easy.

No matter how well internal controls are designed, they provide only reasonable, not absolute, assurance that things will not go wrong. **Reasonable assurance is a goal worth pursuing.**

Idle Curiosity Leads to Guilty Plea

On January 14, 2009, a former State Department employee, Dwayne F. Cross, of Upper Marlboro, MD., pleaded guilty in U.S. District Court to illegally accessing confidential passport applications.

In the regular course of his employment, Cross had access to the State Department's computer databases, including the Passport Information Elec-

tronic Records System (PIERS).

In his guilty plea, Cross admitted that between 2002 and 2007, he logged onto the PIERS database and viewed the passport applications of more than 150 celebrities and non-celebrities. These included members of the media, family members, friends, associates and others, without any



official government reason to do so. He claimed his sole purpose in accessing and viewing these passport applications was idle curiosity.

Cross could face up to a year in prison and a \$100,000 fine, or probation and community service.

Assessable Unit Managers' Corner

- ★ Among items now available on the MIC Webpage are the Assessable Unit (AU) Manager Training and self scoring Questionnaire. All OCIO AU Managers are encouraged to review the training. Please visit the MHS CIO Website at <http://www.health.mil/mhscio/> and select Managers' Internal Control Program.
- ★ Reminder - New employees should complete the MIC Program Annual Training within 60 days of beginning employment with the Office of the Chief Information Officer. Training is available on MHS Learn, an enterprise solution for training. A link to the MHS Learn site is located in the Training section of the MIC webpage identified above.

Audit Reviews Highlight Internal Control

In January, the Department of Defense Inspector General (DoD IG) released the results of a second review regarding DoD contracting through the U.S. Department of Veterans Affairs (VA). It was determined that while VA contracting officials and DoD management officials showed some improvement, there was still inconsistent compliance with procurement regulations when making acquisitions through VA. As a result, DoD organizations had no assurance that the purchases made through the VA were based on best value or that VA used effective and efficient acquisition procedures. Thus, DoD continued to incur potential Antideficiency Act violations. Additionally, it was determined that a material internal control weakness existed, as defined by DoDI 5010.40, "Managers' Internal Control (MIC) Program," January 2006. The report stated that sites visited encountered problems while implementing and executing policy. Contracting, financial, and accounting officials did not comply with regulations and statutes. To read more about this report (D-2009-043), please visit <http://www.dodig.mil/Audit/reports/fy09/09-043.pdf>.

During an internal control and data reliability audit, classified and sensitive information was discovered in two unclassified Department of Defense (DoD) systems used by the U.S. Marine Corps (USMC): Deployable Disbursing System (DDS) and Electronic Document Access/Voucher Process System (EDA/VPS). This occurred because a policy, an internal control to ensure that finance personnel were adequately aware of classification guidelines, had not been developed by the USMC. In addition, adequate measures to remove classified information from the systems had not been taken by that organization. Recommendations were made for the removal of material found. Ultimately, the Defense Finance and Accounting System temporarily shut down the affected DDS and EDA/VPS systems to remove the classified and sensitive information. To read more about this report (D-2009-054), please visit <http://www.dodig.mil/Audit/reports/fy09/09-054.pdf>.



"Internal Control is the essence of management accountability."