



# Chief Information Officer Managers' Internal Control Program



## INFORMATION BULLETIN

Volume 8, Issue 1

December 30, 2010

### Special Message:

**One of the true joys of the Holiday Season is the opportunity to say "Thank You" to everyone involved with the MICP for all your hard work and dedication. We also extend our warmest thoughts and best wishes for a very**

**Happy New Year!**



***"Be sure you put your feet in the right place, then stand firm."***

***~ Abraham Lincoln***

## Internal Controls: Why Do They Matter?

Why do internal controls matter? Perhaps the best answer is another question: What would happen if there were none? Imagine trying to conduct any kind of business, achieve any strategic goal, protect information and tangible assets, or achieve any continuity of effort without them: No plan of action, no established procedure, no documentation of previous accomplishments and methodologies, no line of authority for decision making, no security. Maybe our efforts would be successful, but at what cost in time, money, and wasted effort? More likely, every-

one would be heading off in his or her own direction, and little progress towards any common goal would actually take place.

The fact is internal controls, in one form or another, probably have been around for as long as humans have lived in organized societies. At the societal level we call them customs, traditions, and laws. At the business and government level we give them names like policy, guidance, standard operating procedures, asset libraries, inventory lists, and so on. Internal controls help provide the structure that allows us to minimize the risk of

loss, waste, fraud, and mismanagement. Well designed controls help increase productivity and provide reasonable assurance of achieving expected results. At their best, effective controls become such intrinsic parts of an activity that we scarcely realize they are controls. Only when controls fail, are circumvented, or ignored do the consequences quickly draw our attention.

In short, internal controls matter because they help us accomplish our work, achieve our goals and effectively use resources.

## Don't Overlook Segregation of Duties

Segregation of duties is an internal control activity that decreases or helps prevent the occurrence of both innocent errors and/or intentional fraud. At the most basic level, segregation of duties means that no single individual has control over two or more phases of any operation or financial transaction.

The usefulness of segregation of duties is obvious

when dealing with financial transactions where there is always a potential for fraud.

In the area of operations segregation of duties provides two key benefits:

1. A deliberate fraud is more difficult when it requires a collusion of employees; and
2. It is much more likely that unintentional errors will be found.

If it is potentially possible for a single person to carry out and conceal errors and/or irregularities in the course of performing daily activities, most likely that person has been assigned (or allowed access to) incompatible duties or responsibilities. With this in mind, managers should ensure a cross-check of duties when assigning responsibilities.

*(Continued on page 2)*

# Don't Overlook Segregation of Duties cont.

If staffing limitations make it impossible to avoid such a situation then mitigating controls should be developed and implemented.



There should always be more than one set of eyes overseeing any operation or transaction.

<i>An individual who...</i>	<i>Should not...</i>	<i>Instead,</i>	<i>Before</i>
Prepares a document, such as a contract, an activities report, or meeting minutes	Approve the same document.	The document should be reviewed for content, accuracy, and adherence to guidance by at least one other qualified person	Submitting for approval by appropriate authority.
Initiates a purchase request	Approve the purchase request.	The request should be reviewed for adherence to guidance and availability of funds by a knowledgeable neutral party	Submitting for review and approval by appropriate authority.
Maintains/Enters information in a database	Decide what data should be entered.	Subject matter experts should provide the data and review database generated reports	Submitting for review and approval by appropriate authority.

## MICP Anti-Snooze Brain Teaser Double Puzzle

Effective, well-designed internal *controls* facilitate achieving *mission* goals, minimizing the occurrence of *fraud*, *waste*, and *mismanagement*. As an added *benefit* they minimize the potential for *risk* becoming *vulnerability*. *Monitoring* and evaluating the efficiency of controls, including *policy* and existing *procedure*, helps ensure control *weakness* is identified.

### Word Scramble

- EFTNBIE
- OTSLONRC
- ARDUF
- SMEMGIETNAAMN
- OSSINMI
- OITNINGMRO
- YOILC
- DRUCEPREO
- ISRK
- RLIYIVTEUBANL
- SATEW
- NKWSEEAS

### Unscramble

- □ □ □ □ □ □ □
- □ □ □ □ □ □ □
- □ □ □ □
- □ □ □ □ □ □ □ □ □ □ □ □ □
- □ □ □ □ □ □ □
- □ □ □ □ □ □ □ □ □
- □ □ □ □ □ □ □
- □ □ □ □ □ □ □ □ □ □ □
- □ □ □ □
- □ □ □ □ □ □ □ □ □ □ □ □ □
- □ □ □ □ □ □ □
- □ □ □ □ □ □ □

### Word Search

G M W A S T E E D S L G R  
 M O N I T O R I N G D O R  
 B E N E F I T F R A U D U  
 V U L N E R A B I L I T Y  
 W E A K N E S S K M O P M  
 I O M F N E Y B S G S G E  
 P O L I C Y I B K R N K M  
 V P R M U L A O O L L R E  
 R F E Y C O N T R O L S E  
 D I N N P R O C E D U R E  
 M I S S I O N F I N L G E  
 N R I S K D M E A I M S B  
 M I S M A N A G E M E N T

## Maryland Man “Recycles” Stolen Government Property

Levon Smith of Annapolis pleaded guilty on October 20 to theft of government property as part of a scheme to steal and sell copper cables and other materials used in foreign military operations. While working as a Senior Material Control Analyst for AAI Corporation, Smith removed cables and other government property on more than 40 occasions between June of 2008 and October 2009. The government purchased the materials and parts for AAI

to install in U.S. property, including unmanned aerial vehicles (drones). Presenting an expired Arizona driver’s license as identification, Smith sold approximately \$340,000 worth of government materials to a recycler in Rosedale, MD. He received only about \$22,000 from the recycling company.

“Theft of Defense Department property is an issue that reverberates throughout the contracting process.

Safety concerns and costs increase and literally everyone pays the price. Our men and women serving in harm’s way deserve better,” said the Special Agent in Charge, Defense Criminal Investigative Service – Mid-Atlantic Field Office.



Smith faces a maximum sentence of 10 years in prison.

Source: U.S. Department of Justice, Press Release.

## Assessable Unit Managers’ Corner

It’s that time of year again and **Self Assessment Reviews** are under way. One of the many responsibilities of the Assessable Unit (AU) Manager is to ensure that internal control reviews and testing are conducted properly and in a timely manner.



A minimum of **three people** per AU must participate in the Self Assessment Review. Participants may be contractor or government, or a combination of the two. The review should reflect a consensus of all participants.

**Testing** is an important aspect of any internal control review. Don’t fear the “T” word. Testing proves or disproves opinions about the efficiency and effectiveness of controls, and can identify weaknesses that otherwise might be overlooked.

## Audit Reviews Highlight Internal Control

In an audit report released in November, GAO concluded that weaknesses in information security controls at the Federal Deposit Insurance Corporation (FDIC) constituted a significant deficiency in internal controls over its information systems and data. Until FDIC corrects the security weaknesses identified during this year’s audit, it faces an elevated risk of the misuse of federal assets, unauthorized modification or destruction of financial information, inappropriate disclosure of sensitive information, and disruption of critical operations. FDIC did not have policies, procedures, and controls in place to ensure the appropriate segregation of incompatible duties, adequately manage the configuration of its financial information systems, and updated contingency plans. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities such as effectively developing, documenting, and implementing security policies, and implementing an effective continuous monitoring program. Until these weaknesses and program deficiencies are corrected, FDIC will not have sufficient assurance that financial information and assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. To read more about this report (GAO-11-29), please visit <http://www.gao.gov/new.items/d1129.pdf>.

Also in November, GAO reported that federal agencies have taken steps to secure wireless networks, but more can be done to improve security and to limit vulnerability to attack. GAO identified a range of leading security practices for deploying and monitoring secure wireless networks and technologies that can help secure these networks. Existing government-wide guidelines and oversight efforts do not fully address agency implementation of leading wireless security practices. Until agencies take steps to better implement these leading practices, and OMB takes steps to improve government-wide oversight, wireless networks will remain at an increased vulnerability to attack. To read more about this report (GAO-11-43), please visit <http://www.gao.gov/new.items/d1143.pdf>.



*“We are responsible for our decisions in our personal life, so why shouldn’t we be just as accountable in our work life.”*

*~ C. Pulsifer*