



# Chief Information Officer Managers' Internal Control Program



## INFORMATION BULLETIN

Volume 7, Issue 2

March 30, 2010

### **Special Message:**

Spring is here and development of the Annual Statement of Assurance report is in full swing. Assessable Unit (AU) Managers should take special note of the AU Managers' Corner on page 3 identifying responsibilities associated with this report.



*“Internal controls are an integral part of an organization, not a separate set of requirements.”*

## Self Assessment Reviews - Even Toyota Could Benefit From Them

*“It is always more rewarding to find and correct your own weaknesses than have them pointed out by someone else.”*

Successful organizations employ means of internal evaluation to improve their operations. Assessing internal controls is an important part of that evaluation. Even world renowned businesses are susceptible to poorly functioning internal controls.

Evaluation of controls should be a “Best Practice” for all businesses. Self assessment leads to enhanced controls over processes, programs, and activities; increases effectiveness and efficiency of operations; and facilitates effective decision making by management. Scheduled Self Assessment Reviews (SARs) provide an opportunity to take a close look at internal controls on a regular basis, focusing directly on the controls’ effectiveness. Strengths as well as weaknesses can be identified through SARs.

During a SAR, functions/ activities are examined to verify that inputs, actions, and outputs are in accor-

dance with established procedures, plans, or methods. Related internal controls are tested to determine their effectiveness and efficiency.

Steps to follow for testing internal controls:

- Step 1. Select Function(s) for Testing.** Determine which components of the function will be tested.
- Step 2. Establish Testing Objectives.** Decide which controls you are going to test.
- Step 3. Determine Expected Results.** Establish the criteria which determine whether the controls are successful.
- Step 4. Select Participants.** Eliciting input from others involved in the function provides a more accurate picture.
- Step 5. Select Method of Testing.** Determine the testing technique(s) to use.
- Step 6. Prepare for Test.** Gather and/or create the input needed for the test.
- Step 7. Conduct the Test.** Set aside sufficient time for performing the test.
- Step 8. Evaluate the Test Results.** Compare the results to the criteria established in Step 3. Note any differences, determine the causes of the

differences, and decide if actions are required.

**Step 9. Report the Test Results.** Inform management of test results and any required action.

### **Follow-up:**

**Step 10. Develop Corrective Actions.** If weaknesses are identified, develop/implement corrective actions and monitor them until the desired results are achieved.

**The ultimate purpose of performing a SAR is to ensure that implemented internal controls are achieving their intended results.**

In addition, SARs contribute information and supporting documentation for the Annual Statement of Assurance. Data from SARs provide an easily accessible audit trail.



# Frequently Asked Questions

## Q. Why are internal controls so important?

- A. First and foremost, they are the first line of defense against fraud, waste, and mismanagement.** As such, they are of interest to Congress, Office of Management and Budget, Government Accountability Office, Offices of Inspectors General, U.S. Treasury, Agency Management, Media, and Taxpayers. **Internal controls are of interest to everyone.**



## Q. Are there different types of controls?

- A. There are five broad categories of control: Managerial, Program/Operational, Accounting, Administrative, and Financial.**

1. **Managerial controls** include overall policy, planning, organization, and internal review functions.
2. **Program/Operational controls** involve activities related to the mission of the program or organization. They focus on performance and efficiency of operations.
3. **Accounting controls** relate to safeguarding assets and reliability of data. These controls focus on accountability and performance measures. This includes managing physical and intellectual assets.
4. **Administrative controls** comprise methods and procedures that address operational efficiency and adherence to management policies. They are intended to ensure compliance.
5. **Financial controls** apply to activities and processes involving money, typically the authorization for payment or collection of money. These controls focus on accountability for funds, authorizations, and safeguards.

## Q. How extensively should internal controls be tested?

- A. This is a management decision, usually based on the level of risk while taking into account other factors.** As a general rule, plan to test controls related to significant functions and high risk activities. Take into consideration factors such as: how routine or complex are the controls; the history of their functioning; whether or not there is any margin of acceptability for error; and/or the value or sensitivity of the control objective.

## Q. Exactly *what is a material weakness*?

- A. It is a weakness judged serious enough by management to be reported to higher authority.** Weaknesses that jeopardize agency mission, violations of statutory/regulatory requirements, and control failures that significantly weaken safeguards against fraud, waste, and mismanagement may be judged to be material weaknesses.

## Q. What are the differences between *inherent, internal, and external risks*?

- A. Inherent risks are due to the nature of an activity.** Performing dangerous activities has inherent risk of injury or other adverse occurrence.

**Internal risk is an adverse action that comes from within an agency/organization.** Employee theft is an example of internal risk.

**External risk is any adverse action that comes from outside the agency/organization.** Natural disasters, terrorist activities, or legislative actions that affect an agency's/organization's mission are forms of external risk.



## Q. In the Annual Statement of Assurance report, why reasonable assurance? Why not absolute assurance?

- A. Reasonable assurance is a judgment by management that controls are operating as intended, based upon available information.** This judgment is dependent on the quality of the available information. Absolute assurance can not be guaranteed because unexpected, undetected errors or irregularities may occur due to inherent limitations in any administrative or accounting system.

## TRICARE - Seriously Defrauded

On January 15, 2010, Sandra Elliott of Linden, NC, pled guilty to defrauding TRICARE and Medicaid through fraudulent billing practices, along with aiding and abetting.

In 2006, Elliott began establishing a small chain of educational centers purporting to provide tutoring, physician ordered mental health services, and early intervention services. By routinely billing TRICARE and Medicaid for services which were not provided or were unwarranted, she expanded the

chain to four center locations by 2009, with more planned. In addition, federal and state investigators determined that licensed practitioners no longer associated with the centers were being listed in billing submissions. Unlicensed employees were used to provide language and speech therapy, and psychological services. The loss to the government is expected to exceed \$1 million.



According to the stipulations of her

Plea Agreement, Elliott has agreed to forfeit two automobiles, a recreational vehicle, and \$201,791.00, all of which have been seized.

The maximum penalty for these charges is up to ten years imprisonment, followed by up to three years of supervised release, and a fine of up to \$250,000.

For more information, please see: [http://www.justice.gov/usao/nce/press/2010-jan-15\\_02.html](http://www.justice.gov/usao/nce/press/2010-jan-15_02.html)

## Assessable Unit Managers' Corner

Each year the MHS CIO submits an Annual Statement of Assurance (ASA) report, as required by Congress, documenting whether there is reasonable assurance that the organization's internal controls are achieving their intended objectives. This ASA report addresses the evaluation of the CIO Managers' Internal Con-

trol Program and represents the CIO's informed judgment as to the overall adequacy and effectiveness of internal control within the organization.

The CIO's judgment is based solely on the ASA input received from the



OCIO Divisions/Program Offices. Therefore, the Assessable Unit Manager for each Division/Program Office must ensure that all ASA (TAB A) questions are appropriately addressed and that the input is comprehensive, timely, and accurate.

## Audit Reviews Highlight Internal Control

In January 2010, GAO released a report on the results of a Veterans Affairs (VA) investigatory report which cited deficiencies in the Marion, Illinois, VA Medical Center's (VAMC) credentialing and privileging processes and oversight of its surgical program. Internal control standards state that agencies should clearly define key areas of authority and responsibility, establish appropriate lines of reporting, assess the quality of performance over time, and include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. VA's 2008 oversight policies assign responsibility. However, they do not specify how to assess compliance with credentialing and privileging policies, nor do they specify how to follow up and ensure that identified weaknesses have been promptly resolved. New guidance, provided in August 2009, addresses compliance; however, it does not describe a process to ensure resolution of findings. GAO recommends that VA develop a formal mechanism to systematically review VAMC credentialing and privileging files and performance monitoring for compliance with VA policies. To read more about this report (GAO-10-26), please visit <http://www.gao.gov/new.items/d1026.pdf>.

According to a DoDIG report, released in January 2010, United States Marine Corps (USMC) internal controls over payments processed through the Deployable Disbursing System (DDS) were not adequate to ensure the reliability of the data processed. Among the internal control problems identified were inadequacies in payment authorizations, lack of separation of authorization and payment duties, inadequate access controls, and the lack of a centralized database of transactions processed through DDS. Access controls were considered inadequate because USMC used 14 multiple user accounts and 14 generic user accounts to process a combined total of \$52.7 million in payments. In addition, USMC made 32 duplicate payments totaling \$2.5 million, funds that could be put to better use if collected. To read more about this report (DoDIG No. D-2010-037), please visit <http://www.dodig.mil/Audit/reports/FY10/10-037.pdf>.



*“Wasted effort equals wasted time and wasted money.”*