



# Chief Information Officer Managers' Internal Control Program



## INFORMATION BULLETIN

Volume 7, Issue 1

December 17, 2009

### Special Note:

*One of the real joys of the Holiday Season is the opportunity to say Thank You. We agree and would like to say a special thanks to everyone for all their hard work and dedication.*

*We would also like to extend our warmest thoughts and best wishes for a wonderful holiday and a very Happy New Year*



*“Nothing is perfect — Everything can be improved.”*

## Improving Performance Beyond Internal Controls

**You have just completed your annual Assessable Unit Review, your Risk Assessments, and your Self Assessment Review. You have identified weaknesses in your processes, and you want to improve your performance. Where do you go now?**

Two methods for process improvement are Value Stream Mapping and Lean Six Sigma.

**Value Stream Mapping (VSM)** is a visual method of depicting the entire flow of a process, and at the same time depicting the details of a process. It is a lean planning tool which can help simplify information flow, identify and eliminate waste, and streamline process flow. With VSM, cross-functional teams walk and map the current process and information flow, showing not only the process, but the information systems that support the process. It is normally used for evaluating an established process in order to identify opportunities for improvement.



**Lean Six Sigma (LSS)** is a methodology that an organization can use to improve its key processes.

LSS analyzes data, produced over a period of time, in order to identify bottlenecks or other obstacles. It can be applied to any business or operational practice which produces data that can be analyzed. In addition, LSS provides a framework for performance improvement through the DMAIC project method. DMAIC stands for Define, Measure, Analyze, Improve, and Control; five interconnected phases of the improvement process. LSS can be very effective for improving performance in complex situations. It can be applied to processes that involve the efforts of multiple offices or groups, or processes that involve multiple procedures, provided data is available for analysis.

\*\*\*

data, which may not be readily available.

- It shows how process flow and information flow are interconnected.
- It addresses the entire process rather than discrete parts of the process.
- It may identify processes which can benefit from an LSS approach to performance improvement.

### What are the benefits of Lean Six Sigma?

- It focuses attention on process management at all organizational levels.
- It improves customer relationship by addressing quality.
- It improves the efficiency and effectiveness of processes by aligning them with the organization's needs.
- It is a measureable way to track performance improvement.

### What are the benefits of Value Stream Mapping?

- It relies on the experience and first hand knowledge of individuals and groups involved in the process, rather than statistical

**Both methodologies are adaptable to a variety of situations and can help achieve success in performance improvement.**

# MICP Knowledge Challenge

## ACROSS

2. DODI 5010.40 is the Department of Defense \_\_\_\_\_ that requires the establishment of the Managers' Internal Control Program (MICP).

5. \_\_\_\_\_ are what make internal control work. Everyone must do their part.

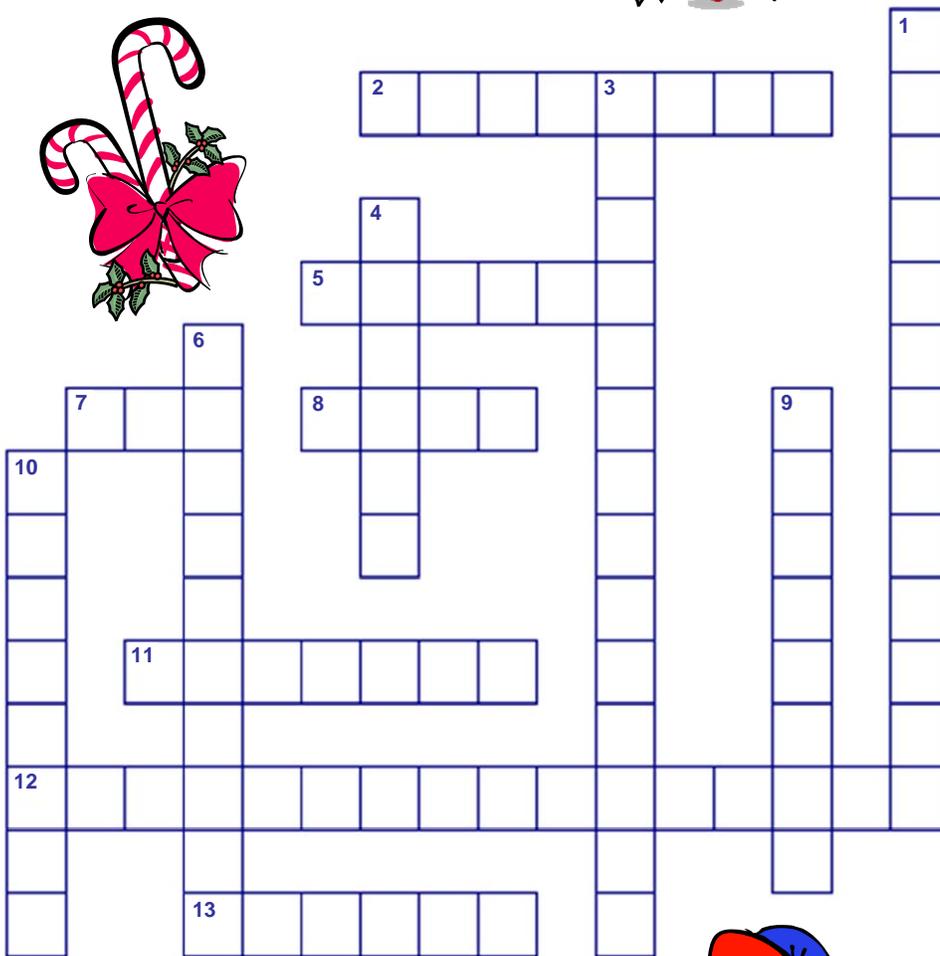
7. \_\_\_\_\_ is the acronym for Annual Statement of Assurance.

8. \_\_\_\_\_ is the possibility an event will occur and adversely effect the achievement of internal control objectives possibly resulting in the loss of Government resources due to fraud, waste, or mismanagement.

11. Internal Controls are all the control \_\_\_\_\_ used to accomplish a defined purpose or objective.

12. The CIO MICP is designed to implement effective and efficient \_\_\_\_\_ on a day-to-day basis.

13. Internal controls should be \_\_\_\_\_ to determine if they are functioning as intended.



## DOWN

1. Reasonable assurance is a management judgment of the \_\_\_\_\_ of the internal controls in place and is reported through the Annual Statement of Assurance.

3. An \_\_\_\_\_ is any organizational, functional, or other applicable subdivision of an organization that allows for adequate internal control analysis.

4. An internal control \_\_\_\_\_ is the evaluation and testing of internal controls to determine whether necessary controls are in place and producing the intended results.

6. Evaluation of cost and benefits of internal controls requires estimates and judgment by \_\_\_\_\_.

9. A \_\_\_\_\_ is a subdivision of an Assessable Unit.

10. An \_\_\_\_\_ is the lowest level where the internal controls can be identified and assessed.

### Word Bank

Activity, ASA, Assessable Unit, Effectiveness, Function, Guidance, Internal Controls, Management, Methods, People, Review, Risk, Tested



## Crime Costs More Than It Pays

On October 19, 2009, Wilfred J. Bouton pleaded guilty to one count of conspiracy to traffic in stolen Government property. Until July of this year, Bouton was a Gunner's Mate First Class in the United States Navy.

From 2007 - 2009, while assigned to an explosive ordinance disposal unit at

Whidbey Island Naval Air Station, Bouton stole gun sights and other gun-related accessories from his unit's armory. He sold the stolen equipment to an individual for approximately \$90,000.

Bouton was arrested on July 22, 2009; discharged from the Navy on

August 11; and indicted, along with two other individuals, in September. He is scheduled for sentencing on January 8, 2010, and faces a possible sentence of 5 years in prison and a fine of up to \$250,000.



Could better inventory controls have prevented this?

## Assessable Unit Managers' Corner

One of the many responsibilities of the Assessable Unit (AU) Manager is to ensure that internal control reviews (ICRs) and testing are conducted properly and in a timely manner. The ICR type utilized by the MIC Program Office is the Self Assessment Review (SAR). The SAR is designed to assess the organization's internal controls and determine if they are effective, efficient, and operating as intended.

Testing of the primary internal controls is an important and **required part of the SAR**. It involves ensuring that controls are: (1) actually being used as designed; and (2) accomplishing the desired objectives. Testing will also help to identify internal control weaknesses requiring corrective action and/or provide each manager with the

opportunity for implementing new internal controls or initiating improvements to existing controls.

Offices with AUs scheduled for review this fiscal year must complete a SAR by February 26, 2010.



## Audit Reviews Highlight Internal Control

During a performance audit that took place throughout FY09, GAO reviewed the cyber critical infrastructure plans and related documentation of 24 major executive branch agencies in the Washington, D.C. area. GAO determined that the majority had not fully addressed the criteria specified in Homeland Security Presidential Directive 7 and associated OMB instructions. It also determined that existing plans have not been updated, at least partially because OMB did not direct agencies to do so periodically. GAO considers some of the unaddressed criteria to be essential to effective planning for the protection of cyber assets. GAO recommended that federal agencies be directed to expeditiously update their plans to fully address OMB's cyber critical infrastructure planning requirements. They also recommended that follow-up be performed to ensure that updated plans fully meet OMB requirements and are being effectively implemented. To read more about this report (GAO 10-148), please visit <http://www.gao.gov/new.items/d10148.pdf>.

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can be unintentional or intentional, targeted or non-targeted, and can come from a variety of sources, including criminals, terrorists, and adversarial foreign nations, as well as hackers and disgruntled employees. Compounding the growing number and kinds of threats, GAO, along with agencies and their inspectors general, has identified significant weaknesses in the security controls in federal information systems, resulting in pervasive vulnerabilities. These include deficiencies in the security of financial systems and information, and vulnerabilities in other critical federal information systems. GAO has identified weaknesses in all major categories of information security controls at federal agencies. Multiple opportunities exist to enhance cyber-security. In light of weaknesses in agencies' information security controls, GAO and inspectors general have made hundreds of recommendations to improve security, many of which agencies are implementing. To read more from this Statement for the Record (GAO-10-230T), please visit <http://www.gao.gov/new.items/d10230t.pdf>.



*"Quality is not an act, it is a habit"*

*~ Aristotle*