



# Chief Information Officer Managers' Internal Control Program INFORMATION BULLETIN



Volume 9, Issue 1

December 30, 2011

## Special Message

Special thanks to all who have worked so diligently in promoting and instituting effective internal controls. We in the Manager's Internal Control Program look forward to working with all of you in the upcoming year. May the New Year bring you all prosperity!

**Happy New Year!**



**Quality is far more important than quantity when developing internal controls.**

## Communities of Practice: Facilitating Communication and Solutions

Whether informing stakeholders or circulating important information to all levels of an organization, effective communication is important to the organization's success. However, clear and effective communication across internal and external organizational boundaries can be difficult to achieve. One solution is establishment of Communities of Practice (CoPs).

In our organization "The Communities of Practice, which are sponsored by Ms. Mary Ann Rockey, provide a setting for practitioners of various disciplines to share best practices, expertise, and pertinent knowledge with one another, as well as problem-solve and provide support for fellow colleagues. CoPs serve as a forum for defining, testing, and certifying the processes and best practices for standardized efforts. Further, CoPs allow individuals to interact *across* organizational boundaries which contributes to the discovery of solutions.

In the past 18 months, five

CoPs have been successfully implemented. This endeavor has been a success in part because of the collaborative contributions of each CoP community member which have yielded a number of accomplishments." - LCDR Monique Davis.

Among the most successful is the Risk Management Community of Practice (RSKM CoP), established in June 2010. In addition to promoting dialog among risk management practitioners from multiple disciplines, the RSKM CoP provides a platform for investigating a variety of risk methodologies and best practices, including Enterprise Risk Assessment Methodology (ERAM) and Software Engineering Institute (SEI) Taxonomy Based Risk Management applications as well as locally developed risk mitigation and tracking systems and practices aimed at the project level. Examination of other methodologies and tools currently in use across the Military Health System and Veterans Affairs is anticipated in the coming year. Although there are not

many, some important differences have been noted in the terms utilized in some of the methodologies currently being practiced. These differences are significant enough to lead potentially to miscommunication and misunderstanding between local risk managers and leadership or auditors. As a result, the Community began developing a uniform taxonomy (terminology) with mapping of terms to known methodologies to reduce the potential for miscommunication and misunderstanding. This work, while still in progress, is nearly ready for presentation to leadership for consideration. Recognizing that there is no single methodology applicable to all situations, the intent is to provide a taxonomy which can be applied regardless of the process area or the risk management methodology being used.

If you are interested in participating in the RSKM CoP or one of the other Communities of Practice, please contact LCDR Monique Davis for more information. (Monique.Davis@tma.osd.mil)

# A Few Words from the Department of Defense Managers Internal Control Program

The Department of Defense (DoD) is committed to having fully auditable financial statements by 2017, the deadline established by Congress in the National Defense Authorization Act of 2010. The Department is:

- Using a streamlined approach that focuses on improving and auditing the information most often used to manage,
- Holding leaders accountable to achieve long and short-term Financial Improvement and Audit Readiness (FIAR) goals through a governance process, and
- Providing funding to DoD Components to improve systems, processes, and controls.

The Department manages financial improvement activities through the FIAR Plan, which provides the strat-

egy, methodology and means for monitoring progress to achieve Congress' audit readiness requirement. The FIAR Plan also serves to advance the Department's fiscal stewardship and improve the financial information needed to manage the Department.

The FIAR Plan organizes and prioritizes the financial improvement efforts of the Military Departments and Defense Agencies (the Components). It ensures that the Components' financial improvement plans are aligned with the business transformation initiatives and systems modernization efforts identified in the Enterprise Transition Plan (ETP). Integration with the ETP is essential because audit readiness cannot be achieved by most of the Components until system improvements identified in the ETP are successfully completed.

Since 2005, when the FIAR Plan was

first issued, much has been accomplished to improve financial management across the Department; however, much remains to be done. Although DoD cannot produce auditable financial statements today, the Department effectively manages its budgets, appropriations and expenditures, as verified by its ability to effectively support the nation's warfighters, two wars and other worldwide operations. To find information on DoD's accomplishments and to read about DoD's FIAR goals and priorities please visit the following website at <http://comptroller.defense.gov/improving.html>

OFFICE OF THE UNDER SECRETARY OF DEFENSE  
(COMPTROLLER)



## 5 Tips for Managing Risk at Any Level in Any Process Area

1. **Anticipate and understand your risks, both external and internal. Ask every "What if..." question you can think of.**
2. **Use appropriate controls and try to make sure they are not easily circumvented or compromised. They are no good if they don't work or are not relevant.**
3. **Don't confuse compliance with safety and security. Creating a control may satisfy regulatory requirements, but the control needs to work or you might as well not have it.**
4. **Re-assess risks and their controls regularly and often enough to accommodate evolving conditions. Don't wait for a control failure to trigger re-evaluation of controls and/or re-assessment of risks.**
5. **Always consider your cost/benefit ratio. Return on investment is important and should be measurable or demonstrable.**

## Don't Try to Cheat on Travel

John R. Brock, 52, of Crofton, Md., a former civilian employee of the Armed Forces Institute of Pathology (AFIP) pleaded guilty on October 13, 2011, to making more than \$485,000 in false travel claims using the Defense Travel System. AFIP is a component of the Department of Defense.

As part of his guilty plea Brock admitted that, from September 2008 through

April 2011, he submitted 99 false travel vouchers totaling \$485,535 for expenses that were never incurred. He admitted that he submitted the claims through the Defense Travel System using the profile of a former AFIP employee.

At sentencing, scheduled for Jan. 3, 2012, Brock faces up to five years in prison and a \$250,000 fine, as well as

supervised release following any prison term. Brock may also have to repay or forfeit property totaling \$485,535.



Source: <http://www.dodig.mil/IGInformation/IGInformationReleases/1358CRM.pdf>

## Assessable Unit Managers' Corner

Risk Management is no longer confined to risk management specialists only. It has become an integral part of several key process areas. Therefore, all managers, whatever their functional areas, should be aware and take a proactive stance in the risk arena. It is important to understand how to quantify the tradeoffs of risk against the potential return. Failure to understand risk can have an adverse action on



the programs and the projects we deploy. Consequently, we should keep the following in mind as we address risk management issues.

the programs and the projects we deploy. Consequently, we should keep the following in mind as we address risk management issues.

- Increase the transparency of your risk management program to satisfy staff and stakeholders
- Keep on top of the continuing evolution of best practices, risk policies, and methodologies and associated risk infrastructures

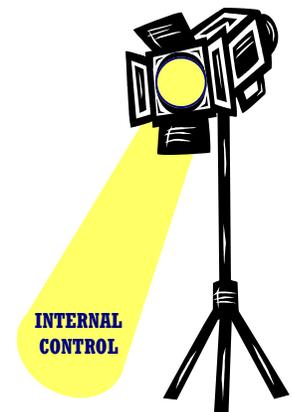
- Implement and efficiently communicate an organization-wide Enterprise Risk Management (ERM) approach that encompasses business strategic, tactical and operational views and legal and regulatory compliance
- Utilize risk performance measurements, risk methodologies, and risk taxonomy as you navigate complex risk areas

## Audit Review Highlights Internal Controls

September 23, 2011 - In a testimony before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, U.S. House of Representatives the Government Accountability Office (GAO) indicated that Department of Defense (DoD) financial management has been on GAO's high-risk list since 1995 and, despite several reform initiatives, remains on the list today. Pervasive deficiencies in financial management processes, systems, and controls, and the resulting lack of data reliability, continue to impair management's ability to assess the resources needed for DoD operations. DoD spends billions of dollars each year to maintain key business operations intended to support the warfighter, including systems and processes related to the management of contracts, finances, the supply chain, support infrastructure, and weapon systems acquisition. These operations are directly impacted by the problems in financial management. In addition, long-standing financial management weaknesses have precluded DoD from being able to undergo the scrutiny of a financial statement audit. Some of the key challenges that DoD must address for its financial management to improve to the point where DoD is able to produce auditable financial statements include:

- committed and sustained leadership,
- effective plan to correct internal control weaknesses,
- competent financial management workforce,
- accountability and effective oversight,
- well-defined enterprise architecture, and
- successful implementation of the enterprise resource planning systems.

For more from this testimony, please visit: <http://www.gao.gov/new.items/d11933t.pdf>



*Acknowledging the reality of risk is the first step in managing it.*

# MICP Resolutions for a **Happy New Year!**



**R**

Take personal **responsibility** for following internal controls governing mission activities.



**E**

**Educate** new employees and coworkers about the value of internal controls.



**S**

Meet the **standards** established by the Government Accountability Office Standards for Internal Controls for Federal Government.



**O**

Make it a habit to **observe** internal controls in action, and take advantage of **opportunities** to improve them when appropriate.



**L**

Adhere to Federal **law** (FMFIA of 1982) requiring institutionalization of internal controls throughout the federal government.



**V**

Recognize that well designed, effective internal controls are **vital** to achieving mission.



**E**

**Execute** internal controls as integral parts of every-day business activities.



**D**

**Deliver** good products with the help of good controls.

