



Chief Information Officer Managers' Internal Control Program INFORMATION BULLETIN



Volume 8, Issue 3

September 30, 2011

Special Message:

With the end of one fiscal year and the beginning of a new one, the MICP Office would like to take this opportunity to say "Thank you!" for all your hard work and continuous efforts to maintain an effective control environment.



"Making good decisions is a crucial skill at every level."

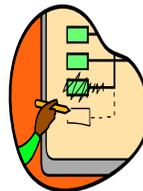
~ P. Drucker

Maintaining Stability in the Face of Uncertainty

At a time when a variety of events such as enterprise wide reorganization and BRAC produce uncertainty and stress, well designed, institutionalized internal controls provide stability and continuity. They enable operations to continue with a reasonable degree of certainty and predictability.

Fluid organizational changes involving realignment of management responsibilities and/or personnel can cause confusion regarding levels/lines of authority and communication. In such an environment, up-to-date Organization and Flow Charts delineating responsibilities and lines of communication for both the larger organization and within individual offices help ensure that management and staff stay adequately informed. They

facilitate communication across organizational and intra-organizational boundaries. This is especially important when enterprise mission objectives are realigned among lower level organizations. Maintaining basic activity level controls help ensure important activities continue to function properly to accomplish mission objectives. Well designed, executable controls such Standard Operating Procedures, Handbooks, and other definitive



guidance facilitate redistribution of responsibilities and duties at the activities level.

Within our organizational segment, BRAC could be an internal controls success story. Logistics planning and preparation for the physical move began early on. Facilities management

stay actively engaged in planning and assigning office/cubicle space. Records Management began encouraging review and appropriate long term storage activities or file disposal almost from the moment the move was announced, arranging regular meetings to address the process and provide guidance. These efforts should minimize the amount of hardcopy files transported and stored in the new facility and reduce the possibility of lost or misplaced documents as we settle in.

When all personnel do their part, there should be little or no interruption to operations.



Everyday Internal Controls

Internal controls are a daily part of our experience both at work and in our personal lives, even when we don't recognize them. Their importance is often misunderstood, ignored, or undervalued. Internal controls help ensure programs and re-

sources are protected from fraud, waste, mismanagement, and misappropriation of funds. They help ensure mission and program objectives are efficiently and effectively accomplished. ***Internal controls are the policies, procedures, guid-***

ance, and instructions that help us perform our tasks. They prevent risks from becoming reality or mitigate the consequences if they do. How can something so important be so often undervalued?

(Continued on page 2)

Everyday Internal Controls cont.

If we identify how internal controls are associated with work tasks that all of us either perform or are affected by regularly, we can better understand how internal controls help us prevent or mitigate the risks associated with achieving our organizational goals. The following table provides examples of common risks associated with everyday tasks. Take a moment to consider how these risks are prevented or mitigated both in your work environment and beyond. What safeguards (internal controls) are in place and practiced by you and/or your organization?

Activity Area	Associated Risks
Office Security	Theft or misuse of office equip and/or sensitive data; theft of files or other written resources
CAC or PIV Cards	Loss or theft
Computer Usage	Theft, loss, or damage of computer equipment, especially laptops used away from the office; misuse or loss of data; viruses
File/Data Maintenance	Files/Data unavailable to decision makers because lost, misplaced, damaged, or poorly organized

Recognizing the value of daily or routine internal controls is vital to the mission. Putting those controls into practice is even more vital.

A Little Follow-Up for the Curious

Over several years we have shared reports on various crimes where internal controls were circumvented or otherwise failed. Sentences for these crimes are often handed down many months later. The table below contains follow-up information on some of these reports. Internal controls provide important safeguards but they are not a guarantee against mismanagement, fraud, or corruption. In some cases individuals simply ignored controls. Maybe they didn't see any harm in what they were doing. In other cases, determined individuals found a way to circumvent controls, at least temporarily. In the end, however, they were caught and punished. ***Internal controls are serious business.***

CIO MICP Information Bulletin Article Title	Volume, Issue	Crime	Sentence	Information Source
When Retirement Plans Go Bad	V 6, Is 1	Felony Violation of Post Government Employment Restriction	2 years' probation and \$2,000 fine	http://www.justice.gov/criminal/pin/docs/arpt-2009.pdf
Idle Curiosity Leads to Guilty Plea	V 6, Is 2	Illegally Accessing Confidential Passport Applications	12 months' probation and 100 hours of community service	http://www.justice.gov/opa/pr/2009/March/09-crm-259.html
Distance Doesn't Prevent Detection	V 6, Is 3	Multiple Charges including Bribery, Honest Services Fraud, Money Laundering, and transactions with criminal proceeds	Sentence information not yet available (As of March 2, 2011, 16 individuals have been convicted or pled guilty in this ongoing investigation)	http://www.justice.gov/opa/pr/2011/March/11-crm-263.html
Crime Costs More Than It Pays	V 7, Is 1	Theft and Sale of Sensitive Military Equipment	2 years in prison followed by 3 years supervised release and \$62,311.42 restitution	http://www.justice.gov/usao/ct/Press2010/20101007-2.html
TRICARE – Seriously Defrauded	V 7, Is 2	Aiding and Abetting Healthcare Fraud	10 years in prison and \$1.885 million restitution	http://www.dodig.mil/iginformation/IGInformationReleases/LindenSentencing.pdf
Marine Captain Charged with Contract Skimming	V 7, Is 3	Conspiracy to Commit Wire Fraud & filing and False Tax Return	6 years in prison	http://www.justice.gov/usao/cac/pressroom/pr2011/016.html
Maryland Man "Recycles" Stolen Government Property	V 8, Is 1	Theft and Sale of \$340K worth of Copper Cables and other Government Property	1.5 years in prison followed by 3 years supervised release	February 11, 2011 press release http://www.justice.gov/usao/md

Rank Doesn't Protect a Fraudster

A retired colonel in the U.S. Army was sentenced August 16, 2011 to 12 months in prison for her role in a scheme to pay bribes for contracts awarded in support of the Iraq war.

Levonda J. Selph, 57, pleaded guilty in June 2008 to one count of bribery and one count of conspiracy. According to the charges, then-Lt. Colonel Selph

served as chair of a selection board for a \$12 million contract to build and operate several Department of Defense warehouses in Iraq. In return for a vacation to Thailand and other things of value totaling approximately \$9,000, Selph accepted fraudulent bids from a co-conspirator contracting firm and helped that firm win the contract award.



In addition to her prison term, Selph was sentenced to three years of supervised release and was ordered to pay a \$5,000 fine and \$9,000 in restitution.

Source: <http://www.justice.gov/opa/pr/2011/August/11-crm-1053.html>

Assessable Unit Managers' Corner

The start of a new fiscal year is a good time for Assessable Unit (AU) Managers to review their internal control roles and responsibilities. AU Managers bear final responsibility/accountability for:

1. Ensuring all mission areas are covered by an AU
2. Ensuring risk assessments are conducted/reviewed annually
3. Ensuring internal controls are in place to mitigate risks and provide

reasonable assurance that government assets are protected from fraud, waste, and mismanagement

4. Ensuring internal controls are documented and communicated to appropriate personnel
5. Ensuring internal control reviews and testing are conducted properly and in a timely manner
6. Overseeing and monitoring corrective action plans for all weaknesses

7. Ensuring input for the Annual Statement of Assurance is comprehensive, timely, and accurate for their mission area

Well developed, institutionalized controls provide stability and continuity of operations, helping prevent wasted time and effort and ensuring a desirable level of accountability for government assets and resources, especially during times of change.

Audit Reviews Highlight Internal Control

In a report on Department of Defense (DoD) Cyber Efforts, released in July 2011, the Government Accountability Office (GAO) focused on DoD's efforts to better address cybersecurity threats, citing among other things, a lack of clarity in guidance regarding command and control authorities and chains of command. GAO recommends that DOD (1) establish a timeframe for deciding on whether to complete a separate joint cyberspace publication and for updating the existing body of joint publications, (2) clarify command and control relationships regarding cyberspace operations and establish a timeframe for issuing the clarified guidance, and (3) more fully assess cyber-specific capability gaps, and (4) develop a plan and funding strategy to address them. DOD agreed with the recommendations. To read more about this report (GAO-11-75), please visit <http://www.gao.gov/new.items/d1175.pdf>.

In a report released June 21, 2011, GAO cited internal control issues at the Internal Revenue Service (IRS). Among these were ineffective internal controls for identifying duplicate instances of First-Time Homebuyer Tax Credit claims during FY 2010, out-of-date lists of officials authorized to approve manual refunds at two IRS service center campus' (SCCs), and inconsistent application of approval requirements for requesting and receiving services from vendors, to name a few. The issues reported increase the risk that IRS may not prevent or promptly detect and correct (1) unauthorized or improper refunds, purchases, or promotions; (2) errors in the hours credited or amounts paid to staff; (3) loss or theft of cash receipts or taxpayer information; (4) security and control deficiencies at its SCCs and processing facilities; (5) data errors in its property records; and (6) improper disclosure of taxpayer and other sensitive data. To read more about this report (GAO-11-494r), please visit <http://www.gao.gov/new.items/d11494r.pdf>.



“Efficiency is doing things right; effectiveness is doing the right things.”

~ P. Drucker