



Information Management, Technology & Reengineering
and Joint Medical Information Systems
Managers' Internal Control Program



INFORMATION BULLETIN

Volume 4, Issue 4

September 30, 2007

Special Message:

Fall is here and it's time to **KICK-OFF** the FY 2008 annual internal control management cycle. AU Managers and Representatives should take special note of the AU Managers' Corner on page 3 listing the upcoming internal control activities.



FY08 Kick-Off

"The fundamental principles of internal control are rooted in well established organizational techniques and practices."

\$ BILLIONS Lost Each Year to Fraud \$

According to the Association of Certified Fraud Examiners (ACFE) Report to the Nation on Occupational Fraud & Abuse, US companies lose 5% of their annual revenue to fraud. That translates to over \$650 billion in losses annually.

Occupational fraud is defined by the ACFE as "the use of one's occupation for personal enrichment through deliberate misuse or misapplication of the employing organization's resources or assets."

The ACFE's report is based on a study of 1,134 fraud cases investigated by Certified Fraud Examiners. The top four industries most affected by fraud were banking/financial services

(148 cases); **government/public administration (119 cases)**; manufacturing (101 cases); and **health care (89 cases)**.

According to the report, the most common means for identifying fraud among all industry types was hotline tips, which accounted for 34% of all cases. Other means included accidental discovery (25%), internal audits (20%), **internal controls (19%)**, external audits (12%), and notification by law enforcement (3.8%). The high percentage rate of accidental discovery demonstrates that **organizations need to focus more on improving their internal controls and internal audits.**



As part of their study on the effectiveness of measures used to prevent/limit fraud, the ACFE found that although external audits were the most common type of anti-fraud control used, they were the least effective. Companies that used external audits actually suffered greater loss from fraud than those who did not. Other **more effective methods included internal audits, fraud awareness/ethics training**, fraud hotlines, and surprise audits.

To read more visit the ACFE website at <http://www.acfe.com/>.

Copyright 2006 by the Association of Certified Fraud Examiners, Inc.

Internal Control Myths & Facts

MYTHS

- Internal control starts with a strong set of policies and procedures.
- Internal control: That's why we have auditors!
- Internal control is a finance thing.
- Internal controls are essentially negative, like a list of "thou-shalt-nots."
- Internal controls take time away from accomplishing our core missions.**

FACTS

- Internal control starts with a strong control environment.
- While auditors play a key role in the system of control, management is the primary owner of internal control.
- Internal control is integral to every aspect of business.
- Internal control makes the right things happen the first time.
- Internal controls should be built "into" not "onto" business processes.**

GAO Standards - Internal Control Framework

The GAO Standards for Internal Control provide the overall framework for establishing and maintaining internal control to prevent fraud, waste, and mismanagement. The standards define the minimum level of quality acceptable for internal control and provide the basis against which internal control is to be evaluated.

ALL INTERNAL CONTROLS FALL WITHIN ONE OF THESE FIVE STANDARDS.



1. Control Environment: Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management. **A positive control environment is the foundation for all other standards.**

Key Factors: 

- Integrity and Ethical Values - Management sets the organization's ethical tone and ensures it is clearly communicated to all personnel.
- Management's Commitment to Competence - All personnel need to maintain a level of competence that allows them to accomplish their assigned duties.
- Management's Philosophy and Operating Style - Management determines the degree of risk the organization is willing to take.
- Delegation of Authority - Delegation covers authority and responsibility for operating activities, reporting, relationships, and authorization protocols.
- Organizational Structure - The

organizational structure provides the framework for planning, directing, and controlling operations in order to achieve organizational objectives.

- Human Capital Policies and Practices - Policies and practices related to orienting, training, evaluating, and supervising personnel must be established.

2. Risk Assessment: Internal control should provide for an assessment of the risks the organization faces from both external and internal sources. Risk assessment is the identification and analysis of relevant risks associated with achieving agency objectives.

Key Factors: 

- Clear and consistent objectives must be established before risk can be properly assessed.
- Management needs to comprehensively identify risks.
- Once identified, risks should be analyzed for possible effects and internal controls (mitigation strategy) developed.
- Internal and external risks must be identified, documented, and assessed.

3. Control Activities: Control activities help ensure that management's directives are carried out and mission objectives are achieved. Control activities occur at all levels and functions of the organization. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and procedures and mechanisms associated with each of the organization's activities.

Key Factors: 

- Control activities are an integral part in planning, implementing, and reviewing.
- Control activities are essential to accountability for stewardship of

government resources and achieving effective results.

- Examples of control activities: reviews by management at the functional or activity level; management of human capital; segregation of duties; physical controls of vulnerable assets; and controls over information processing.



4. Information and Communications: Information should be recorded and communicated to management and others within the organization in a form and within a time frame that enables them to carry out their responsibilities.

Key Factors: 

- Information is needed throughout the organization to achieve all of its objectives.
- Organizations must have relevant, reliable, and timely communications.
- Effective communications should occur in a broad sense with information flowing down, across, and up the organization.

5. Monitoring: Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

Key Factors: 

- Internal controls should be designed to ensure that ongoing monitoring occurs in the course of normal operations.
- Separate internal control reviews should be conducted to determine the controls' effectiveness at a specific time.
- Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved.

STEALING DOESN'T PAY

Two former Office of Personnel Management (OPM) employees plead guilty last month to stealing over \$27,000 from the U.S. Treasury. Over a 7 month period, the two employees used their positions as accounting technicians to divert electronic payments into personal accounts.

After discovering the accounting irregularities, OPM's Inspector General was called in to conduct a full investigation. The two felons could spend up

to 10 years in prison, but under federal sentencing guidelines they may only face 6 months in jail, home confinement, and/or a period of probation.

OPM Director, Linda Springer said in a statement August 17, that "as stewards of the public trust, we have a responsibility to ensure against fraud, and we have checks and balances in place to uphold sound fiscal accountability."

This situation serves as a valuable

lesson not only for OPM, but for all agencies. **It demonstrates the need for and the importance of reviewing and monitoring internal controls to help prevent and detect fraud.**



Assessable Unit Managers' Corner

As the beginning of a new fiscal year approaches, the MIC Program Office would like to remind all **Assessable Unit (AU) Managers** of the upcoming internal control activities.



FY 2008 MIC Program Schedule

ACTIVITY		DATE	Responsibility
1.	Review/Update the MIC Program	Oct	All
2.	Review/Update Assessable Units	Oct - Nov	AU Managers/Reps
3.	Develop Annual Internal Control Plan	Oct	MIC Program Office
4.	Revalidate/Perform Risk Assessments	Oct - Dec	AU Managers/Reps
5.	Conduct Internal Control Reviews	Oct - Feb	AU Managers/Reps
6.	Annual MIC Program Training	Nov - Jan	AU Managers/Reps
7.	Prepare Annual Statement of Assurance	Feb - Jun	MIC Program Office/AU Managers/Reps

Audit Reviews Highlight Internal Control

In a recent review of four Veterans Affairs (VA) locations, the GAO determined that a **weak overall control environment** and persistent weaknesses in inventory control and accountability put VA IT equipment at risk of theft, loss, and misappropriation. This posed a continuing threat to the security of the sensitive information stored on the equipment. Results from tests performed by the GAO and physical inventories conducted by the four VA locations identified several thousand missing IT equipment items including 53 computers possibly containing sensitive information. The GAO also found that while the VA did have policies in place, **they lacked the proper guidance needed for them to be effective and they weren't being adequately enforced.** To read more about this report (GAO-07-505) please visit http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm.

In their report on the Identification and Reporting of Improper Payments through Recovery Auditing, the DoD IG stated that the Under Secretary of Defense (Comptroller) (USD (C))/Chief Financial Officer (CFO) **did not have adequate internal controls** to fully implement a recovery audit program. The IG also determined that DoD's program was less than effective in identifying and recovering overpayments to contractors and that DoD had not adequately reported on the amount recovered by its program. These results were based on the IG's findings that USD(C)/CFO personnel did not: effectively manage recovery audit contracts; develop a plan to correct obstacles encountered during past recovery audits such as denials to data access, poor data quality, and excessive oversight; comply with existing policies for reporting on recovery audits; and seek out best practices from other DoD entities' recovery audit efforts. To read more about this report (D-2007-110) please visit http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm.



"Management is responsible for establishing specific internal control policies and procedures and employees are responsible for ensuring that established internal controls are followed and applied."