



Information Management, Technology & Reengineering and Joint Medical Information Systems

Manager's Internal Control Program

INFORMATION BULLETIN



Volume 3, Issue 2

March 27, 2006

Special Note:

Beginning in April, the DoD IG will be conducting a compliance audit on the TMA Manager's Internal Control Program. All offices should ensure their internal control documentation and files are up-to-date.



"Management must instill a control environment that fosters integrity and ethical values, and a commitment to excellence. This requires clearly communicating expectations to staff, assigning responsibilities and authority to make decisions to the appropriate level, and routinely monitoring performance."

Independent Review of TMA's Internal Control Processes Highlight the Need for Change

In order to enhance the TRICARE Management Activity (TMA) Manager's Internal Control (MIC) Program, the TMA Management Control Office requested a contractor perform an independent review of the internal control processes.

Specifically the contractor was asked to: 1) review the "as is" internal control processes; 2) develop suggestions for process improvements; and 3) suggest ways to improve consistency across the TMA Directorates.

The contractor determined

that the TMA MIC Program was operating at a phase 2 level according to the "Internal Controls Maturity Framework." Phase 2, known as the informal state, implies that control activities are designed and in place, but they are not adequately documented or tested.

Other findings highlighted in the report include the absence of: documented controls, self assessment reviews, testing, and internal control training.

The final report included a list of 10 recommendations which were designed to

advance the TMA MIC Program to a phase 4 or monitored level. At this level the TMA MIC Program would have standardized controls with periodic testing for effective design and operation.

Special note regarding the Information Management, Technology & Reengineering (IMT&R)/Joint Medical Information Systems MIC Program—the report stated that the "IMT&R Directorate appears to have the most rigorous procedures for reviewing internal controls."

New Requirements in the DoDI 5010.40 "Managers' Internal Control (MIC) Program Procedures"

One of the new requirements in the recently revised Department of Defense Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006, is the establishment of Assessable Unit (AU) Managers. AU Managers must be the head of the assessable unit and are responsible for managing all internal control activities per-

taining to an AU.

AU Managers must also have a critical element in their performance appraisal addressing their MIC Program performance.

In addition to the Overall Annual Statement of Assurance (ASA), all entities who produce stand alone financial statements will now be required to submit a Financial Reporting

ASA. This report is based solely on the effectiveness of internal controls specific to financial reporting.

The new instruction also places stronger emphasis on the importance of internal control reviews and the need for prompt and effective action to correct weaknesses found during these reviews.

Leadership and Ethical Standards

In a recent review on management and oversight in acquisition organizations, the Defense Science Board (DSB) Task Force observed, during reviews with industry academics, that expectations for ethical behavior extends to everyone in the organization. However, the primary emphasis is on leadership. The commitment of leadership in “high integrity organizations,” or organizations where ethics has become a part of their culture is very apparent.

Leadership takes on the responsibility of maintaining ethical behavior throughout the organization. They ensure that standards and norms are enforced consistently and effectively and that they are communicated to all staff. Ethical behavior is often recognized and/or rewarded, and highlighted in organizational communications.

The Department of Defense (DoD) has some aspects of being an ethically grounded organization, but it “lags behind ... in creating a systematic, integrated approach and in demonstrating the kind of leadership necessary to drive ethics to the forefront of organizational behavior. Leadership in DoD should be more proactive to ensure that values and ethics are the foundation for all employees.”

In their final report, the Task Force recommended that the DoD “... explicitly articulate its vision and values as an ethically grounded organization, in much the same fashion that the Department expects of its contractors.” More specifically the Task Force recommended that



the Secretary of Defense put ethics at the forefront of DoD communications. To do so, they suggested that the Secretary of Defense institutionalize an orientation program for new leadership that emphasizes: the values and objectives of the DoD; the importance of leadership to sustain the ethical culture of the DoD; and the performance expectations for all individuals to support the achievement of these objectives and promote an ethical environment. It is then up to leadership to ensure that the vision and values of the DoD flow-down to all individuals.

Source – *Report of the DSB Task Force on “Management Oversight in Acquisition Organizations.”* To learn more about this review please visit http://www.acq.osd.mil/dsb/reports/2005-03-GAO_Report_Final.pdf

Why DOCUMENT Policies and Procedures?

Documenting policies and procedures is not only an important aspect of internal control, but it is also a good general business practice. **Documentation should cover all aspects of an organization’s operations.**

Here are the top 5 reasons for documenting policies and procedures.

1. Continuity – If an employee leaves the organization, the policy/procedure still exists in its entirety. Documented policies and procedures allow new staff to understand expectations quickly.



2. Communication – Oral communications are easy to forget, misunderstand, and misinterpret. Documented policies and procedures can provide a more clear and concise direction.

3. Benchmark – Documented policies and procedures can provide constant, reliable information which can be assessed in order to determine efficiency and effectiveness.

4. Reference – Referring to a document can be quicker, easier,

more consistent and more reliable than asking a co-worker.

5. Audit Trail – Documentation provides a history of decisions and their rationale. This is especially important if the process owner has left the organization and questions arise.

Documenting policies and procedures and making them accessible to employees helps provide day-to-day guidance to staff and is a major aspect of internal controls.

Source – *The Auditor’s Report Vol 3, Issue 1*

Contractors in the Government Workplace

Although contractors and government employees are working toward a common goal, there are some key distinctions that need to be made.

- Remember, contractor employees

are not federal employees.

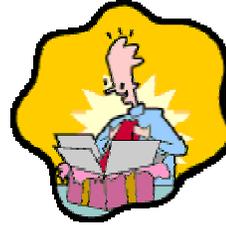
- Ensure contractor personnel wear distinctive badges and can be easily identified, including in E-mail correspondence.

- Watch what you discuss and where you discuss it. The hallways, bathrooms, and other common areas are not secure areas for discussing sensitive information.

Continued on next page

Contractors in the Government Workplace Cont'd

- When you attend a meeting in which sensitive information is about to be discussed, ensure that you know who is in the room and determine whether the information can be disseminated to them.
- Respect and adhere to established rules and guidelines that define the employer-employee relationship between contractors and their employees.
- Safeguard proprietary, privacy act, and other sensitive and nonpublic information. Release of certain types of information to contractor employees to analyze, create charts and graphs, enter into databases, etc., could violate the Procurement Integrity Law, the Trade Secrets Act, the Privacy Act, or other laws or regulations.
- Beware of gifts from contractors. Even if they work in government space they are still considered "outside sources" and the rules for gift giving are very different than the rules for gift giving between Federal employees.
- Resolve inappropriate appearances created by close relationships between government employees and contractors.
- Do not require contractors to perform "out of scope" work, personal services, or "inherently governmental functions." The services that the contractor is required to provide through its employees are set out in the contract. There are no "...and other duties as assigned."



How the Institute of Internal Auditor's Defines Internal Controls

- S** - Safeguarding of assets
- C** - Compliance with policies, laws, and procedures
- A** - Accomplishment of goals and objectives
- R** - Reliability of information in records
- E** - Efficient and economic operations



Audit Reviews Highlight Internal Control

During a recent review of the Security Status for Systems Reported in DoD Information Technology (IT) Databases, the DoD IG found that the information in the IT Registry and the Information Technology Management Application (ITMA) is unreliable because the DoD CIO and CFO communities did not **enact sufficient controls or conduct reviews** to ensure the accuracy, consistency, and synchronization of data between these databases. The information in the IT Registry and ITMA is used by DoD to report the security status of IT systems; in compiling the Federal Information Security Management Act and the Privacy Act reports; and in DoD IT budget requests and justifications. The DoD, OMB, and Congressional Committees will continue to make **management decisions based on erroneous data** unless the DoD develops and enforces effective internal quality assurance controls to ensure that the information contained in these databases is correct, accurate, and complete. To learn more about the IG's findings please visit <http://www.dodig.mil/audit/reports/FY06/06-042.pdf>.

In the December 7, 2005, audit report titled "Defense Finance and Accounting Service (DFAS) Corporate Database (DCD) User Access Controls," the DoD IG reported that DFAS did not have adequate internal controls over access to the DCD. The DCD contains "sensitive accounting data, and vendor and employee tax identification numbers, bank routing and account numbers, names, addresses and phone numbers," and if the proper access controls are not in place there is a greater risk that this information will be misused. Specific weaknesses identified in the report include: lack of controls ensuring inactive accounts are deactivated; non-compliance with the DoDI 8500.2; and **inadequate internal procedures**. To learn more about the IG's findings please visit <http://www.dodig.mil/audit/reports/FY06/06-033.pdf>.



"We cannot totally control all risks, but must balance the probability and impact against the cost of control."