

Army Regulation 11-2

Army Programs

Managers' Internal Control Program

**Headquarters
Department of the Army
Washington, DC
4 January 2010**

UNCLASSIFIED

SUMMARY of CHANGE

AR 11-2

Managers' Internal Control Program

This major revision, dated 4 January 2010--

- o Changes the title of the publication from Management Control to Managers' Internal Control Program (cover).
- o Adds policy on internal control over financial reporting (para 2-2).
- o Changes terminology from Management Control Evaluation Checklist to Internal Control Evaluation (para 2-5).
- o Realigns the standards for internal control (app B).
- o Adds Internal Control Reporting Categories for use in classifying and reporting material weaknesses (app C).
- o Changes performance agreement requirements to include internal control administrators at the assessable unit level (reporting organizations) and above (throughout).
- o Changes terminology from Management Control Plan to Internal Control Evaluation Plan (throughout).
- o Changes the terminology from management control administrator to internal control administrator (throughout).
- o Makes administrative changes (throughout).


Army Programs

Managers' Internal Control Program

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:


JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation implements Public Law 97-255; Title 31, United States Code, Section 3512; Office of Management and Budget Circular A-123, Management's Responsibility for Internal Controls; and DODI 5010.40. This regulation is revised to increase the involvement and accountability of commanders and managers. It does not contain instructions for the evaluation of Army accounting systems. Those instructions are provided in DOD 7000.14-R, Volume 1.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. This regulation remains in effect during all levels of mobilization. Combatant commands and Joint activities for which the Army is Executive Agent are supported by the Army Managers' Internal Control Program.

Proponent and exception authority.

The proponent of this regulation is the Assistant Secretary of the Army for Financial Management and Comptroller. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25-30 for specific guidance.

Army management control process.

This regulation contains internal controls and provides an Internal Control Evaluation for use in evaluating key internal controls (appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Assistant Secretary of the Army for Financial Management and Comptroller (SAFM-FOM), 109 Army Pentagon, Washington, DC 20310-0109.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and

Blank Forms) directly to Assistant Secretary of the Army for Financial Management and Comptroller (SAFM-FOM), 109 Army Pentagon, Washington, DC 20310-0109.

Committee Continuance Approval.

The Department of the Army committee management official concurs in the establishment and/or continuance of the committee(s) outlined herein. AR 15-1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the U.S. Army Resources and Programs Agency, Department of the Army Committee Management Office (AARP-ZA), 2511 Jefferson Davis Highway, 13th Floor, Taylor Building, Arlington, VA 22202-3926. Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, as found in the AR 15-1, then the proponent will follow all AR 15-1 requirements for establishing and continuing the group as a committee.

Distribution. This regulation is available in electronic media only and is intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

*This regulation superseded AR 11-2, dated 1 August 1994.

Contents (Listed by paragraph and page number)

Chapter 1

Authority and Responsibilities, page 1

Section I

General, page 1

Purpose • 1-1, *page 1*

References • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Statutory authority • 1-4, *page 1*

Section II

Responsibilities, page 1

Secretary of the Army • 1-5, *page 1*

Assistant Secretary of the Army for Financial Management and Comptroller • 1-6, *page 1*

Headquarters, Department of the Army functional proponents • 1-7, *page 2*

Administrative Assistant to the Secretary of the Army • 1-8, *page 3*

Auditor General • 1-9, *page 3*

Inspector General • 1-10, *page 3*

Senior Management Council • 1-11, *page 3*

Reporting Organizations • 1-12, *page 3*

Senior Responsible Officials • 1-13, *page 4*

Assessable Unit Managers • 1-14, *page 4*

Commanders of installations, major subordinate commands, table of organization and equipment divisions, and State Adjutants General • 1-15, *page 5*

Internal Control Administrator • 1-16, *page 5*

Internal Review Directors/Chiefs • 1-17, *page 5*

Director, Defense Finance and Accounting Service-Indianapolis Center • 1-18, *page 5*

Chapter 2

Policy and Requirements, page 6

Army Managers' Internal Control Program policy • 2-1, *page 6*

Internal control over financial reporting • 2-2, *page 6*

Reasonable assurance • 2-3, *page 7*

Key internal controls • 2-4, *page 7*

Internal control evaluations • 2-5, *page 8*

Internal control evaluation plans • 2-6, *page 8*

Identifying, reporting, correcting, and tracking material weaknesses • 2-7, *page 9*

Use of internal review, audit, and inspection reports • 2-8, *page 10*

Army reporting requirements • 2-9, *page 10*

Required documentation • 2-10, *page 10*

Performance agreements • 2-11, *page 11*

Appendixes

A. References, *page 14*

B. Government Accountability Office Standards for Internal Control in the Federal Government, *page 15*

C. Internal Control Reporting Categories, *page 19*

D. Internal Control Evaluation, *page 20*

Contents—Continued

Figure List

Figure 2-1: Format of an appendix for an Internal Control Evaluation, *page 12*

Figure 2-2: Format of an appendix for an internal control evaluation process not involving the use of evaluations, *page 13*

Glossary

Chapter 1

Authority and Responsibilities

Section I

General

1–1. Purpose

This regulation prescribes policies and responsibilities for the Army's Managers' Internal Control Program (MIC Program). The provisions of this regulation apply to all Army organizations and programs.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Statutory authority

a. The Army's MIC Program meets the requirements of the Accounting and Auditing Procedures Act of 1950, as amended by the Federal Managers Financial Integrity Act (FMFIA) of 1982, PL 97–255 (codified at Title 31, United States Code, Section 3512 (31 USC 3512)). The Accounting and Auditing Procedures Act of 1950 is implemented within the executive branch by Office of Management and Budget (OMB) Circular A–123, and within DOD by DODI 5010.40.

b. The FMFIA requires the head of each executive agency to—

(1) Establish internal controls to provide reasonable assurance that obligations and costs are in compliance with applicable laws; all assets are safeguarded against waste, loss, unauthorized use, or misappropriation; revenues and expenditures are properly recorded and accounted for; and programs are efficiently and effectively carried out according to the applicable law and management policy.

(2) Report annually to the President and Congress on whether these internal controls comply with the requirements of the FMFIA, including—

(a) Identifying any material weaknesses in these internal controls, along with plans for their correction.

(b) Reporting on whether accounting systems comply with the principles, standards, and related requirements prescribed by the Comptroller General of the United States, including deficiencies and plans for their correction.

Section II

Responsibilities

1–5. Secretary of the Army

The Secretary of the Army (SA) will sign and submit an annual statement of assurance to the Secretary of Defense on the status of the Army's internal controls and include a separate specific statement on internal control over financial reporting (ICOFR) as required by OMB Circular A–123, Appendix A (Implementation Plans).

1–6. Assistant Secretary of the Army for Financial Management and Comptroller

a. The ASA(FM&C) has delegated responsibility to the Deputy Assistant Secretary of the Army (Financial Operations), as executive agent for providing overall guidance and direction for implementing the Army Management Internal Control Program.

b. The Director, Management Services Directorate will—

(1) Formulate Army policy for implementing the FMFIA and issue administrative guidance and instructions.

(2) Analyze documents from Congress, the U.S. Government Accountability Office (GAO), OMB, the Comptroller General, the Office of the Secretary of Defense, and others related to the FMFIA to identify and effect needed changes to the Army MIC Program.

(3) Advise and represent the ASA(FM&C) on matters involving the Army MIC Program.

(4) Provide guidance and technical assistance directly to internal control administrators (ICAs) at Headquarters, Department of the Army (HQDA), Army Commands (ACOMs), Army Service Component Commands (ASCCs), and Direct Reporting Units (DRUs).

(5) Prepare and staff the SA's annual statement of assurance on internal controls including ICOFR and provide periodic updates as required on previously reported material weaknesses.

(6) Coordinate with the U.S. Army Audit Agency (USAAA) and HQDA functional proponents on the identification of internal control weaknesses that merit reporting as material weaknesses in the SA's annual statement of assurance.

(7) Develop internal control training materials for use by reporting organizations and their assessable units; HQDA

functional proponents; and Army schools that provide executive development and management training; and audit, inspection, and other organizations whose personnel assess the effectiveness of internal controls.

(8) Develop and maintain a tracking system to ensure that material weaknesses reported in the SA's annual statement of assurance are corrected in a timely manner. Feedback will be provided within 30 days to reporting organizations on the material weaknesses submitted to ASA(FM&C) that require action by HQDA and were not reported in the SA's annual statement of assurance.

(9) Develop and staff the Army position on reports by GAO, USAAA, DOD Inspector General (DODIG) and similar organizations on the overall Army MIC Program.

(10) Develop and maintain a current inventory of functional areas with key internal control evaluations on the ASA(FM&C) Web site.

(11) Coordinate with the USAAA on the annual audit of the MIC Program (see para 1-9h).

(12) Coordinate and monitor HQDA functional proponents' progress toward developing and maintaining policies and regulations that include effective internal controls.

(13) Develop and maintain an inventory of Army assessable units based on annual input from HQDA functional proponents, ACOMs, ASCCs, and DRUs.

c. The Director, Financial Reporting will—

(1) Issue guidance to HQDA functional proponents on implementing ICOFR, to include completing all ICOFR deliverables on time.

(2) Advise and represent the ASA(FM&C) on matters involving ICOFR.

(3) Provide advice and technical guidance to the ACOMs, ASCCs, and DRUs in developing process narratives, process flows, and conducting risk assessments and testing for ICOFR.

(4) Submit OMB Circular A-123, Appendix A deliverables required by Office of the Secretary of Defense on time.

(5) Prepare the annual statement of assurance on ICOFR and staff with the Director, Management Services for inclusion into the SA's annual statement of assurance.

(6) Ensure ICOFR material weaknesses include corrective action plans and update at least annually.

(7) Respond to auditor requests during audit or examination of ICOFR information.

1-7. Headquarters, Department of the Army functional proponents

The HQDA functional proponents, for their areas of functional responsibility will—

a. Develop and maintain policies and regulations that include effective internal controls.

b. Determine, through risk assessment, the key internal controls. Develop an internal control evaluation or identify an alternative method to test those controls and include the prescribed test method in applicable Army Regulation.

c. Ensure that key internal controls in regulations are reviewed and evaluations updated as needed; and that ASA(FM&C) is notified to update the inventory of evaluations.

d. Review material internal control weaknesses submitted by ACOM/ASCC/DRUs and HQDA functional proponents to determine if they need additional coordination, assess their materiality, and provide written feedback in accordance with the tasking memorandum to Assistant Secretary of the Army for Financial Management and Comptroller (SAFM-FOM), 109 Army Pentagon, Washington, DC 20310-0109 and the reporting organization recommending that the material internal control weakness be—

(1) Returned to the reporting organization for monitoring and resolution at a lower level. The HQDA functional proponent shall provide guidance and assistance as required to ensure that the weakness is corrected.

(2) Accepted as an issue requiring action, but not reported as an Army-level material weakness. The HQDA functional proponent shall coordinate with SAFM-FOM, USAAA, the reporting organization and other stakeholders as required, to determine the appropriate corrective action.

(3) Adopted as a HQDA-level material weakness for inclusion in the SA's annual statement of assurance. The HQDA functional proponent shall then develop a material weakness corrective action plan in coordination with the reporting organization, staffing it with other stakeholders as required, SAFM-FOM and USAAA. The corrective action plan should be developed within 30 days and must include achievable milestones that will ultimately result in validated correction of the weakness.

e. Track the progress in correcting material weaknesses reported in the SA's annual statement of assurance and material weaknesses reported by the ACOMs, ASCCs, and DRUs and provide status updates when requested by ASA(FM&C).

f. Assist ASA(FM&C) in composing and reviewing the SA's annual statement of assurance to maintain effective quality control over the accuracy of information reported.

g. Assess and provide guidance and feedback to the reporting organizations on specific actions required at all levels to address and resolve reported material weaknesses in the proponent's functional area of responsibility (para 1-7d) upon completion of the assessment.

h. Issue ICOFR instructions requiring ACOMs, ASCCs, and DRUs to validate specific process flows, narratives and internal controls for their operational areas.

1–8. Administrative Assistant to the Secretary of the Army

The AASA will—

a. Implement and administer the Army’s MIC Program for HQDA functional proponent responsibilities within the Office of the Secretary of the Army (OSA) and for Joint DOD activities supported by OSA and assigned to the AASA. In addition to the SA and Office of the Administrative Assistant, the HQDA reporting organizations include the Under Secretary of the Army, the Deputy Under Secretary of the Army, Deputy Under Secretary of the Army (Business Transformation). Exceptions to this responsibility are the Assistant Secretary of the Army for Acquisition, Logistics, and Technology; Assistant Secretary of the Army for Civil Works; ASA(FM&C); Assistant Secretary of the Army for Installations and Environment; Assistant Secretary of the Army for Manpower and Reserve Affairs; General Counsel; Chief Information Office/G–6; The Inspector General; The Auditor General; Chief of Legislative Liaison; Chief of Public Affairs; and the Director, Office of Small and Disadvantaged Business Utilization. These elements will comply with paragraphs 1–7 and 1–12 of this regulation.

b. Coordinate with the Director of the Army Staff to resolve issues of proponent responsibility for ARs and material weaknesses.

c. Ensure that all Army Regulations explicitly address Manager’s Internal Control Program responsibilities and that evaluations of key internal controls are presented in the prescribed format under a separate appendix.

1–9. Auditor General

The Auditor General, in addition to responsibilities in paragraphs 1–7 and 1–12, will—

a. Provide technical advice, assistance, and consultation on internal controls to HQDA functional proponents as necessary.

b. Evaluate, during the normal course of audits, the effectiveness of internal controls, the adequacy of internal control evaluations, and the adequacy of actions taken to correct material weaknesses.

c. Provide periodic reports to ASA(FM&C) summarizing internal control and systemic weaknesses identified in USAAA audits.

d. Identify proposed Army-level material weaknesses and provide the information to HQDA functional proponents when requested by ASA(FM&C) for possible reporting in the SA’s annual statement of assurance.

e. Prepare and submit an annual statement of assurance to the SA assessing implementation and adequacy of the MIC Program. Include in the annual statement of assurance the section related to ICOFR as prescribed in OMB Circular A–123, Appendix A and DOD guidelines.

f. Coordinate with ASA(FM&C) and submit annually to the DODIG a list of potential Army material weaknesses identified during audits, along with the Army position on these potential material weaknesses.

g. Coordinate with the ASA(FM&C) for review and audit of the program to comply with OMB Circular A–123, Appendix A and DOD guidelines.

h. The USAAA will coordinate with command audit focal points and notify commands and activities of its planned audits in accordance with current Army notification procedures to the greatest extent possible before the entrance conference or start of fieldwork (see AR 36–2, para 2–5).

1–10. Inspector General

The Inspector General, in addition to the responsibilities listed in paragraphs 1–7 and 1–12, will consider during the normal course of inspections, internal controls in the assessment of systemic issues and problems and make appropriate recommendations.

1–11. Senior Management Council

A Senior Management Council will be convened through special sessions of the Senior Level Steering Group (SLSG)/ Senior Assessment Team (SAT). Chaired by the Office, Assistant Secretary of the Army for Financial Management and Comptroller and representing all HQDA functional proponents, this council will meet as needed to provide advice on internal control matters, including the identification of internal control and systemic weaknesses that merit reporting in the SA’s annual statement of assurance. The SLSG/SAT will serve as the senior team responsible for overseeing the OMB Circular A–123, Appendix A program. Reporting organizations are encouraged to establish senior management councils that function in a similar fashion. Before convening, a senior management council must meet the requirements of AR 15–1.

1–12. Reporting Organizations

The HQDA functional proponents (less Secretariat elements covered by the AASA), ACOMs, ASCCs, and DRUs are the primary reporting organizations in the Army MIC Program. The heads of these organizations are responsible for

understanding and applying the GAO Standards for internal control in the Federal Government and carrying out the MIC Program within their organizations and will—

a. Provide the leadership and support needed to promote an effective MIC Program and to ensure that internal controls are in place and operating effectively.

b. Designate a senior responsible official (SRO) to ensure that the MIC Program is effectively implemented within their organization.

c. Designate the assessable units within the organization and provide updates to ASA(FM&C) when directed.

d. In accordance with ICOFR annual guidance from the ASA(FM&C), oversee the preparation of all process flows and narratives for relevant processes and sub processes and document internal controls in place.

e. Report significant deficiencies indicating the absence or ineffectiveness of internal controls and those weaknesses that warrant attention of HQDA for awareness or assistance in correcting. Potential material weaknesses should be reported to HQDA through command channels in a timely manner.

(1) The SAFM–FOM will review the weakness reported and will forward it to the appropriate HQDA functional proponent(s) for evaluation.

(2) The HQDA functional proponents will review internal control weaknesses submitted by ACOM/ASCC/DRUs in accordance with paragraph 1–7*d* to determine if they need additional coordination, assess their materiality and provide written feedback to SAFM–FOM.

(3) The proposed HQDA material weakness and action plan will then be briefed to the SLSG/SAT for validation and approval. If approved, the material weakness and associated milestones will be included as part of the SA’s annual statement of assurance. The SAFM–FOM will then use the minutes of each SLSG meeting as a medium to communicate the status of reported weaknesses to ACOM, ASCC and DRU commanders. Recommendations not resulting in a material weakness for the Army’s annual statement of assurance, but requiring action from HQDA functional proponents may be monitored by the SLSG to ensure timely resolution.

f. Implement corrective actions that may be made at the local level to correct the weaknesses. The reporting organization should then report the actions taken to enhance internal controls they believe to be significant accomplishments in Tab A of their Annual Statement of Assurance.

g. Sign and submit an annual statement of assurance to ASA(FM&C) in compliance with annual guidance that accurately describes the status of internal controls within their organization, provides required certifications that controls related to financial and non-financial reporting are in place and effective, and provides updated material weaknesses (in required format) that were reported throughout the year and the plans for corrective action.

1–13. Senior Responsible Officials

Designated by the head of the reporting organization, the SRO has overall responsibility for ensuring the implementation of an effective MIC Program within that organization. In this regard, the SROs will—

a. Advise the head of the reporting organization on the implementation and status of the organizations MIC Program and the leadership and support needed to promote an effective MIC Program.

b. Designate an ICA to administer the MIC Program within the reporting organization and to serve as a focal point for all internal control matters.

c. Oversee the preparation of an annual statement of assurance that accurately describes the status of internal controls in the reporting organization, to include, if applicable, ICOFR, and fully discloses any internal control or systemic material weaknesses along with plans for their correction.

1–14. Assessable Unit Managers

Designated by the head of the reporting organization, these commanders or managers of assessable units are responsible for understanding and applying the GAO Standards for internal control in the Federal Government and will—

a. Designate an ICA to administer the MIC Program within the assessable unit and provide the leadership and support needed to ensure that the MIC Program is implemented and operating effectively.

b. Ensure that—

(1) Managers and ICA(s) are trained and understand their internal control responsibilities. Refresher training should be conducted as necessary to maintain currency with changes in operational environment, laws, policies, directives from higher headquarters, as well as any time that the organization has been impacted by turnover in managers, the ICA, or significant personnel rotations.

(2) Managers are responsible for identifying internal and external risks that may prevent their organization from meeting its objectives. Managers are also responsible for establishing or enhancing internal controls to mitigate identified risks and ensure their effectiveness. Tools for use in developing risk assessments are available at <http://asafm.army.mil/offices/FO/IntControl.aspx?OfficeCode=1500>. Use of locally devised methods and tools to fit organizational specific needs and requirements is encouraged.

(3) An internal control evaluation plan (ICEP), which describes how key internal controls in the assessable unit will be evaluated over a five-year period, is established and maintained.

(4) Internal control evaluations are conducted according to the ICEP and the requirements of this regulation.

- (5) Required documentation on each completed internal control evaluation is retained, subject to audit/inspection.
- c. Assessable unit managers (AUMs) or principal deputy, certify the results of required internal control evaluations.
- d. Identify and report material weaknesses for the Assessable Unit consistent with guidance in paragraph 1–12e.
- e. Sign and submit to the next higher command level a feeder annual statement of assurance for the assessable unit.

1–15. Commanders of installations, major subordinate commands, table of organization and equipment divisions, and State Adjutants General

In conjunction with program guidance issued by their ACOM, ASCC, or DRU, these commanders and State Adjutants General will—

- a. Ensure that required internal control evaluations are conducted according to the governing ICEP.
- b. Ensure that internal control responsibilities are explicitly covered in the performance agreements of commanders, managers, and ICAs down to and including the assessable unit level.

1–16. Internal Control Administrator

The ICA is a Government employee, military or HQDA civilian, designated by the SRO to administer the MIC Program within the reporting organization. The ICA(s) designated by AUMs below the reporting organization level should have similar duties. Contractors may not function as ICAs, but may assist an ICA with most administrative tasks related to the preparation of the annual statement of assurance. Organizations are responsible for determining grade level, but the rank should be proportionate to the level of responsibility. The ICA will—

- a. Advise the SRO or AUM on the implementation and status of the organization's MIC Program and keep commanders and managers informed on internal control matters.
- b. Identify the organization's requirements for MIC Program training and arrange that training.
- c. Develop and maintain an ICEP based on the applicable regulations and associated evaluations and any additional areas identified by commanders and AUMs.
- d. Facilitate the process for identifying and reporting material weaknesses in accordance with paragraph 1–12e of this regulation.
- e. Prepare an annual statement of assurance for the signature of the commander or principal deputy (reporting organization level) and ensure that it is transmitted to ASA(FM&C) in compliance with annual guidance. The annual statement of assurance must accurately describe the status of internal controls within their organization, provide required certifications that controls related to financial and non-financial reporting are in place and effective, and provide updated material weaknesses (in required format) reported throughout the year.
- f. The ICA below the reporting organization level will similarly comply with paragraph 1–16e, but will prepare a feeder annual statement of assurance for the assessable unit in accordance with instructions from higher headquarters that provides support for higher command level annual statements of assurance.
- g. The ICA will ensure that the organization's Internal Review (IR) Office, if one is assigned to the command or staff element, reviews the organization's annual statement of assurance and provides an assessment of its thoroughness and validity before it is approved and signed by the head of the organization.
- h. Ensure that organizational material weaknesses are closely monitored until corrected and retain all required documentation supporting the annual statement of assurance and the correction of material weaknesses.

1–17. Internal Review Directors/Chiefs

In their capacity as heads of IR offices will—

- a. Provide technical advice, assistance and consultation on internal controls to AUMs within their organizations as necessary.
- b. Evaluate, during the normal course of reviews, the effectiveness of internal controls and the adequacy of internal control evaluations and actions taken to correct material weaknesses.
- c. Identify and recommend any internal control or systemic weaknesses that may merit reporting as material weaknesses based on analysis of IR reports and external audit reports.
- d. If aligned at the headquarters of a reporting organization or assessable unit, review the organization's annual statement of assurance and provide an assessment of its thoroughness and validity.
- e. Notify the SRO, applicable AUMs and ICAs on the status of external inspection and audit findings and recommendations that may warrant reporting as a material weakness in the annual statement of assurance.

1–18. Director, Defense Finance and Accounting Service-Indianapolis Center

Until all Army finance and accounting operations and systems are capitalized, the Director, Defense Finance and Accounting Service-Indianapolis Center (DFAS-IN) is responsible for—

- a. Determining key internal controls in finance and accounting and the appropriate evaluation methods and explicitly identifying the controls and methods in governing policy directives.

b. Providing overall guidance and direction to managers of Army accounting system for the evaluation, improvement, and reporting on Army accounting systems.

c. Conducting analysis and review of financial reporting processes, conducting risk assessments, modifying or implementing new internal controls to mitigate the changing environment, and preparing and submitting reports as required by ASA(FM&C) in adherence to OMB Circular A-123, Appendix A.

Chapter 2

Policy and Requirements

2-1. Army Managers' Internal Control Program policy

a. All commanders and managers have an inherent responsibility to establish and maintain effective internal controls, assess areas of risk, identify and correct weaknesses in those controls and keep their superiors informed. The FMFIA and OMB Circular A-123, Appendix A codify this inherent responsibility.

b. Heads of reporting organizations and AUMs are responsible for understanding and applying the GAO Standards for internal control in the Federal Government and for conducting internal control evaluations of key controls identified by HQDA functional proponents in applicable Army Regulations.

c. Heads of reporting organizations and AUMs will give high priority to prompt correction of material weaknesses and to the effective implementation of internal controls that—

(1) Are identified as key internal controls by HQDA functional proponents. (Source: Proponent Regulations and separate guidance).

(2) Pertain to the DOD high risk areas identified by OMB. (Source: Annual guidance).

(3) Pertain to any other high risk areas identified by DOD or Army leadership. (Source: Annual guidance).

(4) Pertain to areas of vulnerability they themselves have identified or have been identified by external entities such as USAAA or DODIG.

(5) Directly support the accomplishment of Army goals. (Source: Army Strategic Plan).

d. Heads of reporting organizations and AUMs must be forthright in reporting material weaknesses in key internal controls. The chain of command should encourage prompt and full disclosure of such problems and ensure that commanders and managers are not penalized for reporting material weaknesses.

e. Reporting organizations will be segmented into assessable units consisting of subordinate organizations headed by senior managers, preferably at the general officer or Senior Executive Service level, but not lower than an O-6, GS-15 or National Security Personnel System (NSPS) equivalent. In exceptional cases where the grade structure does not support having an AUM at this level, the AUM will be the senior military or HQDA civilian functional manager.

f. Performance agreements for Army commanders, managers, and ICAs with internal control responsibility down to and including assessable unit level must include an explicit statement of this responsibility to permit appropriate evaluation (see para 2-11).

g. Under separate ICOFR instructions from the HQDA functional proponents, reporting organizations will validate specific process flows, narratives, and internal controls for their operational areas.

h. No Army activity or program is exempt from the requirements of the FMFIA and OMB Circular A-123, Appendix A. This includes all personnel assigned to Army organizations and reporting organizations for which the Army serves as the executive agent.

(1) The Army MIC Program is not intended, however, to limit or interfere with matters such as statutory development or interpretation, determination of program requirements, resource allocation, rule-making, or other discretionary policy-making activities.

(2) For activities or functions that are contracted out, Army managers performing related functions that are inherently governmental in nature (for example, property accountability, contract administration, and quality assurance) must comply with the requirements of this regulation. If a contractor is expected to conduct internal control evaluations, the responsibility must be included as a contract requirement.

2-2. Internal control over financial reporting

a. The ASA(FM&C) is required to prepare an annual statement of assurance on ICOFR, which includes the annual statement of assurances prepared by each Army financial statement reporting entity (General Fund, Army Working Capital Fund, and the Civil Works Fund). The ICOFR annual statement of assurance must be based on an assessment strictly following the requirements of OMB Circular A-123, Appendix A; the Chief Financial Officers Council's Implementation Guide; DOD annual guidance, and Department of the Army annual guidance.

b. The assessments of internal controls within the FMFIA over financial reporting process may disclose material weaknesses identified in the reliability of financial reporting within the financial reporting process of the quarterly and annual financial statements. This annual statement of assurance will describe the plans and schedules to correct any

material weaknesses reported using the same format for the material weaknesses status reports as provided in the annual guidance for preparing the fiscal year annual statement of assurance.

2-3. Reasonable assurance

a. Background. In the context of the FMFIA, "reasonable assurance" refers to a satisfactory level of management confidence that internal controls are adequate and operating as intended. Inherently a management judgment, reasonable assurance recognizes that acceptable levels of risk exist that cannot be avoided because the cost of absolute control would exceed the benefits derived.

b. Basis for reasonable assurance. The determination of reasonable assurance is a subjective management judgment. The subjectivity of this judgment can be reduced significantly by considering the following:

(1) The degree to which all managers understand and adhere to the GAO Standards for internal control in the Federal Government.

(2) The degree to which managers are held formally accountable for the effectiveness of their internal controls and are evaluated on their performance in this regard.

(3) The timeliness, adequacy, and results of internal control evaluations, including the correction of any internal control weaknesses detected.

(4) Assessments from other sources (for example, IR engagements, audits, inspections, and investigations); media coverage; and direct management reviews or assessments by senior officials.

(5) Supporting annual statements of assurance from subordinate commanders, managers, or AUMs.

c. Reporting. At each level, the annual determination of reasonable assurance is a management judgment, based on all available information, on whether internal controls are operating as intended. The head of each reporting organization must submit an annual statement of assurance that provides two assessments of reasonable assurance that internal controls are in place and operating effectively: one for the overall internal control program and one for ICOFR.

(1) Where the annual statement of assurance provides an unqualified annual statement of assurance, it should be supported by clear indications that subordinate commanders and designated AUMs—

(a) Understand and adhere to the GAO Standards for internal control in the Federal Government.

(b) Are formally held accountable for the effectiveness of their internal controls.

(c) Have evaluated key internal controls as required by applicable ICEPs.

(d) Have reported material weaknesses, if any, and have taken corrective action to resolve them.

(2) Where the annual statement of assurance provides a "qualified" annual statement of assurance, the area or areas in question should be specified and related to material weaknesses being reported.

2-4. Key internal controls

a. General. The MIC Program does not attempt to evaluate internal controls for every requirement imposed on managers. It recognizes the principle that the cost of internal controls must not exceed the benefit derived. This constraint is captured in the concept of reasonable assurance. The Army accepts a certain amount of risk by requiring that AUMs concentrate on the adequacy of internal controls, as specified in the GAO Standards for internal control in the Federal Government, and key internal controls, as specified by HQDA functional proponents. Key internal controls are those controls that are absolutely essential for ensuring that key processes operate as intended and that resources are safeguarded from fraud, waste, and misuse. Various factors might be considered in deciding which controls are the key controls, but the fundamental criterion is the severity of adverse impact should the control fail or fail to be used (that is, a key control is one whose failure would "break" or seriously impair the system). The determination of key internal controls must be based on recognition that properly conducted internal control evaluations impose a significant cost on Army managers and that these managers must be able to give priority attention to the true key controls.

b. Identification. By definition, all Army Regulations are internal control documents that directly relate to one of the five GAO Standards for internal control in the Federal Government (see app B). Army Regulations are a medium to communicate guidance, describe command and control relationships, leverage risk and contribute to good management of Government resources and human capital. Headquarters, Department of the Army functional proponents must use their professional judgment to explicitly identify the key internal controls essential to their program and, where applicable, develop evaluations for those controls requiring testing and include them in an appendix to the governing Army Regulation (see para 2-5d). The HQDA functional proponent's process for determining the key internal controls should be based on an analysis of acceptable risks conducted in coordination with USAAA to ensure a common baseline for audit purposes and executive-level approval of key controls to make sure that excessive coverage is avoided.

c. Revisions. After the initial determination of key internal controls, HQDA functional proponents must reevaluate this determination whenever major deficiencies are identified (for example, by management reviews, IR engagements, audits or inspections); when policies are significantly revised or when standard systems are modified or replaced. Any standard internal control evaluations that are affected must also be revised to ensure consistency in published guidance.

d. Supplementation. Field organizations may supplement internal controls identified by HQDA functional proponents. The key internal controls HQDA functional proponents identify are the minimum requirement for the internal

control evaluation. Suggested changes to these key internal controls may be submitted directly to the HQDA functional proponent. Commanders and managers should require additional coverage in internal control evaluations to address command-unique or location-unique circumstances. Field organizations are encouraged to perform a risk assessment on these internal control processes during the development of the annual ICEP.

2-5. Internal control evaluations

a. General. An internal control evaluation is a detailed, systematic, and comprehensive examination of the key internal controls to determine whether they are in place, being used as intended, and effective in achieving their purpose including internal controls related to financial reporting (OMB Circular A-123, Appendix A). The evaluation must be based on the actual testing of these key internal controls using one of several methods: direct observation, file and document analysis, sampling or simulation. The evaluation of key internal controls must result in a specific determination of their effectiveness. Finally, the evaluation must be supported by documentation that clearly indicates who conducted the evaluation and when, what methods were used to test the key controls, evaluation results, what internal control deficiencies (if any) were detected, and what corrective actions were taken.

b. Requirement. Formal internal control evaluations of key internal controls must be conducted at least once every five years. Commanders/managers may require more frequent evaluation based on leadership emphasis, personnel turnover, audit/inspection findings, change in mission, and so on. The ASA(FM&C) will maintain a current inventory of functional areas on the ASA(FM&C) Web site of areas where HQDA functional proponents have identified key internal controls, as well as, information on the governing Army Regulation and any suggested or required methods for conducting the evaluation.

c. Certification. The AUM's certification that a required internal control evaluation has been conducted will be documented on DA Form 11-2 (Internal Control Evaluation Certification). Certification, in block 7 of DA Form 11-2, will include a statement of the method used (evaluation or alternate method) and how compliance was tested; summary of results; list of any deficiencies identified (indicate no deficiencies if there were none); and what corrective action(s) have been taken, as well as what deficiencies are pending correction. The form is available in electronic media on the Army Publishing Agency Web site under forms.

d. Methods for evaluating internal controls. The HQDA functional proponents may identify an internal control evaluation process for use in evaluating key internal controls. All internal control evaluations will be conducted in one of two ways:

(1) *Internal control evaluations.* The HQDA functional proponent may develop an internal control evaluation and publish it as an appendix in the governing Army Regulation for use by managers in evaluating key internal controls. Figure 2-1 is the format for an internal control evaluation. The evaluation identifies the key internal controls and provides managers a tool to evaluate the effectiveness of these controls. Commanders and managers may use an evaluation to conduct their internal control evaluations or, as an alternative, they can use an existing management review process of their own choosing, so long as the method chosen meets the basic requirements of an evaluation outlined in this paragraph.

(2) *Existing management review processes.* In many areas, existing management review processes may meet, or can be modified to meet, the basic requirements of an internal control evaluation. Some of these processes are unique to a specific functional area, while others are more generic, such as the use of local inspector general, IR personnel or the command review and analysis process. The HQDA functional proponents may suggest an existing management review process for evaluating key internal controls; or they may require the use of a specific functional management review process, so long as it is an existing Armywide process and one for which they are the functional proponent. The HQDA functional proponents must provide the necessary information as an appendix to the governing Army Regulation. Figure 2-2 is the format for identifying key internal controls and evaluation processes if an evaluation is not provided. Unless the HQDA functional proponent requires the use of an existing Armywide functional management review process, commanders and managers are free to choose the method of evaluation.

e. Signature. The DA Form 11-2 shall be signed by the evaluator in block 6a; the form will be certified by the AUM in block 8a(2). Electronic signatures may be used.

2-6. Internal control evaluation plans

The ICEP is the written plan for conducting required internal control evaluations within the assessable unit over a five-year period. The ICEP need not be lengthy and any format may be used, so long as it covers the key internal controls identified by HQDA functional proponents and communicates clearly to subordinate managers what areas are to be evaluated and who will conduct the evaluation and when. The ICEP may be developed at either the reporting organization or the assessable unit level. It may be structured by functional areas (for example, information security, maintenance of real property) or by major organizational components (Director of Logistics, Director of Contracting). It should list the governing ARs that identify key internal controls or method to be used for conducting the evaluation. The ICEP must be kept current and used to monitor progress to ensure that all internal control evaluations are conducted as scheduled. The ASA(FM&C) will develop and maintain a current inventory of functional areas with key internal controls on the ASA(FM&C) Web site.

2-7. Identifying, reporting, correcting, and tracking material weaknesses

a. Background. The absence or ineffectiveness of internal controls constitutes a deficiency, weakness, or material weakness that must be corrected. Whether the weakness is serious enough to be considered material and reported to the next level of command is a management judgment that must be made based on the criteria outlined in paragraphs 2-7c and 2-7d. This includes the potential to cause a material misstatement in the Army annual financial statements. The reporting of material weaknesses is not a new requirement because managers have always had an inherent responsibility to keep the next level of management informed of sensitive problems and issues. The ability of management at all levels to detect, or be aware of, internal control or systemic weaknesses and to take corrective action is the fundamental goal of the FMFIA.

b. Reporting process. Significant deficiencies indicating the absence or ineffectiveness of internal controls and those weaknesses that warrant attention of HQDA for awareness or assistance in correcting should be submitted by the reporting organization. Material weaknesses should be reported to HQDA through command channels in a timely manner; however, the frequency of reporting is a command prerogative.

(1) Reporting organizations are encouraged to proactively implement those corrective actions that may be made at the local level to correct the weaknesses. The activity should then report the significant actions taken to enhance internal controls as positive accomplishments in Tab A of their annual statement of assurance.

(2) The SAFM-FOM will review the weakness reported and will forward it to the appropriate HQDA functional proponent(s) for evaluation.

(3) The HQDA functional proponents will review material weaknesses in internal controls submitted by ACOMs/ASCCs/DRUs to determine if they need additional coordination, assess their materiality, and provide written feedback within 10 business days to SAFM-FOM and the reporting organization recommending that the material weakness be—

(a) Returned to the reporting organization for monitoring and resolution at a lower level. The HQDA functional proponent shall provide guidance and assistance as required to ensure that the weakness is corrected.

(b) Accepted as an issue requiring action, but not reported as an Army-level material weakness. The HQDA functional proponent shall coordinate with SAFM-FOM, USAAA, the reporting organization and other stakeholders as required, to determine the appropriate corrective action.

(c) Adopted as a HQDA-level material weakness for inclusion in the SA's annual statement of assurance. The HQDA functional proponent shall then develop a material weakness corrective action plan in coordination with the reporting organization, staffing it with other stakeholders as required, SAFM-FOM and USAAA. The corrective action plan should be developed within 30 days and must include achievable milestones that will ultimately result in validated correction of the weakness.

(4) The proposed HQDA material weakness and action plan will then be briefed to the SLSG/SAT for validation and approval. If approved, the material weakness and associated milestones will be included as part of the SA's annual statement of assurance. The SAFM-FOM will then use the minutes of each SLSG meeting as a medium to communicate the status of reported weaknesses to ACOM, ASCC, and DRU commanders. Recommendations not resulting in a material weakness for the Army's annual statement of assurance, but requiring action from HQDA functional proponent may be monitored by the SLSG to ensure timely resolution.

c. Essential criteria for material weaknesses. To be considered material, a weakness must meet the following two conditions—

(1) It must involve a weakness in internal controls, such as the controls are not in place, are not being used or are inadequate. Resource deficiencies in themselves are not internal control weaknesses.

(2) It must warrant the attention of the next level of command, either because that next level must take action or because it must be aware of the problem. This requires a management judgment, particularly in determining whether the next level of command must be aware of a weakness. The fact that a weakness can be corrected at one level does not exclude it from being reported to the next level because the sharing of important management information is one of the primary reasons for reporting a material weakness.

d. Other factors. To assist in making judgments on whether internal control weaknesses are material, the following factors should be considered: actual or potential loss of resources; sensitivity of the resources involved; magnitude of funds, property or other resources involved; actual or potential frequency of loss; current or probable media interest (adverse publicity); current or probable congressional interest (adverse publicity); unreliable information causing unsound management decisions; diminished credibility or reputation of management; impairment of essential mission; violation of statutory or regulatory requirements; information security risk; and public deprivation of needed government services. Additionally, a material weakness related to financial reporting would be one that could potentially result in a material misstatement in annual financial statements. Materiality levels and thresholds are determined by each level in the chain of command for a reported material weakness. The HQDA functional proponents, in coordination with ASA(FM&C), will make the final decision on materiality before the Army annual statement of assurance is submitted to the SA.

e. Correction. Each material weakness reported, including those related to ICOFR, must include a plan of corrective action. DOD requires that the last milestone in this plan validate that the corrective actions have in fact resolved the weakness. Material weaknesses may not be closed until this validation milestone has been accomplished. Detailed

guidance for reporting material weaknesses is provided in ASA(FM&C)'s annual instructions for the preparation of feeder annual statement of assurance.

f. Tracking. As indicated previously, material weaknesses are reported to higher headquarters either because that level must be aware of the weakness or because it must take corrective action. In the case of material weaknesses reported for awareness, reporting organizations are responsible for tracking the weakness to ensure that corrective actions are completed and the weakness is effectively resolved. In the case of material weaknesses reported for corrective action, tracking of the weakness will depend on the higher headquarters' disposition of the issue. The system established to track material weaknesses should not duplicate the normal tracking functions of IR organizations. Tracking of an audit or IR finding may well meet the requirement for tracking of a reported material weakness. Keep in mind, however, that a finding by auditors or IR personnel and a material weakness identified by management may not be identical; they may be different in scope and may have different corrective actions. Where the material weaknesses are significantly different, the tracking system used must be able to effectively track the correction of the material weakness.

2-8. Use of internal review, audit, and inspection reports

a. Headquarters, Department of the Army functional proponents, commanders, and AUMs can often take corrective or preventive action based on problems identified in IR, audit and inspection reports. Such reports may address an internal control problem at only one installation, but managers throughout the Army can use these reports to identify potential problems in their own areas of responsibility and take timely preventative action.

b. Internal review, audit and inspection organizations ensure distribution of their reports to managers with primary and collateral interests at all reporting organizations. In addition, The Auditor General and Army Inspector General organizations prepare summaries of internal control weaknesses identified in their reports. The DODIG also publishes periodic summaries of internal control weaknesses identified in its reports and those of GAO. The ASA(FM&C) periodically distributes these summaries to ICAs at reporting organizations in order to facilitate correction and mitigation of reported weaknesses and to ensure that managers can benefit from lessons learned at other activities. Finally, The Auditor General supports the development of the SA's annual statement of assurance by identifying potential Army material weaknesses for consideration by HQDA functional proponents.

2-9. Army reporting requirements

The FMFIA requires the Secretary of Defense to submit an annual statement of assurance to the President and Congress on the status of internal controls within DOD. In addition, OMB requires periodic updates on the status of material weaknesses DOD previously reported. The OMB Circular A-123, Appendix A also requires an annual statement of assurance related to ICOFR. The Army supports DOD in meeting these requirements in two ways—

a. Annual Statement of Assurance. Annually the SA must submit the annual statement of assurance, including ICOFR, to the Secretary of Defense for use in preparing the DOD annual statement of assurance to the President and Congress. The SA's annual statement of assurance is based primarily on annual statements of assurance from HQDA functional proponents and commanders and managers of ACOMs, ASCCs, and DRUs. The ASA(FM&C) will issue instructions, in advance, for the preparation of these annual statements of assurance.

b. Periodic update. The Army is required to report to the Office of the Secretary of Defense any major changes in the plans for correcting material weaknesses. The ASA(FM&C) will issue appropriate guidance in advance for updates on Army material weaknesses.

2-10. Required documentation

a. Internal control evaluations plan. The ICEP will serve to document the required schedule of internal control evaluations within the assessable unit or the reporting organization. The ICEP will identify those areas to be evaluated, the year for the evaluation and the official responsible for ensuring that the evaluation is conducted. Internal control evaluations must be supported by specific documentation, regardless of the method used to conduct the evaluation. At a minimum, this supporting documentation must clearly indicate who conducted the evaluation, the date the evaluation was conducted, what methods were used to test key internal controls, what internal control weaknesses (if any) were detected, and what corrective actions were taken. The completion of the DA Form 11-2 is certification that the evaluation was performed and appropriately documented. It is not intended to serve as a substitute for documenting the evaluation. All supporting documentation used to reach conclusion(s) must be referenced on DA Form 11-2 and either attached or available for review. Documentation must be sufficient enough for an independent reviewer to reach the similar conclusion(s).

b. Annual statements of assurance and material weaknesses. Reporting organizations are responsible for maintaining copies of their annual statements of assurance, along with complete supporting documentation. Organizations responsible for tracking the correction of material weaknesses are also responsible for maintaining documentation on the status, effectiveness and validation of corrective actions. The HQDA functional proponents are responsible for monitoring and documenting the correction of material weaknesses reported in the SA's annual statement of assurance and those material weaknesses requiring HQDA-level oversight to resolve but not included in the Army's annual statement of assurance.

c. *Retention.* Documentation on internal control evaluations conducted, annual statements of assurance submitted and material weaknesses reported must be maintained according to AR 25-400-2.

- (1) Assessable units must retain required documentation on the most recent internal control evaluation.
- (2) Reporting organizations must retain copies of their annual statements of assurance and supporting documentation in accordance with the Army Records Information Management System (ARIMS).
- (3) Reporting organizations must retain documentation on material weaknesses in accordance with ARIMS.
- (4) Retain the records for three fiscal years after submission; if a material weakness is reported, then retain the records for three years after the weakness is resolved and HQDA no longer requires reports on the status.

2-11. Performance agreements

a. *Background.* The OMB Circular A-123, Appendix A requires the performance agreements of senior managers include an explicit statement of responsibility for internal controls. The responsibility includes ICOFR as outlined in OMB Circular A-123, Appendix A.

b. *Implementation.* Supervisors must include an explicit statement of responsibility for internal controls in the performance agreements of commanders, managers, and ICAs responsible for the execution or oversight of effective internal controls, down to and including assessable unit level. The absence of an explicit statement of responsibility must be based on the supervisor's determination that the individual does not have significant management responsibilities.

(1) For military officers, the responsibility should be included under "Major Performance Objectives" in Part IV of DA Form 67-9-1 (Officer Evaluation Report Support Form).

(2) For "senior system" civilian employees under the Total Army Performance Evaluation System, the responsibility should be included under "Major Performance Objectives/Individual Performance Standards" in Part IV of DA Form 7222-1 (Senior System Civilian Evaluation Report Support Form).

(3) For NSPS personnel, the mandatory Army supervisory objective fulfills the requirement for internal control responsibilities. For non-supervisory personnel, internal control responsibilities should be captured under Job Objectives and Contributing Factors, Part E of DD Form 2906 (Department of Defense National Security Personnel System (NSPS) Performance Appraisal).

(4) For nonappropriated fund personnel, guidance on performance standards is provided in AR 215-3.

(5) For other performance and evaluation systems not mentioned, follow the governing regulation or published guidance for the specific system's performance objectives.

c. *Application.* The explicit statement of responsibility should be brief and may take any form, but it must be specific enough to provide individual accountability. Supervisors may use a stand-alone element or may include the internal control responsibility as part of a broader element. The following are examples of explicit statements that would suffice:

(1) *Headquarters, Department of the Army functional proponents.* These individuals should comply with paragraphs 1-7 and 1-12 of this regulation.

(2) *Army Command, Army Service Component Command, and Direct Reporting Unit commanders and managers.* These individuals should comply with paragraph 1-12 of this regulation.

(3) *Senior responsible officials.* These individuals should comply with paragraph 1-13 of this regulation.

(4) *Assessable unit managers.* These individuals should comply with paragraph 1-14 of this regulation.

(5) *Internal control administrators.* These individuals should comply with paragraph 1-16 of this regulation.

Appendix X (insert the appropriate letter) Internal Control Evaluation

X-1. Function. The function covered by this evaluation is (indicate the function covered by the evaluation)

X-2. Purpose. The purpose of this evaluation is to assist (indicate the intended users) in evaluating the key internal controls listed. It is not intended to cover all controls.

X-3. Instructions. Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, simulation, other). Answers that indicate deficiencies must be explained and the corrective action identified in supporting documentation. These internal controls must be evaluated at least once every five years. Certification that the evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification)

X-4. Test Questions. (Insert the test questions worded so that negative answers indicate an internal control deficiency or weakness)

a.

b.

c.

X-5. Supersession. This evaluation replaces the evaluation(s) for (insert the task/subtask covered by the previous evaluation) previously published in (insert the previous AR number, dated _____).

X-6. Comments. Help make this a better tool for evaluating internal controls. Submit comments to (insert the complete mailing address for HQDA functional proponent).

Figure 2-1. Format of an appendix for an Internal Control Evaluation

Appendix X *(insert the appropriate letter)* Internal Control Evaluation Process

X-1. Function. *(Indicate the function to be evaluated)*

X-2. Key Internal Controls. *(List the key internal controls to be evaluated)*

a.

b.

c.

X-3. Internal Control Evaluation Process.

*(Briefly describe the existing management review process that is suggested or required for use in evaluating the key internal controls identified. For any process to be **required**, it must be an existing Army wide functional process the HQDA functional proponent is responsible for. If no process is suggested or required, indicate "None.")*

Figure 2-2. Format of an appendix for an internal control evaluation process not involving the use of evaluations

Appendix A References

Section I

Required Publications

This section contains no entries.

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read a related publication to understand this publication. Army Regulations are available on the Army Publishing Directorate (APD) Web site at <http://www.apd.army.mil>. DOD directives and instructions are available at <http://www.dtic.mil/whs/directive>.

AR 11-7

Internal Review Program

AR 15-1

Boards, Commissions, and Committees - Committee Management

AR 25-30

The Army Publishing Program

AR 25-55

The Department of the Army Freedom of Information Act Program

AR 25-400-2

The Army Records Information Management System (ARIMS)

AR 36-2

Audit Services in the Department of the Army

AR 215-3

Non-appropriated Funds Personnel Policy

AR 340-21

The Army Privacy Program

DODD 5000.01

The Defense Acquisition System

DODD 8000.01

Management of the Department of Defense Information Enterprise

DODI 5010.40

Managers' Internal Control (MIC) Program Procedures

DOD 7000.14-R, Volume 1

General Financial Management Information, Systems and Requirements

GAO-01-1008G

Internal Control Management and Evaluation Tool (Available at <http://www.gao.gov/>.)

OMB Bulletin 01-09

Form and Content of Agency Financial Statements (Available at http://www.whitehouse.gov/omb/bulletins_default/.)

OMB Circular A-76

Performance of Commercial Activities (Available at <http://www.whitehouse.gov/omb/circulars/>.)

OMB Circular A-123, Appendix A

Management's Responsibility for Internal Control (Available at <http://www.whitehouse.gov/omb/circulars/>.)

PL 97-255

Federal Managers' Financial Integrity Act of 1982 (Available at <http://thomas.loc.gov/bss/>.)

31 USC 3512

Executive agency accounting and other financial management reports and plans (Available at <http://uscode.house.gov/search/criteria.shtml>.)

Section III Prescribed Forms

DA Form 11-2

Internal Control Evaluation Certification (Prescribed in para 2-5c.)

Section IV Referenced Forms

DA Form 67-9-1

Officer Evaluation Report Support Form

DA Form 2028

Recommended Changes to Publications and Blank Forms

DA Form 7222-1

Senior System Civilian Evaluation Report Support Form

DD Form 2906

Department of Defense National Security Personnel System (NSPS) Performance Appraisal

Appendix B Government Accountability Office Standards for Internal Control in the Federal Government

B-1. Standards

The Comptroller General of the United States established these standards for defining the minimum level of quality acceptable for internal control in government and providing the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency's operations: programmatic, financial, and compliance. However, they are not intended to limit or interfere with duly granted authority related to developing legislation, rule making, or other discretionary policy-making in an agency. These standards provide a general framework. In implementing these standards, management is responsible for developing the detailed policies, procedures, and practices to fit their agency's operations and to ensure that they are built into and an integral part of operations. Paragraphs B-2 through B-6, below, present short, concise statements for each of these standards and provides additional information to help managers incorporate the standards into their daily operations.

B-2. Control environment

a. Standard. 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.

b. Implementation.

(1) A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment.

(2) One factor is the integrity and ethical values maintained and demonstrated by management and staff. Agency management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate.

(3) Another factor is management's commitment to competence. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling, and performance appraisals.

(4) Management's philosophy and operating style also affect the environment. This factor determines the degree of risk the agency is willing to take and management's philosophy towards performance-based management. Further, the

attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control.

(5) Another factor affecting the environment is the agency's organizational structure. It provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

(6) The environment is also affected by the manner in which the agency delegates authority and responsibility throughout the organization. This delegation covers authority and responsibility for operating activities, reporting relationships, and authorization protocols.

(7) Good human capital policies and practices are another critical environmental factor. This includes establishing appropriate practices for hiring, orienting, training, evaluating, counseling, promoting, compensating, and disciplining personnel. It also includes providing a proper amount of supervision.

(8) A final factor affecting the environment is the agency's relationship with the Congress and central oversight agencies such as OMB. Congress mandates the programs that agencies undertake and monitors their progress and central agencies provide policy and guidance on many different matters. In addition, Inspectors General and internal senior management councils can contribute to a good overall control environment.

B-3. Risk assessment

a. Standard. Internal control should provide for an assessment of the risks the agency faces from both external and internal sources.

b. Implementation.

(1) A precondition to risk assessment is the establishment of clear, consistent agency objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the Government Performance and Results Act, and forming a basis for determining how risks should be managed.

(2) Management needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entity-wide and activity level. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments.

(3) Once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding how to manage the risk and what actions should be taken. The specific risk analysis methodology used can vary by agency because of differences in agencies' missions and the difficulty in qualitatively and quantitatively assigning risk levels.

(4) Because governmental, economic, industry, regulatory, and operating conditions continually change, mechanisms should be provided to identify and deal with any special risks prompted by such changes.

B-4. Control activities

a. Standard. Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's control objectives.

b. Implementation.

(1) Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

(2) Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes.

(3) Activities may be classified by specific control objectives, such as ensuring completeness and accuracy of information processing.

(4) There are certain categories of control activities that are common to all agencies. Examples include the following—

(a) Top Level Reviews of Actual Performance. Management should track major agency achievements and compare these to the plans, goals, and objectives established under the Government Performance and Results Act.

(b) Reviews by Management at the Functional or Activity Level. Managers also need to compare actual performance to planned or expected results throughout the organization and analyze significant differences.

(c) Management of Human Capital. Effective management of an organization's workforce—its human capital—is essential to achieving results and an important part of internal control. Management should view human capital as an asset rather than a cost. Only when the right personnel for the job are on board and are provided the right training,

tools, structure, incentives, and responsibilities is operational success possible. Management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved. Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization's success. As a part of its human capital planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.

(d) *Controls Over Information Processing.* A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control accounts, and controlling access to data, files, and programs. Further guidance on control activities for information processing is provided below under "Control Activities Specific for Information Systems."

(e) *Physical Control Over Vulnerable Assets.* An agency must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.

(f) *Establishment and Review of Performance Measures and Indicators.* Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.

(g) *Segregation of Duties.* Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

(h) *Proper Execution of Transactions and Events.* Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered into. Authorizations should be clearly communicated to managers and employees.

(i) *Accurate and Timely Recording of Transactions and Events.* Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.

(j) *Access Restrictions to and Accountability for Resources and Records.* Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

(k) *Appropriate Documentation of Transactions and Internal Control.*

1. Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

2. These examples are meant only to illustrate the range and variety of control activities that may be useful to agency managers. They are not all-inclusive and may not include particular control activities that an agency may need.

3. Furthermore, an agency's internal control should be flexible to allow agencies to tailor control activities to fit their special needs. The specific control activities used by a given agency may be different from those used by others due to a number of factors. These could include specific threats they face and risks they incur; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

(l) *Control Activities Specific for Information Systems.* There are two broad groupings of information systems control - general control and application control. General control applies to all information systems-mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

1. *General Control.* This category includes entity-wide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. More specifically:

a. Data center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also include job set-up and scheduling procedures and controls over operator activities.

b. System software control includes control over the acquisition, implementation, and maintenance of all system software including the operating system, data-based management systems, telecommunications, security software, and utility programs.

c. Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by agency personnel. Specific control activities include frequent changes of dial-up numbers; use of dial-back access; restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords.

d. Application system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements; authorizations for undertaking projects; and reviews, testing, and approvals of development and modification activities before placing systems into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user's needs, and that it is properly placed into operation.

2. *Application Control.*

a. This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data.

b. General and application control over computer systems are interrelated. General control supports the functioning of application control, and both are needed to ensure complete and accurate information processing. If the general control is inadequate, the application control is unlikely to function properly and could be overridden.

c. Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the needed controls should be identified and implemented.

B-5. Information and communications

a. *Standard.* Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities.

b. *Implementation.*

(1) For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the agency to achieve all of its objectives.

(2) Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on fixed assets, inventories, and receivables. Operating information is also needed to determine whether the agency is achieving its compliance requirements under various laws and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently.

(3) Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.

B-6. Monitoring

a. *Standard.* Internal control monitoring should assess the quality of performance over time and ensure that the findings of audit and other reviews are promptly resolved.

b. *Implementation.*

(1) Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

(2) Separate evaluations of control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as

review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General or an external auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.

(3) Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to—

(a) Promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations,

(b) Determine proper actions in response to findings and recommendations from audits and reviews, and

(c) Complete, within established time frames, all actions that correct or otherwise resolve the matters brought to managements attention.

(4) The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that—

(a) Corrects identified deficiencies,

(b) Produces improvements, or

(c) Demonstrates the findings and recommendations do not warrant management action.

Appendix C

Internal Control Reporting Categories

C-1. Reporting categories

When reporting a material weakness in internal controls, the DOD component will identify which function the material weakness concerns.

C-2. Reporting guidelines

The following will be used as the reporting categories used to classify the material weaknesses:

a. *E3.1. Research, Development, Test, and Evaluation.* The basic project definition, approval, and transition from basic research through development, test, and evaluation and all DOD and contractor operations involved in accomplishing the project work, excluding the support functions covered in separate reporting categories such as Procurement and Contract Administration.

b. *E3.2. Major Systems Acquisition.* Items designated as major systems and are subject to the procedures of the Defense Acquisition Board, the Military Services Acquisition Review Councils, or the Selected Acquisition Reporting System. DOD Directive 5000.01 may be helpful when evaluating a weakness for inclusion in this category.

c. *E3.3. Procurement.* The decisions to purchase items and services with certain actions to award and amend contracts (e.g., contractual provisions, type of contract, invitation to bid, independent Government cost estimate, technical specifications, evaluation and selection process, pricing, and reporting).

d. *E3.4. Contract Administration.* The fulfillment of contractual requirements including performance and delivery, quality control and testing to meet specifications, performance acceptance, billing and payment controls, justification for contractual amendments, and actions to protect the best interests of the Government.

e. *E3.5. Force Readiness.* The operational readiness capability of combat and combat support (both Active and Reserve) forces based on analyses of the use of resources to attain required combat capability or readiness levels.

f. *E3.6. Manufacturing, Maintenance, and Repair.* The management and operation of in-house and contractor-operated facilities performing maintenance and repair and/or installation of modifications to materiel, equipment, and supplies. Includes depot and arsenal-type facilities as well as intermediate and unit levels of military organizations.

g. *E3.7. Supply Operations.* The supply operations at the wholesale (depot and inventory control point) level from the initial determination of material requirements through receipt, storage, issue reporting, and inventory control (excluding the procurement of materials and supplies). Covers all supply operations at retail (customer) level, including the accountability and control for supplies and equipment of all commodities in the supply accounts of all units and organizations (excluding the procurement of material, equipment, and supplies).

h. *E3.8. Property Management.* Construction, rehabilitation, modernization, expansion, improvement, management, and control over real and installed property, and facilities (both military and civil works construction) and includes all phases of property life cycle management. Also covers disposal actions for all materiel, equipment, and supplies including the Defense Reutilization and Marketing System.

i. *E3.9. Communications and/or Intelligence and/or Security.* The plans, operations, systems, and management activities for accomplishing the communications and intelligence missions and safeguarding classified resources (not peripheral assets and support functions covered by other reporting categories). Also covers the DOD programs for protection of classified information.

j. *E3.10. Information Technology.* The design, development, testing, approval, deployment, use, and security of

automated information systems (using a combination of computer hardware, software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting or displaying information) and other technologies for processing management information. This includes requirements for justification of equipment and software. DOD Directive 8000.01 may be helpful when evaluating a weakness for inclusion in this category.

k. E3.11. Personnel and/or Organization Management. Authorizations, recruitment, training, assignment, use, development, and management of military and civilian personnel of the Department of Defense. Also includes the operations of headquarters organizations. Contract personnel are not covered by this category.

l. E3.12. Comptroller and/or Resource Management. The budget process, finance and accounting, cost analysis, productivity and management improvement, and the general allocation and continuing evaluation of available resources to accomplish mission objectives. Includes pay and allowances for all DOD personnel and all financial management areas not covered by other reporting categories, including those in connection with OMB Circular A-76 (reference (p)).

m. E3.13. Support Services. All support service functions financed from appropriated funds not covered by the other reporting categories such as healthcare, veterinary care, and legal and public affairs services. All nonappropriated fund activities are also covered by this category.

n. E3.14. Security Assistance. Management of DOD Foreign Military Sales, Grant Aid, and International Military Education and Training Programs.

o. E3.15. Other (Primarily Transportation). All functional responsibilities not contained in sections E3.1. through E3.15., including management and use of land, sea, and air transportation for movement of personnel, materiel, supplies, and equipment using both military and civilian sources.

p. E3.16. Financial Reporting. Processes, procedures, and systems used to prepare, compile, and generate the DOD financial statements according to reference (c); reference (h); the Federal Accounting Standards Advisory Board (FASAB) guidance (reference (q)); the Department of the Treasury Manual (references (r) and (s)) and financial reporting guidance established by OMB Bulletin 01-09 and OMB Circular A-136 (references (t) and (u)); and DOD 7000.14-R (reference (v)).

q. E3.17. Organization Structure and Analysis. Processes and procedures, used to update the organization structure to meet changes in mission and workload. Evaluation of formal structures to minimize management layers to the minimum required for effective management of the workforce. Comparison of skills required to support current and future mission, functions and workload as well as the actual assigned personnel. Develop long-term action plans to meet workload changes and to ensure transparency of operations for the workforce and higher headquarters.

Appendix D

Internal Control Evaluation

D-1. Function

The function covered by this evaluation is the administration of the MIC Program.

D-2. Purpose

The purpose of this evaluation is to assist AUMs and ICAs in evaluating the key internal controls outlined. It is not intended to cover all controls.

D-3. Instructions

These key internal controls must be formally evaluated at least once every five years or whenever the ICA changes. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2. Evaluation test questions are outlined in paragraph C-4, above, and are intended as a start point for each applicable level of internal control evaluation. Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, simulation, other). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation.

D-4. Test questions

- a.* Are key internal controls identified in the governing Army Regulations? (HQDA functional proponents only.)
- b.* Are internal control evaluations provided or alternate evaluation methods identified to test key internal controls? (HQDA functional proponents only.)
- c.* Is local internal control guidance available that defines internal control responsibilities and required actions?
- d.* Are AUMs, managers and ICAs trained in, and do they understand, their internal control responsibilities?
- e.* Are explicit statements of internal control responsibility included in performance agreements for commanders, AUMs and ICAs down to and including the assessable unit level?
- f.* Is an ICEP established and maintained to describe how key internal controls will be evaluated over a five-year period?

g. Are internal control evaluations conducted in accordance with the ICEP and prompt action taken to correct any internal control weaknesses detected?

h. Is the SRO advised of potential material weaknesses detected through internal control evaluations or from other sources?

D-5. Supersession

This evaluation replaces the management control evaluation checklist previously published in AR 11-2, Management Control, 1 August 1994.

D-6. Comments

Help to make this a better tool for evaluating internal controls. Submit comments to ASA(FM&C), (SAFM-FOM), 109 Army Pentagon, Washington, DC 20310-0109.

Glossary

Section I Abbreviations

AASA

Administrative Assistant to the Secretary of the Army

ACOM

Army Command

AR

Army Regulation

ARIMS

Army Records Information Management System

ASA(FM&C)

Assistant Secretary of the Army for Financial Management and Comptroller

ASCC

Army Service Component Command

AUM

assessable unit manager

DA

Department of the Army

DFAS-IN

Defense Finance and Accounting Service-Indianapolis

DOD

Department of Defense

DODD

Department of Defense Directive

DODI

Department of Defense Instruction

DODIG

Department of Defense Inspector General

DRU

Direct Reporting Unit

FMFIA

Federal Managers' Financial Integrity Act

GAO

Government Accountability Office

GS

General Schedule

HQDA

Headquarters, Department of the Army

ICA

internal control administrator

ICEP

Internal Control Evaluation Plan

ICOFR

internal control over financial reporting

IR

internal review

MIC Program

Managers' Internal Control Program

NSPS

National Security Personnel System

OMB

Office of Management and Budget

OSA

Office of the Secretary of the Army

SA

Secretary of the Army

SAFM-FOM

Secretary of the Army for Financial Management Comptroller

SAT

Senior Assessment Team

SLSG

Senior Level Steering Group

SRO

senior responsible official

USAAA

U.S. Army Audit Agency

Section II**Terms****Alternative internal control evaluation**

Any existing management review process that meets the basic requirements of an internal control evaluation that assesses the key internal controls, evaluates the controls by testing them, and provides the required documentation. These existing management review processes may be unique to a specific functional area or they may be generic, such as the Command Inspection Program or reviews by IR evaluators.

Assessable unit

Reporting organizations are segmented into assessable units, which in turn are responsible for conducting internal control evaluations in accordance with the ICEP.

Assessable unit manager (AUM)

The military or civilian head of an assessable unit. Preferably at the general officer or Senior Executive Service level, but not lower than an O-6, GS-15 or NSPS equivalent. In exceptional cases where the grade structure does not support having an AUM at this level, the AUM will be the senior military or HQDA civilian functional manager. The AUM ensures the results of required internal control evaluations are certified.

Financial statement reporting entity

For the Army, these include the General Fund, Army Working Capital Fund, and the Civil Works Fund (Corps of Engineers).

Government Accountability Office Standards for Internal Control in the Federal Government

The standards issued by the GAO to be applied by all managers in the Federal Government in developing, establishing and maintaining internal controls.

Headquarters, Department of the Army functional proponent

The HQDA principal responsible for policy and oversight of a particular functional area.

Internal control administrator (ICA)

The individual designated by the SRO to administer the MIC Program for a reporting organization. Assessable unit managers designate ICAs below the reporting organizational level.

Internal control evaluation

A periodic, detailed assessment of key internal controls to determine whether they are operating as intended. This assessment must be based on the actual testing of key internal controls and must be supported by documentation (that is, the individual(s) who conducted the evaluation, the date of the evaluation, the methods used to test the controls, any deficiencies detected and the corrective action taken).

Internal control evaluation plan

The written plan that describes how required internal control evaluations will be conducted over a five-year period. The ICEP need not be lengthy and any format may be used, so long as it covers the key internal controls HQDA functional proponents identified and communicates clearly to subordinate managers what areas are to be evaluated, who will conduct the evaluation, when and how.

Internal control over financial reporting (ICOFR)

The ICOFR is a process designed to provide reasonable assurance regarding the reliability of financial reporting. Reliability of financial reporting means that management can reasonably make the following assertions: (1) all reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date (existence and occurrence); (2) all assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (completeness); (3) all assets are legally owned by the agency and all liabilities are legal obligations of the agency (rights and obligations); (4) all assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation); (5) the financial report is presented in the proper form and any required disclosures are present (presentation and disclosure); (6) the transactions are in compliance with applicable laws and regulations (compliance); (7) all assets have been safeguarded against fraud and abuse; and (8) documentation for internal control, all transactions, and other significant events is readily available for examination.

Internal controls

The rules, procedures, techniques, and devices employed by managers to ensure that what should occur in their daily operations does occur on a continuing basis. Internal controls include such things as the organizational structure itself (designating specific responsibilities and accountability), formally defined procedures (for example, required certifications and reconciliations), checks and balances (for example, separation of duties), recurring reports and management reviews, supervisory monitoring, physical devices (for example, locks and fences), and a broad array of measures used by managers to provide reasonable assurance that their subordinates are performing as intended.

Key internal controls

Those internal controls that must be implemented and sustained in daily operations to ensure organizational effectiveness and compliance with legal requirements. Key internal controls are identified by HQDA functional proponents in their governing Army Regulations and establish the baseline requirement for internal control evaluations conducted by AUMs.

Material weakness

A material weakness is a significant deficiency, or combination of significant deficiencies, that result in a reasonable possibility that a material misstatement will not be prevented or detected. The absence or ineffectiveness of internal controls constitutes an internal control weakness. For an internal control weakness to be considered a material weakness, two conditions must be met. It must involve a weakness in internal controls, such as internal controls are not

in place, are not being used or they are inadequate and it must warrant the attention of the next higher level either for awareness or action. The determination of materiality is reevaluated at each successive level of command.

Reasonable assurance

An acceptable degree of confidence in the general adequacy of internal controls to deter or detect material failures in complying with the FMFIA objectives. The determination of reasonable assurance is a management judgment based upon the effectiveness of internal controls and the extent of internal control deficiencies and material weaknesses.

Reporting organization

The HQDA Staff agencies (less Secretariat elements covered by the AASA), ACOMs, ASCCs, and DRUs. These are the organizations that submit annual statements of assurance directly to ASA(FM&C) for the SA.

Risk

The probable or potential adverse effects from inadequate internal controls that may result in the loss of government resources through fraud, error, or mismanagement.

Risk assessment

The process of evaluating the risks in a functional area based on the key internal controls that are in place. Specifically, risk assessment is measuring two quantities of the risk, the magnitude of the potential loss, and the probability that the loss will occur. In addition, the key internal controls employed to reduce risk should not exceed the benefits derived.

Senior management council

A committee or board of senior functional officials convened to advise the head of an organization on internal control matters, including the identification of internal control weaknesses that merit reporting as material weaknesses. At HQDA, a senior management council is convened through special sessions of the Senior Level Steering Group chaired by the ASA(FM&C) and representing all HQDA functional proponents.

Senior responsible official (SRO)

Designated by the head of the reporting organization, the SRO has overall responsibility for ensuring the implementation of an effective MIC Program within that organization.

Test question

A question in an internal control evaluation designed to help an AUM determine whether a key internal control is in place and operating as intended.

Section III

Special Abbreviations and Terms

This section contains no entries.

UNCLASSIFIED

PIN 053422-000

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 261

PIN: 053422-000

DATE: 01- 7-10

TIME: 13:50:09

PAGES SET: 29

DATA FILE: C:\Wincomp\r11-2.FIL

DOCUMENT: AR 11-2

SECURITY: UNCLASSIFIED

DOC STATUS: REVISION