Headquarters
Department of the Army
Washington, DC
16 July 2024

Department of the Army Pamphlet 11–2

Army Programs

Risk Management and Internal Control Program

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant to the Secretary of the Army

History. This is a new Department of the Army pamphlet.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, the U.S. Army Reserve, and Department of the Army Civilians unless otherwise stated.

Proponent and exception authority. The proponent of this publication is the Assistant Secretary of the Army (Financial Management and Comptroller). The proponent has the authority to approve exceptions or waivers to this publication 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 publication 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 requirements.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to usarmy.pentagon.hqda-asa-fm.mbx.army-mngrs-internal-cntl-prog@army.mil.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

SUMMARY

DA Pam 11–2
Risk Management and Internal Control Program

This new publication, dated 16 July 2024—

- Provides detailed guidance for execution of the Risk Management and Internal Control Program (throughout).

- The procedures in this document cover the Internal Control Cycle and address requirements described in federal regulations governing internal control and risk management (throughout).

Contents (Listed by chapter and page number)

Chapter 1
Introduction

Section I

General

1–1. Purpose
This pamphlet provides information on how to plan, document, evaluate, remediate, and report on the Risk Management and Internal Control (RMIC) Program requirements. It provides procedures for executing policies established in AR 11–2. It contains instructions, processes, formats, reporting requirements, and guidelines used to carry out the Army's RMIC Program. While this pamphlet primarily addresses RMIC functions applicable to all Soldiers (Active, Reserve, and Guard) and Department of the Army (DA) Civilians, it also contains procedures on the management of agency, command, and installation level RMIC functions.

1–2. References, forms, and explanation of abbreviations
See appendix A. The abbreviations, brevity codes, and acronyms (ABCAs) used in this electronic publication are defined when you hover over them. All ABCAs are listed in the ABCA directory located at https://armypubs.army.mil/.

1–3. Associated publications
Policy associated with this pamphlet is found in AR 11–2.

1–4. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in the Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

Section II

Roles and Duties

1–5. Reporting organization
Office of the Secretary of the Army (SECARMY) elements/offices and Army Staff offices Headquarters, Department of the Army (HQDA), Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs) are the primary Reporting Organizations (ROs) in the Army RMIC Program. The Head of the Reporting Organization (HRO) will—

a. Accurately describe the organization's key risks, internal control evaluations, significant deficiencies, Material Weaknesses (MWs), and Corrective Action Plans (CAPs), the status of internal controls (including fraud prevention) within their organization.

b. Prepare an Annual Statement of Assurance (ASOA) feeder package for submission to the Director, Army Risk Management, in compliance with AR 11–2, ASOA guidance, supplemental guidance, and this pamphlet. The submission will include—

(1) An Assurance Memo that expresses an opinion (reasonable assurance, assurance, or unable to provide assurance) on the overall effectiveness of internal controls within the RO.
(2) Risk Assessment and Internal Control Evaluation Plan (ICEP).
(3) A complete Internal Control Evaluation appendix submission.
(4) Report on the status of new and prior-year MWs and significant deficiencies within the organization.
(5) Reportable Antideficiency Act (ADA) violations.
(6) RMIC Training Report.
(7) Listing of significant accomplishments within the RO.

(8) System owners report on the status of systems that generate financial information impacting the Army financial statements in accordance with 31 USC 3512, Public Law 104–208, OMB Circular No. A–123, M–13–23, Appendix D, and the Office of the Assistant Secretary of the Army (OASA) Financial Management and Comptroller (FM&C) annual financial management systems guidance.

(9) Any additional submissions deemed significant as required by AR 11–2 or submission requested by the Director, Army Risk Management.

1–6. Designated risk management and internal control roles

a. In accordance with AR 11–2, ROs will designate, in writing by an appointment memorandum, DA Soldiers and DA Civilians to perform the following RMIC Program roles, except for the HRO which is designated by position from the Director, Army Risk Management:

(1) Senior Responsible Official (SRO).

(2) Assessable Unit Managers (AUM) and Commanders.

(3) Internal Control Administrator (ICA).

(4) Internal Control Evaluator (ICE).

b. Designated ICAs of U.S. Army National Guard have responsibility for RMIC functions.

c. Contract personnel are prohibited from serving in the role of HRO, SRO, AUM, and ICA. The roles are inherently governmental and must be independent of the function assessed. Military personnel, Government employees, or contract support staff may perform the duties of the ICE if they are independent of the process under evaluation. Individuals fulfilling the role of the ICE may not perform the day-to-day duties or provide reviews and approvals associated with the control(s) under evaluation.

d. See figure 1–1 for the RMIC reporting structure. There are multiple SROs and AUMs within the Management-level depending on the RO's structure.

e. See figures 1–2, 1–3, 1–4, and 1–5, or sample appointment memorandums.

f. See paragraphs 1–8, 1–9, 1–10, 1–11, and 1–12 for HRO, SRO, AUM, ICA, and ICE duties.

g. Performance Appraisals and evaluations. The GAO–14–704G requires the Control Environment to have Management "evaluate performance and hold individuals accountable for their internal control responsibilities". Collectively, the requirements facilitate the assignment of authority and responsibility within the Control Environment to ensure results are achieved.

(1) Implementation. Supervisors of government employees will include an explicit statement of responsibility for internal controls in the performance appraisals and evaluations of commanders, SROs, AUMs, ICAs, and ICEs responsible for the execution or oversight of effective internal controls (including the assessable unit (AU) level). Supervisors will reference the objectives outlined in the applicable duties and appointment memos for incorporation into performance appraisals and evaluations. If the appropriate military or civilian performance evaluation system cannot accomplish this task, an appointment memo will suffice. The absence of an explicit statement is only acceptable when a supervisor determines the individual does not possess significant internal control management responsibilities.

(2) Application. The explicit statement of responsibility is brief, may take any form, and is explicit 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.

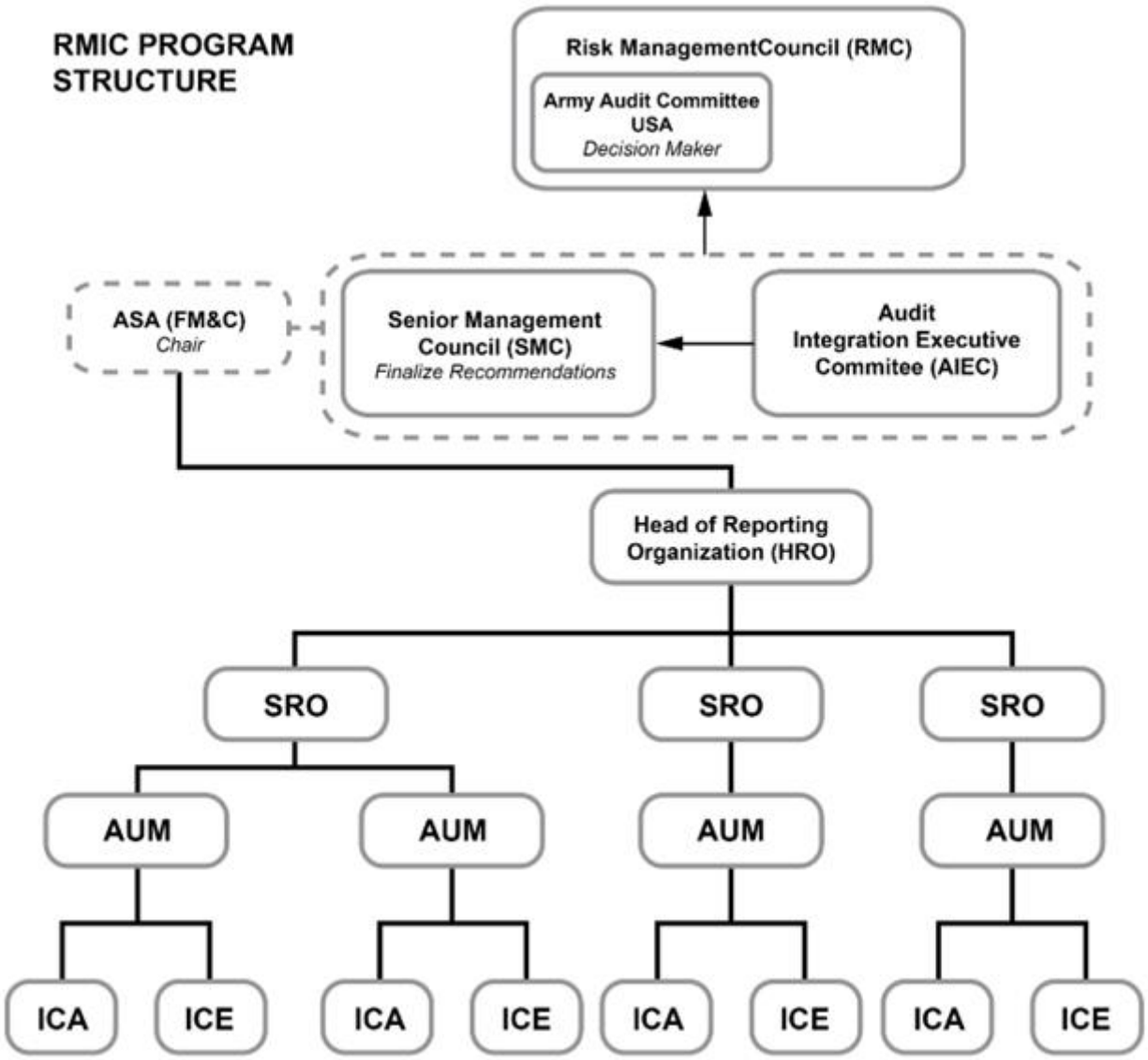


Figure 1–1. Risk Management and Internal Control Reporting Structure

1–7. Head of the reporting organization duties

The HRO is designated by position and does not require an appointment memorandum. The HRO is responsible for executing the RMIC Program within their respective organization by understanding and applying the GAO standards for internal control in the Federal Government, carrying out the RMIC Program within their respective organization, and will—

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

b. Appoint the SROs and AUMs to ensure the effective implementation of the RMIC Program. This appointment is evidenced with an appointment letter signed by the HRO.

c. Appoint ICA(s) to administer RMIC activities within the RO to serve as the organizational lead administrators for all internal control matters.

d. Designate or appoint ICE(s) to conduct monitoring of internal controls reported in the ICEP and evaluate the effectiveness of internal controls. This is not an inherently governmental role and the ICE must

be independent of the function assessed. Only DA Soldiers and Civilians can be appointed. Contractors are designated.

e. Ensure all appointed roles are appointment by memorandum are trained and to ensure they understand their internal control responsibility in accordance with Section II of this pamphlet.

f. Designate the AUs within the organization and provide updates to the Director, Army Risk Management.

g. Ensure programs and functions establish and maintain effective internal controls and identify in ARs the key internal controls that require formal evaluation as stated in AR 25–30.

h. Periodically review associated ARs to identify and implement changes related to the internal control process and to support the five-year publication lifecycle in accordance with DA Pam 25–40.

i. Ensure the application of financial risk management is present in risk assessments and as required by the Director, Army Risk Management.

j. Execute a prioritized assessment of the organization's risks in accordance with the ASOA guidance issued at the beginning of the Fiscal Year (FY).

k. Concur on the RO's ICEP. The Principal Deputy or SRO may sign for the HRO in their absence.

l. 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. Report potential MWs to HQDA through command channels in a timely manner.

m. Implement corrective actions to correct MWs, significant deficiencies and control deficiencies. Report on corrective actions deemed significant accomplishments in the annual ASOA.

n. Sign and submit an ASOA feeder package to the Director, Army Risk Management. The Principal Deputy may sign for the HRO in their absence. In the case a Principal Deputy must sign, organizations must provide justification as to why the appointed personnel is not available to sign.

1–8. Senior responsible official duties

The HRO will appoint SRO(s) responsible for the organization's implementation of an effective RMIC Program (see fig 1–2). https://armyeitaas.sharepoint-mil.us/sites/asa-fmc-afsa/sitepages/rmichome.aspx. The SRO(s) will perform the following duties:

a. Ensure the effective implementation of the RMIC Program within the organization.

b. Advise the HRO on the implementation and status of the organization's RMIC Program and support needed to promote an effective RMIC Program.

c. Appoint AUM(s) to provide oversight of the organization's RMIC and ensure proper execution of functions.

d. Appoint ICA(s) to administer RMIC activities within the RO to serve as the organizational lead administrators for all internal control matters. This appointment is evidenced with an appointment letter signed by the SRO.

e. Designate or appoint ICE(s) to conduct monitoring of internal controls reported in the ICEP and evaluate the effectiveness of internal controls. This is not an inherently governmental role and must be independent of the function assessed. Only DA Soldiers and Civilians can be appointed. Contractors are designated.

f. Oversee execution of a risk assessment of the organization's strategic and business process risks and provide concurrence on the ICEP.

g. Review the ASOA to ensure compliance with annual guidance and supplemental guidance, accurate description of the organization's key strategic risks, internal control evaluations, significant deficiencies, MWs, and related CAPs, the status of internal controls (including fraud prevention) within their organization, and any additional supporting information requested by the Director, Army Risk Management.

h. Report on the status of internal control program functional areas to the Director, Army Risk Management upon request.

i. Complete the RMIC Role Based Training course located in the Army Learning Management System (ALMS) no later than 60 days from the date of this memorandum unless taken within the past two years. Refresher training is required to be taken every 2 years.

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

[OFFICE SYMBOL] [DD Month YYYY]

MEMORANDUM FOR [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_ NAME]

SUBJECT: Fiscal Year [YYYY] Appointment of Senior Responsible Officials for the Risk Management and Internal Control (RMIC) Program – [Organization's Name]

1. References:

   a. AR 11-2 (RMIC Program), DD Month YYYY.

   b. DA PAM 11-XX (RMIC Program Execution), DD Month YYYY.

2. As Head of the Reporting Organization (RO) for the [Organization Name]'s execution of the internal control program, I hereby appoint the following to serve as the [Senior Responsible Officials (SROs) or Senior Responsible Official (SRO)] at each organization effective as of this memorandum's signature date. The appointment is valid until revoked:

   a. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

   b. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

3. The minimum SRO duties are outline in DA PAM 11-XX, Section 1-8. Additional duties are listed below:

   a. [Add Additional Duties]

[Title First_Name Last_Name]
[RMIC_Role_Title]
[Organization_Name]

DISTRIBUTION:
[ORGANIZATION_NAME]

Figure 1–2. Senior Responsible Official Memo Template

1–9. Assessable unit managers and commanders

The HRO or SRO will appoint an AUM, https://armyeitaas.sharepoint-mil.us/sites/asa-fmc-afsa/sitepages/rmichome.aspx, to perform the following duties (see fig 1–3):

a. Appoint ICA(s) to administer RMIC activities within the AU and provide the leadership and support needed to ensure the RMIC Program is implemented and operating effectively. This appointment is evidenced with an appointment letter signed by the AUM.

b. Designate or appoint ICE(s) to conduct monitoring of internal controls reported in the ICEP and evaluate the effectiveness of internal controls. This is not an inherently governmental role and must be independent of the function assessed. Only DA Soldiers and Civilians can be appointed. Contractors are designated.

c. Complete the RMIC Role Based Training course located in the ALMS no later than 60 days from the date of this memorandum unless taken within the past two years. Refresher training is required to be taken every two years.

d. Ensure that—

(1) ICAs and ICEs are trained and understand their internal control responsibilities. Refresher training is conducted every other year, or more frequently at the discretion of the Commander, to keep up to date with changes in the operational environment, laws, policies, directives from higher Headquarters (HQs), as well as any time the organization has been impacted by turnover in managers, the ICA, or significant personnel rotations. Further training requirements may be communicated by the Director, Army Risk Management.

(2) Managers identify internal and external risks that may prevent their organizations from executing their mission, potentially impacting operational excellence. Managers also establish or enhance internal controls to mitigate identified risks and ensure their effectiveness. Risk assessment instructions are provided by the Director, Army Risk Management in the annual RMIC guidance.

(3) An ICEP is established utilizing the annual risk assessment, prior-year results, inspections, and other audits, which may be certified by the AUM or Principal Deputy.

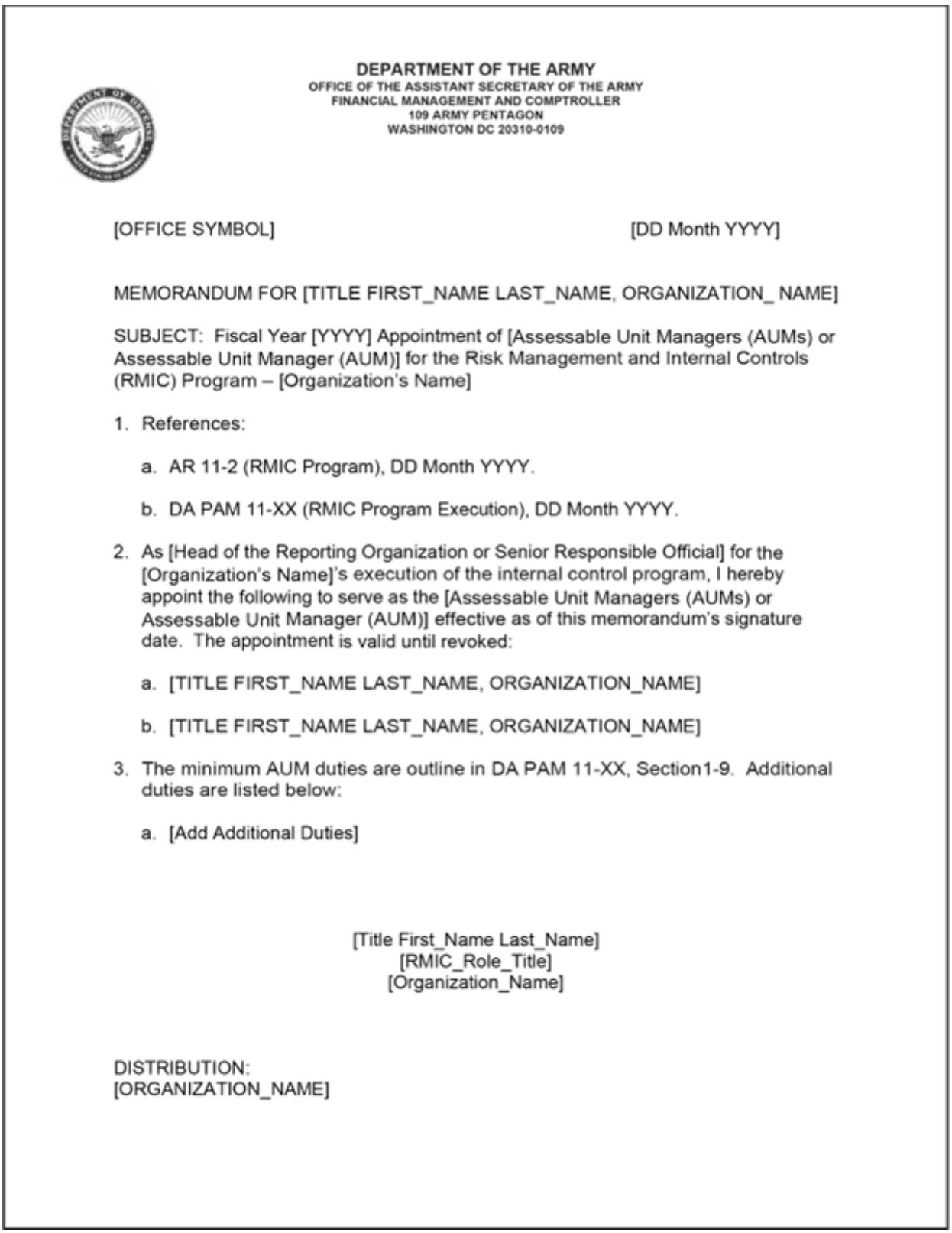
(4) Internal control evaluations are conducted according to the ICEP, the requirements of AR 11–2, and annual guidance issued by the Director, Army Risk Management.

(5) Required documentation on each completed internal control evaluation is retained, subject to audit and/or inspection.

(6) The AUM certifies the results of required internal control evaluations in DA Form 11–2 (Internal Control Evaluation Certification). When necessary, this responsibility can be delegated to the Principal Deputy only.

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

f. Sign and submit to the next higher command-level an ASOA feeder package for the AU. The Principal Deputy may sign for the AUM.



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
FINANCIAL MANAGEMENT AND COMPTROLLER
109 ARMY PENTAGON
WASHINGTON DC 20310-0109

[OFFICE SYMBOL] [DD Month YYYY]

MEMORANDUM FOR [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_ NAME]

SUBJECT: Fiscal Year [YYYY] Appointment of [Assessable Unit Managers (AUMs) or Assessable Unit Manager (AUM)] for the Risk Management and Internal Controls (RMIC) Program – [Organization's Name]

1. References:

   a. AR 11-2 (RMIC Program), DD Month YYYY.

   b. DA PAM 11-XX (RMIC Program Execution), DD Month YYYY.

2. As [Head of the Reporting Organization or Senior Responsible Official] for the [Organization's Name]'s execution of the internal control program, I hereby appoint the following to serve as the [Assessable Unit Managers (AUMs) or Assessable Unit Manager (AUM)] effective as of this memorandum's signature date. The appointment is valid until revoked:

   a. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

   b. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

3. The minimum AUM duties are outline in DA PAM 11-XX, Section1-9. Additional duties are listed below:

   a. [Add Additional Duties]

[Title First_Name Last_Name]
[RMIC_Role_Title]
[Organization_Name]

DISTRIBUTION:
[ORGANIZATION_NAME]

Figure 1–3. Assessable Unit Managers Memo Template

1–10. Internal control administrator duties

The HRO, SRO, or AUM will appoint an ICA, https://armyeitaas.sharepoint-mil.us/sites/asa-fmc-afsa/sitepages/rmichome.aspx, to perform the following duties (see fig 1–4):

a. Advise the SRO or AUM on the implementation and status of the organization's RMIC Program and keep commanders and managers informed on internal control matters.

b. Identify and arrange the organization's requirements for RMIC trainings.

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 MWs, significant deficiencies, and control deficiencies.

e. Prepare an ASOA feeder package for signature by the HRO, commander, or Principal Deputy and ensure transmission to the Director, Army Risk Management, in compliance with annual guidance. The ASOA feeder package must accurately describe the status of internal controls over operations, reporting, and compliance within their organization, report on the level of assurance of whether controls are in place, effective, and provide updated MWs (in the required format) reported throughout the year.

f. Ensure that MWs reported in the ASOA are closely monitored until corrected and retain all required documentation supporting the ASOA and the correction of MWs.

g. Complete the RMIC Role Based Training course located in the ALMS no later than 30 days from the date of this memorandum unless taken within the past two years. Refresher training is required to be taken every 2 years.

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
FINANCIAL MANAGEMENT AND COMPTROLLER
109 ARMY PENTAGON
WASHINGTON DC 20310-0109

[OFFICE SYMBOL] [DD Month YYYY]

MEMORANDUM FOR [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_ NAME]

SUBJECT: Fiscal Year [YYYY] Appointment of [Internal Controls Administrators (ICAs) or Internal Controls Administrator (ICA)] for the Risk Management and Internal Controls (RMIC) Program – [Organization's Name]

1. References:

   a. AR 11-2 (RMIC Program), DD Month YYYY.

   b. DA PAM 11-XX (RMIC Program Execution), DD Month YYYY .

2. As [Head of the Reporting Organization or Senior Responsible Official or Assessable Unit Manager] for the [Organization's Name]'s execution of the internal control program, I hereby appoint the following to serve as the [Internal Control Administrators (ICAs) or Internal Control Administrator (ICA)] effective as of this memorandum's signature date. The appointment is valid until revoked:

   a. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

   b. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

3. The minimum ICA duties are outline in DA PAM 11-XX, Section 1-10. Additional duties are listed below:

   a. [Add Additional Duties]

[Title First_Name Last_Name]
[RMIC_Role_Title]
[Organization_Name]

DISTRIBUTION:
[ORGANIZATION_NAME]

Figure 1–4. Internal Control Administrator Memo Template

1–11. Internal control evaluator duties

The HRO, SRO, or AUM will appoint an ICE, https://armyeitaas.sharepoint-mil.us/sites/asa-fmc-afsa/sitepages/rmichome.aspx. This is not an inherently governmental role, and the ICE must be independent of the function assessed. Only DA Soldiers and DA Civilians require an appointment memorandum (see fig 1–5). Contractors may be designated to serve in this role. The ICE is to perform the following duties:

a. Conduct monitoring of internal controls reported in the ICEP and evaluate the effectiveness of internal controls in accordance with the RMIC ASOA Guidance.

b. Identify any internal control or systemic weakness that may merit reporting as internal controls deficiencies, significant deficiencies, or MWs based on ICEP processes.

c. Gather and analyze information to support conclusions about the effectiveness of the internal controls over operations, reporting, and compliance at the RO.

d. Perform independent evaluations over internal controls and processes for which the ICE does not execute the day-to-day functions or provide approval/reviews for processes in which controls are under evaluation.

e. Document evidence of the assessment in DA Form 11–2 (Internal Control Evaluation Certification) for key processes and mission-critical controls outlined in the RO or AU's ICEP.

f. Notify the SRO, and/or applicable AUMs and ICAs, on the status of their evaluation and findings that may warrant reporting in their RO's ASOA feeder package.

g. Communicate any recommendations to the AUM for coordination with the RO leadership.

h. Provide technical advice, assistance, and consultation to the entity under review on internal controls, routine business matters, accounting matters as an ancillary part of a financial audit, and/or matters within their educational and technical expertise.

i. Ensure results of monitoring from internal control evaluations and supporting documentation are maintained and available for audit.

j. Complete the RMIC Role Based Training course located in the ALMS no later than 30 days from the date of this memorandum unless taken within the past two years. Refresher training is required to be taken every 2 years.

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
FINANCIAL MANAGEMENT AND COMPTROLLER
109 ARMY PENTAGON
WASHINGTON DC 20310-0109

[OFFICE SYMBOL] [DD Month YYYY]

MEMORANDUM FOR [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_ NAME]

SUBJECT: Fiscal Year [YYYY] Appointment of [Internal Controls Evaluators (ICEs) or Internal Controls Evaluator (ICE)] for the Risk Management and Internal Controls (RMIC) Program – [Organization's Name]

1. References:

   a. AR 11-2 (RMIC Program), DD Month YYYY.

   b. DA PAM 11-XX (RMIC Program Execution), DD Month YYYY.

2. As [Head of the Reporting Organization or Senior Responsible Official or Assessable Unit Manager] for the [Organization's Name]'s execution of the internal control program, I hereby appoint the following to serve as the [Internal Control Evaluators (ICEs) or Internal Control Evaluator (ICE)] effective as of this memorandum's signature date. The appointment is valid until revoked:

   a. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

   b. [TITLE FIRST_NAME LAST_NAME, ORGANIZATION_NAME]

3. The minimum ICE duties are outline in DA PAM 11-XX, Section 1-11. Additional duties are listed below:

   a. [Add Additional Duties]

[Title First_Name Last_Name]
[RMIC_Role_Title]
[Organization_Name]

DISTRIBUTION:
[ORGANIZATION_NAME]

Figure 1–5. Internal Control Evaluator Memo Template

1–12. Army service providers

Service providers supporting Army are responsible for providing assurances and communicating the relationship between the service provider's controls and Army's user controls. The Army and the service provider collectively manage the risks of third-party provider activities through Service Organization Control (SOC) 1 Type 2 reporting, also referred to as the Statement on Standards for Attestation Engagement No. 18 report. An assessment of third-party service provider internal controls is part of a comprehensive effort to evaluate both the controls over reliability of reported financial data. Army service providers will—

a. Conduct analysis and review of financial reporting processes and conduct risk assessments; where applicable, modify, or implement new internal controls to mitigate the changing environment.

b. Prepare and submit reports as required by the Director, Army Risk Management, in adherence to OMB (Office of Management and Budget) Circular No. A–123 appendices and memorandums.

c. Coordinate with their RO to report on the results of testing for incorporation into the ASOA feeder package.

1–13. Commanding General, United States Army Corps of Engineers

The Commanding General, United States (US) Army Corps of Engineers (USACE) will submit a certification as part of the compliance assertion that provides reasonable assurance with no exceptions, assurance with exceptions, or unable to provide assurance for Corps of Engineers Financial Management System II.

1–14. Independent external auditor

31 USC 501, Public Law 101–576 (Chief Financial Officers (CFO) Act of 1990, Sec. 304) requires agency financial statements to be audited in accordance with Generally Accepted Accounting Principles (GAAP) by the Inspector General (IG) or an independent external auditor as determined by the IG or head of the agency. The IG or independent external auditor will issue an audit report to the agency head and Comptroller General.

Section III

Risk Management and Internal Control Cycle Overview

1–15. Internal control cycle

Every Department of Army employee is inherently responsible for safeguarding Federal assets and the efficient delivery of military services. Army leaders and managers are responsible for establishing goals and objectives for operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unanticipated events. The Army is responsible for implementing management practices that identify, assess, respond, and report on risks. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats, and identify previously unknown opportunities to improve the efficiency and effectiveness of government operations. In accordance with OMB Circular No. A–123 M–16–17, the Army is responsible for establishing and maintaining an internal control program that mitigates risks aligned to the SECARMY priority objectives in addition to risks to operations, reporting, and compliance. Risk mitigation occurs through the implementation of internal controls. Internal controls are policies, procedures, and other mechanisms in place to ensure an organization, function, program, or activity's mission is achieved. Examples of control activities include segregation of duties and secondary reviews/reconciliations. Army's ROs rely on internal controls to provide reasonable assurance of effective and efficient operations and compliance with applicable laws and regulations. The RMIC Program consists of five phases (see fig 1–6) that are discussed in further detail in the next sections of this pamphlet: Planning, Documentation, Testing, and Evaluation, Remediation, and Validation, and Reporting.

a. The Planning Phase includes identifying the program scope through materiality and a risk-based approach. This entails identifying risks to achieving the SECARMY's priority objectives by conducting a risk assessment on material financial and non-financial processes to the RO, as well as incorporating other areas of interest and those required by regulation.

b. The Documentation Phase focuses on capturing the lifecycle of business processes to identify controls in place and control gaps. This is accomplished by documenting end-to-end processes in narratives, process maps, completing a risk and control matrix (RCM), capturing controls in the Army Control Catalog

(ACC), and so forth. The Documentation Phase also incorporates an evaluation of the controls in place to determine if they are designed correctly to prevent or detect the associated risk.

c. The Testing and Evaluation Phase leverages a risk-based approach to conduct evaluations to determine if a control is operating effectively to mitigate the risk and determine the extent and consistency to which controls are applied in the execution of the process.

d. The Remediation and Validation Phase is implemented when control failures occur, and CAPs are created to document milestones to outline a remediation strategy for the control failure. Validation occurs only after all milestones are met and supporting documentation indicating the root cause of the control failure is in fact remediated.

e. The Reporting Phase requires Army to provide assertions over the operational effectiveness of internal controls in accordance with Public Law 97–255 and OMB Circular A–123, M–18–16, Appendix A. This information is reported in the ASOA submission with the accompanying appendices that provide additional support to substantiate the assertions reported and the status of the overall program.

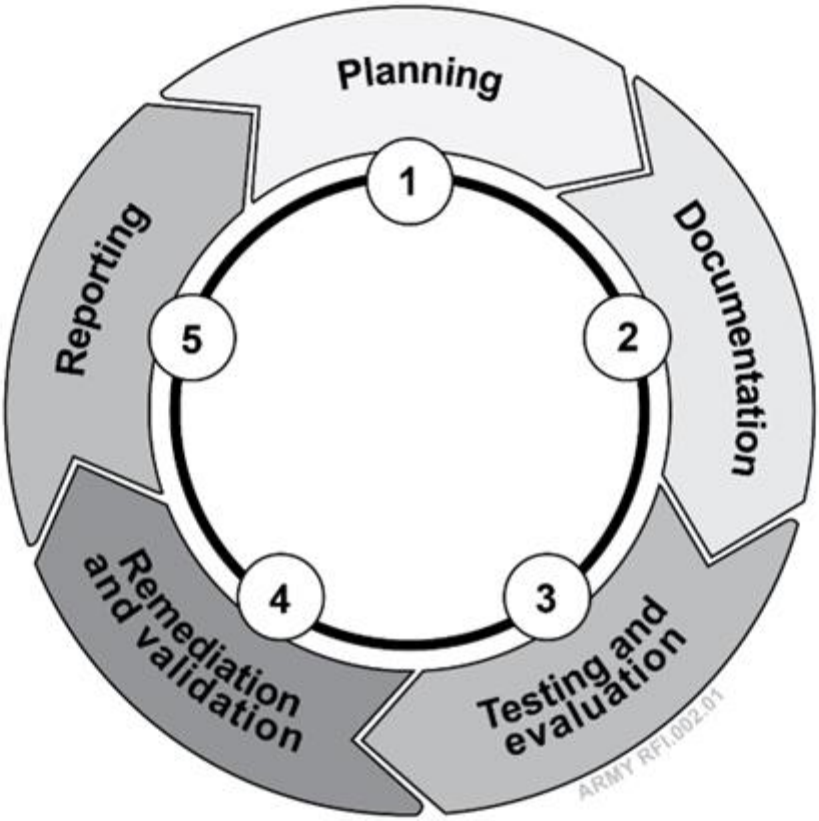


Figure 1–6. Risk Management and Internal Control Cycle

Chapter 2
Planning

2–1. Materiality

Materiality is defined as the threshold by which information, if omitted or misstated, could influence economic decisions users make based on presented information. Therefore, materiality is a factor leveraged in the Planning Phase, along with risk identification, to scope the financial areas of focus. The Army Audit Committee, with the support of the Director, Army Risk Management, will determine the financial materiality threshold for Army on an annual basis in accordance with OMB Circular No. A–123 M–18–16,

Appendix A, and the Generally Accepted Government Auditing Standards. The methodology is documented and includes the rationale and basis for the materiality assessment. Financially material business processes are identified and communicated in the ASOA guidance for ROs to execute in their internal control testing. Materiality is defined in both financial and non-financial terms based on quantitative and qualitative factors. Informed judgements regarding materiality are made based on awareness of circumstances along with the understanding of the size and nature of a potential event. Financial-related materiality is based on missing or incorrect information in financial statements or documents which could influence the decisions made by Army's leadership and its stakeholders. Non-financial materiality includes areas significant to Army that may impact the organization's reputation or mission-critical operations.

a. The Assistant Secretary of the Army (ASA) FM&C conducted the following activities to identify materiality beginning in FY2021—

(1) Determining Planning Materiality. The GAO–18–601G defines financial materiality as a percentage threshold for planning purposes. To determine planning materiality for the current year, the Director, Army Risk Management, will examine Army's financial position from the prior-year's financial statements, and assess a percentage based upon best practices. This information is used to determine the material and relevant financial statement line items.

(2) Significant Financial and Non-Financial Reporting Elements. The Director, Army Risk Management, will identify the significant financial reporting elements that pose the highest risk to producing reliable financial statements by evaluating individual accounting line items separately and in aggregate for materiality and risks. The Director, Army Risk Management, will establish the threshold used to determine significant financial accounts (based on audit best practices). The Army Audit Committee and ROs will establish the thresholds for non-financial areas deemed significant for reviews. Consideration will be given to reports and findings issued by the GAO Office of the IG, Department of Defense (DoD) IG, Department of the Army Inspector General (DAIG), US Army Audit Agency (USAAA), local IGs, Internal Review (IR), the independent external auditor, and ROs.

(3) Map Material Areas to ROs. The Director, Army Risk Management, will map the material financial areas to ROs based on the process, function, or program. The materiality threshold is communicated to Army's ROs at the beginning of the RMIC year (as defined in the annual RMIC guidance) to ensure internal control evaluations are conducted on material areas during the year.

b. ROs will incorporate areas material to their organization within the ICEP and conduct internal control evaluations over the respective areas in accordance with the procedures listed in the Testing and Evaluation Section.

2–2. Enterprise risk management

a. Enterprise Risk Management. Enterprise Risk Management (ERM) informs better decision-making, broadens senior leaders' views across a portfolio of risks, illustrates linkages between risks, and provides improved insight to prioritize and manage key risks to mission delivery more effectively. The SECARMY will support the Office of the Secretary of Defense (OSD) efforts to conduct an annual performance and strategic review that incorporates risk identification and analysis in accordance with OMB Circular No. A–123, M–16–17 ERM requirements and OMB Circular No. A–11's requirements for Performance and Strategic Reviews. The SECARMY is responsible for setting the tone at the top for ERM and ensuring expectations are communicated throughout the Army. ERM facilitates the Army's management activities through integration of risk management to support strong and effective internal controls within the Army's operations. The SECARMY will report to OSD the Army's strategic objectives for priority areas outlined in the Army's Strategy and identify key enterprise risks aligned to the execution of priority areas. The unclassified information is captured in the Armywide risk profile.

b. Risk Profiles. Risk profiles provide analysis of the risks an agency encounters pursuing strategic objectives that arise from its activities and operations and identifies the appropriate options for addressing significant risks. The Armywide risk profile prioritizes significant risks and considers risk from a portfolio perspective by identifying sources of uncertainty, both positive (opportunities) and negative (threats). The identification, measurement, and assessment of the organization's risk related to mission delivery should provide the framework for Army's senior leaders to determine reasonable assurance that the objectives are met, and that Army can organize, train, equip, prepare, and maintain readiness. A risk profile provides a comprehensive view that will enhance Army's ability to identify significant organizational risks, understand the combined impact of those risks, and facilitate the development of the appropriate responses. The Army Audit Committee will govern the risk management functions for Army in compliance with OMB

Circular No. A–123 M–16–17 and OSD by providing oversight for Army's risk profile. The Army Audit Committee will oversee the completion of the risk assessment on an annual basis, at minimum, and revisit throughout the year, as appropriate. The Army's enterprise risk profile will incorporate risk ratings for likelihood of occurrence and impact of each identified risk and identify activities that mitigate the impact to the Army's operations. The following paragraphs will provide a high-level overview of risk identification and evaluation–

c. Determining Acceptable Level of Risk. An acceptable level of risk is determined by identifying the risk tolerance and risk appetite. The risk appetite is the limitation to the amount and type of risks the Army is willing to accept to execute its mission. Risk tolerance is the level of variance the Army will accept in meeting its objectives if the risks were to materialize.

(1) The Army Audit Committee will determine the risk appetite by identifying limitations to the amount and type of risks the Army is willing to accept to execute its mission.

(2) The HRO will determine the risk tolerance for their respective organization and the AU based on the RMIC guidance, with approval from the Army Audit Committee.

(3) Consideration is given to the risk appetite and risk tolerance when the Army Audit Committee and ROs determine their response to risks.

d. Aligning Risks to Objectives. The SECARMY will communicate strategic objectives (priority areas) throughout the organization. ROs will complete a risk assessment inclusive of strategic, operations, reporting, and compliance risks (for their AUs). RO's will identify risks for the following objectives:

(1) Strategic objectives are aligned to both the Army's and the RO's mission and strategic goals.

(2) Operations objectives are aligned to the efficient and effective consumption of the Army and the RO's resources in the execution of administrative and program operations (to include fraud and financial).

(3) Reporting objectives are aligned to the reliability of data leveraged to produce the Army's and the RO's reports (that is, financial reports, performance reports, and so forth).

(4) Compliance objectives are aligned to compliance activities with applicable laws and regulations (to include financial management systems).

e. Fraud. Considering fraud in the risk assessment is one of the first proactive steps to prevent, detect, or monitor fraud.

f. Risk Profile - Risk Identification. The Army Audit Committee and ROs will continuously identify inherent risks for the objectives identified in paragraph 2–2*b.* of this section along with the accompanying residual risks. Inherent risk represents the risk of an activity occurring when internal controls are not in place. Residual risk is the risk that remains once a control is applied. Once inherent and residual risks are identified, the Army Audit Committee and ROs will reevaluate the risks to identify and incorporate emerging matters and changes to the control environment. ROs will properly assess each risk using a clearly defined metric, as instructed by the Director, Army Risk Management, in the annual guidance, to evaluate likelihood of occurrence and impact to the RO's mission. Risks are documented in a clear and concise manner to easily identify priority areas and facilitate monitoring.

(1) The RO is responsible for evaluating the risk assessment results from all AUs into one consolidated assessment that is representative of the RO, unless otherwise directed by the Director, Army Risk Management.

(2) Prior to final submission of the risk profile to the Director, Army Risk Management, the RO will brief the HRO for endorsement to ensure the risk profile is representative of the RO.

g. Risk Profile - Risk Response. Identification of a risk response will inform decision-making within Management's processes such as strategic reviews, Army policies, operations planning, and budget formulation. Considering the selected risk appetite and risk tolerance levels discussed in paragraph 2–2*a*. of this section, the HRO will assess their response to the identified risks utilizing one of the Risk Response Categories—

(1) Acceptance of a risk entails that action will not be taken by the RO to respond to a risk.

(2) Avoidance of a risk requires action to be taken to no longer perform the activity within the operational process causing the risk.

(3) Reduction of a risk implies the RO will reduce the likelihood of occurrence or impact to the Army's mission. When suitable, risk reduction is the preferred method.

(4) Sharing risks implies the operation involving the risk is transferred internally or external to Army or shared across the entire organization.

h. Risk Profile Review. The Army Audit Committee and ROs will annually reassess the Armywide risk profile and determine if the risk response is still applicable, identify new risks, or assess if the likelihood

and impact have changed for previously identified risks. On an annual basis the Director, Army Risk Management, will perform the following activities:

(1) Implement a risk management review process to evaluate the efficiency of the risk identification process.

(2) Validate if new or emerging risks are appropriately communicated to senior leadership.

i. Risk Profile - Proposed Action. The RO will develop internal controls for risks that Management determined the appropriate response to be acceptance, sharing, or reduction. This risk assessment will influence the frequency of internal control monitoring and scope planned for future years by each RO's Management.

j. Fraud Risk Working Group. The Fraud Risk Working group will be established to ensure that the Army has a robust and effective fraud risk management program in place. The working group's primary purpose is to identify, assess, and manage fraud risks within the Army.

2–3. Risk identification and assessment

A risk assessment is an iterative process that identifies and evaluates existing and potential risks (threats and hazards) to an organization from achieving its strategic objectives by affecting its assets, operations, and/or processes. Risk assessments standardize an organization's approach to risk and vulnerability identification, facilitates risk prioritization, and prompts the documentation and realization of current and planned risk responses (risk mitigation). These risk responses/mitigations are the organizations' internal controls. While organizations cannot respond to all risks, they must identify, measure, assess, and prioritize risks related to mission achievement. While a single iteration of the risk assessment is required to be reported annually to the RMIC Program, risk identification and assessments should be performed continuously throughout the year per OMB Circular No. A–123 M–16–17. The RO will execute the following functions for the risk assessment—

a. Align identified risks to the Secretary of the Army strategic objectives.

(1) Indicate if the risk is linked to a strategic priority.

(2) Identify if the risk is associated with a financial or non-financial business process.

b. Conduct an inherent risk assessment.

(1) Inherent risk represents the risk of an activity occurring when internal controls are not in place. The assessment will include determining the likelihood of occurrence and its potential impact.

(2) The evaluator will indicate the current risk response using one of the following risk response categories, and provided a description of activities aligned with the response—

(a) Acceptance of a risk entails that action will not be taken by the RO to respond to a risk.

(b) Avoidance of a risk requires action to be taken to no longer perform the activity within the operational process causing the risk.

(c) Reduction of a risk implies the RO will reduce the likelihood of occurrence or impact to the Army's mission through implementation of internal controls, training, or other risk mitigation actions. Risk reduction is the preferred method.

(d) Sharing risks implies the operation involving the risk is shared between different Army entities.

c. Conduct a residual risk assessment.

(1) Residual risk is the risk that remains once a control is applied. The assessment will include determining the likelihood of occurrence and its potential impact.

(2) The assessor will indicate a proposed risk response which includes identification of the existing management process that will be used to implement and monitor proposed actions. This may include actions communicated during the Army's strategic review process and budgeting process. The proposed risk response is usually leveraged when actions aligned to the current risk response have not been met.

d. Fraud. It is imperative to understand the causes of fraud – pressure and incentive, opportunity, and rationalization which are commonly referred to as the fraud triangle. Conducting a risk assessment that incorporates fraud mitigation allows management to actively identify and assess what types of fraud risks their organization is susceptible to, and to evaluate whether internal controls are in place to prevent or detect these risks. This process provides management with the opportunity to address significant fraud risks and consider potential actions to reduce and mitigate the likelihood and impact of those risks. Fraud risk management is an ongoing process and ROs should leverage the leading practices in the GAO Fraud Risk Management Framework (GAO–15–593SP) to perform assessment updates on a recurring basis and/or when there are significant changes to functions and processes within the Army. Fraud considerations include—

(1) Fraudulent financial statements and other false reporting. Intentionally misstating or manipulating the financial statements or other non-financial reports to potentially make an organization appear to be more or less profitable; more stable or creditworthy; or to otherwise deceive or mislead internal or external users of this financial or other reporting information.

(2) Misappropriation of assets. The theft or misuse of organizational assets for a direct or indirect benefit.

(3) Corruption. An individual using his or her influence to obtain unauthorized benefits for the individual and/or their organization contrary to that individual's duty to his or her organization.

(4) When evaluating fraud ROs should consider risks related to payroll, beneficiary payments, grants, large contracts, information technology (IT) and security, asset safeguards, and purchase, travel, and fleet cards; and, collecting, and analyzing data from reporting mechanisms on detected fraud to monitor fraud trends.

(5) Risk associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of Personally Identifiable Information.

(6) Fraud risk in strategic plans ensure the Army professionals involved in planning for, reviewing, awarding, and managing deliverables under contract and throughout the acquisition lifecycle receive training on fraud indicators and risks.

(7) Review of budget authority from sources such as appropriations legislation and identify any areas in which there is a risk of violating the ADA.

2–4. Prior-year findings and internal/external Reports

The HRO should avoid duplicating reviews which assess internal controls by coordinating efforts with other internal control activities to the extent possible. Consider the following types of information when planning evaluations—

a. Prior-Year Deficiencies. Managers must consider deficiencies at the RO level reported in the previous year, as well as prior-year Army and DoD challenges. The following factors must be considered—

(1) Any changes that have affected the nature of the deficiencies.

(2) Whether critical milestones reported the previous year still appropriately describe the corrective actions to be taken and progress toward meeting the milestones are on schedule.

(3) Whether the root causes have been fixed for deficiencies that are now considered resolved.

b. Current Year Evaluations and Information. Managers must consider available current year information to determine whether any new deficiencies have surfaced, or any previously undetected deficiencies exist. The following information must be considered—

(1) Current year internal and external reviews, audits, appraisals, and other types of evaluations and any deficiencies that were disclosed.

(2) Activity reports and other existing mechanisms for reporting to management and any deficiencies that were disclosed.

(3) Day-to-day knowledge of the program or administrative functions that would indicate whether deficiencies exist.

(4) Deficiencies identified through ongoing improvement-related initiatives.

(5) Deficiencies uncovered by reviews or audits in other areas that may also exist in the program or administrative function being evaluated.

(6) Information on the status of contractor quality and performance.

c. Use of Audit, and Inspection Reports. Consideration should be given to reports issued by GAO Office of the Inspector General (OIG), DoDIG, DAIG/USAAA, local IGs, IR, and the independent external auditor ROs can often coordinate internal control evaluation planning actions based on control weaknesses identified in GAO OIG/DoDIG/DAIG/USAAA/local IGs/IR/independent external auditor audits or inspection reports, and RO findings. ROs are encouraged to incorporate the results into their risk assessment and ICEP activities. 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.

d. Strategic Plans, Budgets, Annual Performance Plans, and Customer Needs. The strategic plan, budget, annual performance plans, and needs of customers are critical information that must be considered in determining whether deficiencies exist. The following factors should be considered—

(1) Difficulties in meeting the goals and/or objectives in the RO or the Army's strategic plan.

(2) Difficulties in achieving the performance targets in the RO or the Army's performance plans.

(3) Deficiencies for which funding has been requested and/or identified in the budget, and deficiencies in meeting customer needs.

2–5. Internal control evaluation plan

The ICEP is the written plan that captures internal control evaluations within the RO over a 5-year period (covering the current year and following 4 years). Each RO's ICEP captures the planned internal control evaluations for all internal controls identified in the RO's risk assessment. The risk assessment and ICEP will demonstrate a clear link between the RO's risks, the internal controls mitigating those risks, the frequency of the internal control evaluations, and the evaluation results of control testing.

a. Controls are evaluated at a frequency based on the level of residual risk.

(1) Controls that mitigate risks with a high-level residual risk rating should be evaluated on an annual basis.

(2) Controls that mitigate risks with a medium-level or low-level residual risk rating should be evaluated on a two-to-five-year rotation.

b. Adequately planning this effort will ensure a structured approach to identifying control deficiencies on an ongoing basis.

c. Additionally, ROs may be directed to conduct reviews in areas that should be incorporated into the ICEP based on materiality, identified control gaps, ARs, or as directed by the Director, Army Risk Management.

Chapter 3
Documentation

3–1. Process narrative and supporting documentation

a. Process and/or equivalent documentation support the continuity of military operations and provides a written set of instructions that clearly define the end-to-end functions of a business process. When developing process documentation consideration is given to the reason, function, and applicability of the procedure. At minimum, the process documentation will capture an overview of the process, internal controls, and IT controls, applicable regulations, and responsible parties. The documentation should provide a basic understanding of the flow of transactions, including—

(1) The control objectives and associated risks, and linkage to the control activities designed to reduce inherent or process risks.

(2) The individuals responsible for performing each procedure and how often the procedure is performed.

(3) How transactions are initiated, authorized, processed, recorded, and reported.

(4) Control type (that is., manual, automated, or Information System Dependent).

(5) Procedures for correcting and reprocessing previously rejected transactions and correcting erroneous transactions by adjusting entries.

b. The U.S. Army Financial Management Command (FMCOM) Business Process Management (BPM) Team captured the Army's financial end-to-end processes and housed this information in the Army Process Portal. ROs should leverage this information to conduct internal control evaluations.

(1) The ACC contains a listing of the Army's entity level controls, operational business process controls, financial business process controls, IT controls, and complimentary user entity controls that have been cataloged. The controls within the catalog are both Armywide and entity level controls. The documented internal controls are to formalize the identification of internal controls that mitigate the risk of financial statement error, fraud, and operational risk to an acceptable level. The control catalog is a continuous work in progress and is required to be updated as Army policies and procedures change. If an RO identifies a financial control that is not in the ACC, the RO is required to develop the control documentation with the HQDA RMIC and FMCOM BPM teams to ensure the key financial controls are properly vetted and included in the ACC.

(2) Process Cycle Memo. The Process Cycle Memo (PCM) is both instructional and informative in nature. The PCM, along with the process details, encompasses the specific processes and procedures for Army financial and BPM consistent with, and in support of, Army's regulations and policies. The Purpose of the PCM is to identify the process narrative, risks, and key controls to aid the organization in performing risk assessments and internal control testing. PCMs—

(a) Outline and describe the process and sub-processes.

(b) Identify the responsible staff or office.

(c) Highlig.ht internal controls and key internal controls, controls that are implemented to sustain daily operations to ensure organizational effectiveness and compliance with legal requirements.

(d) Identify information systems involved in the process. Desk procedures, manuals, and other similar documents can be used as a Business Process Narrative or to supplement a Business Process Narrative.

(3) Process Maps. The Process Map is a visual depiction of the end-to-end process that highlights roles within a process, internal controls, creation of a United States Standard General Ledger (USSGL) entry, generation of key supporting documents and enterprise resource planning transaction codes. Process Maps also include the decision points and alternate paths a process may take. The purpose of the Process Maps is to provide Army organizations with a visualization of Army policy and guidance, and to support the testing of repeatable standard business processes.

(4) Risk Control Matrix. The Army Financial Statement Assurance RCM utilizes the documented BPM Maps, Details, and Narratives, as well as OMB Circular No. A–11 Preparation, Submission, and Execution of the Budget's Risk Assertions to align controls to the Army Financial Statement Risk. The RCM is used to document how the Army's internal controls address and mitigate control gaps. Each risk is assigned one of three risk categories, which are USSGL Impact, Manual Entry or Key Supporting Documentation (KSD) Creation or Change. Additionally, every risk is assigned Financial Statement Assertion Risk (Existence/Occurrence, Completeness, Valuation/Accuracy, Rights, and Obligations, Presentation, and Disclosure). The purpose of the RCM is to provide Army organizations and external users with documented risk and control matrices which give reasonable assurance that controls are in place to mitigate risks as well as identify risks within the business processes that are not currently being mitigated. The RCMs are available upon request.

(5) For non-financial business processes the RO should leverage the governing regulations to conduct control evaluations or develop standard operating procedures that align with organizational objectives.

Chapter 4
Testing and Evaluation

4–1. Testing and evaluation overview

During the Testing and Evaluation phase, each RO is responsible for evaluating the adequacy of its internal controls over business processes that do not have a financial statement impact to determine whether they conform to the principles and standards established by OMB Circular No. A–123 M–16–17 and the GAO Green Book. Business processes with a financial statement impact will be performed through the centralized internal testing program supported by FMCOM. Programs significant to mission accomplishment and high-risk programs should be evaluated to determine if internal controls over those programs are designed properly and operating effectively. Evaluation results will determine whether management can provide reasonable assurance that internal controls have been implemented and are operating effectively. The sections that follow address requirements for creating a test plan, performing, and documenting testing, the methodology for selecting test samples and decisions made when performing testing. All controls designed effectively should be tested at least once within the five-year period identified in the RO's ICEP.

4–2. Test of design

The documentation of processes and sub-processes provides the foundation of information needed for assessing control design. The information pertaining to process objectives, risks, and controls, allows process owners to assess whether controls are designed to achieve process objectives efficiently and effectively, considering the associated risk of error. The assessment of control design efficiency focuses on whether the process is over controlled or if there is redundancy in operations whereas the assessment of control design effectiveness will focus on whether controls are designed properly to mitigate risks, cannot be bypassed, and will prevent a material misstatement or error from occurring.

a. Prior to conducting the assessment of control effectiveness, if the assessment of control design determines a key control is not designed to achieve process objectives efficiently and effectively, testing of the "failed control", or an ineffective control, is not needed; the conclusion is the component did not design and implement an adequate control to be tested.

b. If there's a failed control, the AU will need to identify the compensating controls that mitigate the weakness, take corrective action to ensure an adequate key control is designed and implemented throughout the component, and then test to ensure it was implemented properly.

c. If there's no mitigating control a control gap is identified, remediated, and documented within the process.

d. If the control or policy does not address the process risk, the tester will coordinate with the HQDA RMIC to revisit the process documentation, and the parties will work with the process owner to revisit the control or identify and implement new controls.

e. Procedures to test design effectiveness include a combination of inquiry of appropriate personnel, observation of the business process, examination, and inspection of relevant documentation, and re-performance of the control. Preferably, walkthroughs of business processes conducted by AUs, that include the procedures above, ordinarily are enough to evaluate design effectiveness.

f. The tester will—

(1) Verify the attributes needed to test the control.

(2) Obtain KSDs.

(3) Perform a review of the process leveraging an approach from above.

(4) Execute testing leveraging a test plan.

(5) Document and report result in the test plan and follow up with the appropriate parties.

g. If a walkthrough shows actual practices circumvent or do not consistently apply key controls established for the process, testing of the operating effectiveness of the "failed key controls" is not needed; the conclusion is that the RO has not yet adequately implemented key controls. If this situation is found, RO management will switch to remediation efforts rather than expend resources testing key controls that are "broken" (not implemented); that is, the RO's management will need to identify the compensating controls that mitigate the weakness and take corrective actions to ensure key controls are implemented adequately and applied consistently. Once corrected, the key controls are tested for operating effectiveness.

4–3. Test of effectiveness

a. Controls deemed to be effectively designed need to be tested to determine the extent to which they were applied and the consistency of their application. Testing the operating effectiveness of a control helps the RO determine that objectives are met and that the controls can provide reasonable assurance that they can be relied upon to effectively prevent or detect an error or fraud from occurring. ROs will perform test of effectiveness utilizing techniques discussed in the sections that follow. The following steps should be taken by the RO—

(1) Determine which controls to test, and when and how the controls will be tested. This information is captured in the ICEP using the ACC.

(2) Designate an ICE to perform testing. Develop and obtain all necessary documentation to include test plans, KSDs, and so forth.

(3) Perform testing in accordance with the selected methodology and procedures. Document test results in the test plan.

(4) Analyze test results obtained to conclude on the effectiveness of the control.

(5) Ensure that an independent reviewer with sufficient knowledge of the process and control can review the documentation and results and reasonably arrive to the same conclusions.

b. The costs of a sound internal control system should not outweigh the benefits derived from it. ROs must prioritize testing activity and focus resources on required control areas, high-risk areas, and/or areas and systems for which they are designated as owners. Any remaining testing resources should be used to test additional areas as needed or required.

4–4. Testing strategy

a. Consideration of an external audit agency and IR Engagements. The local ICA should coordinate with the local IR activity on a periodic basis to determine which recent audits, attestations, and other engagements have been performed at the local command/activity which involved the evaluation of locally performed internal controls. As relevant audits are identified during this process, the ICA should request for local business process and control owners to consider audits involving the controls they are responsible for when planning local internal control testing efforts for these controls. Local business process and control owners must gain a thorough understanding of the specific tests performed and attributes reviewed during engagements performed by external audit agencies and local IR activities and the results

of these tests to leverage the work performed during these engagements. In some cases, the work from these engagements can be used to complement local internal control testing efforts, allowing the local testing to be accomplished with a reduced sample size or through modified testing procedures. The local business process and control owners and ICE(s) should work together to determine if the work performed during one or more recent audits, attestations, or other engagements can be leveraged in this manner to enhance local internal control testing efforts for controls the business process and control owner is responsible for.

b. Assessing Control Environment Considerations. The controls for each process and sub-process can vary among ROs and organizational units within ROs. Test plans should be designed to be flexible and take into consideration the risk of the process, prior period weaknesses and findings from IR teams. Table 4–1 below provides a list of additional items to consider according to risk factor when developing test plans.

Table 4–1
Items to Consider for Testing According to Risk Factor

High-Risk Factors	• Likelihood that a control is bypassed during peak processing periods. • The potential for management override of a control. • The potential risk of fraud.
Low-Risk Factors	• The extent to which the controls have been subjected to ongoing monitoring activities throughout the year. • The likelihood that a control will continue to operate as intended until year-end.
Other Factors	• The nature of the control and its significance in achieving the control objective and whether more than one control achieves a particular objective. • Whether significant changes in the volume or nature of transactions might adversely affect control design or operating effectiveness. • Whether there have been changes in the design of the control. • The degree to which the control relies on the effectiveness of other controls (that is, the control environment or information system general controls). • Whether the control relies on performance by an individual or is automated. • Changes in related processes.

c. There are four types of Testing Methods that can be used to validate if a control is operating effectively – inquiry, observation, examination/inspection, and re-performance. The diagram in Figure 4–1 below explains each type of testing method and shows the difference in reliability among the methods. As illustrated by the vertical arrow on the left side of the diagram, examination, and re-performance are the most reliable testing methods.

(1) Inquiry tests are conducted by making either oral or written inquiries of entity personnel involved in the application of specific control activities to determine what they do or how they perform a specific control activity. Such inquiries are typically open-ended. Generally, evidence obtained through inquiry is the least reliable evidence and is generally corroborated through other types of control tests (Examination/Inspection and/or Re-performance). Inquiry regarding a control's effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively. The reliability of evidence obtained from inquiry depends on various factors, such as:

(a) The competence, experience, knowledge, independence, and integrity of the person of whom the inquiry was made—evidential reliability is enhanced when the person possesses these attributes.

(b) Whether the evidence was general or specific—specific evidence is usually more reliable than is general.

(c) The extent of corroborative evidence obtained from several personnel is usually more reliable than evidence obtained from only one.

(d) Whether the evidence was provided orally or in writing—evidence provided in writing is generally more reliable than evidence provided orally.

(2) Observation tests are conducted by observing personnel performing control activities in the normal course of their duties. Observation generally provides highly reliable evidence that a control activity is

properly applied when the ICE is there to observe it; however, it provides no evidence the control was in operation at any other time. Consequently, observation tests are supplemented by corroborative evidence obtained from other tests (such as Examination/Inspection and/or Re-performance) about the operation of control activities at other times. However, observation of the control provides a higher degree of assurance than inquiries. This is often used in tests of design.

(3) Examination/Inspection of evidence often is used to determine whether manual control activities are being performed. Examination/Inspection tests are conducted by examining documents and records for evidence (such as the existence of initials or signatures, and review of past reconciliations) that a control activity was applied to those documents and records.

(a) System documentation, such as operations manuals, flow charts, and job descriptions, may provide evidence of control design but do not provide evidence that control activities are operating and applied consistently. To use system documentation as part of the evidence of effective control activities, the ICE will obtain additional evidence on how the control activities were applied.

(b) Because documentary evidence generally does not provide evidence concerning how effectively the control was applied, the ICE generally supplements inspection tests with observation or inquiry of persons applying the control. For example, the ICE generally supplements inspection of initials on documents with observation or inquiry of the individuals who initialed the documents to understand the procedures they followed before initialing the documents.

(4) Re-performance—it will normally be necessary for the ICE to reperform the control activity to obtain sufficient evidence of its operating effectiveness. For example, a signature on a voucher package to indicate the signer approved it does not necessarily mean the person carefully reviewed the package before signing. The package may have been signed based on only a cursory review (or without any review). As a result, the quality of the evidence regarding the effective operation of the control might not be sufficiently persuasive. If that is the case, the ICE will reperform the control (such as checking for attributes like prices, extensions, and additions) as part of the test of the control. In addition, the ICE might inquire of the person responsible for approving voucher packages what he or she looks for when approving packages, and how many errors have been found within voucher packages. The ICE also might inquire of supervisors whether they have any knowledge of errors that the person responsible for approving the voucher packages failed to detect.

(5) When inquiry or observation are selected the RO will combine two or more methodologies to execute evaluations to provide greater assurance (inquiry and observation cannot be combined).

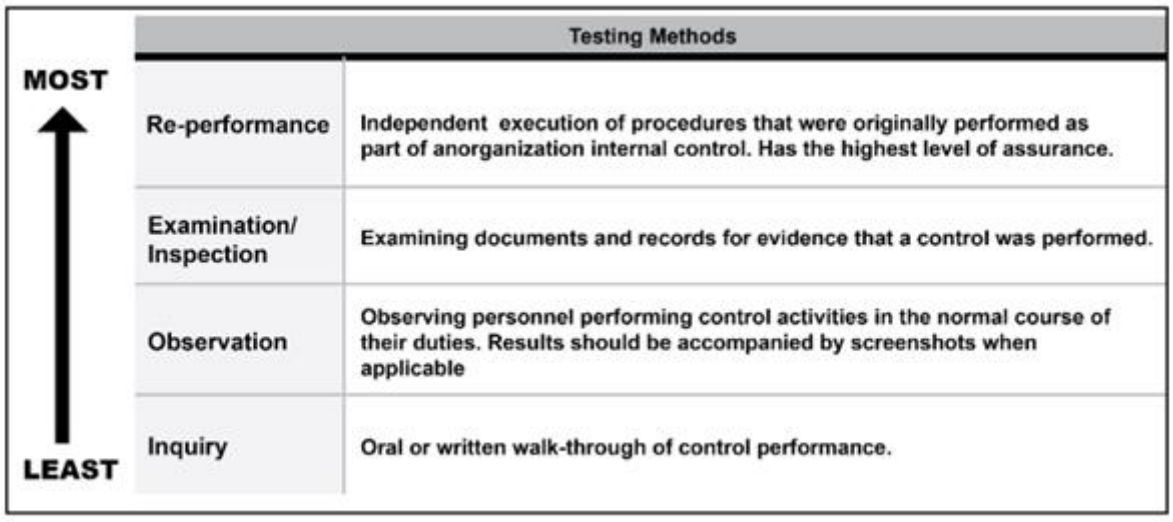


Figure 4–1. Testing Methods

d. Identifying Attributes and Information Needs. The ICE should gather and review process documentation for controls to be tested. The ICE can leverage attributes identified by the ASA (FM&C) within test plans or develop attributes for incorporation into the test plan. For financial controls, review the financial statement assertions that are covered by the control to determine the evidence or attributes that would need to be reviewed to satisfy that those assertions. An attribute can range from a signature on a reconciliation to an exception report generated automatically.

4–5. Creating a test plan

As mentioned previously, OMB Circular No. A–123 M–16–17 requires agencies to have assessment documentation processes that provide verifiable results. To ensure the Army's compliance with this requirement and to facilitate review and use of assessments, ROs are required to include certain information in the documentation supporting their OMB Circular No. A–123 M–16–17 assessment. For example, all key decisions, including the sampling methodology and results of testing, need to be documented in the test plan. Documentation of the methodology and results should be detailed enough to allow an independent third-party to duplicate the testing and arrive at the same conclusions. In addition, when deficiencies are identified during testing, a copy of the documentation evidencing the deficiency should be maintained with the test plan.

a. Methods of documenting testing include test plans, AR checklists and other formal methods that enable the reviewer to assess controls and provide sufficient evidence of the assessment.

b. The ASA (FM&C) will provide a test plan template to assist ROs in documenting a test of sample of transactions/activities and the results. The template, when adequately completed, will provide all the details necessary to satisfy OMB's assessment documentation requirements, that is, the assessment objectives, attributes tested, period covered by the testing, population, nature, and frequency of the control, sample size, method of selecting the sample, and results.

c. ROs may create their own test plans to align with areas for evaluation. Test plans developed by ROs should cover, at minimum, the information provided in test plans issued by ASA(FM&C) to include procedures planned to gain evidence to support the operating effectiveness of each control, control exceptions, and summary of testing results.

d. A test plan should be created for each test performed; however, one plan can cover testing of multiple controls, especially if the frequency of the controls and/or the control objectives are the same or similar.

4–6. Population identification and sample selection

a. To identify a sample for testing the ICE must obtain a population of transactions that meet the scoped requirements and identify the sampling methodology. Table 4–2 provides the Sampling Procedures.

Table 4–2
Sampling Procedures

Determination of the Test Objectives	The ICE must first identify the control to be tested and gains an understanding of what the control is intended to achieve.
Defining the Control Exceptions (that is, Control Deviations)	The ICE needs to define what constitutes a Control Exception (that is, Control Deviation). Specifically, a Control Exception (Control Deviation) is a departure from the expected performance of the prescribed control. For example, a prescribed control for disbursements requires supporting documentation (that is, Voucher, Receiving Report, Purchase Order) to be attached to an invoice before payment is made. A Control Exception (Control Deviation) would be the lack of supporting documentation attached to a paid invoice.
Defining the Population	The ICE needs to identify the class of transactions or set of items from which the ICE needs to draw a conclusion about the control effectiveness. As a further step, the ICE needs to validate the completeness of the Population and consider the overall validity of the data before the application of sampling procedures can be made. Deviations and issues with data integrity are documented and reported to the appropriate parties.
Sample Selection Methods	The ICE will select any of the following methods for Sample Selection: 1. Random Sampling Selection Approach: The auditor selects a random sample by matching random numbers generated by a computer or a random number table. 2. Systematic Sampling Selection Approach: The auditor determines a uniform interval by dividing the number of items in the population by the sample size. For example: Population - 20,000 items Sample - 100 items Interval = every 200th item (20,000 items / 100 items) The ICE selects every 200th item from the starting point. A random starting point is used to allow every item in the population an equal chance of being selected. 3. Haphazard Sampling Selection Approach: The auditor selects items from the population without any special reason for inclusion or exclusion of items from the sample. For example: An Auditor selects from a file cabinet voucher regardless of size, amount, or any other characteristics.

b. Determination of Sample Size for Manual Control Activities. The ICE will identify the sample size using Table 4–3. The sample sizes provided in the following table serve as the minimum number of items to test for the control assessment in accordance with the DoD Internal Control Over Financial Reporting Guidance. As noted in the table, the sample size is dependent on the frequency of the control performance.

Table 4–3
Minimum Sample Size vs. Total Population for Manual Control Activities

Frequency of	Population	Annual	Quarterly	Acceptable Number

Table 4–3
Minimum Sample Size vs. Total Population for Manual Control Activities—Continued

Control Performance	Size	Sample Size	Sample Size	of Deviations
Annual	1	1	1	0
Quarterly	4	2	1	0
Monthly	12	3	1	0
Weekly	52	10	3	0
Daily	250	60	15	1
Multiple Times Per Day	Over 250	160	40	4

c. If a control is performed in a cadence not listed above (that is, ad hoc) consider how often the control is performed throughout the testing year and align it to the closest population size listed in Table 4–3 to determine the minimum number of items to test.

d. Automated Control Activities. The ICE should refer to GAO–09–232G developed by the GAO when testing IT controls since Federal Information System Controls Audit Manual includes specific requirements from Federal Managers' Financial Integrity Act (FMFIA), Federal Financial Management Improvement Act (FFMIA) and Federal Information Security Modernization Act (FISMA).

4–7. Documenting test results

a. Test results should support management's judgment as to whether a control is operating adequately or not.

b. On the test plan, there is a section titled Test Results. This is where a quantified written summary of the test results is placed. The summary must state whether the attributes tested were satisfied or not satisfied and any exceptions (and so forth, "2 out of 15 invoices with a total value of $250,000 were not date stamped. All other attributes tested were adequately satisfied.").

c. Exceptions noted in testing regarding the design of internal controls indicate control deficiencies.

d. A DA Form 11–2 should accompany each test plan, serving as the cover sheet to capture activities that occurred during testing.

e. ROs are responsible for capturing all results in the Internal Control Evaluation Appendix.

4–8. Documenting evidence to ensure results are verifiable

a. The description of evidence supporting control tests must be specific. For example, the description for any interview, walk-through/observation, or examination (including a test of a sample of transactions/activities) must include the following.

(1) Interview: Name, title, and contact information (phone and email) of person(s) interviewed and date of interview.

(2) Walk-through/Observation: Date and time of walk-through/observation and description of activity observed. Include the name, title, and contact information (phone and email) of any participants or observers.

(3) Examination: Date of examination and description of objects examined (and so forth, purchase order number, invoice number, specifications, procedures, mechanisms, activities). Include the title of any document reviewed, as well as the date of the document; time frame covered by the document, if applicable (and so forth, the document reviewed may be a computer-generated report covering activity for a particular time frame); and source of the document (and so forth, name of person who provided it, website address).

b. In addition to the above, the ICE should identify the attributes tested. An attribute is a characteristic within documentation that may be referred to during an evaluation to validate its existence or inexistence. For example, if Attribute A is "Verify that the reconciliation was approved," the ICE should annotate an A on the supporting documentation where it evidences approval (and so forth, a signature). This annotation will support the testing performed and facilitate the review of testing. The ICE may then annotate on the test plan that the appropriate attribute is present.

c. For the controls tested by examining a sample of transactions/activities, the method for selecting the sample (that is, judgmental, systematic, or random selection) needs to be described in sufficient detail such that the sampled items could be re-selected, and the test re-performed, if needed.

4–9. Classification of control deficiencies

To identify internal control deficiencies, ROs should document and accumulate all control exceptions (failures) found during control testing of operating effectiveness. A control exception exists when procedures used to evaluate operating effectiveness indicate that a control did not operate as intended. For example, an ICE might find that key information was not properly reconciled, or designated duties were not fulfilled by the assigned individual.

a. When an RO identifies a control exception, it should consider the results in relation to management's overall evaluation of internal control and determine whether the exception potentially indicates there is a deficiency in the design of the control, the effectiveness of the control when implemented or both.

b. After considering knowledge of the process, existing information, underlying management principles, and the results of reviews, the HRO must determine the significance of any internal control deficiencies identified by the ICE and whether they are required to be reported.

c. The RO will classify internal control deficiencies in one of the following areas listed in the following table in accordance with the classification from OMB Circular No. A–123 M–16–17.

4–10. Identifying, tracking, and reporting control deficiencies

a. Control Deficiency Identification. Deficiencies exist in a process when the process or control's design, implementation, or operation does not allow stakeholders, in the normal course of performing their assigned functions, to achieve the organization's objectives. Control deficiencies can be classified in one or more of the following categories—

(1) Deficiency in design: results from a lack of or insufficient controls necessary to meet control objectives.

(2) Deficiency in implementation: results when a properly designed control is not implemented correctly or as intended.

(3) Deficiency in operation: results when a properly designed control does not operate as designed or when the control owner performing the control does not have adequate competency and/or authority to perform the control effectively.

b. When an exception is identified and the likelihood of the exception re-occurring is more than remote, the exception is identified as a control deficiency. The control deficiency can be further classified as a significant deficiency or MW based on materiality or impact to Army operations. Classification of deficiencies are further discussed in Table 4–4.

c. Reporting Self-Identified Material Weaknesses & Significant Deficiencies. For control deficiencies determined to be either significant or material ROs must then report the information to those charged with governance. Significant deficiencies and MWs are reported to the HRO, and MWs are reported to OASA FM&C and the applicable HQDA functional proponent. Whether the MWs identified are command-level or Armywide, the HQDA functional proponent will provide guidance and assistance to ensure the MWs are corrected.

d. Detailed guidance for reporting MWs is provided by the OASA (FM&C) in the ASOA guidance accompanying appendix.

(1) Reporting Requirements. Significant deficiencies are internal to the Army and are not reported to external organizations.

(2) Army systemic MWs, along with a summary of corrective actions, are reported to OSD for consolidation with other DoD agencies and reported to OMB and congress through the Agency Financial Report. Each significant deficiency and MW require a CAP.

e. Reporting Process. MWs are reported to HQDA through command channels in a timely manner; however, the frequency of reporting is at the command's discretion.

(1) The Director, Army Risk Management, will review all self-identified MWs reported by ROs. MWs submitted to the Director, Army Risk Management, by ACOMs, ASCCs, and DRUs are reported to the appropriate HQDA functional proponent(s). The proponent will determine if additional coordination is required by assessing the potential impact of the significant deficiency or MW and provide written feedback

within an appropriate timeframe. The functional proponent will instruct the RO on the activities to address the MW:

(2) The Director, Army Risk Management, will facilitate the return of the functional proponent's recommendation of the MW or significant deficiency to the RO for monitoring and resolution at the lower level.

f. MWs considered to be significant Armywide issues are submitted to the Army Audit Committee and briefed for concurrence. If all members concur, the MW and associated CAP milestones are included as part of the SECARMY's ASOA. The Director, Army Risk Management, will use the minutes of each Army Audit Committee meeting as a medium to communicate the status of reported weaknesses.

Table 4–4
Classification of Internal Control Deficiencies

Category	Definition	Control Requirement
Control Deficiency	A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks. A deficiency in design exists when (1) a control necessary to meet a control objective is missing or (2) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.	Internal to the organization and not reported externally. Progress against CAPs must be periodically assessed and reported to agency management.
Significant Deficiency	A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A significant deficiency that the Agency Head determines to be significant enough to report outside of the Agency as a material weakness. In the context of the GAO Green Book, non-achievement of a relevant principle and related component results in a material weakness.	Internal to the organization and not reported externally. Progress against CAPs must be periodically assessed and reported to agency management.
Material Weakness	A material weakness in internal control over operations might include, but is not limited to, conditions that: • Impact the operating effectiveness of Entity Level Controls • Impair fulfillment of essential operations or the mission • Deprive the public of needed services • Significantly weaken established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest A material weakness in internal control over reporting is a significant deficiency which the Agency Head determines significant enough to impact internal or external decision-making and reports outside of the Agency as a material weakness. A material weakness in internal control over external financial reporting is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's	Material weaknesses and a summary of corrective actions must be reported to OMB and Congress through the Agency Financial Report, Performance, and Accountability Report or other management reports. Progress against CAPs must be periodically assessed and reported to agency management.

Table 4–4
Classification of Internal Control Deficiencies—Continued

Category	Definition	Control Requirement
	financial statements will not be prevented, or detected and corrected, on a timely basis. A material weakness in internal control over compliance is a condition where management lacks a process that reasonably ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving Agency objectives.	

Chapter 5
Testing and Evaluation – Testing Based on Requirements and Directives

OMB Circular No. A–123 appendices and memorandums recognize that organizations are subject to numerous regulatory requirements, including, but not limited to, the subjects listed in this section.

5–1. Office of Management and Budget Circular No. A–123, M–18–16, Management of Reporting and Data Integrity Risk

The 31 USC 6101, Public Law 113–101 expanded the Federal Funding Accountability and Transparency Act (FFATA) to increase transparency of federal spending by disclosing direct agency expenditures and linking federal contract, loan, and grant spending information to federal agency programs. The Digital Accountability and Transparency (DATA) Act requires agencies to adopt government-wide data standards to improve the accuracy, completeness, and consistency of federal spending information reported to the US Department of the Treasury (Treasury). On June 6, 2018, OMB published Memorandum M–18–16 entitled "Appendix A to OMB Circular No. A–123, Management of Reporting and Data Integrity Risk" which requires the creation of a Data Quality Plan to identify a control structure tailored to address identified risks over data quality.

a. Data Quality Plan. Army will maintain a Data Quality Plan in accordance with OMB requirements that captures—

(1) The organizational structure, key stakeholders, and key processes providing internal controls for reporting on spending data.

(2) Management's responsibility to supply quality data to meet the reporting objectives for the DATA Act in accordance with OMB Circular No. A–123, M–18–16.

(3) A risk assessment to include agency identified high-risk reporting data and DATA elements specifically expressed in the DATA Act.

(4) A testing plan to evaluate whether spending data is linked through the inclusion of the award identifier in the agency's financial system, and reported with plain English award descriptions, along with other attributes to include assessment of internal controls related to federal spending data compilation, review, dissemination, and monitoring.

b. Risk Assessment. The Director, Financial Information Management will leverage the current risk assessment process to identify significant risks in the following areas:

(1) *Accuracy of Data Elements.* Amounts and other data relating to recorded transactions are recorded in accordance with the DATA Act Information Model Schema, the Reporting Submission Specifications and agree to authoritative source records.

(2) *Completeness of Quarterly Submission.* All transactions and events are recorded in the proper reporting period. Data elements have been reported in the appropriate files for A through F (refer to Table 5–1. DATA Act Files).

(3) *Timeliness of Quarterly Submission.* Reporting of the Army DATA Act submission to the Treasury is in accordance with federal wide reporting submission dates found at: https://www.fiscal.treasury.gov/data-transparency/resources.html.

c. File Reconciliation. The Director, Financial Information Management will coordinate with stakeholders across Army to identify the financial systems of record needed to for the DATA Act extraction and

reporting process. The Director, Financial Information Management will make sure the financial attributes generated by the Army's financial systems of record, include the award identifier to link to the award data reported under the requirements of FFATA, as amended.

d. Quarterly Certification. The Quarterly certifications of data submitted by the Army's Senior Accountable Official (SAO) should be based on the consideration of the data quality plan and the internal controls documented in their plan, as well as other existing controls that may be in place, in the annual assurance statement process. Table 5–1. DATA Act Files are the assurances to support DATA Act certifications on internal controls over DATA Act submissions (chart CFO Council Data Quality Playbook).

Table 5–1
Digital Accountability and Transparency Act Files

DATA Act File & Authoritative Source	SAO Assurance Required
File A: Appropriations Account **Authoritative Source:** The Report on Budget Execution and Budgetary Resources (SF 133) derived from Governmentwide Treasury Account Symbol (GTAS) data	The reporting objective is that the data reported in File A match the authoritative source (that is, SF 133) and that all Treasury Account Symbols are reported not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.
File B: Object Class and Program Activity **Authoritative Source:** The SF 133 derived from GTAS data	The reporting objective is that the total amount reported in File B matches the authoritative source (that is, SF 133) and that Program Activity and Object Class Codes are reported based on the published guidance in OMB Circular No. A–11.
File C: Award Financial **Authoritative Source:** Component Accounting Systems	The reporting objective is that the data reported in File C match the authoritative source (that is, Army financial systems).
File D1: Procurement Award Attributes **Authoritative Source:** Applicable Army Procurement Systems	The reporting objective is that for data reported pursuant to FFATA (P.L. 109–282) as amended by the DATA Act of 2014, they are sourced from and match the applicable Army Procurement Systems at the time of quarterly reporting.
File D2: Financial Assistance Award Attributes **Authoritative Source:** Applicable Army Award-Management Systems/Files (for award description, award title, and so forth.) Financial Assistance Awardee data in the System for Award Management prior to receiving a federal award (for prime financial assistance awardee information)	The reporting objective is that data reported in File D2 match the authoritative source (that is, Army Award-Management Systems/Files) for award-level data and the authoritative source (that is, System for Award Management) at the time of the award for prime awardee information.
File E: Highly Compensated Officer Data **Authoritative Source:** System for Award Management	Army will leverage assurances based on the internal controls of the system owner, the General Service Administration in accordance with OMB Circular No. A–123 M–16–17. In addition, for procurement-related awards, agencies will leverage the existing OMB guidance on sub-award data quality.
File F: Sub-Award Attributes **Authoritative Source:** Applicable Army Sub-Award Management Systems/Files	

5–2. Office of Management and Budget Circular No. A–123, A Risk Management Framework for Government Charge Card Program

OMB Circular No. A–123 Appendix B, A Risk Management Framework for Government Charge Card Programs establishes standard minimum requirements and suggest best practices for government charge card programs. This includes maintaining a charge card management plan which consists of the written formal policies and procedures to assure the system of internal control is followed to minimize the potential for fraud, waste, and errors.

5–3. Office of Management and Budget Circular No. A–123, M–21–19, Requirements for Payment Integrity Improvement

OMB Circular No. A–123 Appendix C, Requirements for Payment Integrity Improvement provides an infrastructure of legislative and administrative requirements for agencies to abide by to prevent improper payments made on purchase cards through reporting of susceptible programs that include estimation of improper payments, annual reporting, semi-annual or quarterly reporting, and development of CAPs for implementation where program deficiencies exist.

5–4. Office of Management and Budget Circular No. A–123, M–13–23, Compliance with the Federal Financial Management Improvement Act of 1996

Systems owners will assess compliance with financial management systems requirements and report the results of such assessment, accordingly. System owners will leverage the guidance issued by the Director, Financial Information Management to report on compliance in the following three FFMIA Section 803 (a) requirements:

a. To ensure reliable financial reporting, effective, and efficient operations & compliance with applicable laws and regulations.

b. To report accounting information in accordance with GAAP. In other words, accounting information follows the Statements on Accounting Standards, Interpretations, Technical Bulletins, Implementation guides and other pronouncements issued by the Federal Accounting Standards Advisory Board, American Institute of Certified Public Accountants Industry Audit and Accounting Guides as well as practices widely recognized & prevalent in the Federal Government.

c. The financial events will be recorded applying the requirements of the USSGL guidance in the Treasury Financial Manual issued by the Bureau of Fiscal Service.

5–5. Information Technology controls

IT Controls consist of the annual assessment of information systems security controls required by the FISMA, and the annual audit of the financial statements required by the CFO Act of 1990. The federal guidance and methodology to establish and assess IT controls includes National Institute of Standards and Technology (NIST) Special Publication 800–53 and OMB Circular No. A–130 Management of Federal Information Resources, and Federal Information System Controls Audit Manual. IT system owners, per DA Pam 25–2–14, must continuously test and self-monitor the effectiveness of their IT controls. Continuous monitoring of Army financial systems is critical for auditability.

a. The Director, Financial Information Management will provide a list of critical systems for assessment and coordinate with key stakeholders to execute assessments.

b. OMB Circular No. A–123 M13–23 Appendix D defines IT controls as both Information Technology General Controls (ITGCs) and Business Process Application Controls (BPACs). ITGCs are the pervasive controls at the IT Infrastructure level. ITGCs include the structure, policies, and procedures that apply to Army's overall operations, creating the IT business environment in which significant financial systems and BPACs operate. The following NIST control families, at a minimum, are required in the system owner assessment of the design and operating effectiveness of the following key ITGCs—

(1) *Access Controls*: Management of information system accounts to include, but not limited to identifying account types, requiring approvals for account creation, ensuring segregation of duties regarding users' roles, process for removing accounts, and the monitoring/review of user accounts.

(2) *Identification and Authentication*: Establishment of a process to include, but not limited to ensuring that users are uniquely identified in the system, implementing strong password-based authenticators, and requiring passwords be changed periodically in organizational defined time requirements.

(3) *Incident Response*: Establishment of a process to include, but not limited to implementing an incident handling capability for security incidents that includes preparation, detection, and analysis, containment, eradication, and recovery.

(4) *System and Information Integrity*: Establishment of a process to include, but not limited to establishing an interface strategy that includes the process for validations and edits, ownership of the interface process, and error resolution/monitoring.

(5) *Security Assessment and Authorization*: Conducted a security assessment to include, but not limited to, developing, and monitoring plan of action and milestones, authorizing connections from the information system as defined by its authorization boundary, to other information systems through the use of Interconnection Security Agreements, documenting each connection, the interface characteristics, security requirements, and the nature of the information communicated.

(6) *Contingency Planning*: Establishment of a contingency plan that includes, but is not limited to, clearly defined responsibilities for recovery, and detail instructions for restoring operations and that has been distrusted to applicable parties and approved by key senior management.

(7) *Planning*: Establishment of an entity wide security management program that includes, but is not limited to, providing the security categorization of the system, and outlining required security awareness training, includes security incident response procedures and management internal testing procedures, includes an overview of the security requirements for the system, and has been approved by senior management.

(8) *Risk Assessment*: Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

(9) *Configuration Management*: Establishment of a process regarding system changes to include, but not limited to, standard versus non-standard change process, emergency change requests, and monitoring of changes to the system.

(10) *Audit and Accountability*: Establishment of an audit logging process to include, but not limited to defining auditable events in the system and ensuring appropriate review and follow up is conducted regarding audit log reports.

c. Application controls (automated or manual) support the completeness, accuracy, validity, confidentiality, and availability of data during processing associated with financial transactions. All the NIST Special Publication 800–53 control families are required in the system owner assessment of the design and operating effectiveness of the following key BPACs–

(1) General Application Security.

(2) Data prepared for input is complete, valid, and reliable to include appropriate edits and validations.

(3) Data is processed by the application completely, on time, and in accordance with established requirements (and so forth, review of transaction logs, documented processing and posting conditions).

(4) Data output is protected from unauthorized modification or damage and is distributed in accordance with policies to ensure access to reports is authorized and user access to output data is monitored and reviewed. (and so forth, output reconciliation and review).

(5) Master data is protected and shared between multiple applications (and so forth, vendor file).

(6) Data is documented to include transaction logs, posting conditions, and warning/error messages/rejections/error communications documentation is reviewed for appropriateness after action items are taken as necessary (that is, reconciliation, and exception handling).

(7) Interface processing is timely, accurate, and complete between systems and other feeder and receiving systems on an ongoing basis. A defined interface strategy to include, but not limited to, an interface Memorandum of Agreement (MOA) and interface error resolution/monitoring.

(8) Data management systems enforce user authentication/authorization, role-based access privileges, segregation of duties, data confidentiality, and application processing.

d. System owners should continue to update system and controls documentation as appropriate and identify and remediate root causes of IT control deficiencies and Notice of Finding and Recommendations (NFRs) utilizing a risk-based approach.

e. The key IT controls noted above should be evaluated annually. These efforts will strengthen security controls across the Army IT business environment and will help demonstrate our commitment to Information Security Continuous Monitoring in accordance with DA Pam 25–2–14.

5–6. Service organization controls

Service providers supporting the Army are responsible for providing assurances and communicating the relationship between the service provider's controls and Army's user controls. Army and the service provider collectively manage the risks of third-party provider activities through SOC 1 Type 2 reporting, also referred to as the Statement on Standards for Attestation Engagements No. 18 report. An assessment of computer related controls is part of a comprehensive effort to evaluate both the controls over and reliability of reported financial data. Army service providers will—

a. Conduct analysis and review processes within the scope of the SOC 1 report, conduct risk assessments, modify, or implement new controls to mitigate the changing environment, and prepare and submit reports as required by the Director, Army Risk Management, in adherence to OMB Circular No. A–123 M–16–17.

b. Provide the Army with a SOC 1 Report on Controls at the Service Organization relevant to the Army's processes and controls to be reviewed by Army to evaluate the effect of the controls at the service organization on the Army's controls for financial reporting.

c. Establish a Service Agreement (for instance, an MOA, Memorandum of Understanding, Service Level Agreement and so forth.) with each User Entity supported by the Service Organization. Ensure these agreements are documented on a Fiscal Service Interagency Agreement Forms 7600A General Terms and Condition and 7600B Order Funding where appropriate in accordance with DoD 7000.14–R, Volume 11A, Chapter 3 and recorded in the Treasury's G-Invoicing system.

d. The Army's independent external auditor conducts annual Information ITGC testing as part of the Financial Statement audit and SSAE18 Examination. The ITGC testing is limited to only selected in-scope systems for the audit. Based on the results of the Testing NFR and Performance Improvement Opportunities are identified and issued to the Army. As part of Army's remediation activities, the OASA (FM&C) conducts various initiatives to address control gaps impacting the financial statements. The following are the key activities conducted by OASA (FM&C) to address existing and potential control gaps not yet identified by the independent external auditor—

(1) Work with various commands and process/system owners to identify root cause of the issue and develop and implement effective CAPs.

(2) Conduct workshops to assist with the acceleration of CAP remediation.

(3) Conduct mock audit walkthroughs to prepare system owners and help reduce the number of NFRs issued during the audit. Additionally, mock walkthroughs help to identify performance improvement opportunities and potential control gaps.

(4) Risk-based validation of newly designed and implemented Information System controls to assess satisfactory remediation of NFRs. Validation of NFRs also proactively identifies internal control gaps which enhances effectiveness and efficiency of operations and compliance with applicable laws and regulations.

Chapter 6
Remediation and Validation

6–1. Corrective actions

Army managers are responsible for taking timely and effective action to correct deficiencies identified during assessments of internal control. Correcting deficiencies is an integral part of management's accountability and is considered a priority by the RMIC Program. ROs are to develop corrective actions for all internal control deficiencies categorized as significant deficiencies and MWs, using the RMIC CAP Template, Figure 6–1 format consistent with the level of detail required by the RMIC CAP Template. This process is applicable to findings reported by the GAO OIG/DoDIG/DAIG/USAAA/local IGs/IR/independent external auditor/RO.

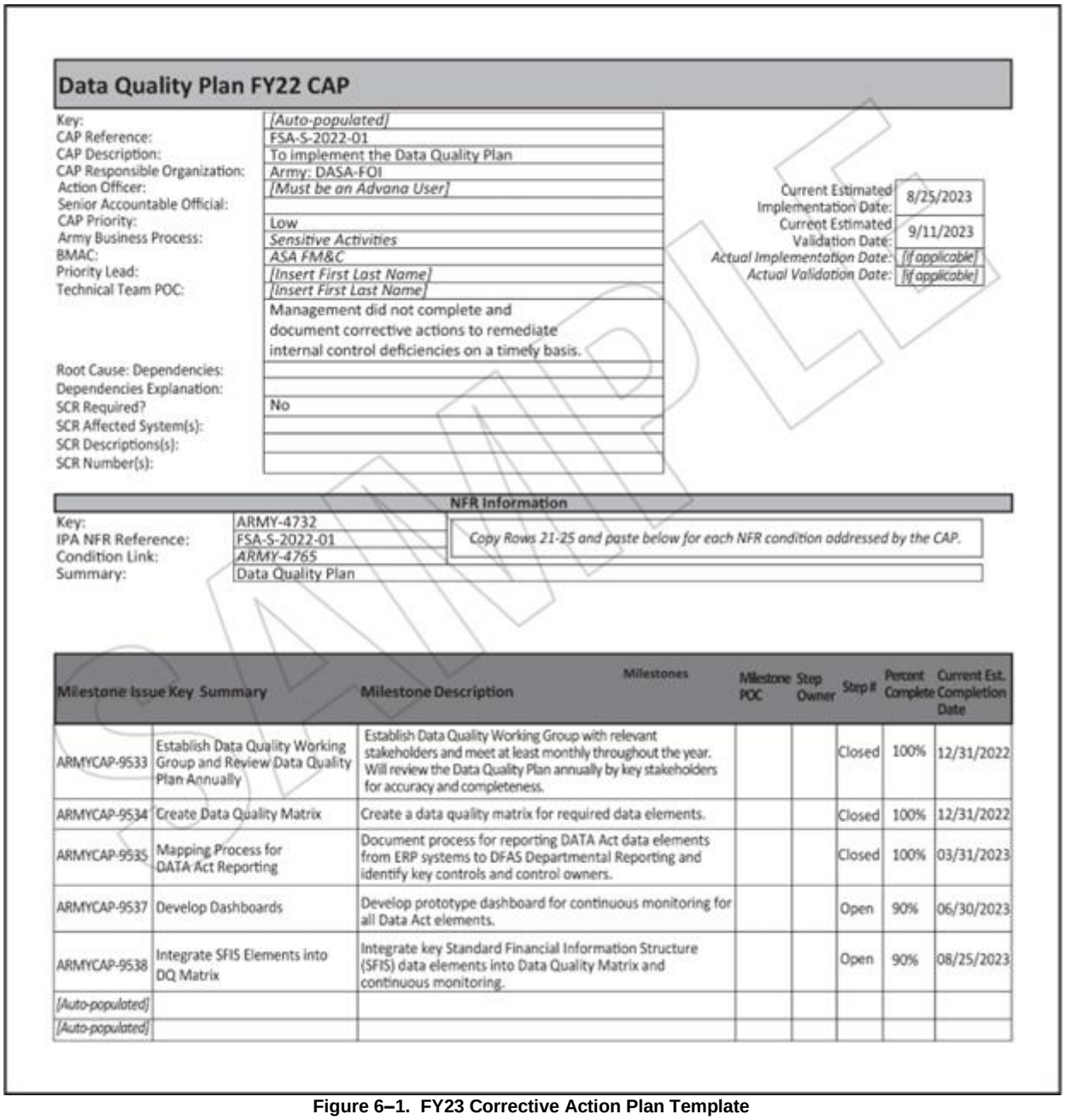
a. Once the process owner accepts the control deficiency or is issued a NFR or equivalent from the DoDIG, USAAA, RO, or the independent external auditor, the process owner will follow the CAP development timeline communicated by OSD.

b. The RO will identify a CAP development owner to liaise and perform a root cause analysis of the identified deficiencies to ensure adequate steps are in place to mitigate the finding(s) identified. It is recommended that each RO consider alternative risk mitigation strategies and perform a cost-benefit analysis to determine the most cost-effective solution to resolve deficiencies.

c. DoD requires the final CAP milestone to be an independent evaluation that validates the corrective actions have in fact resolved the deficiency. Validation is further discussed in paragraph 6–2.

d. Reporting. Activities within CAPs performed to remediate MWs are reported in the RO's ASOA, or as instructed by the Director, Army Risk Management.

e. OASA (FM&C) may at any time request status of corrective actions related to MWs.



Data Quality Plan FY22 CAP

Key:	*[Auto-populated]*
CAP Reference:	FSA-S-2022-01
CAP Description:	To implement the Data Quality Plan
CAP Responsible Organization:	Army: DASA-FOI
Action Officer:	*[Must be an Advana User]*
Senior Accountable Official:	
CAP Priority:	Low
Army Business Process:	*Sensitive Activities*
BMAC:	*ASA FM&C*
Priority Lead:	*[Insert First Last Name]*
Technical Team POC:	*[Insert First Last Name]*
	Management did not complete and document corrective actions to remediate internal control deficiencies on a timely basis.
Root Cause: Dependencies:	
Dependencies Explanation:	
SCR Required?	No
SCR Affected System(s):	
SCR Descriptions(s):	
SCR Number(s):	

Current Estimated Implementation Date:	8/25/2023
Current Estimated Validation Date:	9/11/2023
Actual Implementation Date:	*[if applicable]*
Actual Validation Date:	*[if applicable]*

NFR Information

Key:	ARMY-4732	*Copy Rows 21-25 and paste below for each NFR condition addressed by the CAP.*
IPA NFR Reference:	FSA-S-2022-01	
Condition Link:	*ARMY-4765*	
Summary:	Data Quality Plan	

Milestones

Milestone Issue Key	Summary	Milestone Description	Milestone POC	Step Owner	Step #	Percent Complete	Current Est. Completion Date
ARMYCAP-9533	Establish Data Quality Working Group and Review Data Quality Plan Annually	Establish Data Quality Working Group with relevant stakeholders and meet at least monthly throughout the year. Will review the Data Quality Plan annually by key stakeholders for accuracy and completeness.			Closed	100%	12/31/2022
ARMYCAP-9534	Create Data Quality Matrix	Create a data quality matrix for required data elements.			Closed	100%	12/31/2022
ARMYCAP-9535	Mapping Process for DATA Act Reporting	Document process for reporting DATA Act data elements from ERP systems to DFAS Departmental Reporting and identify key controls and control owners.			Closed	100%	03/31/2023
ARMYCAP-9537	Develop Dashboards	Develop prototype dashboard for continuous monitoring for all Data Act elements.			Open	90%	06/30/2023
ARMYCAP-9538	Integrate SFIS Elements into DQ Matrix	Integrate key Standard Financial Information Structure (SFIS) data elements into Data Quality Matrix and continuous monitoring.			Open	90%	08/25/2023
[Auto-populated]							
[Auto-populated]							

Figure 6–1. FY23 Corrective Action Plan Template

6–2. Armywide corrective action plan validation

Validation of a CAP occurs only after all milestones are met and the control owner is able to have the control tested and provide support indicating that the root cause of the control failure is in fact remediated. CAP owners will leverage the Army CAP Management Standard Operating Procedures to manage CAP validation.

a. Prior to submitting the CAP for validation, the RO should conduct internal testing to support the control is operating effectively. In the event exceptions are noted, the RO should incorporate additional CAP milestones for completion before seeking validation.

b. As self-identified Armywide MWs are remediated, the RO has the option to have the local IR office complete the validation or to request an external party complete the validation. ROs will maintain evidence of remediation and validation for audit purposes. Based on the completed CAP validation report, the Army Audit Committee will vote to downgrade or remove the MW. If downgraded or removed, the OASA (FM&C) will submit a MW removal memorandum to the Office of the Undersecretary of Defense – Comptroller (OUSD–C) along with documentation to support the validation and CAP completion.

c. If a remediated MW is related to an independent external auditor finding, the MW can only be removed when the independent external auditor concurs with the completion and effectiveness of implemented remediation activities. The same also applies for deficiencies identified by other organizations such GAO OIG/DoDIG/DAIG/USAAA/local IGs/IR/independent external auditor, where the identifying organization is responsible for validation.

6–3. Continuous monitoring of corrective actions

a. OASA (FM&C) recommends that ROs review CAPs at least quarterly, ensuring that the corrective actions in process are planned adequately to address root causes and timelines and are practical and achievable.

b. ROs are to submit CAPs for self-identified MWs for quarterly status reporting beginning in Q1 FY23. Further instructions and a template will be provided by ASA (FM&C) via the Enterprise Task Management System.

c. Periodic update. The Army is required to report to the OSD any major changes in the plans for correcting MWs (CAPs). The Director, Army Risk Management, will issue appropriate guidance, in advance, for updates on Army MWs.

Chapter 7
Reporting

7–1. Annual statement of assurance

The Reporting phase requires the Army to provide assertions over the operational effectiveness of internal controls in accordance with FMFIA. Explicit statements for OMB Circular No. A–123, M–18–16, Appendix A, the scope of Internal Control over Reporting (ICOR) including both internal and external reporting functions and financial and business process operations reporting. These statements must include opinions over reporting objectives under ICOR. The reporting categories will be referenced as ICOR-Financial Reporting, ICOR-Financial Systems and Internal Control Over Reporting-Operations (ICOR–O), with ICOR–O to include the entity's business process operations reporting as well as business systems reporting business operations data. This information is reported in the Army ASOA submission with the accompanying appendices that provide additional support to substantiate the assertions reported and the status of the overall program.

a. Annually, per AR 11–2, each RO should assemble and submit to the OASA (FM&C) an ASOA feeder package with the accompanying appendices per the instructions provided in the ASOA Guidance.

b. The feeder package submitted to OASA (FM&C) must support the level of assertion stated in the RO's assurance memo and at minimum, must include the following in accordance with FMFIA Section 2—

(1) A statement of Management's responsibility for establishing and maintaining adequate internal controls for the Army.

(2) A statement identifying the OMB Circular No. A–123 M–18–16, Appendix A, as the framework used by the Army to conduct the assessment of the effectiveness of internal controls over operations, reporting, and compliance.

(3) An explicit statement as to whether controls are effective. The levels of assurance are discussed in paragraph 7–2.

(4) All MWs existing within the current reporting year.

(5) A summary of the CAPs for MWs, a description of deficiencies, the status of CAPs, and the timeline for resolution will be included in the ASOA.

c. If an RO does not submit an ASOA feeder package and/or any of the accompanying appendices then the Head of RO must document the non-submission and justification via memorandum and submit to the OASA (FM&C) Director, Army Risk Management.

d. The OASA (FM&C) will consolidate the ASOA feeder package submissions into the Army ASOA and report to OUSD–C.

7–2. Reasonable assurance

a. Background. In the context of the FMFIA, an assertion of "reasonable assurance" refers to a satisfactory level of Management's 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 potentially exceeds the benefits derived. Determining 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 (GAO Green Book).

(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 MWs 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 ASOA submissions from subordinate commanders, managers, or AUMs.

b. 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.

(1) The Head of each RO must submit an ASOA that provides an assessment of reasonable assurance that internal controls are in place and operating effectively for operations, reporting, and compliance. In addition, the following ROs must also provide a certification statement for internal controls over financial systems:

(a) Commanding General, USACE.

(b) Director, Financial Information Management, OASA (FM&C).

(c) Director, Audit Readiness, OASA (FM&C).

(2) The ASOA is 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 (GAO Green Book).

(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 MWs, if any, and have taken corrective action to resolve them.

c. Determining the level of assertion. Where the ASOA provides a "modified" statement of assurance, the area or areas in question are specified and related to MWs reported.

(1) The level of assurance is supported by conclusions from the assessment of internal controls.

(2) If one or more MWs is pervasive in an area identified within the GAO Green Book framework, the SECARMY cannot conclude the Army's internal control system is effective. Consideration is given to internal controls in each supporting area (operations, reporting, and compliance). According to OMB Circular No. A–123 M–16–17, Management is required to state a direct conclusion about whether internal controls are effective. The statement must take one of the following forms:

(a) Reasonable assurance – internal controls are operating effectively or integrated financial management systems (IFMS) are conformant with federal requirements (no MWs reported).

(b) Assurance – internal controls are operating effectively with the exception of one or more MWs explicitly noted, or IFMS do not conform with federal requirements.

(c) Unable to Provide assurance – reasonable assurance cannot be provided in one or more of the following circumstances: (1) Internal controls appear to be operating effectively because few or no assessments were conducted, or a process was not in place; (2) One or more noted MWs are pervasive across key operations, indicating a failure in an Entity Level Control; and (3) IFMSs are substantially noncompliant with federal requirements.

7–3. Annual statement of assurance appendices

At minimum, ROs are required to submit the following appendices in their ASOA feeder packages–

a. Statement of Assurance Memo. This statement is signed by the HRO and asserts the overall opinion on controls as well as the separate opinions for controls over operations, reporting, and compliance. Each RO's Statement of Assurance Memo must include a statement reflecting the effectiveness of Internal Controls Over Reporting (to include both internal and external reporting functions) financial and operational internal controls. The statements are provided in paragraphs 7–2*c*(2)(*a*) through 7–2*c*(2)(*c*).

b. Risk Assessment and Internal Control Evaluation Plan. The Risk Assessment and ICEP are now combined into a single appendix to reflect the new format. The Risk Assessment and ICEP require two submissions: (1) an approved submission in the first quarter of the FY, and (2) an updated submission with the final ASOA feeder package. The Risk Assessment should include the Army's reporting, operations, and compliance risks. Each risk will need to be rated as high, medium, or low. At least annually, ROs assess the likelihood and impact of inherent risk, the effectiveness of mitigating activities to address risk and the residual risk remaining after a control is applied. The risk assessment should drive the ICEP for the organization, which should reflect the controls applied to mitigate the risks. The rating of high, medium, or low will determine the required testing frequency for the controls identified. The Risk Assessment and ICEP submission made on behalf of the RO must have the concurrence of the SRO before proceeding with testing. For each control tested for the year, the RO is required to complete and retain the DA Form 11–2 and all supporting documentation.

c. Internal Control Evaluation. This appendix serves to capture the controls tested by the RO per the ICEP during the RMIC year and the results noted. The documented results should support the basis for management's reported level of assurance over the operating effectiveness of internal controls. If the control was tested multiple times at an RO during the year, the results will be summarized into one reportable entry.

d. Antideficiency Act Violations. The ADA imposes restrictions on the amounts of obligations or expenditures that agencies may make and OMB Circular No. A–11, Section 150, Administrative Control of Funds outlines requirements for the administrative control of funds under the ADA. The RO will report any ADA violations for the FY. The reported ADA violations will be reconciled with HQDA IR to determine the completeness of reported violations. If the RO does not have any reportable violations, then return the appendix and mark "Not Applicable" within the document.

e. Material Weaknesses and Significant Deficiencies. This appendix requires ROs to report all MWs (including self-identified MWs and MWs identified by internal and external auditors) determined as of the date of the ASOA signature to be pervasive across the organization, potentially impacting other ROs and requiring attention from the HQ level. The Army Audit Committee will vote during the third quarter meeting each year to determine if self-identified MWs and significant deficiencies should be elevated to an Armywide level based on the details provided. It is important for ROs to include details in CAPs and target remediation dates.

f. Significant Internal Control Program Accomplishments. This appendix provides a description of all significant internal control improvements achieved by an RO's internal control program. Significant accomplishments can be categorized as follows: RMIC Priority Areas, RMIC Program Management, and Financial and Business Process Operations Objectives.

g. Risk Management and Internal Control Training. This appendix reflects completed role-based training by assigned individuals within the RO. Training frequency varies by role.

h. Requirements. The aforementioned minimum submission requirements may be modified annually resulting from OSD or auditor requests.

Chapter 8
Additional Program Functions

8–1. Documentation retention

Process documentation, documentation on internal control evaluations conducted, ASOA submissions, and MWs reported must be maintained in accordance with DoD 7000.14–R, Volume 1, Chapter 9, Figure 9–1.

a. ROs must retain and house process documentation for key process areas that support their annual assessment.

b. ROs must retain documentation on MWs, control deficiencies, and control assessments in accordance with DoD 7000.14–R, Volume 1, Chapter 9, Figure 9–1.

Appendix A

References

Section I

Required Publications

Unless otherwise indicated, all Army publications are available on the Army Publishing Directorate website at https://armypubs.army.mil. DoD publications are available on the Executive Services Directorate website at https://www.esd.whs.mil. CFO Council publications are available at https://www.cfo.gov/. United State Code and Public Law publications are available on the Congress website at https://www.congress.gov/. OMB Circulars are available at https://www.whitehouse.gov/. GAO publications are available at https://www.gao.gov/.

AR 11–2
Risk Management and Internal Control Program (Cited in para 1–1.)

CFO Council
Data Quality Playbook (Cited in para 5–1*d*.)

DA Pam 25–2–14
Risk Management Framework for Army Information Technology (Cited in para 5–5.)

GAO–09–232G
Federal Information System Controls Audit Manual (Cited in para 4–6*d*.)

GAO–14–704G
Standards for Internal Control in the Federal Government (Cited in para 1–6*g*.)

GAO–15–593SP
A Framework for Managing Fraud Risks in Federal Programs (Cited in para 2–3*d*.)

GAO–18–601G
Financial Audit Manual (Cited in para 2–1*a*(1).)

OMB Circular No. A–123, M–13–23, Appendix D
Compliance with the Federal Financial Management Improvement Act of 1996 (Cited in para 1–5*b*(8).)

OMB Circular No. A–123, M–16–17
Management's Responsibility for Enterprise Risk Management and Internal Control (Cited in para 1–15.)

OMB Circular No. A–123, M–18–16, Appendix A
Management of Reporting and Data Integrity Risk (Cited in para 2–1.)

Public Law 97–255
Federal Managers' Financial Integrity Act (FMFIA) (Cited in para 1–15*e*.)

Public Law 101–576
Chief Financial Officers Act of 1990 (Cited in para 1–14.)

Public Law 104–208
Federal Financial Management Improvement Act (FFMIA) (Cited in para 1–5*b*(8).)

Public Law 113–101
Digital Accountability and Transparency (DATA) Act of 2014 (Cited in para 5–1.)

31 USC 501
Chief Financial Officers Act of 1990 (Cited in para 1–14.)

31 USC 3512
Executive agency accounting and other financial management reports and plans (Cited in para 1–5*b*(8).)

31 USC 6101
Definitions (Cited in para 5–1.)

Section II

Prescribed Forms

This section contains no entries.

Appendix B

Internal Control Reporting Categories

B–1. Reporting Guidelines

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

B–2. Reporting Categories

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

a. Communication, 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). It also covers the DoD programs for protection of classified information.

b. 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. It 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–123.

c. 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, according to OMB Memorandum, Conducting Acquisition Assessments under OMB Circular A–123; and guidance issued by DoD Acquisition, Technology, and Logistics “Assessment of Acquisition Functions” under OMB Circular A–123.

d. Financial reporting (pertaining to Internal Control over Reporting-Financial Reporting). Processes, procedures, and systems used to prepare, compile, and generate the DoD financial statements according to OMB Circular A–123, and DoD 7000.14–R, Volume 1, Chapter 3; the Federal Accounting Standards Advisory Board guidance, GAAPs; the Department of the Treasury Financial Manual, Volume 1, Federal Agencies and U.S. Government Standard General Ledger; and the financial reporting guidance established by OMB Circular A–136.

e. Financial systems (pertaining to Internal Control over Reporting-Financial Systems) conformance with Federal requirements. The assessment, evaluation, and reporting of achievement or material weakness(es) of the IFMS’s conformance with Federal requirements for financial systems in accordance with 31 USC 1101, 31 USC 3512, and 31 USC 7501; OMB Circular A–127; and DoD 7000.l4–R Volume 1, Chapter 3.

f. Force readiness. The operational readiness capability of combat and combat support (both Regular Army and Army Reserve) forces based on analyses of the use of resources to attain required combat capability or readiness levels.

g. 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. DoDD 8000.01 may be helpful when evaluating a weakness for inclusion in this category.

h. Major systems acquisition. Items designated as major systems, subject to the procedures of the Defense Acquisition Board, the Military Services Acquisition Review Councils, or the Selected Acquisition Reporting System. DoDD 5000.01 and DoD 8910.1–M may be helpful when evaluating a weakness for inclusion in this category.

i. 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. It includes depot and arsenal-type facilities as well as intermediate and unit levels of military organizations.

j. Other (primary transportation). All functional responsibilities not represented by any other functional category, including management and use of land, sea, and air transportation for movement of personnel, materiel, supplies, and equipment using military and civilian sources.

k. Personnel and/or organization management. Authorizations, recruitment, training, assignment, use, development, and management of military and Civilian DoD personnel. It also includes the operations of HQs' organizations. Contract personnel are not covered by this category.

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

m. Property management. Construction, rehabilitation, modernization, expansion, improvement, management, and control over real property (both military and civil works construction), to include installed equipment, and personal property. It also covers disposal actions for all materiel, equipment, and supplies including the Defense Reutilization and Marketing System.

n. 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.

o. Security assistance. Management of DoD foreign military sales, grant aid, and International Military Education and Training Programs.

p. 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). It 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).

q. Support services. All support service functions financed from appropriated funds not covered by the other reporting categories such as health care, veterinary care, and legal and public affairs services. All non-appropriated fund activities are also covered by this category.

Glossary of Terms

Annual Statement of Assurance
The ASA represents the agency head's informed judgement as to the overall adequacy and effectiveness of internal controls within the agency relating to operations, reporting, and compliance. Section 2 of FMFIA requires the head of each executive Agency annually submit to the President and the Congress (1) a statement on whether there is reasonable assurance that the Agency's controls are achieving their intended objectives; and (2) a report on MW in the Agency's control. The Army's ASOA is required by OSD for consolidation into the DoD ASOA submission to Congress.

Army Audit Committee
A committee or board of senior functional officials convened to advise the Head of an organization on risk and internal control matters, including the identification of risks and internal control weaknesses that merit the attention of Army leadership and reporting as MWs.

Assessable Unit
ROs are segmented into AUs, which in turn are responsible for conducting internal control evaluations in accordance with the ICEP.

Assessable Unit Manager
The military or civilian Head of an AU. Preferably at the general officer or senior executive service level but not lower than an O–6, GS–15, or equivalent. In exceptional cases where the grade structure does not support having an AUM at this level, the AUM is the senior military or HQDA Civilian functional manager. The AUM ensures that the results of required internal control evaluations are certified.

Attribute
An attribute is a characteristic defined in process documentation to which the evaluator can assign descriptions to analyze characteristics in a given population to validate internal control function.

Brevity code
A shortened form of frequently used phrases, sentences, or a group of sentences normally consisting entirely of upper-case letters (for example, COMSEC for communications security).

Enterprise Risk Management
An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges, and improved insight about how to prioritize and manage risks to mission delivery more effectively.

Entity Level Control
Entity Level Controls are controls that have a pervasive effect on an entity's internal control system and may pertain to multiple components. Entity level controls may include controls related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring.

Financial Statement Reporting Entity
For the Army, these include the general fund, Army working capital fund, and the civil works fund (Corps of Engineers).

Fraud Risk Management
A sub-division of ERM. A framework that encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks in all levels of the organization.

Government Accountability Office Standards for Internal Control in the Federal Government
The standards issued in the GAO Green Book GAO–14–704G to be applied by all managers in the Federal Government in developing, establishing, and maintaining internal controls.

Head of Reporting Organization
The person who is responsible for executing the RMIC Program within their respective organization by understanding and applying the GAO standards for internal control in the Federal Government, carrying out the RMIC Program within their respective organization.

Headquarters, Department of the Army functional proponent
The HQDA principal responsible for policy and oversight of a functional area.

Internal Control Administrator
The individual appointed by the SRO to administer the RMIC Program for a RO. The AUMs designate ICAs below the RO 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 individuals 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 are conducted over a 5-year period. The ICEP is based on the risk assessment results and includes who will conduct the evaluation, when, and how. It covers the key internal controls HQDA functional proponents identified and communicates clearly to subordinate managers what areas are to be evaluated.

Internal Control Evaluator
The individual(s) designated by the AUM to administer the internal control evaluation. This is not an inherently government role and must be independent of the function assessed.

Internal Controls
The rules, procedures, techniques, and devices employed by managers to ensure that what occurs 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 essential internal controls implemented and sustained in daily operations to ensure organizational effectiveness and compliance with legal requirements. Key controls must operate effectively to reduce the risk to an acceptable level.

Material Weakness
A MW 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 MW, two conditions must be met:
a. It must involve a weakness in internal controls (such as internal controls are not in place, are not being used, or they are inadequate).
b. 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 MWs.

Reporting Organization
The HQDA staff agencies, ACOMs, ASCCs, and DRUs. These are the organizations that submit ASOAs directly to ASA (FM&C) for consolidation and submission to the SECARMY.

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, the risk assessment measures two qualities or attributes of the risk:
a. The magnitude of the potential loss.
b. The probability that the loss will occur. In addition, the key internal controls employed to reduce risk need not exceed the benefits derived.

Senior Responsible Official
Designated by the HRO, the SRO has overall responsibility for ensuring the implementation of an effective RMIC Program within that organization.

Service Provider
An organization providing services to Army, for which these services are likely to be relevant to Army's internal controls over financial reporting. This is an external entity providing a service to the Army, which holds responsibility for communicating the SOC 1 report as well as performing controls (which are inclusive of corrective actions over those controls).

Significant Deficiency
Significant Deficiency is a pervasive internal control weakness that disrupts or disables good order of financial and nonfinancial operations rendering unacceptable risk levels with potential for fraud, waste, abuse, mismanagement, and loss of life or limb.

Test of Design
An assessment of the design of a control to determine if it meets the relevant risks that the control is intended to cover, and to determine whether the controls have been implemented as designed.

Test of Effectiveness
An assessment of the design of the control to determine that it was performed consistently over a period of time.