Headquarters
Department of the Army
Washington, DC
16 July 2024

***Army Regulation 11–2**

Effective 16 August 2024

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 publication is a major revision. The portions affected by this revision are listed in the summary of change.

Authorities. This regulation implements DoDI 5010.40.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, 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.

Army internal control process. This regulation contains internal control provisions and identifies key internal controls that must be evaluated (see appendix B).

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.
Committee management approval statement. AR 15–39 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the Office of the Administrative Assistant to the Secretary of the Army, Special Programs Directorate at email usarmy.pentagon.hqda-hsa.mbx.committee-management@army.mil. Further, if it is determined that an established "group" identified within this regulation later takes on the characteristics of a committee as found in AR 15–39, then the proponent will follow AR 15–39 requirements for establishing and continuing the group as a committee.

Distribution. This regulation 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.

*This regulation supersedes AR 11–2, dated 4 January 2010.

SUMMARY of CHANGE

AR 11–2
Risk Management and Internal Control Program

This major revision, dated 16 July 2024—

- Changes the program title from Managers' Internal Control Program to the Risk Management and Internal Control Program (cover).
- Update's responsibilities of all roles (chap 1).
- Requires appointment of members to the Army Audit Committee (para 1–7*d*).
- Communicates the risk management governance structure to enhance the flow of information throughout Army (para 1–8).
- Incorporates language for Internal Control Over Reporting (para 1–8*f*).
- Establishes the Army's Continuous Monitoring Program to centralize the testing of Internal Control Over Reporting-Financial Reporting (para 1–9).
- Communicates the requirement to establish and maintain financial management systems in accordance with 31 USC 3512 note (para 1–16*b*(8)).
- Updates existing risk and internal control requirement (para 2–1).
- Incorporates an Enterprise Risk Management framework as required by Office of Management and Budget Circular No. A–123, M–16–17 (para 2–2).
- Aligns the Risk Management and Internal Control Program's implementation with the Government Accountability Office's Federal Government Standard for Internal Controls (para 2–2*a*)
- Revises the requirements of how internal control evaluations are conducted and documented to support a risk-driven program (para 2–4).
- Internal Control Evaluations (formally known as checklists) remain a component of the program (para 2–4).
- Implements the assurance reporting requirements for internal control processes in accordance with 31 United States Code 3512 (para 2–9).

Contents (Listed by chapter and page number)

Chapter 1
Introduction

Section I

General

1–1. Purpose
This regulation establishes and prescribes requirements for the Risk Management and Internal Control (RMIC) Program. The head of Army Reporting Organizations (ROs) must establish a RMIC Program to evaluate and report on the effectiveness of internal controls throughout their organization and subordinate organizations. The head of Reporting Organizations (HROs) will implement internal controls to mitigate risks. HROs will perform risk assessments, develop, implement, and conduct internal control testing to help the Army achieve its mission. The RMIC Program will be executed in accordance with this policy, the Annual Statement of Assurance (ASOA) Guidance issued by the Office of the Assistant Secretary of the Army (OASA) (Financial Management and Comptroller (FM&C)), and Department of the Army (DA) Pamphlet (DA Pam) 11–2 guidance. The RMIC Program's ASOA Guidance and supplementary information correspond with the policy prescribed in this regulation and guidance found in DA Pam 11–2, and serves as the authoritative guidance, detailing the requirements for RMIC Program execution.

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
Procedures associated with this regulation are found in DA Pam 11–2.

1–4. Responsibilities
See Section II of this chapter

1–5. 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

Responsibilities

1–6. Secretary of the Army
See DA Pam 11–2 for mandatory procedures. Pursuant to the requirements of Office of Management and Budget (OMB) Circular No. A–123 appendices and memorandums, Federal Financial Management Improvement Act (FFMIA) (31 United States Code (USC) Section 3512 note) Government Performance and Results Act Modernization Act of 2010 (GPRAMA) (Public Law (PL) 111–352), Government Accountability Office (GAO) 14–704G, and DoDI 5010.40, the Secretary of the Army (SECARMY) will—

a. Support the Office of the Secretary of Defense's (OSD) efforts to conduct an annual performance and strategic review that incorporates risk identification and analysis in accordance with OMB Circular A–123, M–16-17's Enterprise Risk Management (ERM) requirements and OMB Circular A–11's requirements for Performance and Strategic Reviews.

b. Report to OSD the Army's strategic objectives for priority areas outlined in the Army's Strategy (and other strategic plans) to identify key enterprise risks aligned to the execution of priority areas.

c. Maintain an environment of accountability within the Army that supports an effective system of internal control to achieve its mission.

d. Provide an opinion in the ASOA on the overall adequacy and effectiveness of the system of internal control and the Army's ability to meet its objectives.

e. Submit the ASOA to the Office of the Undersecretary of Defense-Comptroller (OUSD–C) and provide a copy to the Director of Financial Improvement and Audit Readiness.

1–7. Assistant Secretary of the Army (Financial Management and Comptroller)

The ASA (FM&C) will—

a. Delegate responsibility for facilitation and implementation of the Army RMIC Program to the Deputy Assistant Secretary of the Army (Financial Operations and Information) (DASA–FOI). See DA Pam 11–2 for mandatory procedures.

b. Ensure the Director, Army Risk Management within the DASA–FOI performs responsibilities listed in paragraph 1–8.

c. Ensure the Director, Financial Information Management (FIM) within the DASA–FOI performs responsibilities listed in paragraph 1–10.

d. Establish and provide oversight for the Army Audit Committee to include appointing members to perform the responsibilities in paragraph 2–1.

1–8. Director, Army Risk Management

The Director, Army Risk Management will—

a. Establish the following roles within the RMIC Program for execution within each RO. See the DA Pam 11–2 for mandatory procedures for the established roles.

(1) 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 and carrying out the RMIC Program within their respective organization.

(2) Senior Responsible Official (SRO) is the individual designated by the HRO. The SRO has overall responsibility for ensuring the implementation of an effective RMIC Program within that organization. See DA Pam 11–2 for mandatory procedures.

(3) Assessable Unit Manager (AUM) is the military or civilian head of an assessable unit and may be designated by the HRO or SRO. See DA Pam 11–2 for mandatory procedures.

(4) Internal Control Administrator (ICA) is the individual designated by the HRO, SRO, or AUM to administer the RMIC Program for the RO. The AUMs designate ICAs below the RO level.

(5) Internal Control Evaluator (ICE) is the individual(s) designated by the HRO, SRO, or AUM to administer the internal control evaluation. This is not an inherently governmental role and must be independent of the function assessed. See DA Pam 11–2 for mandatory procedures.

b. Assist the ASA (FM&C) in formulating Army policy for implementation of Federal Managers' Financial Integrity Act (FMFIA) (31 USC 3512), OMB Circular No. A–123 appendices and memorandums, DoDI 5010.40, and all other applicable internal control regulations. Issue administrative and procedural guidance and instruction for program execution, to include a DA Pam, ASOA Guidance and supplemental guidance.

c. Periodically analyze documents from Congress, GAO, OMB, the Comptroller General, OSD, and others to identify and implement changes to the Army RMIC Program and to support the five-year publication lifecycle in accordance with DA Pam 25–40.

d. Develop and oversee the governance and implementation of the ERM framework and annual risk assessment to OSD.

e. Establish, develop, and distribute program documentation that supports the facilitation and execution of the RMIC Program and provide a reporting mechanism for the ASOA.

f. Advise and represent ROs on matters involving Internal Control Over Reporting-Financial Reporting (ICOR–FR), Internal Control Over Reporting-Operations (ICOR–O), and Internal Control Over Reporting-Financial Systems (ICOR–FS).

g. Conduct the annual financial materiality assessment to determine the scope of the RMIC Program. See DA Pam 11–2 for mandatory procedures.

h. Provide guidance and technical assistance directly to ROs for implementation and assessment of internal controls. See DA Pam 11–2 for mandatory procedures.

i. Develop and facilitate training with command-level and field-level organizations.

j. Administer trainings to key stakeholders to include Monthly Office Hour meetings, issuing Quarterly Newsletters, conducting instructor-led trainings for Armywide summits/conferences, and developing curriculum for reoccurring RMIC Program trainings.

k. Coordinate with Army HROs to facilitate the completion of the ASOA feeder packages.

l. Consolidate ASOA feeder package submissions from ROs into the SECARMY's ASOA and submit to OUSD–C through the staffing process.

m. Collect and review the Continuous Monitoring Program (CMP) draft financial risk profiles and deficiencies analysis and the ROs' draft risk profiles and deficiency analysis.

n. Review material internal control weaknesses submitted by Headquarters, Department of the Army (HQDA) functional proponents to determine if additional coordination is required.

o. Coordinate with the U.S. Army Audit Agency (USAAA) and HQDA functional proponents to identify internal control deficiencies that merit reporting as material weaknesses (MWs) in the SECARMY's ASOA.

p. Develop internal control training materials for use by ROs, their assessable units, HQDA functional proponents, Army schools that provide executive development and management training, audit, inspection, and other organizations whose personnel assess the effectiveness of internal controls.

q. Develop and maintain a tracking system to ensure that MWs reported in the SECARMY's ASOA are corrected in a timely manner.

r. Ensure adequate monitoring activities are performed to obtain assurance regarding the effectiveness of Internal Control Over Reporting (ICOR) for the Army as a whole. This involves obtaining appropriate assurances from reporting units of the Army.

s. Monitor RO compliance with program requirements.

t. Develop and staff the Army's position on reports by GAO, Department of Defense Inspector General (DoDIG), USAAA and similar organizations on the overall Army RMIC Program.

u. Develop and maintain a list of completed MWs and significant deficiencies (SDs) as they are removed from the RO's MW and SD Appendix.

v. Develop and maintain an inventory of Army ROs through assessable units based on annual input from HQDA functional proponents, Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs).

w. Provide advice and technical guidance to HQDA functional proponents on how to use process narratives, process flows, conducting risk assessments, and monitoring for ICOR–FR, ICOR–O, and ICOR–FS.

x. Submit OMB Circular No. A–123 deliverables to OUSD–C.

y. Ensure internal controls with MWs in operations, reporting, and compliance include Corrective Action Plans (CAPs). CAPs must be updated at least annually. SDs also require a CAP.

z. Ensure timely CAP development for all systemic MWs and conduct monitoring of approved CAPs.

aa. Respond to auditor requests during audit or examination of ICOR–FR, ICOR–O, and ICOR–FS information.

bb. Develop and maintain a list of Entity Level Controls (ELCs) for reporting.

cc. Develop and maintain an Army Control Catalog.

dd. Conduct periodic assessments of ROs to determine compliance with guidance issued by the Director, Army Risk Management.

ee. Coordinate with the Director, FIM to develop and maintain the Digital Accountability and Transparency Act of 2014 quality plan for the Army pursuant to the requirements of Public Law 113–101, and OMB Circular No. A–123, M–18–16, Appendix A.

ff. Develop, update, and maintain templates for ASOA feeder package submissions.

gg. Designate the RMIC Program Manager as the OSD Fraud Reduction Task Force Representative.

hh. Develop, implement, and maintain an ERM Framework to include Fraud Risk Management (FRM) integrated into the RMIC program.

1–9. Director, Continuous Monitoring Program, Risk Management and Internal Control

The Director, CMP, RMIC will—

a. Provide overall CMP, governance, review, and reporting.

b. Establish CMP guidance and validation of Armywide reporting CAPs.

c. Review and report program progress to Army Executive Leadership.

d. Oversee the development and governance of a centralized internal testing program over business processes with a financial statement impact.

e. Establish and maintain financial management systems in accordance with FFMIA and OMB Circular No. A–123, M–23–06, Appendix D, to substantially comply with Federal Financial Management System Requirements, applicable Federal accounting standards, and the U.S. Standard General Ledger (USSGL) at the transaction level.

f. Develop and publish FFMIA guidance in addition to facilitating testing with system owners.

g. Report the appropriate system evaluation results in the ASOA feeder package submission through DASA–FOI.

h. Advise and represent ROs on matters involving ICOR–FR.

i. Develop procedural guidance in the DA Pam 11–2.

1–10. Director, Financial Information Management

The Director, FIM will—

a. Manage the Army's Data Quality Plan, perform testing of data quality elements, and report results in the ASOA.

b. Develop and implement the Army Financial Information Guidance and Plan of Action & Milestones which communicates key FFMIA management activities to Army financial management, financial information stakeholders, system owners, security managers, and resource managers.

1–11. United States Army Financial Management Command, Director, Process Management & Compliance

The Director, PMC will—

a. Provide advice and technical guidance to the ACOMs, ASCCs, and DRUs on how to interpret process narratives and process flows as well as conducting risk assessments, and monitoring for ICOR–FR.

b. In coordination with Director, Army Risk Management and Director, CMP, RMIC:

(1) Support the development and execution of a centralized internal testing program over business processes with a financial statement impact.

(2) Provide guidance and technical assistance directly to ROs for implementation and assessment of financial internal controls.

(3) Develop and maintain an Army Control Catalog for financial report controls.

(4) Advise and support ROs on matters involving ICOR–FR.

c. Perform additional duties at the request of the Director, Financial Operations and Accounting, OASA (FM&C)–DASA (FOI).

d. Develop and facilitate training with command-level and field-level organizations.

e. Coordinate with Army HROs to facilitate the completion of the ASOA feeder packages.

f. Develop internal control training materials for use by ROs, their assessable units, HQDA functional proponents, Army schools that provide executive development and management training, audit, inspection, and other organizations whose personnel assess the effectiveness of internal controls.

1–12. The Auditor General, United States Army Audit Agency

The Auditor General, USAAA, in accordance with the functional responsibilities delegated by the SECARMY and prescribed in AR 36–2, will—

a. Provide technical advice, assistance, and consultation on internal controls to the Army Audit Committee, as necessary.

b. Evaluate during the normal course of audits executed by USAAA, the effectiveness of internal controls, the adequacy of internal control evaluations, and the adequacy of actions taken to correct MWs. The Director, Army Risk Management may request additional evaluations of internal controls and MWs through the established process identified in AR 36–2.

c. Provide periodic reports to the Director, Army Risk Management, summarizing internal control and systemic weaknesses identified in USAAA audits.

d. Identify proposed Army-level MWs and provide the information to HQDA functional proponents, when requested by the Director, Army Risk Management, for reporting in the SECARMY's ASOA.

e. Coordinate with the Director, Army Risk Management, and submit annually to the DoDIG a list of potential Army MWs identified during audits, along with the Army's position on the potential MWs.

1–13. Department of the Army Inspector General
The DAIG will consider (during the normal course of inspections) internal controls when assessing systemic issues and problems and will make appropriate recommendations.

1–14. Internal Review directors and/or chiefs
Where there are existing IR offices established, IR Directors, IR Chiefs, and other heads of Army IR offices, in accordance with the functional responsibilities delegated by the SECARMY and prescribed in AR 11–7, will—

a. Provide technical advice, assistance, and consultation on internal controls to the SRO and AUMs within their respective commands/activities, as necessary.

b. Evaluate, during the normal course of audits, the effectiveness of internal controls, the adequacy of internal control evaluations, and actions taken to correct MWs involving the subject matter.

c. Analyze USAAA, IR, and external audit reports affecting the local command/activity as they are released to identify findings involving control weaknesses which may warrant reporting as MWs or impact the RO's assessment of its internal control environment and notify the SRO, applicable AUMs, and applicable ICAs of these control weaknesses on a periodic basis or as they are identified.

d. Evaluate the local command/activity ASOA for thoroughness, validity, and compliance with current ASA (FM&C) ASOA guidance prior to the time the HRO approves and submits the ASOA to ASA (FM&C).

e. Independently evaluate as feasible, the implementation of local command/activity CAP milestones to validate whether the corrective actions taken have in fact resolved the MWs the CAPs were intended to remediate.

1–15. Headquarters, Department of the Army functional proponents
The HQDA Proponents will—

a. Develop or advise on the development of policies and regulations that support an effective internal control environment.

b. Determine, through risk assessment, the key risk areas to include FRM, and controls for evaluation in accordance with the monitoring requirements outlined in DA Pam 11–2 and the ASOA Guidance.

c. Review internal control MWs submitted by ACOMs, ASCCs, and DRUs to determine if deficiencies require additional coordination, assess their materiality, and provide written feedback.

d. Track the progress of correcting MWs reported in the SECARMY's ASOA in addition to MWs reported by the ACOMs, ASCCs, and DRUs and provide status updates when requested by the Director, Army Risk Management.

e. Assist the Director, Army Risk Management, in composing and reviewing the SECARMY's ASOA to maintain effective quality control over the accuracy of information reported.

1–16. Heads of Reporting Organizations
SECARMY elements/offices and HQDA Staff offices, ACOMs, ASCCs, and DRUs are the primary ROs in the Army RMIC Program. The HRO will—

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

b. Prepare an ASOA feeder package for submission to the Director, Army Risk Management, in compliance with this regulation, ASOA guidance, supplemental guidance, and DA Pam 11–2. See DA Pam 11–2 for mandatory procedures. The submission will include—

(1) An Assurance Memo that expresses an opinion (reasonable assurance with no exceptions, assurance with exceptions, 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 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 note (Federal Financial Management

Improvement Act), OMB Circular No. A–123, M–23–06, Appendix D, and the OASA (FM&C) annual financial management systems guidance.

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

1–17. Commanders of installations, major subordinate commands, and table of organization and equipment divisions

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

a. Ensure the HRO conducts the required internal control evaluations according to the governing ICEP and communicate the results to the ICA.

b. As applicable, ensure that internal control responsibilities are explicitly documented in the employee performance management system "objectives" or "elements" and the Officer Evaluation Report support forms of commanders, managers, and ICAs (including ICAs at the assessable unit level).

1–18. Chief, National Guard Bureau

The CNGB will ensure State Adjutants General will—

a. Direct the HROs to conduct the required internal control evaluations according to the governing ICEP and communicate the results to the ICA.

b. As applicable, ensure that internal control responsibilities are explicitly documented in the employee performance management system "objectives" or "elements" and the Officer Evaluation Report support forms of commanders, managers, and ICAs (including ICAs at the assessable unit level).

Chapter 2
Program Requirements

2–1. The Army Audit Committee

In accordance with OMB Circular No. A–123, M–16–17 the SECARMY will establish a body to govern risk and internal control responsibilities throughout the organization. The governing entity is referred to as the Army Audit Committee and will execute the following requirements—

a. Provide oversight for the strategic direction of the Army's RMIC Program.

b. Ensure Army's implementation of OMB and Department of Defense (DoD) requirements related to risk and internal controls by communicating the RMIC Program's objectives throughout the Army.

c. Assist DA senior leaders with implementing an internal control framework and fostering an organizational environment that supports continuous awareness of internal controls, including complementary user entity controls from service providers. See DA Pam 11–2 for mandatory procedures.

d. Determine the Armywide risk appetite and risk tolerance levels.

e. Maintain an open and transparent culture that supports the identification and prioritization of risks and a collaborative response.

2–2. Enterprise risk management

The Chief Financial Officers and Performance Improvement Councils' Playbook: "Enterprise Risk Management for the U.S. Federal Government", defines ERM as 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 more effectively. See DA Pam 11–2 for mandatory procedures.

a. OMB Circular No. A–123, M–16–17 requires Agencies to integrate ERM into the RMIC Program to include establishing internal controls to manage fraud risk. An implemented ERM capability is to be coordinated with the strategic planning and review process established by the GPRAMA and internal control processes required by FMFIA and the GAO Green Book. Therefore, ERM reinforces the purposes of FMFIA and GPRAMA and supports improvements in running an effective and efficient Government.

b. Army personnel will consider the following requirements in developing and maintaining a FRM framework. The GAO's FRM Framework (GAO–15–593SP) provides best practices to create fraud risk profiles within the ERM program. OMB Circular No. A–123, M–16–17 requires the use of GAO's FRM Framework in managing federal programs at all levels in the organization and to integrate as part of ERM

within the RMIC program. Financial and administrative controls relating to fraud and improper payments are required by 31 USC 3357. OMB Circular No. A–123, M–21–19, Appendix C implements the Payment Integrity Information Act of 2019 (PL 116–117), the GAO Green Book provides standards in assessing fraud risk, and the DoD Statement of Assurance Execution Handbook provides DoD-wide requirements in implementing FRM. See DA Pam 11–2 for mandatory procedures.

c. The SECARMY in coordination with the Army Audit Committee is responsible for ERM. ERM enables senior leaders with better decision making, improving accountability and the effectiveness of Army's programs and mission-support operations.

d. ERM is used to identify challenges from the bottom up and top-down approach, bring them to the attention of Army leadership, and to develop solutions. The RO's risk assessment reported in the ASOA Risk Assessment and ICEP Appendix will be incorporated into the Armywide ERM risk profile to include fraud risk. The ERM risk profile is used in the decision making for Army's strategic objectives reported to OSD and throughout the organization. Refer to the DA Pam 11–2 for detailed information. See DA Pam 11–2 for mandatory procedures.

2–3. Established program documentation

The following program documentation is required. A brief description along with minimum requirements are listed below. Reporting requirements are updated annually as part of the ASOA Guidance. The Director, Army Risk Management is responsible for maintaining program documentation content and format (see para 1–8). See DA Pam 11–2 for mandatory procedures.

a. Assurance Memo. The Assurance Memo template provides an opinion over the operational effectiveness of internal controls in accordance with FMFIA. The memo 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.

b. Risk Assessment and Internal Control Evaluation Plan Appendix. The Risk Assessment and ICEP template links risks and the associated controls that require evaluation. The Risk Assessment and ICEP sets the course of action for testing for the year and should be continuously updated as additional risks and controls are identified.

(1) The Risk Assessment allows users to assess inherent and residual risks to Army's objectives, as well as the RO's objectives.

(2) The ICEP captures the internal control evaluations planned for a 5-year period (covering the current year and following 4 years). Adequately planning will ensure a structured approach to identifying control deficiencies on an ongoing basis.

(3) At minimum, the Director, Army Risk Management, will require the following information in the ICEP—

(a) Content structured by business process area.

(b) Description of key controls as identified in the process.

(c) Identification of Individual or group(s) responsible for conducting the evaluations.

(d) Determination of frequency and monitoring method to be used for conducting the evaluation (information for determining rationale is communicated in the annual RMIC Program guidance).

(e) Identification of governing ARs, federal regulations, or standard operating procedures.

(4) The SRO or AUM must sign and submit the Risk Assessment and ICEP approval memorandum prior to commencing internal control evaluations. See DA Pam 11–2 for mandatory procedures.

(a) HROs will clearly communicate to the AUMs the areas to be evaluated and the frequency of evaluations.

(b) The HROs will designate their ICE(s) to conduct evaluations. It is at the AUMs discretion to identify the ICEs to conduct the evaluations. The evaluator performing the testing should be independent from the function being performed and evaluated. See DA Pam 11–2 for mandatory procedures.

(5) The HRO will incorporate key internal controls or processes identified by HQDA functional proponents and the Director, Army Risk Management, into the ICEP. HROs may be directed to conduct reviews in areas in addition to their ICEP based on materiality, identified control gaps, ARs, or as directed by the Director, Army Risk Management.

c. Internal Control Evaluation Appendix. The Internal Control Evaluation appendix summarizes the internal control test results to support the opinion in the assurance memo. The Internal Control Evaluation will be supported by the DA Form 11–2 (Internal Control Evaluation Certification). See paragraph 2–4 for additional information on internal control evaluations.

d. Entity Level Control Matrix Appendix. The ELCs have a pervasive effect on the Army's internal control system.

e. Reportable Anti-Deficiency Act Violations Appendix. HROs will report any Anti-Deficiency Act violations or mark the template as "Not Applicable".

f. Material Weaknesses and Significant Deficiencies Appendix. HROs will report all MWs and SDs as part of the feeder package.

g. Significant Internal Control Program Accomplishments Appendix. HROs will report all significant internal control improvements achieved in the fiscal year.

h. Risk Management and Internal Control Program Training Appendix. HROs are required to complete the minimum role-based training requirements and report it in this appendix.

i. DA Form 11–2. The DA Form 11–2 is required to accompany each RO's test plan, serving as the cover sheet to capture activities that occurred during testing. ASA (FM&C) and the Commander, U.S. Army Financial Management Command will evaluate the form as part of RMIC Program compliance. At minimum, the form captures logistical information, test methodology, sample size, control deficiencies, and identifies the individual conducting the evaluation. See DA Pam 11–2 for mandatory procedures.

2–4. Internal control evaluations

a. Internal control evaluations are designed to identify deficiencies that diminish an organization's effectiveness in achieving its objectives related to operational efficiency, regulatory compliance, and reliability of reporting. The overall focus of internal control monitoring is to evaluate activities in place to mitigate the RO's identified risks and to specifically obtain sufficient competent evidence about the design and operating effectiveness of control activities. The evaluator performing the testing should be independent from the function being performed and evaluated. See DA Pam 11–2 for mandatory procedures.

b. This policy establishes the use of internal control evaluations. Internal control evaluations come in different formats such as test plans, the DA Form 11–2 and other formal test methods that enable the reviewer to assess controls and provide sufficient evidence of the assessment. The ASOA Guidance will communicate the appropriate combination of documentation for conducting internal control evaluation such as—

(1) DA Form 11–2. The AUMs certify completion of an internal control evaluation by providing concurrence on the DA Form 11–2. The remarks box will include a description of the test method used. If the designated testing methodology was not used, an explanation of the alternate method is required in the remarks box. The form is available in electronic media on the Army Publishing Directorate's website under forms (https://armypubs.army.mil). See DA Pam 11–2 for mandatory procedures.

(2) Test Plans. Test Plans will capture the appropriate level of detail to support the conclusions reached. This includes testing methodology, population, and sample selection, individual samples evaluated, and so forth. See DA Pam 11–2 for mandatory procedures.

(a) HROs may leverage standardized test plans issued by the RMIC Program.

(b) HROs may develop test plans to meet their individual evaluation needs if the test plans produced meet the minimum requirements communicated by the Director, Army Risk Management.

(3) AR Internal Control Evaluation. The HQDA functional proponent may develop or identify key controls for incorporation into an Internal Control Evaluation and publish it as appendix B in the governing AR for use by managers and ICEs to guide evaluations of the effectiveness of the listed controls.

(a) Testing. Substantial testing must be conducted to support the questionnaire responses. Figure 2–1 is the format for the Internal Control Evaluation. Commanders and managers may use the functional proponent's published evaluation or, as an alternative, may use an existing management review process of their own choosing, so long as the method chosen meets the basic requirements of an evaluation outlined in this paragraph. Functional proponents are encouraged to review their publications at a minimum of every 18 months and, as appropriate, revise the publication at least every five years (see AR 25–30 for specific requirements).

(b) Alternative Internal Control Evaluations. In many areas, existing management review processes may meet, or be modified to meet, the basic requirements of an internal control evaluation. Some of the processes are unique to a specific functional area, while others are more generic, such as the use of local, inspector general, IR personnel, or the command review and analysis process. The HQDA functional proponents may suggest an existing management review process for evaluating key internal controls; or they may require the use of a specific functional management review process, so long as it is an existing Armywide process and one for which they are the functional proponent. The HQDA functional proponents

must provide the necessary information as an appendix to the governing AR in accordance with DA Pam 25–40. Figure 2–2 is the format for identifying key internal controls and evaluation processes if an Internal Control Evaluation is not provided. Unless the HQDA functional proponent requires the use of an existing Armywide functional management review process, commanders, and managers are free to choose the method of evaluation.

Appendix B Internal Control Evaluation
B—1. Function. The function covered by this evaluation is (indicate the function covered by this questionnaire).
B—2. Purpose. The purpose of this evaluation is to assist (indicate intended users) in evaluating the key internal controls listed. It is intended as a guide and does not cover all controls.
B—3. Instructions. Answers must be based on the actual testing of key internal controls by utilizing one of four test methods which are Inquiry, Observations, Examination, or Re-performance. Inquiry regarding a control's effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively and generally is corroborated through other types of control tests (observation or inspection). Answers that indicate deficiencies must be explained and corrective action identified in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on a DA Form 11-2 (Internal Control Evaluation Certification).
B—4. Key Control Questions. (Insert the key control questions worded so that negative answers indicate an internal control deficiency or weakness. Include key control and list of key supporting documentation).
a.
b.
c.
B—5. Supersession. This evaluation replaces the evaluation(s) for (insert the task/subtask covered by the previous evaluation) previously published in (insert the previous AR number, dated ____).
B—6. Comments. Help to make this a better tool for evaluating internal controls. Submit comments to (insert the complete mailing address for HQDA functional proponent.

Figure 2–1. Appendix Format using the Key Internal Control Questionnaire

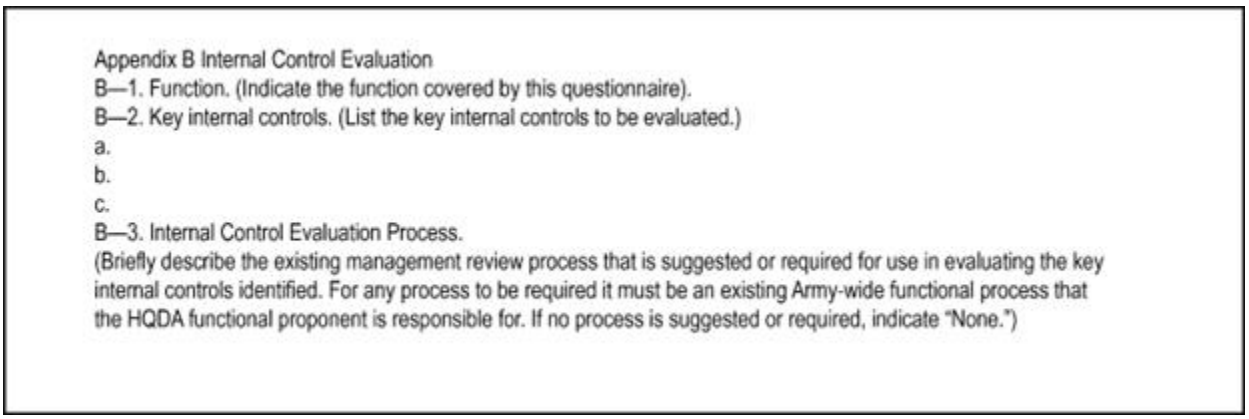

Figure 2–2. Appendix Format using an Alternative Internal Control Evaluation

2–5. Federal Financial Management Improvement Act of 1996

a. FFMIA, Section 803(a) requires that each agency establish and maintain financial management systems that "substantially" comply with (1) Federal Financial Management System Requirements, (2) applicable Federal Accounting Standards and (3) the USSGL at the transaction level. See DA Pam 11–2 for mandatory procedures.

(1) The Act's purposes include providing uniform accounting standards, requiring systems to support full disclosure of Federal financial data, increasing the accountability and credibility of federal financial management, improving the performance, productivity, and efficiency of Federal Government financial management, and establishing financial management systems to support controlling the cost of Federal Government.

(2) The DoD Financial Management Regulation (DoD 7000.14–R, Volume 1, Chapter 2) requires the reporting of accounting information in accordance with generally accepted accounting principles. The Federal Accounting Standards Advisory Board is designated by the American Institute of Certified Public Accountants as the source of generally accepted accounting principles. The Federal Accounting Standards Advisory Board develops accounting standards and principles for the U.S. Government. Army personnel must adhere to the generally accepted accounting principles hierarchy prescribed in the Statement of Federal Financial Accounting Standards 34.

(3) Pursuant to the DoD Financial Management Regulation, financial events must be recorded by applying the requirements of the USSGL guidance in the Treasury Financial Manual (TFM) and DoD USSGL transaction library (See TFM, Volume 1, Chapter 1000 for specific requirements).

b. The Director of FIM (DASA–FOI) will facilitate testing with system owners in accordance with the FFMIA guidance.

(1) Army HROs, in close coordination with system owners, portfolio managers, and Information System Security Officers must confirm annual FFMIA compliance is completed in accordance with OMB Circular No. A–123, M–23–06, Appendix D; DoD 7000.14R, Volume 1, Chapter 3 and DoDI 8510.01.

(a) The HRO must ensure Army financial systems and mixed system records are maintained relevant to financial statement audit, ICOR, and ICOR–FS in the Financial Improvement and Audit Remediation Systems Database (FSD).

(b) OSD requires the status of FFMIA in FSD to support annual FFMIA compliance and Statement of Assurance reporting. This information includes the System Name, Date Validated, Validating Organization, an MW Indicator (as a result of the FFMIA assessment), and rationale for excluding a system from FFMIA compliance requirements.

(2) DASA–FOI tests select Information Technology controls annually and reviews results to inform FFMIA Compliance oversight responsibilities.

(a) Systems Owners that attest to being inappropriately scoped in must submit a waiver with justification for adjudication.

(b) Justifications related to anything other than an inappropriate Business Enterprise Architecture (BEA) Assertion requires signature by an Officer-06 or General Schedule-15. Justification related to an

inappropriate BEA Assertion requires signature by a General Officer or a member of the Senior Executive Service.

(c) Systems non-compliant with appropriate requirement(s) must submit remediation plans detailing how and within what timeframe appropriate requirement(s) will be implemented.

c. DASA–FOI will report the appropriate system evaluation results in the ASOA feeder package through OASA (FM&C).

2–6. Use of internal review, audit, and inspection reports

a. HQDA functional proponents, commanders, and AUMs can often take corrective or preventive action based on issues identified in USAAA, Local Office of Inspector General, IR, Independent Public Accountant (IPA) audits and inspection reports. HROs are encouraged to incorporate the results into their annual evaluation results. Such reports may address an internal control problem at only one installation, but managers throughout the Army may use the reports to identify potential problems in their own areas of responsibility and take timely preventative action.

b. The heads of IR, audit, and inspection organizations will ensure distribution of their reports to managers with primary and collateral interests at all ROs. In addition, USAAA, and DAIG prepares summaries of internal control weaknesses identified in their reports. The DoDIG also publishes periodic summaries of internal control weaknesses identified in its reports and those of GAO.

c. The ASA (FM&C) periodically distributes these summaries to ICAs at ROs to facilitate correction and mitigation of reported weaknesses and to ensure that managers can benefit from lessons learned at other activities. Finally, USAAA supports the development of the SECARMY's ASOA by identifying potential Army MWs for consideration by HQDA functional proponents.

2–7. Classification of control deficiencies

a. Control Deficiency Identification. Control deficiencies exist when the design or operation of a control does not allow stakeholders, in the normal course of performing their assigned functions, to satisfactorily accomplish their assigned functions or inhibits the prevention or detection of misstatements on a timely basis. See DA Pam 11–2 for mandatory procedures.

(1) Significant Deficiency: A significant deficiency (SD) is a control deficiency or a combination of control deficiencies, that in management's judgment, represents significant deficiencies in the design or operation of internal controls that could adversely affect the DoD and OSD Component's ability to meet its internal control objectives. See DA Pam 11–2 for mandatory procedures.

(2) Material Weakness: A MW is a specific instance of a failure in a system of control or lack of control that would significantly impair fulfillment of agency's mission, violate statutory or regulatory requirements, or significantly weaken safeguards against waste, loss, unauthorized use or misappropriation of funds, property, or other assets. The material weakness may present a major impact to the environment, safety, security, or readiness of the command. A MW can lead to a material misstatement in Army's annual financial statements or failure to execute its operations. The ability of personnel at all levels to detect and communicate internal control or systemic weaknesses and to take corrective action is the fundamental goal of FMFIA. A financial reporting material weakness is a SD, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. See DA Pam 11–2 for mandatory procedures. For an IC deficiency to be considered an MW, it must meet the following criteria—

(a) Criteria 1: Must involve a weakness in ICs—such as the controls are not in place, are not being used, or are inadequate to address stated objectives or financial statement risks. To be material the deficiency must result in one or more of the following: impairment or potential impairment of the Army's essential operations or missions; threatened image, reputation, or credibility of the Army; significant weakening of established safeguards against waste, fraud, abuse, and mismanagement of resources; demonstrated substantial noncompliance; compromised or weakened information security; or determined during an external inspection and upheld as a significant finding. Resource deficiencies in themselves are not internal control weaknesses.

(b) Criteria 2: The deficiency warrants the attention of the next level of command, either for awareness or action. The fact that a weakness can be corrected at one level does not exclude it from being reported to the next level because the sharing of important management information is one of the primary reasons for reporting an MW.

(c) Additional Factors for Consideration: In addition to the two criteria stated above, to assist in making judgments on whether internal control weaknesses are material, the HRO will consider the following factors: actual or potential loss of resources; sensitivity of the resources involved; magnitude of funds, property, or other resources involved; actual or potential frequency of loss; current or probable media interest (adverse publicity); current or probable congressional interest (adverse publicity); unreliable information causing unsound leadership decisions; diminished credibility or reputation of Army's leadership; violation of statutory or regulatory requirements; and public deprivation of needed government services.

b. Reporting Self-Identified Material Weaknesses and Significant Deficiencies. For control deficiencies determined to be either SDs or MWs, HROs must report the findings to those charged with governance in the related HQDA functional area (for example, HQDA functional proponent, command leadership). HROs report SDs and MWs to the appropriate HQDA functional proponent. The HQDA functional proponent will provide guidance and assistance to the ROs to ensure the MWs are corrected. Detailed guidance for reporting MWs is provided by the Director, Army Risk Management, in the ASOA guidance which outlines the preparation of feeder ASOA packages.

(1) Reporting Requirements. Significant deficiencies are internal to the Army and are not reported in the statement of assurance to the Secretary of Defense. Army-systemic MWs, along with a summary of corrective actions, are reported to OUSD–C for consolidation with other DoD agencies and reported to OMB and Congress through the ASOA.

(2) Each SD or MW will require one or more CAPs. CAPs must be periodically assessed and reported to Army leadership. DA Pam 11–2 provides additional information on CAPs.

c. Reporting Process. Army HROs will report MWs through the appropriate channels.

(1) The Director, Army Risk Management, will review all self-identified MWs reported. The Director, Army Risk Management will coordinate MW submissions from ROs with the appropriate HQDA functional proponent(s). The HQDA functional proponent will determine if additional coordination is required by assessing the potential impact of the SD or MW and provide written feedback within an appropriate timeframe. The HQDA functional proponents will instruct the RO on the activities to address the MW.

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

(3) The Director, Army Risk Management, will consolidate and submit MWs considered to be significant Armywide issues to the Army Audit Committee and brief the Committee 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.

2–8. Corrective actions

The absence or ineffectiveness of internal controls constitutes a control deficiency that results in a finding. For each finding reported by the DoDIG, USAAA, RO, or IPA, a strategy to mitigate the deficiency is captured step-by-step in the CAP. In general, CAPs must include achievable milestones in reasonable timeframes that will ultimately mitigate the root cause of the control deficiency. See DA Pam 11–2 for mandatory procedures.

a. CAPs for MWs identified by the RO, that are not deemed to be Army-systemic, must be validated. The HRO has the option to have the local IR office do the validation or to request DoDIG, USAAA, or the identifying agency to complete the validation. The required validation is to ensure the CAP is implemented as planned. See DA Pam 11–2 for mandatory procedures.

b. For IPA identified MWs, the IPA will perform further monitoring to determine whether the deficiency remains.

c. Upon validation of completed CAPs—

(1) For self-identified MW deemed Army-systemic, the Army Audit Committee will take into consideration the results of the CAP evaluation and vote for further action to either downgrade the MW to a SD or remove the MW. See DA Pam 11–2 for mandatory procedures.

(2) For DoDIG, USAAA, and IPA findings, the Army Audit Committee has sole authority to downgrade or remove the MW based on the CAP evaluation results and consideration of IPA findings (for example, the Army Audit Committee should not downgrade if the IPA still identifies the deficiency as an MW).

(3) Completed CAPs must be reported in the MW and SD Appendix to the Director, Army Risk Management in support of paragraph 1–8*u*.

d. Reporting—

(1) Activities within CAPs performed to remediate MWs are reported in the ROs' ASOA, or as instructed by the Director, Army Risk Management.

(2) The Director, Army Risk Management, may at any time request status of corrective actions related to MWs.

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

2–9. Annual Statement of Assurance

See DA Pam 11–2 for mandatory procedures.

The FMFIA requires the OSD to submit an ASOA to the President and Congress on the status of internal controls within the DoD. The Army's system of internal control must provide a level of reasonable assurance communicating the extent to which objectives for operations, reporting, and compliance are achieved. Reasonable assurance is defined in the GAO Green Book as "A high degree of confidence, but not absolute confidence." The ASOA assurance opinions are further described in the DA Pam 11–2. Pursuant to DoDI 5010.40, DoD agencies provide separate and explicit ASOA opinions that express the overall system of control's assurance level effectiveness. The OMB Circular No. A–123, M–18–16, Appendix A also requires an opinion related to ICOR, and OMB Circular No. A–123, M–23–06, Appendix D requires an opinion related to financial management systems. The Army supports DoD in meeting these requirements as follows–

a. ASOA. Annually the SECARMY must submit the ASOA, including opinions of ICOR–FR, ICOR–O, and ICOR–FS to OSD for use in preparing the consolidated DoD ASOA to the President and Congress. This statement is the SECARMY's assessment of the effectiveness of Army's internal controls in accordance with FMFIA.

b. The SECARMY's consolidated ASOA is based primarily on feeder ASOAs submitted by HQDA functional proponents and commanders or directors of ACOMs, ASCCs, and DRUs (collectively referred to as ROs). The Director, Army Risk Management, will issue instructions for the preparation of the feeder ASOAs at the beginning of the RMIC Program reporting year, coinciding with the beginning of the fiscal year. Completion of feeder ASOAs are conducted in accordance with the guidance provided by the Director, Army Risk Management.

c. Internal control evaluation results for the RMIC Program reporting year support the ASOA submission. An independent third party that reviews the documentation needs to understand the conclusions reached as indicated in the Management's opinion on the ASOA. The Director, Army Risk Management, will provide guidance to ROs to support the execution of appendices for the ASOA.

d. The Army's ASOA must include the following, at minimum:

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

(2) A statement identifying the OMB Circular No. A–123, M–18–16, Appendix A, as the framework used by Army to conduct the assessment of the effectiveness of ICOR reporting for external financial/nonfinancial and internal financial/nonfinancial reporting objectives.

(3) An explicit statement as to whether controls are effective. The DA Pam 11–2 provides more information on the assurance levels.

(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.

2–10. Documentation retention

See DA Pam 11–2 for mandatory procedures.

Process documentation, documentation on internal control evaluations conducted, ASOA submissions, and MWs reported must be maintained in accordance with AR 25–400–2.

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

b. HROs must retain documentation on MWs, control deficiencies, and control assessments in accordance with AR 25–400–2.

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. United States Code is available at https://uscode.house.gov/. Public Law publications are available at https://www.congress.gov/. OMB Circulars are available at https://www.whitehouse.gov/. GAO publications are available at https://www.gao.gov/.

AR 11–7
Internal Review Program (Cited in para 1–14.)

AR 15–39
Department of the Army Intergovernmental and Intragovernmental Committee Management Program (Cited in the title page.)

AR 25–30
Army Publishing Program (Cited in the title page.)

AR 25–400–2
Army Records Management Program (Cited in para 2–10.)

AR 36–2
Audit Services in the Department of the Army (Cited in para 1–12.)

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

DA Pam 25–40
Army Publishing Program Procedures (Cited in para 1–8*c*.)

DA Pam 25–403
Army Guide to Recordkeeping (Cited in para 1–5.)

DoD 7000.14–R, Volume 1
General Financial Management Information, Systems and Requirements (Available at https://comptroller.defense.gov/) (Cited in para 2–5*a*(2).)

DoD Statement of Assurance Execution Handbook
(Available at https://ousdc.sp.pentagon.mil/sites/rmic/rmic%20guidance%20and%20additional%20resources/forms/allitems.aspx) (Cited in para 2–2*b*.)

DoDI 5010.40
Managers' Internal Control Program Procedures (Cited in the title page.)

DoDI 8510.01
Risk Management Framework for DoD Systems (Cited in para 2–5*b*(1).)

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

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

OMB Circular No. A–123, M–23–06, Appendix D
Management of Financial Management Systems - Risk and Compliance (Cited in para 1–9*e*.)

OMB Circular No. A–123, M–16–17
Management's Responsibility for Enterprise Risk Management and Internal Control (Cited in para 2–1.)

OMB Circular No. A–123, M–18–16, Appendix A
Management of Reporting and Data Integrity Risk (Cited in para 1–8*ee*.)

OMB Circular No. A–123, M–21–19, Appendix C
Requirements for Payment Integrity Improvement (Cited in para 2–2*b*.)

Playbook: Enterprise Risk Management for the U.S. Federal Government
(Available at https://comptroller.defense.gov/portals/45/documents/micp_docs/authoritative_laws_and_regulations/final-erm-playbook.pdf) (Cited in para 2–2.)

31 USC 3512 note
Federal Financial Management Improvement Act (FFMIA) of 1996 (Cited in para 1–16*b*(8).)

Public Law 111–352
Government Performance and Results Act Modernization Act (GPRAMA) of 2010 (Cited in para 1–6.)

Public Law 113–101
Digital Accountability and Transparency Act of 2014 (Cited in para 1–8*ee*.)

Public Law 116–117
Payment Integrity Information Act of 2019 (Cited in para 2–2*b*.)

Treasury Financial Manual, Volume 1, Chapter 1000
Purpose and Plan of the Treasury Financial Manual (Available at https://tfm.fiscal.treasury.gov/home.html) (Cited in para 2–5*a*(3).)

31 USC 3357
Financial and administrative controls relating to fraud and improper payments (Cited in para 2–2*b*.)

31 USC 3512
Federal Managers' Financial Integrity Act (Cited in para 1–8*b*.)

Section II

Prescribed Forms
Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website at https://armypubs.army.mil.

DA Form 11–2
Internal Control Evaluation Certification (Prescribed in para 2–3*c*.)

Appendix B

Internal Control Evaluation

See DA Pam 11–2 for mandatory procedures.

B–1. Function

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

B–2. Purpose

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

B–3. Instructions

These key internal controls must be formally evaluated at least once every five years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2. Evaluation test questions are outlined in paragraph B–4, below, and are intended as a start point for each applicable level of internal control evaluation. Answers must be based on the actual testing of key internal controls (for example, inquiry, observation, examination, or re-performance). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation.

B–4. Test Questions

a. Are key internal controls identified in the governing Army regulations? (HQDA functional proponents only).

(1) Key Control. Identification of the Internal controls should be determined by the proponent of the Army regulation.

(2) Key Supporting Documentation. As evidence in the HQDA level Army regulation.

b. Are internal control evaluations provided or alternate evaluation methods identified to test key internal controls? (HQDA functional proponents only.)

(1) Key Control. Internal control evaluations are completed as prescribed in the ICEP and test methods are conducted in accordance with the ASOA Guidance.

(2) Key Supporting Documentation. As evidence by Test plans, Checklists, Signed DA Form 11–2s, and the Internal Control Evaluation Appendix.

c. Is local internal control guidance available that defines internal control responsibilities and required actions?

(1) Key Control. Internal control guidance is current and present in local level documentation.

(2) Key Supporting Documentation. As evidence by Standard Operating Procedures, Appointment letters/memos, Formal Guidance/Memo, SRO memo from ASA (FM&C), Letters of Instructions, Training slides/training roster (informal training/deskside briefings), Training certifications for online training beyond Army Learning Management System/Training Appendix.

d. Are SROs, AUMs, ICAs, and ICEs trained, and do they understand their internal control responsibilities?

(1) Key Control. RMIC roles are adequately trained by completing required Role Base Training every two years and additional training as needed.

(2) Key Supporting Documentation. As evidence by attending, completing, or adhering to Required Army Learning Management System training at a minimum, Additional training at local levels, Annual guidance from OSD and ASA (FM&C), Monthly Touchpoints at the ASA (FM&C) Level, Appointment letters, Letters of Instruction from Program Executive Offices, Kickoff Meetings with RMIC ICAs, ICEs, AUMs, Email communications and Newsletters with additional guidance or clarification.

e. Are explicit statements of internal control responsibility included in performance agreements for SROs, AUMs, ICAs, and ICEs down to and including the assessable unit level?

(1) Key Control. Appointed RMIC roles will be rated in their performance appraisals and evaluations to hold individuals accountable for their internal control responsibilities.

(2) Key Supporting Documentation. As evidence by yearly annual evaluations such as Officer Evaluation Reports, Contribution-Based Compensation and Appraisal System, Contribution plans, Defense Performance Management and Appraisal System.

f. Is an ICEP established and maintained to describe how key internal controls will be evaluated over a 5-year period?

(1) Key Control. The ICEP sets the internal control evaluations frequency as it relates to the annual risk level assessed or the prescribed AR whichever is more frequent.

(2) Key Supporting Documentation. As evidenced by the ICEP located in the annual Risk Assessment and ICEP Appendix and concluded in the Internal Control Evaluation Appendix.

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

(1) Key Control. The Internal Control Evaluation Appendix is traceable to the ICEP and MW and SD Appendix is traceable to the Internal Control Evaluation Appendix within the same Fiscal Year.

(2) Key Supporting Documentation. As evidence by test plans, checklists, signed DA Form 11–2s, Internal Control Evaluation Appendix, and the MW and SD Appendix that outlines any CAPs or remediation, Risk Assessment and ICEP Appendix and any risk mitigation of MW and significant deficiencies.

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

(1) Key Control. The SRO is actively involved and included in communications regarding internal control evaluations and other potential internal control deficiency meeting discussions.

(2) Key Supporting Documentation. As evidence by Quarterly Update Briefs to Senior Leaders, Ad Hoc briefings to Senior Leaders as thing arise, Briefings to AUMs and SROs that cover the entirety of the RMIC process/plan/progress, ASOA signed by SRO, SRO Assessments, Staffing forms and screenshots/printouts of task management systems or document staffing tools.

B–5. Supersession

This evaluation replaces the evaluation previously published in AR 11–2, dated 4 January 2010.

B–6. Comments

Help to make this a better tool for evaluating internal controls. Submit comments to Assistant Secretary of the Army (FM&C) (SAFM–FOA), usarmy.pentagon.hqda-asa-fm.mbx.army-mngrs-internal-cntl-prog@army.mil.

Glossary of Terms

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

Annual Statement of Assurance
The ASOA 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 Under SECARMY 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
Any organizational, functional, programmatic, or other applicable subdivision of an organization that allows for adequate IC analysis. An assessable unit's functions include the documentation, identification, and insertion of controls associated with a specific sub-function in order to mitigate identified risk. The assessable unit is required to have an appointed and adequately trained assessable unit manager.

Assessable Unit Manager
The government employee selected by appropriate functional leadership that is responsible for the Risk Management and Internal Control Program requirements of the assessable unit. The assessable unit manager must be a government employee, to prevent inherently governmental functions from being performed by contracted employees and possess an in-depth understanding of the processes and procedures of the assessable unit.

Brevity code
A code word, which provides no security, that serves the sole purpose of shortening of messages rather than the concealment of their content.

Business Process
A business process is a financial and non-financial functional area under control monitoring. Financial business processes are processes which trigger a financial event impacting the general ledger and financial statements as defined in the Army's Control Catalog https://www.usafmcom.army.mil/bps/. Non-financial business processes are defined by the RO and affect the overall operations of the Army. Non-financial business processes do not have a direct impact on the financial statements.

Control Deficiency
A control deficiency is when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to satisfactorily accomplish their assigned functions or inhibits the prevention or detection of misstatements on a timely basis.

Corrective Action Plan
A written document that spells out the specific steps necessary to resolve a material weakness, including targeted milestones and completion dates. Corrective action plans for operational assessment material weaknesses are maintained with the Risk Management and Internal Control Program documentation. Corrective action plans for financial reporting and financial systems material weaknesses are maintained in the Financial Improvement Audit Readiness Planning Tool.

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

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.

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 and carrying out the RMIC Program within their respective organization.

Internal Control Administrator
The individual designated by the SRO to administer the RMIC Program for the 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 Certification
A certification documented in DA Form 11–2. This certification is signed by the AUM. This Form summarizes and document the completed internal control testing results. The DA Form 11–2 should accompany each test plan, serving as the cover sheet to capture activities that occurred during testing.

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 organization, policies, and procedures that help program and financial managers to achieve results and safeguard the integrity of their programs by reducing the risk of adverse activities. 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, and physical devices (for example, locks, and fences).

Key Internal Control Questionnaire
Formally referred to as checklists. The Key Internal Control Questionnaire is used to guide evaluations of the effectiveness of the control. Responses to the questionnaire are provided only when substantial testing is conducted to support the responses and is part of the overall internal control evaluation package.

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 specific instance of a failure in a system of control or lack of control that would significantly impair fulfillment of agency's mission, violate statutory or regulatory requirements, or significantly weaken safeguards against waste, loss, unauthorized use or misappropriation of funds, property, or other assets. The material weakness may present a major impact to the environment, safety, security, or readiness of the command. For financial reporting, this would include a reportable condition or combination of reportable conditions that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

Reasonable Assurance
An informed judgment by management regarding the overall adequacy and effectiveness of ICs based upon available information that the systems of ICs are operating as intended according to 31 USC 3512.

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 Head of the RO. The SRO has overall responsibility for ensuring the implementation of an effective RMIC Program within that organization.

Significant Deficiency
A control deficiency or combination of control deficiencies, that in management's judgment, represents significant deficiencies in the design or operation of ICs that could adversely affect the DoD and OSD Component's ability to meet its IC objectives.

Test Plan
A documented methodology used to evaluate the design or assess the effectiveness of the control's operation. A test plan provides detailed test procedures, test results, and includes supporting documentation to support the results.