UNITED STATES FORCES KOREA INSTRUCTION

FKJ8 USFKI 5010.01
DISTRIBUTION: A, B 24 March 2026

UNITED STATES FORCES, KOREA (USFK)
RISK MANAGEMENT AND INTERNAL CONTROL PROGRAM

Reference(s): See Enclosure E

1. Purpose. To establish policies, procedures, and responsibilities for implementing an integrated Risk Management and Internal Control (RMIC) framework in accordance with OMB Circular No. A-11, A-123, GAO Green Book standards and DoD Instruction 5010.40.

2. Superseded/Canceled. Supersedes USFK Pamphlet 11-1, 22 December 2010.

3. Applicability. This instruction applies only to HQ, USFK.

4. Records Management. CJCSM 5760.01B, Volume II, Joint Staff and Combatant Commands Records Management Manual - Disposition Schedule.

5. Policy. See Enclosure A

6. Responsibilities. See Enclosure B

7. Releasability. Unrestricted. This instruction is approved for public release; distribution is unlimited.

8. Effective Date. This instruction is effective upon receipt.

DAVID B. WOMACK
Major General, USA
Chief of Staff

Enclosures:

A – Policy
B -- Responsibilities
C – GAO Fraud Risk Management (FRM) Framework Integration Requirements
D – Entity-Level Control (ELC) Testing Requirements & Validation Standards
E – References
GL – Glossary

ENCLOSURE A

POLICY

1. The objective of USFK RMIC program is to establish and sustain proper internal controls that provide reasonable assurance of effective and efficient operations, reliable reporting, auditable documentation, and compliance with applicable laws and policies.

2. Internal controls will be embedded into daily mission execution across all assessable units. Continuous monitoring is the primary method for evaluating internal control effectiveness.

3. The RMIC Program applies to mission, operational, administrative, financial reporting, and financial systems activities and includes Internal Control Over Reporting (ICOR). Internal controls must align across end-to-end business processes to ensure risks and dependencies are addressed consistently.

4. Enterprise Risk Management (ERM)- USFK will integrate ERM into RMIC activities because it creates a comprehensive framework that enhances an organization's ability to identify, assess, and mitigate risks across all operational levels

5. Fraud Risk Management (FRM)- USFK will implement fraud risk management practices consistent with the GAO Fraud Risk Framework and DoDI 5010.40. Fraud risks will be assessed and mitigated through preventive and detective controls, and managers are encouraged to report concerns without penalty.

6. Existing information sources, such as audits, inspections, cybersecurity reviews, and oversight assessments, will be used whenever possible. When existing information is insufficient, USFK leadership or SAO will initiate focused internal control review on control effectiveness, operational efficiencies, and compliance on the designated areas.

7. Managers will identify, document, and report internal control deficiencies, including Significant Deficiencies (SDs) and Material Weaknesses (MWs), in accordance with DoDI 5010.40 and the SOA Execution Handbook. Corrective Action Plans (CAPs) will be developed and monitored until deficiencies are resolved.

8. Internal Control (IC) Categories. Internal controls are essential for ensuring the integrity, reliability, and effectiveness of all mission-related, operational, administrative, financial reporting, and financial system activities. USFK will implement the three Internal Control Over Reporting (ICOR) categories defined in DoDI 5010.40 and the DoD SOA Execution Handbook:

a. Internal Control Over Reporting – Financial Reporting (ICOR-FR): Controls that support the accuracy, timeliness, completeness, and reliability of financial reporting. These controls enable USFK to meet requirements under FMFIA, OMB Circular A-123 Appendix A, and the annual SOA Execution Handbook, ensuring that financial reporting risks are identified, assessed, controlled, and remediated as required.

b. Internal Control Over Reporting – Financial Systems (ICOR-FS): Controls over financial management systems that ensure conformance with federal system requirements, including security, configuration management, access controls, continuity planning, and compliance with OMB and GAO standards. These controls ensure that financial systems reliably support financial reporting and operational needs.

c. Internal Control Over Reporting – Operations (ICOR-O): Controls that ensure operational and administrative activities are executed in alignment with mission objectives, regulatory requirements, and organizational policy. These controls support reliability of non-financial reporting and the effective execution of mission-critical processes.

ENCLOSURE B

RESPONSIBILITIES

1. **Chief of Staff, USFK**

a. Designate Senior Accountable Official (SAO) for USFK RMIC program.

b. Issue a tone-at-the-top memo to emphasize leadership commitment to the effectiveness of internal controls and promote an organizational culture that encourages open communication and accountability.

c. Provide operational guidance for the RMIC program and designate areas of interest for review on behalf of the Commander

2. **Senior Accountable Officer (SAO)**

a. Serve as a designated RMIC accountable officer to provide oversight and guidance on timely remediation of the deficiencies through CAPs, accurate reporting, and compliance with RMIC requirement.

b. Annual Statement of Assurance- Sign annual Statements of Assurance that attest to the effectiveness of the internal controls within HQ USFK including any potential material weaknesses or significant deficiencies and the corrective action plan. The annual Statement of Assurance signed will be submitted to the Office of the Deputy Chief Financial Officer, Department of Defense.

c. Program Oversight- Oversee the command-wide process for monitoring, documentation, and resolution of Significant Deficiencies (SDs) and Material Weaknesses (MWs). Ensure timely communication of RMIC issues, risks, and CAP progress through RMIC-designated bodies. This is critical when the risk cannot be mitigated in a timely manner with the available resources or authority.

d. Designation of Key Personnel- Designate USFK RMIC manager and J-staff directorates as Assessable Unit Managers (AUMs) that allows for focused analysis of internal controls. After designation, SAO will advise them on specific RMIC submission requirements to comply with DoDI 5010.40 which governs DoD RMIC program.

3. **Assessable Unit Manager (AUM)**

a. AUMs are responsible for the day-to-day implementation of the RMIC program within their designated areas of responsibility. They are the primary owners of the directorate internal controls and are accountable for ensuring its effectiveness and policy compliance.

b. Internal Control Management- Establish, manage, and evaluate the internal controls within their assessable units to ensure all internal controls are aligned with DoD and USFK RMIC program requirements.

c. Documentation and Record Retention- Maintain and archive all necessary documentation for the assessable unit. This documentation must be organized and readily available for review. Required documents include:

(1) Guidance.

(2) SOP

(3) Process flows and narratives.

(4) Associated risk and control matrices.

(5) Control objectives and activities.

(6) Applicable executive agreements.

d. Risk Assessment and Testing- Conduct periodic risk assessments to identify potential risks that may adversely affect the unit's mission or operations. Perform regular reviews of internal processes and procedures to identify opportunities for improvement.

e. Corrective Action Plan- Upon discovery of a control deficiency, develop a CAP to address the root cause. Set milestone dates for the CAPs and track progress until it is closed. Communicate with the RMIC program manager to develop, track, and update CAPs

4. <u>RMIC Program Manager for Enterprise Risk Management (ERM)</u>

ERM RMIC Manager is responsible for implementing and overseeing the organization's enterprise-wide risk management framework. Their roles include:

a. Risk Identification and Assessment- Identify and assess risks across all organizational levels that could impact strategic objectives and mission success.

b. Risk Mitigation and Response- Develop and implement strategies to mitigate risks, including preventive measures and contingency plans.

c. Risk Integration- Ensure that risk management is embedded into decision-making, strategic planning, and operational processes.

d. Risk Monitoring and Reporting- Continuously monitor the organization's risk profile and provide regular updates to senior leadership and stakeholders.

e. Stakeholder Collaboration- Engage with internal and external stakeholders to ensure a comprehensive and unified approach to managing enterprise risks.

5. **RMIC Program Manager for ICOR-FR**

a. ICOR-FR Program Manager focuses on ensuring the accuracy, reliability, and compliance of financial reporting processes. Their roles include:

b. Financial Reporting Oversight- Monitors internal controls related to financial reporting to ensure compliance with laws, regulations, and accounting standards.

c. Risk Identification- Identifies risks that could lead to material misstatements in financial reports and implementing controls to mitigate those risks.

d. Audit Support- Collaborates with auditors to provide documentation and address findings related to financial reporting.

e. Control Testing- Conducts regular testing and monitoring of financial reporting controls to ensure their effectiveness and reliability.

6. RMIC Program Manager for ICOR-FS

a. ICOR-FS Program Manager is responsible for ensuring the integrity, security, and functionality of financial systems. Their roles include:

b. System Oversight: Managing internal controls over financial systems to ensure data accuracy, security, and compliance.

c. Risk Assessment: Identifying risks related to financial systems, such as cybersecurity vulnerabilities, data breaches, or system failures.

d. System Integration: Ensuring financial systems are aligned with organizational processes and reporting requirements.

e. Compliance Assurance: Verifying that financial systems comply with applicable regulations, policies, and standards.

f. System Optimization: Identifying opportunities for system enhancements to improve efficiency, accuracy, and security.

7. **RMIC Program Manager for ICOR-O**

a. ICOR-O Program Manager focuses on ensuring operational efficiency, effectiveness, and compliance across the organization. Their roles include:

b. Operational Risk Management: Identifying and mitigating risks related to operational processes, such as logistics, procurement, and program execution.

c. Process Improvement: Evaluating and improving operational processes to enhance efficiency and effectiveness.

d. Compliance Monitoring: Ensuring operational activities comply with laws, regulations, and internal policies.

e. Performance Metrics: Developing and monitoring key performance indicators (KPIs) to assess the effectiveness of operational controls.

f. Stakeholder Collaboration: Working with departments and teams to address operational risks and implement best practices.

8. **Fraud Reduction Task Force Representative**

a. Fraud Risk Assessment

(1) Conduct regular assessments to identify areas vulnerable to fraud within the organization.

(2) Evaluate existing processes and controls to determine their effectiveness in preventing fraud.

(3) Collaborate with departments to identify emerging fraud risks and recommend mitigation strategies.

b. Fraud Prevention and Mitigation

(1) Develop and implement fraud prevention policies, procedures, and controls to reduce the likelihood of fraudulent activities.

(2) Promote awareness of fraud risks and prevention strategies through training programs and communication campaigns.

(3) Ensure segregation of duties and other preventive measures are in place to minimize opportunities for fraud

c. Investigation and Response

(1) Support investigations into suspected fraud cases.

(2) Collaborate with internal audit teams, legal departments, and external agencies as needed during fraud investigations.

(3) Recommend corrective actions and process improvements based on investigation findings.

d. Monitoring and Reporting

(1) Monitor transactions and activities for signs of fraud, such as irregularities, anomalies, or suspicious behavior.

(2) Prepare reports on fraud risk trends, incidents, and mitigation efforts for leadership and stakeholders.

(3) Track the effectiveness of fraud reduction initiatives and recommend adjustments as necessary.

9. <u>Primary Audit POC</u>

a. Act as point of contact between the audit team and the organization.

b. Coordinate audit-related activities across departments and teams within the organization.

c. Collect and provide requested documentation, data, and evidence to support the audit process.

10. <u>DAR-Q Coordinator</u>

a. Serve as the primary liaison between the command and the Office of the Under Secretary of Defense (Comptroller).

b. Facilitate communication regarding the DAR-Q process. Ensure that all relevant stakeholders are informed and engaged in the review process.

c. Ensure that the review process adheres to quality control standards as outlined in the DAR-Q framework. Assist in the validation of balances reported on quarterly financial statements.

d. Collect and organize supporting documentation required for the DAR-Q review. Ensure that all necessary documentation is available for review by funds holders and budget submitting officers (BSOs)

e. Provide guidance and support to personnel involved in the DAR-Q process to ensure understanding of their roles and responsibilities. Assist in the development and updating of Standard Operating Procedures (SOPs) related to the DAR-Q.

ENCLOSURE C

GAO FRAUD RISK MANAGEMENET (FRM)

FRAMEWORK INTEGRATION REQUIREMENTS

1. Purpose

This enclosure establishes the minimum requirements for incorporating GAO's Fraud Risk Management (FRM) Framework into USFK RMIC Program. The FRM Framework provides a list of leading practices and control activities to prevent, detect, and respond to fraud, with an emphasis on prevention. USFK AUM will adhere to the DoD leading practices to effectively design, implement, and operate an internal control system that addresses fraud risks as required by DoD OMB Circular No. A-123

2. DoD Fraud Risk Management 10 Leading Practices

DoD Fraud Risk Management 10 Leading Practices
GAO FRM Leading Practice 01: Create an Organizational Culture to Combat Fraud at All Levels of the Agency
GAO FRM Leading Practice 02: Create a Structure with a Dedicated Entity to Lead Fraud Risk Management Activities
GAO FRM Leading Practice 03: Plan regular fraud risk assessment
GAO FRM Leading Practice 04: Identify and assess risks to determine the program's fraud risk profile
GAO FRM Leading Practice 05: Determine Risk Responses and Document an Antifraud Strategy Based on the Fraud Risk Profile
GAO FRM Leading Practice 06: Design and Implement Specific Control Activities to Prevent and Detect Fraud
GAO FRM Leading Practice 07: Develop a Plan Outlining How the Program Will Respond to Identified Instances of Fraud
GAO FRM Leading Practice 08: Conduct Risk-Based Monitoring and Evaluate All Reporting Entities of the Fraud Risk Management Framework
GAO FRM Leading Practice 09: Monitor and Evaluate Fraud Risk Management Activities with a Focus on Measuring Outcomes
GAO FRM Leading Practice 10: Adapt Fraud Risk Management Activities and Communicate the Results of Monitoring and Evaluations

(INTENTIONALLY BLANK)

ENCLOSURE D

ENTITY-LEVEL CONTROL (ELC) TESTING REQUIREMENTS
AND VALIDATION STANDARDS

1. Purpose

This enclosure establishes mandatory ELC testing requirements for USFK in accordance with DoDI 5010.40 and GAO internal control standards. ELCs are foundational controls that impact the reporting entity as a whole, and have a pervasive effect on the Department's internal control system and represent the governance structure within an organization. ELCs consist of the Reporting Entity's structure, policies, procedures, processes, and activities, which help to achieve its mission.

2. ELC Components

a. Control Environment
- Structure, delegation, oversight.
- Ethical culture and required training.
- Competence and accountability.

b. Risk Assessment
- Identify mission, financial, and compliance risks.
- Align risks with objectives and controls.
- Reassess risks based on operational factors.

c. Control Activities
- Ensure compliance with laws and regulations.
- Document control methods, frequency, and evidence.
- Review approvals, reconciliations, Separation of Duties, and access.

d. Information & Communication
- Maintain reliable and accurate information.
- Ensure transparent internal communication.
- Report deficiencies promptly.

e. Monitoring Activities
- Identify and correct deficiencies.
- Validate CAPs.
- Embed monitoring into operations.

3. Testing Methodology- USFK AUMs, SMEs, and RMIC manager will assess the management internal controls by using various methodologies including inquiry, observation, documentation review, walkthroughs, and sampling.

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. Federal Manager's Financial Integrity Act (FMFIA) of 1982

b. Federal Financial Management Improvement Act (FFMIA) of 1996

c. US Government Accountability Office Standards for Internal Control in the Federal Government (Green Book)

d. OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control"

e. GAO-14-704G, "Standards for Internal Control in the Federal Government

f. DoDI 5010.40, "Risk Management and Internal Control (RMIC) Program"

g. DoD 7000.14-R, Financial Management Regulation, Volume 1: "General Financial Management Information, Systems, and Requirements," Chapter 3, "Federal Financial Management Improvement Act Compliance"

h. DoDI 8510.01, "Risk Management Framework for DoD Systems"

i. DoD Statement of Assurance Execution Handbook (published annually, last updated FY25)

(INTENTIONALLY BLANK)

GLOSSARY

Abbreviations

AU	Assessable Unit
AUM	Assessable Unit Managers
CAP	Corrective Action Plan
FRM	Fraud Risk Management
GAO	Government Accountability Office
ICOR-FR	Internal Control Over Reporting – Financial Reporting
ICOR-FS	Internal Control Over Reporting – Financial System
ICOR-O	Internal Control Over Reporting – Operation
MW	Material weakness
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
RMIC	Risk Management and Internal Control
SAO	Senior Accountable Official
SD	Significant Deficiency
SOP	Standard Operating Procedures

(INTENTIONALLY BLANK)