DoD Instruction 5010.40

DoD Enterprise Risk Management and Risk Management and Internal Control Program

Originating Component:	Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
Effective:	December 11, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, as amended
Approved by:	Michael McCord, Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense

Purpose: In accordance with the authority in DoD Directive 5118.03, this issuance establishes policy, assigns responsibilities, and provides procedures for implementing an integrated enterprise risk management (ERM) and risk management and internal control (RMIC) framework in accordance with Office of Management and Budget (OMB) Circular No. A-123 and OMB Circular No. A-11 requirements.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSD, the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. Nothing in this issuance will infringe on OIG DoD statutory independence and authority as articulated in Chapter 4 of Title 5, United States Code (U.S.C.), also known and referred to in this issuance as the "Inspector General Act of 1978," as amended. In the event of any conflict between this issuance and OIG DoD statutory independence and authority, the Inspector General Act of 1978 takes precedence.

1.2. POLICY.

a. The DoD's overarching ERM program supports the efficiency, effectiveness, accountability, and auditability of the DoD's enterprise management operations or mission-specific activities.

b. In support of the DoD's management operations and to meet the intent of OMB Circular No. A-123, this issuance provides the DoD's policy and approach to executing DoD RMIC and ERM activities. The DoD's RMIC program will:

(1) Promote the effectiveness and efficiency of DoD programs and business operations.

(2) Ensure accountability, compliance with laws and regulations, and reliable reporting.

(3) Increase risk awareness and transparency and align Components' risk appetite and tolerance.

(4) Establish the rebranding expectations of the RMIC program and stand up the Integrated Risk Management (IRM) Committee, addressing all sources of financial and business operation risk.

(a) The IRM Committee.

1. The Defense Performance Improvement Council (DPIC) IRM Committee is led by DoD's Deputy Performance Improvement Officer and serves as the DoD's Senior Management Council (SMC) to provide vision, leadership, oversight, and accountability for ERM, internal controls over reporting (ICOR) for operations (ICOR-O), non-financial information technology systems, and fraud risk management (FRM). The DPIC will be supported as necessary by the Deputy Chief Financial Officer. The DPIC's IRM Committee oversees implementation of the DoD ERM Framework, the preparation of the DoD Enterprise

Risk Profile, the analysis and review of DoD Component reported material weaknesses (MWs) and significant deficiencies (SDs) in operations and proposing recommending improvements for DPIC consideration.

2. The IRM Committee will focus on proactively identifying and managing key risks and issues that could limit or prevent the successful implementation of DoD strategic priorities and performance objectives as stated in the National Defense Strategy (NDS) and the DoD Strategic Management Plan (SMP) and produce a comprehensive DoD-level enterprise management operations risk profile based on OMB Circular A-123 requirements.

3. The IRM Committee will integrate monitoring of DoD Component actions addressing top DoD management challenges, as well as DoD Component compliance with Government Accountability Office (GAO) audit recommendations, including priority recommendations and recommendations pertaining to DoD-owned GAO high-risk areas. A listing of top DoD management and performance challenges is available at https://www.dodig.mil/Reports/Top-DoD-Management-Challenges.

(b) The RMIC program will focus on managing ICOR-O; ICOR for financial reporting (ICOR-FR) and financial systems (ICOR-FS); and ICOR for non-financial systems, including externally and internally identified MWs, critical weaknesses, and SDs in those areas. These items' status will be monitored and reported to ensure key financial reporting, financial systems, and business operational deficiencies are being addressed in support of more effective and efficient operations, compliance with applicable laws and regulations, and reliable reporting.

(c) The integrated ERM and RMIC program will focus on managing fraud risks and controls, ensuring all DoD Components report all fraud risks, including those not categorized as MWs or SDs.

1.3. TERMINOLOGY CAVEAT.

When used in this issuance without a designator of "OSD" or "DoD," the term "Component" refers to both the OSD and DoD Components.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO).

In addition to the responsibilities in Paragraphs 2.4. and 2.5., the USD(C)/CFO:

a. Manages and oversees DoD ICOR-FR and ICOR-FS activities.

b. Appoints a DoD-wide RMIC manager for ICOR-FR- and ICOR-FS-related matters.

c. Establishes and owns an RMIC program improvement structure for ICOR-FR and ICOR-FS, including FRM, that considers DoD Component feedback and shares best practices and lessons learned after each statement of assurance (SOA) cycle.

d. Manages DoD-level enterprise business operations in accordance with GAO 14-704G (also known and referred to in this issuance as the "GAO Green Book"), Part 6 of OMB Circular No. A-11, and OMB Circular No. A-123 requirements.

e. Chairs the Financial Improvement and Audit Remediation Governance Board (FGB) pursuant to the January 18, 2022 Deputy Secretary of Defense memorandum (also known as the Defense Business Council Charter).

f. Develops and implements DoD policy to support proactive identification and management of risks and internal controls to support ICOR-FR, ICOR-FS, and FRM in coordination with appropriate functionally aligned stakeholders.

g. Establishes and supervises the execution of uniform DoD policies, principles, and procedures, including terminologies and classifications as necessary, for financial improvement and audit remediation.

h. Publishes the DoD-level enterprise management operations risk profile in the DoD Agency Financial Report.

2.2. PERFORMANCE IMPROVEMENT OFFICER/DIRECTOR OF ADMINISTRATION AND MANAGEMENT (PIO/DA&M).

In addition to the responsibilities in Paragraphs 2.4. and 2.5. and their role as the Performance Improvement Officer of the DoD as delegated in the September 1, 2021, and August 23, 2023, Deputy Secretary of Defense memorandums, the PIO/DA&M:

a. Serves as a member of the FGB.

b. Manages and oversees DoD ICOR-O, including systems, DoD GAO portfolio, and the DoD enterprise ERM program.

c. Appoints a DoD RMIC manager for ICOR-O reporting processes to coordinate and review Component submissions and to monitor compliance in accordance with this issuance, the ICOR-O Guidance, the DoD Annual SOA, and other applicable regulations.

d. Supports the Deputy Secretary of Defense's oversight of DoD-level enterprise business operations in accordance with the GAO Green Book, Part 6 of OMB Circular No. A-11, and OMB Circular No. A-123.

e. Establishes and owns an ERM program improvement structure for ERM that considers DoD Component feedback and shares best practices and lessons learned after each SOA cycle.

f. Recommends ERM, ICOR-O, and DoD GAO portfolio-related topics or issues for review and decision by the DPIC and the Deputy's Management Action Group (DMAG), as appropriate.

g. Develops and implements DoD policy to support proactive identification and management of risks and internal controls to support management of DoD-wide GAO open recommendations and top DoD management challenges, ICOR-O, ERM, and FRM in coordination with the USD(C)/CFO and applicable action officers.

h. Appoints an IRM committee member who will enable annual DoD-level enterprise management operations risk profile submission to OMB in accordance with OMB Circular No. A-123 requirements.

i. Appoints a DoD-level ERM lead to coordinate development of the DoD-level enterprise management operations risk profile.

j. Coordinates with the other Principal Staff Assistants (PSAs), the Director of the Joint Staff, other Component heads, and relevant officials, as necessary, to provide management operations inputs to the Chairman of the Joint Chiefs of Staff's risk assessment, as requested.

k. Leads an annual risk review based on NDS strategic priorities, objectives, and performance goals as stated in the DoD SMP.

2.3. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In addition to the responsibilities in Paragraphs 2.4. and 2.5., the DoD CIO:

a. Chairs the DPIC and serves as a member of the FGB. Reviews and approves ERM and ICOR-O priorities and decisions.

b. Supports Deputy Secretary of Defense oversight of DoD-level enterprise business operations in accordance with the GAO Green Book, Part 6 of OMB Circular No. A-11, and OMB Circular No. A-123.

2.4. PSAs.

The PSAs:

a. Review and assess self-reported MWs and SDs of the Defense Agencies and DoD Field Activities (DAFAs) under their authority, direction, and control and provide an explicit level of assurance regarding internal controls' effectiveness.

b. Designate a point of contact with the authority to lead DoD IRM initiatives and support ICOR-FR, ICOR-FS, ICOR-O, ERM, FRM, GAO, and top DoD management challenges on their behalf.

c. Maintain ownership of any DoD-wide MWs, SDs, and associated risks (including fraud), including:

(1) Reporting on associated corrective actions' status until MWs and SDs are resolved.

(2) Reviewing the reported actions of the DoD Components that pertain to their area of responsibility.

(3) Helping the DoD Components resolve any MWs and SDs.

(4) Identifying and reporting inherent and residual risks.

(5) Providing updates and information on key RMIC initiatives to applicable governance bodies (e.g., FGB, DPIC, DMAG).

d. Support the DoD ERM program by:

(1) Providing inputs to the USD(C)/CFO and the PIO/DA&M on a quarterly basis on enterprise management risk, in alignment with the functional responsibilities of each PSA and in support of the preparation of the annual DoD-level enterprise management operations risk profile.

(2) Identifying and mitigating enterprise risks that functionally align to their area of responsibility and potentially limit or prevent achievement of DoD strategic management and NDS priorities stated in the DoD SMP.

2.5. OSD AND DOD COMPONENT HEADS.

The OSD and DoD Component heads:

a. Establish and maintain ERM and RMIC programs and reporting structures in accordance with existing laws, regulations, and policies.

b. Evaluate financial and business operational risks and the potential impact(s) on the effectiveness and efficiency of the associated business process level risks identified, ensuring they are:

(1) Recorded and prioritized.

(2) Communicated through RMIC-designated bodies when the risk will adversely impact effective, efficient, or compliant achievement of the Component mission and cannot be mitigated in a timely manner given current resources or scope of authority.

c. Appoint a senior accountable official (SAO) for the RMIC program and assessable units to resolve any MWs and SDs, as reported by the DoD RMIC manager or Component RMIC manager. The SAO should be a U.S. Government representative with a minimum grade level of O-6 or GS-15. Appointment is based on the individual's ability to resolve the reported DoD or Component MWs and implement the corrective action plan (CAP) within the timelines reported. The SAO will:

(1) Serve as a subject matter expert (SME) in activities under their responsibility and be accountable for remediation of the CAPs within their area of responsibility.

(2) Report the status of remediation to the FGB and applicable PSAs.

(3) Be responsible for all RMIC and senior leadership reporting of the status of the RMIC program in their appointed assessable units.

d. Designate a Component RMIC manager, who must be a U.S. Government employee, to support compliance with GAO Green Book, Part 6 of OMB Circular No. A-11, and OMB Circular No. A-123 requirements. The Component RMIC manager must notify the FGB and applicable PSA:

(1) When the assigned Component RMIC manager is vacating the position within 10 business days of appointment.

(2) Of a newly appointed Component RMIC manager as soon as possible after identification and appointment.

2.6. SECRETARIES OF THE MILDEPS AND DAFA DIRECTORS.

In addition to the responsibilities in Paragraph 2.5., the Secretaries of the MILDEPs and the DAFA directors:

a. Designate individual(s) responsible for the collection and consolidation of their ICOR-FR, ICOR-FS, ICOR-O, ERM, FRM, GAO, and top DoD management challenges inputs.

b. Evaluate ICOR-FR, ICOR-FS, ICOR-O, ERM, and FRM risks and determine potential impact(s) on the effectiveness and efficiency of the associated business process-level risks identified, ensuring they are:

(1) Recorded and prioritized.

(2) Communicated through designated RMIC forums when the risk will adversely affect effective, efficient, or compliant achievement of their mission and cannot be mitigated in a timely manner given current resources or scope of authority.

c. Manage financial and operational risks determined by their mission, requirements, and cost-benefit analysis to be relevant to sustaining their business operations and mission satisfaction effectively and efficiently.

d. Align the processes, procedures, and outputs required by this issuance with the risk management-related requirements of Section 153 of Title 10, U.S.C., including but not limited to:

(1) DoD SMP.

(2) Strategy, planning, programming, budgeting, and execution.

(3) Defense readiness reporting.

(4) The Chairman of the Joint Chiefs of Staff's risk assessment and analysis process.

SECTION 3: COMPONENT DUTIES

3.1. COMPONENT RMIC MANAGERS.

The Component RMIC managers will:

a. Apply GAO standards for internal control in the U.S. Government in the GAO Green Book to ensure effective and efficient functioning of ICOR-FR, ICOR-FS, ICOR-O, ERM, and FRM processes to provide timely risk transparency to senior leaders and increase the likelihood of achieving objectives in DoD SMP.

b. Align existing risk management processes and develop new ERM strategies, as needed.

c. In coordination with the Deputy Secretary of Defense, PIO/DA&M, USD(C)/CFO, DoD CIO, the other PSAs, and the Secretaries of the MILDEPs:

(1) Generate an annual DoD-level enterprise management operations risk profile.

(2) Incorporate the DoD-level enterprise management operations risk profile into the annual DoD-level agency strategic review as specified in Part 6 of OMB Circular No. A-11.

(3) Obtain DPIC approval for the annual DoD-level enterprise management operations risk profile.

(4) Ensure alignment with and incorporation of the DoD-level strategic review into the annual assessments of the NDS and the DoD SMP.

(5) Provide results of the annual strategic review and the DoD-level ICOR-FR, ICOR-FS, ICOR-O, and DoD-level enterprise management operations risk profile to OMB.

(6) Inform the development of new or revised strategic goals and objectives for inclusion in the National Defense Business Operations Plan.

(7) Review Component and functional ICOR-FR, ICOR-FS, ICOR-O, and DoD-level enterprise management operations risk profiles and provide feedback as appropriate.

d. Monitor ICOR-FR, ICOR-FS, ICOR-O, ERM, and FRM compliance in accordance with this issuance, the annual DoD SOA Execution Handbook for Component SOA instructions, and other applicable guidance.

e. Facilitate the use of SMEs to assess ICOR-FR, ICOR-FS, ICOR-O, enterprise risks, and fraud risks in accordance with the GAO Green Book, OMB Circular No. A-123, and Part 6 of OMB Circular No. A-11 guidance.

f. Coordinate with Component RMIC managers to ensure proper documentation of relevant systems and processes under their purview.

g. Solicit input from SMEs to assess identified or potential ICOR-FR, ICOR-FS, ICOR-O, enterprise risks, and fraud risks and the sufficiency of generated reports.

h. Support Component efforts to identify internal controls objectives and necessary controls.

i. Help vet, verify, validate, and assess conclusions provided by SMEs on the design and effectiveness of existing ICOR-FR, ICOR-FS, ICOR-O, enterprise risks, and fraud risks.

j. Help identify and classify assigned ICOR-FR, ICOR-FS, and ICOR-O deficiencies based on evaluations results.

k. Ensure Components establish FRM programs to identify all relevant risks including all fraud risks and controls related to ICOR-FR, ICOR-FS, ICOR-O; determine information provided is sufficient and appropriate; and confirm inputs are documented, implemented, assessed, and monitored. Component RMIC managers report results in accordance with SOA Handbook requirements.

l. Ensure Components or SMEs develop and execute assigned CAPs to address identified ICOR-FR, ICOR-FS, ICOR-O, enterprise risks, and fraud risks.

m. Ensure documentation of identified opportunities for improvement. Share relevant documentation with key stakeholders to support program improvement.

n. Review Component and external entity (e.g., GAO, OIG DoD) reports to determine adequacy of Component efforts to identify and manage risk.

o. Coordinate updates to the applicable ICOR-FR, ICOR-FS, and ICOR-O sections of the annual DoD SOA Execution Handbook with OSD.

p. Develop content for the DoD-level enterprise management operations risk profile, as needed, in support of OSD.

q. Provide RMIC training to their respective RMIC community.

r. Ensure classified information contained in an SOA is appropriately marked, safeguarded, and disposed of in accordance with Volume 3 of DoD Manual 5200.01 .

s. At the direction of their SAO and in coordination with other relevant personnel:

(1) Complete an annual evaluation of ICOR-FR, ICOR-FS, ICOR-O, fraud risks, and enterprise risks, as applicable, that validates the effectiveness of risk management activities to detect, prevent, and remediate MWs and SDs.

(2) Conduct periodic reviews to assess internal controls identified as critical to improving and enhancing processes critical to support the ongoing DoD financial mission.

(3) Collaborate with the information technology function to ensure cybersecurity procedures:

(a) Fulfill OMB Memorandum M-17-25 requirements.

(b) Define cybersecurity requirements at the Component level.

(c) Ensure cybersecurity procedures are validated by the United States Cyber Command, as determined necessary by both the Component RMIC manager and Component SAO.

(4) Evaluate contractual and other service agreements for effective internal controls, including appropriate discussion of performance risks and how they will be addressed; ensure internal controls are sufficiently detailed, including the relationship of third-party provider activities through which service organizations and customers manage the business operations risks of third-party providers. Service providers and Components must support each other during the internal control cycle, Service Organization Control 1 reporting, complementary user entity controls reporting requirements, and the audit process.

(5) Identify relevant risks and controls related to ICOR-FR, ICOR-FS, ICOR-O, and fraud; validate information provided is sufficient and appropriate; and confirm controls are documented, implemented, assessed, and monitored.

(6) Identify and classify SDs, MWs, and business operations risk in accordance with the annual DoD SOA Execution Handbook.

(7) As applicable, prepare, execute, and monitor CAPs regarding business operations risks and identified deficiencies by management and auditors, in a timely manner, until closed. CAPs are reported on a periodic basis or upon DoD RMIC manager request.

(8) Validate a government employee is appointed as an assessable unit manager (AUM) for each assessable unit, to be under Component RMIC manager responsibility. The Component RMIC manager and the Component head must work collaboratively and:

(a) Use their discretion to identify multiple AUMs or a backup.

(b) May waive the government employee requirement as the involved SAO determines necessary.

(c) Should provide formal documentation stating their intention to waive this requirement.

(9) Provide AUMs sufficient assistance, training, and guidance to fulfill their duties of managing activities specific to their duties within the RMIC program.

(10) Maintain records of RMIC-assigned documentation (i.e., issuances, guidance, control activities, and SOAs) in accordance with the DoD Component or Joint Staff records management policies, procedures, and disposition authorities as approved by the National Archives and Records Administration and in accordance with DoDI 5015.02 and pursuant to Chapters 29, 31, and 33 of Title 44, U.S.C.

(a) Consult with the Component SAOs to:

1. Evaluate and manage the risks associated with business operations to establish internal controls the SAO deems necessary and sufficient.

2. Proactively evaluate, prioritize, report, and address business operations risks that may adversely affect the Component's operations and mission.

3. Maintain a list of business operations risks, in line with the OSD risk assessment template, that is actively updated with inputs from across the organization and acts as an input in the development of the annual DoD-level enterprise management operations risk profile. As the SOA program matures, a formal risk register will be implemented, and the expectation will be to use related templates.

(b) Work collaboratively with applicable stakeholders and SMEs to evaluate new and existing CAPs, validating alignment with RMIC program goals and objectives.

(c) Ensure considerations of business operations risks associated with Service Providers Annual Statement on Standards for Attestation Engagements reports, as applicable to the reporting entity's SOA, coincide with assessment testing of financial systems.

(d) Ensure contractual and other service agreements (e.g., memorandums of understanding) have been evaluated for business operations risks to efficient, effective, and compliant satisfaction of contractually agreed-upon services and products. This activity may be completed by other relevant stakeholders such as the Component's Contracts Management Office or General Counsel for example.

(e) Coordinate with AUMs to document end-to-end processes that support operational, administrative, system, and financial events to assess controls and improve efficiency in the agency.

(f) Actively communicate with the Component SMC on CAPs and the resolution status for, at a minimum, MWs and SDs.

3.2. FRAUD REDUCTION TASK FORCE REPRESENTATIVES.

Components must assign a representative to report, identify, and document mitigation and reduction of the likelihood and impact of fraud. Components should assign a representative to advise mitigation strategies for high-priority fraud risks.

a. Fraud Reduction Task Force representatives should coordinate with program managers, program staff, and assessable unit SMEs to complete FRM requirements in the DoD SOA Execution Handbook (e.g., GAO FRM framework assessment, fraud risk assessment, and fraud risk assessment supporting documentation).

b. Components should develop fraud analytics based on high-risk areas identified through the fraud risk assessment.

c. Fraud Reduction Task Force representatives should:

(1) Be informed of current fraud reduction analytics activities and prioritize risk areas with the highest likelihood for fraud.

(2) Produce actionable results from analytics that are measurable fraud reduction outcomes and other implementation activities to reduce fraud.

(3) Take appropriate action to respond to findings (e.g., OIG DoD and GAO findings).

3.3. ASSESSABLE UNITS AND AUMS.

Components must segment their RMIC reporting structure into assessable units to ensure appropriate risk management and facilitate implementation and evaluation of internal controls determined sufficient by the SAO.

a. Factors to consider when determining segmentation into assessable units include:

(1) Scope of mission.

(2) Area(s) of responsibility.

(3) Standard processes.

(4) Anticipated risk involvement.

(5) Leadership priorities.

b. Component assessable unit segmentation actions must be documented by RMIC managers, and outline how segmentation facilitates implementation and evaluation of controls.

c. Component SAOs and Component RMIC managers may designate AUMs as responsible for one or more assessable units.

d. At the direction of the Component RMIC manager, AUMs will maintain and archive relevant documentation for their respective assessable units. Documentation includes:

(1) Guidance.

(2) Standard operating procedures.

(3) Process flows and narratives.

(4) Associated risk and control matrices.

(5) Control objectives and activities.

(6) Applicable executive agreements.

e. Additional AUM roles include:

(1) Assess the risks that may adversely affect the assessable unit's mission or operation.

(2) Ensure documentation of operational and financial internal controls within the assessable unit.

(3) Review processes and procedures to provide recommendations for enhancement, elimination, or implementation of assessable unit internal controls.

(4) Ensure risk-based internal controls tests of design and tests of effectiveness.

(5) Develop CAPs, set milestone dates and targets, and track progress.

(6) Actively communicate with the RMIC program manager on CAP as required for reporting and resolution of control deficiencies.

3.4. SERVICE PROVIDERS.

The DoD uses many service providers to improve efficiency and standardize business operations. Service providers, including non-DoD service providers, will:

a. Provide a description of their ICOR-FR, ICOR-FS, and ICOR-O processes that may affect the Component control environment, risk assessment, control activities, and information and communication systems.

b. Help the Component understand complementary user entity control requirements and managing third-party service provider activities by providing a Service Organization Control 1, type 2 (i.e., report on management's description of a service organization's system and the suitability of the controls' design and operating effectiveness).

c. Provide a list of service providers, sub-service providers, service provider-owned systems, and support inquiries from the auditor. Military Services and other DoD Component service providers are subject to the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements 18 requirements and generally accepted government auditing standards.

SECTION 4: RMIC EXECUTION

4.1. GENERAL.

Components and relevant PSAs must establish a sustainable annual program to develop, document, and maintain policies, procedures, plans, and assessments to provide accountability, safeguard assets, and determine if reasonable assurance internal controls are operating in accordance with all applicable Federal laws, regulations, and policies.

a. Internal controls should include processes for planning, organizing, directing, performing, controlling, and reporting on information systems and business operations applicable to ICOR requirements, outlined in Appendix A of OMB Circular No. A-123.

b. DoD Components:

(1) Will maintain a cyclical review process to provide alignment to DoD mission, strategic plan, goals, objectives, and business process operations.

(2) Must design and implement internal controls to provide reasonable assurance of achieving all ICOR-FR, ICOR-FS, and ICOR-O objectives related to operations, reporting, and compliance.

(3) Should establish and maintain a risk profile, in line with the OSD risk assessment template, that is actively updated with inputs from across the organization and monitors risks for which the appropriate response includes implementing ICOR-FR, ICOR-FS, and ICOR-O processes in accordance with applicable guidance, laws, and regulations.

4.2. COMPLIANCE.

Components must identify and assess compliance with all applicable Federal laws, regulations, and policies regarding ICOR-FR, ICOR-FS, and ICOR-O processes and systems.

a. Components must establish and maintain internal controls to achieve:

(1) Efficient and effective business process operations.

(2) Reliable financial and business operations systems and reporting.

(3) Compliance with applicable laws, regulations, and policies.

(4) Alignment with GAO FRM framework requirements in GAO 15-593SP to combat fraud and preserve integrity in the DoD's programs.

b. Components must enforce accountability of guidance execution by aligning incentive programs, performance management, and other applicable personal management practices to support risk management and the Components' internal controls systems.

4.3. RMIC PROGRAM FRAMEWORK.

a. The RMIC program framework should:

(1) Leverage the documentation of notices of findings and recommendations, SOA reporting templates, and applicable internal and external findings and recommendations to ensure internal controls are designed, implemented, and functioning to enable DoD management and personnel to achieve control objectives for ICOR-FR, ICOR-FS, and ICOR-O reporting categories (See Paragraph 4.8. for explanations of the different reporting categories).

(2) Meet Component and DoD internal control objectives.

b. Components must assess the effectiveness of internal controls and entity-level controls (ELCs) through a process in accordance with the GAO Green Book, OMB Circular No. A-123, and other OSD-issued supplemental guidance. This process will include:

(1) ICOR-FR, ICOR-FS, and ICOR-O risk assessments, as well as GAO FRM Framework assessment.

(2) Identification, evaluation, and remediation of internal control deficiencies.

(3) Internal controls assessment and validation while leveraging:

(a) Management assessments.

(b) Continuous process improvement project results.

(c) Established best practices.

(d) Recent GAO and OIG DoD audit findings, as applicable.

4.4. DATA ACT QUALITY CONTROL PLAN.

The DoD must consider the DoD's Data Act Quality Control Plan in its annual assertion of the SOA every fiscal year. The annual DoD SOA Execution Handbook will include additional guidance and templates for DoD Components.

4.5. RESOURCE MANAGEMENT.

Components must demonstrate efficient and effective management of resources by:

a. Developing key performance indicators used to identify potential efficiencies and enable Components to track progress and measure key performance indicators impact of efficiency.

b. Considering the cost-benefit implementing tools, techniques, and processes to improve the effectiveness and efficiency of their ICOR-FR, ICOR-FS, and ICOR-O functions.

c. Validating the timely, accurate, and proper storage of documentation in accordance with guidance in DoDI 5015.02.

4.6. CONTRACTUAL AGREEMENTS.

In accordance with the requirements of the April 6, 2009 Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, and applicable Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement guidance, Components must ensure risks and internal controls are addressed and sufficiently described in contractual agreements.

4.7. REPORTING.

Components will follow the procedures established in the GAO Green Book and OMB Circular No. A-123, and further defined in the annual DoD SOA Execution Handbook to perform the annual SOA process. Components must report, in their annual SOA, existing and new SDs, MWs, and associated CAPs when identified.

a. DoD SOA.

The USD(C)/CFO prepares and issues a single annual SOA for the DoD.

b. Component SOA.

Components and other reporting entities must annually prepare a SOA that complies with the annual DoD SOA Execution Handbook requirements. Components base their SOA on the general assessment of the effectiveness of their internal controls over all operations and end-to-end process reporting categories, as described in the annual DoD SOA Execution Handbook.

(1) The Component SOA will be signed by the Component head and submitted to the Secretary of Defense. DAFAs will submit their SOA through the appropriate PSA. The SOA must include a letter, signed by the DoD Component head or their deputy, that asserts levels of assurance, as described in the annual DoD SOA Execution Handbook.

(2) The Component SOA will annually provide the Component head and SMC with an assessment of the overall adequacy and effectiveness of Component internal controls to include:

(a) Reporting categories.

(b) Law.

(c) Regulations.

(d) Policy compliance.

4.8. INTERNAL CONTROL REPORTING CATEGORIES.

a. Financial Reporting.

Components will designate each ICOR-FR and ICOR-FS deficiency into one of these reporting categories:

(1) Budget-to-Report.

Budget-to-report encompasses business functions necessary to plan, formulate, create, execute, and report on the budget and business activities of the entity. It includes:

(a) Updates to the general ledger.

(b) All activities associated with generating and managing the internal and external financial reporting requirements of the entity, including pre- and post-closing entries related to adjustments, reconciliations, consolidations, eliminations, etc.

(2) Hire-to-Retire.

Hire-to-retire encompasses all business functions necessary to plan for, hire, classify, develop, assign, track, account for, compensate, retain, and separate the persons (i.e., Service members, civilian employees, contractors, noncombatant evacuees, volunteers) needed to accomplish aspects of the DoD mission.

(3) Order-to-Cash.

Order-to-cash encompasses all business functions necessary to accept and process customer orders for services and/or inventory held for sale. This includes such functions as managing customers, accepting orders, prioritization of orders, fulfilling orders, performing distribution, managing receivables, and managing cash collections.

(4) Procure-to-Pay.

Procure-to-pay encompasses all business functions necessary to obtain goods and services using procurement processes and procedures including executing procurement requirements, strategy, procurement award and management, receipt and acceptance, entitlement, disbursement, and closeout.

(5) Acquire-to-Retire.

Acquire-to-retire encompasses the business functions necessary to obtain, manage, and dispose of accountable and reportable property (capitalized and non-capitalized assets) through their entire life cycle. It includes functions such as requirements identification, sourcing, contract management, purchasing, payment management, general property, plant and equipment management, and retirement.

(6) Concept-to-Product.

Concept-to-product encompasses all business functions necessary to effectively identify product needs, and plan and execute all necessary activities to bring a product from initial concept to full production.

(7) Cost Management.

Cost management encompasses all business functions necessary to identify, collect, measure, accumulate, analyze, interpret, and communicate cost information to accomplish the many objectives associated with control, decision making, planning, and reporting. This includes cost accounting procedures, costing methodology, cost assignment, period end close, and reporting.

(8) Deployment-to-Redeployment/Retrograde.

Deployment-to-redeployment/retrograde encompasses all business functions necessary to plan, notify, deploy, sustain, recall, and reset tactical units to and from theaters of engagement.

(9) Environmental Liabilities.

The End-to-End Environmental Liabilities Business Process encompasses all business functions necessary to identify environmental cleanup, closure, or disposal issues that represent an environmental liability of the DoD, to develop cost estimates and expenditures related to the actions required to eliminate identified environmental liability, and to report appropriate financial information about the environmental liability.

(10) Market-to-Prospect.

Market-to-prospect encompasses all business functions necessary to establish marketing plans, identify target markets, plan and define marketing campaigns, execute marketing campaigns, and measure and evaluate the performance of marketing campaigns for activities such as nonappropriated funds, defense commissary agency, exchange service, foreign military sales, recruiting, property disposal, military depots, and TRICARE.

(11) Plan-to-Stock.

Plan-to-stock encompasses the business functions necessary to plan, procure, produce, inventory, and stock materials used both in operations and maintenance as well as for sale.

(12) Proposal-to-Reward.

Proposal-to-reward encompasses the life cycle of the grant process from the grantor perspective. It includes all the business functions necessary to plan, solicit, review, award, perform, monitor, and close out a grant.

(13) Prospect-to-Order.

Prospect-to-order encompasses all business functions necessary to generate and sustain sales by pursuing qualified leads, employing effective sales techniques, efficient order processing, maintaining customer relationships, and providing support functions including service, personnel, and financial impacts.

(14) Service Request-to-Resolution.

Service request-to-resolution is the process of performing maintenance on materiel or assets requiring repair or complete rebuild of parts, assemblies, subassemblies, and end-items, including the manufacture of parts, modifications, testing, and reclamation as required. Depot maintenance serves to support all asset categories of maintenance by providing technical/enhancement assistance and performing required defined maintenance beyond their respective depreciable life. It also includes the process whereby buildings and other fixed facilities are maintained and renovated during their life cycle.

(15) Service-to-Satisfaction.

Service-to-satisfaction encompasses all business functions necessary to determine service requirements, secure funding, contract with outside vendor, establish service, and measure customer satisfaction.

b. Operations.

Components will designate each ICOR-O deficiency into one of these reporting categories:

(1) Communications.

Communication requires a sender, a message, and an intended recipient, although the receiver need not be present or aware of the sender's intent to communicate at the time of communication; thus, communication can occur across vast distances in time and space.

(2) Intelligence.

The plans, operations, systems, and management activities for accomplishing the collection, analysis, processing, and dissemination of intelligence to provide guidance and direction to commanders in support of their decisions.

(3) Security.

The plans, operations, systems, and management activities for safeguarding both classified and unclassified resources, not including peripheral assets and support functions covered by other reporting categories. Also covers the DoD programs for protection of classified information.

(4) Comptroller and Resource Management.

The budget process, finance and accounting, cost analysis, productivity and management improvement, and the general allocation and continuing evaluation of available resources to accomplish mission objectives. Includes pay and allowances for all DoD personnel and all financial management areas not covered by other reporting categories, including those connected with OMB Circular No. A-123.

(5) Contract Administration.

The fulfillment of contractual requirements including performance and delivery, quality control and testing to meet specifications, performance acceptance, billing and payment controls, justification for contractual amendments, and actions to protect the best interests of the U.S. Government, in accordance with the April 6, 2009, Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum and the May 21, 2008, OMB Memorandum.

(6) Force Readiness.

The readiness capability of combat and combat support (both Active and Reserve) forces which provide the necessary flexibility to deter potential foes and rapidly respond to a broad spectrum of global threats.

(7) Information Technology.

Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes computers, ancillary equipment, software, firmware, and similar services and related resources, whether performed by in-house, contractor, other intra-agency, or intergovernmental agency resources or personnel.

(8) Acquisition.

The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions.

(9) Manufacturing, Maintenance, and Repair.

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

(10) Personnel and Organizational Management.

Authorizations, recruitment, training, assignment, use, development, and management of military and civilian DoD personnel. Includes the operations of headquarters' organizations. Contract personnel are not covered by this category.

(11) Procurement.

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

(12) Property Management.

Construction, rehabilitation, modernization, expansion, improvement, management, and control over real property (both military and civil works construction), including installed equipment and personal property. Also covers disposal actions for all materiel, equipment, and supplies, including the Defense Logistics Agency Disposition Services.

(13) Research, Development, Test, and Evaluation.

The basic project definition, approval, and transition from basic research through development, test, and evaluation and all DoD and contractor operations involved in accomplishing the project work, excluding the support functions covered in separate reporting categories (e.g., procurement and contract administration).

(14) Security Assistance.

Management of DoD foreign military sales, grant aid, and international military education and training programs.

(15) Supply Operations.

The supply operations at the wholesale level from the initial determination of material requirements through receipt, storage, issue reporting, and inventory control, excluding the procurement of materials and supplies. Covers all supply operations at retail level, including the accountability and control for supplies and equipment of all commodities in the supply accounts of all units and organizations, excluding the procurement of material, equipment, and supplies.

(16) Support Services.

All support service functions financed from appropriated funds not covered by the other reporting categories (e.g., health care, veterinary care, and legal and public affairs services). This category also covers every nonappropriated fund activity.

(17) Science and Technology.

Any initiative pertaining to new doctrine or system innovation, predictions of future capabilities and methodologies, development of necessary practices or methodology, and manifestations of determined necessary materials including equipment as well as planning processes and systems relative to these considerations, including sufficiently implementing planned events.

(18) Other.

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

SECTION 5: ERM EXECUTION

5.1. GENERAL.

ERM is a DoD-wide approach to address the full spectrum of external and internal risks to the DoD SMP by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within Components. ERM enables an agency-wide portfolio view of risks strategically aligned to strategic goals and performance objectives, providing senior leadership better insight into how to prioritize resource allocation and ensure successful achievement of DoD-level enterprise management priorities, as stated in the DoD SMP.

5.2. COMPLIANCE.

a. OMB Circular No. A-123.

OMB Circular No. A-123 requires the DoD to implement an ERM capability that is coordinated with the strategic planning and strategic review process established by the Public Law 111-352 (also known as the "Government Performance and Results Modernization Act of 2010") and internal control processes pursuant to Section 3512 of Title 31, U.S.C. (also known and referred to in this issuance as the "Federal Managers' Financial Integrity Act") and the GAO Green Book, while Component heads and relevant PSAs establish and maintain sustainable policies, procedures, and practices to comply with requirements of OMB Circular No. A-123 and Part 6 of OMB Circular No. A-11.

b. Public Law 116-117.

Public Law 116-117, also known and referred to in this issuance as the "Payment Integrity Information Act of 2019 (PIIA)," requires Federal agencies to identify, report, and reduce improper payments in their programs and activities. PIIA also requires annual reports by inspectors general on their agencies' compliance.

5.3. STRATEGY AND PERFORMANCE.

a. Components establish and maintain:

(1) Annual Component-level strategic goals and performance objectives that align with and support achievement of the DoD-level NDS and DoD SMP (including the DoD Annual Performance Plan and DoD Annual Performance Report).

(2) Consistent approaches to identify and manage risks – sources of uncertainty in the form of threats and opportunities – to Component-level strategic goals and performance objectives.

(3) A comprehensive risk profile while conducting regular assessments to ensure effective risk response.

(4) A listing of all risks, including risks not categorized as an MW or SD, to determine if there is a systemic fraud risk and take proper action to address it.

(5) Address top DoD management challenges, recommendations and DoD-owned or co-owned GAO high-risk area recommendations.

(6) Compliance with GAO audit engagements' requirements and prompt closure of GAO open recommendations.

b. Components will increase the likelihood of achieving their most important priorities and realizing better outcomes by regularly and proactively identifying risks to their strategic goals and performance objectives.

5.4. ERM PROCESS.

a. DoD ERM capability is characterized by a consistent five-step process and enabling tools, which should be applied top-down and bottom-up throughout all levels of the DoD. The top-down approach consists of an annual enterprise risk assessment performed by senior leadership to identify risks to the DoD SMP. The bottom-up approach involves aggregating and analyzing risks to Component-level strategic goals and performance objectives to determine if Component-level risks – either individually or in the aggregate – are likely to limit or prevent the DoD from achieving priorities stated in DoD SMP. ERM supports a portfolio view of risks by aggregating and integrating information for all risk types across the DoD.

b. In accordance with OMB Circular No. A-123, agencies must manage risk in relation to achievement of reporting objectives. DoD ERM should be executed with the SOA process. Components must perform these steps in DoD ERM process to identify and manage risks to priorities in Component-level strategic and performance plans:

(1) Risk Identification.

(a) Risk identification is a structured approach to identify and categorize risks arising in pursuit of DoD strategic goals and performance objectives, as stated in DoD SMP.

(b) A risk taxonomy helps organizations classify, prioritize, and communicate risk information consistently by providing standard category and subcategory definitions and promoting a common risk language. A risk taxonomy facilitates conversations about linkages between and among risk events, promotes shared understanding and terminology across organizations and provides senior leadership with a consistent view of an organization's top risks to facilitate discussions on cross-cutting risk. Cross-cutting risks include, but are not limited to, strategic, operational, financial reporting, technology, extended enterprise, reputational, and compliance risks.

(2) Risk Assessment.

(a) Risk assessment is a methodical approach to apply risk rating criteria to evaluate the overall exposure to identified risks associated with achieving the strategic goals and performance objectives in DoD SMP.

(b) Risk assessment involves estimating the severity of risks in terms of standardized criteria (e.g., risk likelihood and impact scales) using both qualitative and quantitative techniques to evaluate risks on a residual basis (e.g., considering internal controls that are already in place to manage the risk to acceptable levels).

(3) Risk Prioritization.

(a) Risk prioritization is a systematic approach to determine the most critical risks to strategic goals and performance objectives at the DoD and Component levels by applying risk ratings, senior leadership judgment, and other factors to order enterprise risks from higher to lower importance. Taking a deliberate and consistent approach to prioritize enterprise risks allows senior leadership to make risk-informed decisions about optimizing resource allocation to support actionable risk responses.

(b) Prioritization criteria (e.g., adaptability, complexity, velocity, duration, and recovery) help senior leadership evaluate trade-offs between allocating resources to respond to certain risks and choosing to accept other risks that are already managed to acceptable levels.

(4) Risk Response.

(a) Risk response is a deliberate approach to consider, implement, and document appropriate actions to accept, avoid, mitigate, or share– in alignment with risk appetite – associated with strategic goals and performance objectives at the DoD and Component levels.

(b) Risk appetite scales help senior leadership understand and define the level of risk, on a broad level, the DoD is willing to accept in pursuit of its strategic goals and performance objectives.

(c) For each identified risk to Component-level strategic plans, Components should determine underlying root causes, develop and implement specific risk response action plans, and establish clear accountabilities to prevent overall risk from exceeding the DoD risk appetite levels.

(5) Risk Monitoring and Reporting.

(a) Risk monitoring and reporting of internal and external business context in which the DoD and Components operate is a foundational element of DoD ERM capability. Continuous risk monitoring and reporting is accomplished by embedding these capabilities into existing processes to provide Component heads and the DPIC timely and relevant updates on enterprise risks.

(b) DoD performance tolerance levels should be established to serve as guardrails for risk monitoring. If thresholds in the form of key risk indicators are about to be breached, Component AUMs and RMIC managers should notify their leadership that a response may be required.

(c) DoD enterprise risk information is stored in Advana.

(d) DoD and Component-level enterprise management operations risk profiles assist senior leadership and OMB in understanding the aggregate levels and types of risk the DoD is managing to increase the likelihood of achieving its mission-support priorities and strategic priorities.

5.5. CHANGE MANAGEMENT.

Successfully incorporating the DoD's emerging ERM/risk management internal controls – operations (RMIC-O) capabilities will require a change management approach created by the PIO/DA&M that considers each Component's needs to design and deliver effective ERM/RMIC-O training and communication materials. Components must support the operationalization of ERM/RMIC-O by actively participating in ERM/RMIC-O training to increase awareness of ERM/RMIC-O, reduce impacts of change caused by ERM/RMIC-O implementation, and facilitate adoption of ERM/RMIC-O throughout the DoD.

a. ERM/RMIC-O Training.

ERM/RMIC-O training is an essential element of an overall change management program associated with DoD ERM/RMIC-O capability. The PIO/DA&M will develop DoD- and Component-level ERM/RMIC-O training programs to address the needs of stakeholders tasked with key ERM/RMIC-O roles and responsibilities, including:

(1) Senior Leadership.

Senior leadership will receive ERM/RMIC-O training designed to enable them to:

(a) Promote an open risk culture at all levels (i.e., tone at the top) and strengthen support for ERM/RMIC-O.

(b) Define and demonstrate the value proposition of ERM/RMIC-O.

(c) Continue integrating strategy, performance, and risk management to improve outcomes.

(2) Management.

Management will receive ERM/RMIC-O training designed to enable them to:

(a) Promote transparency.

(b) Define and demonstrate the value proposition of ERM/RMIC-O.

(c) Foster risk ownership and accountability.

(d) Facilitate risk identification, assessment, prioritization, response, monitoring, and reporting.

(3) Staff.

Staff will receive ERM/RMIC-O training designed to bolster awareness of critical risks to strategy and performance and encourage knowledge and information sharing.

b. ERM/RMIC-O Communications.

ERM/RMIC-O communications will encourage and support ERM/RMIC-O adoption across the DoD. To promote ERM/RMIC-O implementation and reduce uncertainty among Components, the PIO/DA&M will develop and execute an ERM/RMIC-O stakeholder engagement and approval plan designed to:

(1) Provide an overall framework for managing and coordinating various risk-related communications that must occur, directly or indirectly, during essential phases of ERM/RMIC-O operations.

(2) Deploy tailored communications for stakeholders, providing consistent engagement and support to improve efficiency and effectiveness of operations.

(3) Include guidelines for ongoing information sharing. Relevant critical information about enterprise risks should be identified, captured, communicated, and protected in a form and timeframe that enables senior leadership, management, and staff to carry out their ERM/RMIC-O responsibilities efficiently and effectively, while ensuring operations security.

SECTION 6: ORGANIZATION FUNCTIONS AND COMPONENT SUPPORT

6.1. GOVERNANCE STRUCTURE.

a. The IRM DPIC serves as the DoD-level SMC for ERM, ICOR-O, GAO high-risk areas relevant to the DoD, and management of GAO and OIG DoD open recommendations. The DPIC will refer issues to the DMAG, as appropriate.

b. The FGB serves as the DoD-level SMC for ICOR-FR, ICOR-FS, and FRM. The FGB will refer issues to the DMAG, as appropriate.

c. The Fraud Reduction Task Force is the cross-enterprise tactical team consisting of SMEs and Component representatives who actively work to mitigate high-priority fraud risks that require DoD-wide solutions.

d. The Components will establish an SMC that includes the necessary functional leaders to oversee the assessment of internal controls and monitor the SDs and MWs within their Component.

6.2. COMPONENT SMC.

The Component SMC will:

a. Oversee implementation and sustainment of internal controls to provide reasonable assurance over operations, reporting, and compliance.

b. Incorporate a dedicated platform to facilitate discussions, evaluations, and tracking of the Component RMIC program endeavors within ICOR-FR, ICOR-FS, ICOR-O, and fraud risks, alongside the mandate of the DoD-level enterprise management operations risks profile.

c. Provide governance for the risk management function, to oversee the establishment of the annual DoD-level enterprise management operations risk profile, regular assessment of risk, and development of appropriate risk response.

d. Provide overarching direction on CAP development, monitoring, and estimated completion dates.

e. Drive accountability of senior officials in charge of the resolution of systemic MWs related to their respective programs.

f. Recommend RMIC issues for consideration by the DPIC, FGB, and DMAG or other governance forums, as appropriate.

g. Be involved in identifying and ensuring, where applicable, correction of SDs and MWs relating to their respective programs.

h. Provide their Component head with recommendations on SDs and MWs for input to the annual DoD SOA cycle.

i. Maintain records of each SMC meeting in accordance with guidance in DoDI 5015.02.

6.3. SENIOR ASSESSMENT TEAM (SAT).

The Component SMC should, in accordance with the recommendations in OMB Circular A-123 Appendix A, include a SAT to lead assessments and remediation related to ICOR-FR, ICOR-FS, and ICOR-O. The SAT should:

a. Consist of SMEs in various mission and organizational areas to review and approve policies, programs, and other initiatives related to the strengthening of internal controls and remediation of issues.

b. Provide oversight and accountability for the specific areas of subject matter expertise and report to the SMC.

c. Consider ICOR-FR, ICOR-FS, and ICOR-O in promoting sufficient, efficient, and effective DoD compliance with applicable laws, regulations, and policies.

d. Maintain records for each SAT meeting in accordance with guidance in DoDI 5015.02.

6.4. SAO.

The Component SAO supports the Component head, DoD SMC, or Component SMC. The Component SAO will:

a. Monitor and ensure timely consideration and resolution of Component SDs and MWs.

b. Report the status of corrective action(s) through the appropriate Component RMIC manager and the DoD RMIC manager.

c. Ensure Component personnel monitor the effectiveness of their respective internal controls to ensure timely and effective actions are in place to resolve SDs and MWs.

d. Receive, assess, and communicate with the DoD service provider over service provider self-assessments on the Federal Financial Management Improvement Act of 1996, Public Law 113-283 (also known as the "Federal Information Security Modernization Act of 2014"), the Risk Management Framework certifications and accreditations in accordance with DoDI 8510.01, and any impact to financial and operational processes and systems within the RMIC program.

e. Champion agency-wide efforts to manage ERM and RMIC and advise senior leaders on the strategically aligned portfolio view of agency risks.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AUM	assessable unit manager
CAP	corrective action plan
DAFA	Defense Agency and DoD Field Activity
DMAG	Deputy's Management Action Group
DoD CIO	DoD Chief Information Officer
DPIC	Defense Performance Improvement Council
ELC	entity-level control
ERM	enterprise risk management
FGB	Financial Improvement and Audit Remediation Governance Board
FRM	fraud risk management
GAO	Government Accountability Office
GS	General Schedule
ICOR	internal controls over reporting
ICOR-FR	internal controls over reporting for financial reporting
ICOR-FS	internal controls over reporting for financial systems
ICOR-O	internal controls over reporting for operations
IRM	integrated risk management
MILDEP	Military Department
MW	material weakness
NDS	National Defense Strategy
OIG DoD	Office of Inspector General of the Department of Defense
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act of 2019
PIO/DA&M	Performance Improvement Officer/Director of Administration and Management
PSA	Principal Staff Assistant
RMIC	risk management and internal control

ACRONYM	MEANING
RMIC-O	risk management internal controls – operations
SAO	senior accountable official
SAT	senior assessment team
SD	significant deficiency
SMC	Senior Management Council
SME	subject matter expert
SMP	Strategic Management Plan
SOA	statement of assurance
U.S.C.	United States Code
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense

G.2. DEFINITIONS.

Unless otherwise noted, the following terms are defined for the purpose of this issuance.

TERM	DEFINITION
acquisition	The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services.
activity	An action or short series of actions typically considered trivial or short-term steps in achieving an outcome.
Advana	A single repository that serves as the system of record for all DoD and Component-level enterprise risks.
assessable unit	Any organizational, functional, programmatic, or other applicable subdivision of a Component that allows for adequate independent internal control analysis (i.e., separate and independent of its parent Component).
AUM	A government employee, or contract employee if waived by the assessable unit head, selected by appropriate functional leadership that is responsible for the RMIC requirements of the assessable unit.
business operations	The activities, processes, functions, interfaces, automation, and communication performed to achieve a specified objective. Business operations support but do not include military operations.

TERM	DEFINITION
business operations risk	Uncertainty associated with successfully performing business operations, which exist to define how the strategic plan is implemented or how the business mission of the DoD or its Components is carried out.
CAP	A written document that spells out the specific activities necessary to resolve a deficiency (e.g., MW) and includes targeted milestones and completion dates. CAPs for operational assessment MWs are maintained with the RMIC documentation.
Component RMIC manager	An individual designated and appointed by Component leadership to monitor and oversee a Component's or assessable unit's RMIC program. The action officer for each Component who leads the design, implementation, and performance of the Component's RMIC program and, as applicable, Component AUMs.
control	An action or series of actions established through policies, procedures, techniques, or mechanisms designed to mediate the outcome of an action or series of actions based in prior performance. Control may be the result of mechanical, personnel, or software facilitated manipulation intended to describe or affect the result of prior performance.
corrective action	Action taken to resolve a potential or experienced nonconformance or deficiency.
DoD leadership	Any DoD individual assigned to function in a leadership role influencing or directing the performance of other personnel and responsible for satisfying DoD objectives.
effectiveness and efficiency	Effectiveness is the state of having produced the desired result and having obtained that result with minimal alterative output (e.g., waste). Efficiency describes the process operating and consuming no or minimal unrequired resources (e.g., labor, time) with no waste involved. Outputs measure the quantity of services provided as well as the services' efficiency and effectiveness in output.
ELC	A control having a pervasive effect on an entity's (e.g., Component's) internal control system designed to provide reasonable assurance that objectives related to the entity as a unit are met.

TERM	DEFINITION
enterprise risk	A process or methodology that involves identifying, assessing, responding, and monitoring the risks and opportunities that may affect the achievement of DoD strategic objectives, requiring the attention of DoD senior leadership.
entity	An organization or unit within the DoD, including the DoD as a whole, a Component, assessable unit, or subdivision of a Component that is required to maintain and use independent ELCs.
ERM	An effective organization-level approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within individual programs or functional portfolios.
financial	Of or involving funds, financial reporting, or financial systems.
financial reporting	The documentation of the results of financial system containing measures include recording, verification, validation, and timely description of transactions involving financial revenues, expenditures, transfers, assets, and liabilities.
financial risk	Uncertainty associated with successfully addressing potentials for waste, fraud, or misappropriation of funds and achieving financial auditability including financial reporting (e.g., material misstatements or improper payments). Financial risk can be operational.
financial systems	The operations including transfer, holding, and accounting of fiduciary activities and their status including governance, processes, procedures, and councils used to describe and exercise financial control. Financial systems involve the use of information technology computer systems to transfer, maintain, account, and report fiduciary functions.
finding	Notation and documentation of a nonconformance to laws, regulations, policy, or approved procedure.

TERM	DEFINITION
functional portfolio	A grouping of related projects, programs, processes, and activities that contributes to the readiness of the joint warfighter. These include, but are not limited to: Human resource management. Financial management. Acquisition (e.g., research, development, testing and evaluation, procurement) logistics and supply chain management. Information technology management. Health care management. Real property management. Community services.
inherent risk	Risk existing before the application of defined and documented internal controls.
integrated financial management systems	A unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel, manual or automated processes, procedures, controls, and data necessary to perform financial management functions, manage financial operations of the DoD and DoD Component, and report on the DoD and DoD Component's financial status to central agencies, Congress, and the public.
internal control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that an entity's objectives will be achieved.
issue	A condition, situation, or event that has the potential for or currently is characterized by nonconforming to existing requirements or not promoting effective and efficient business operations.
key performance indicator	A measurable value that indicates the state or level of something, used to track progress toward a goal, objective, or desired outcome within a given timeframe.

TERM	DEFINITION
MW in ICOR	An MW in internal control over compliance is a condition where management lacks a process that reasonably ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving agency objectives.
MW in ICOR-FR	An MW in internal control over external financial reporting is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.
MW in ICOR-FS	Condition or situation determined by Component or DoD leadership as significantly impairing fulfillment of financial operations or DoD fiduciary performance; significantly weakening established safeguards against fiduciary fraud, waste, loss of funds, unauthorized use, or misappropriation of funds, property, or other asset accountability; or involving fiduciary conflicts of interest. May include, but is not limited to, conditions that impact the operating effectiveness of financial ELCs.
MW in ICOR-O	Condition or situation determined by leadership as significantly impairing fulfillment of essential operations or the DoD's mission; depriving the public of needed services; or significantly weakening established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of property, other assets, or conflicts of interest. May include, but not limited to, conditions that impact the operations ELCs' operating effectiveness.
nonconformance	A condition that does not conform to laws, regulations, policies, requirements, specifications, or applicable standards (e.g., the GAO Green Book) or lack of conformance with integrated financial management systems compliance pursuant to Federal requirements prescribed in the Federal Managers' Financial Integrity Act and DoD 7000.14-R.
opportunity	A condition or situation that can be implemented in an activity or process, which may or will lead to improved operations as measured by results, efficiency, effectiveness, or consequent actions.

TERM	DEFINITION
procedure	Description of the performance of a process which should include, as applicable, notation of responsible individuals, itemization of inputs and outputs, itemization of sequential activities within the process, interactions and interfaces and communications, and/or references to required instructions or specifications involved. Procedures must be documented.
process	A sequence of activities performed to transform input(s) to output(s), typically considered as a value-add or statutorily required series of actions in transforming an input to an output.
reasonable assurance	As determined by leadership, a significant but not absolute confidence, based upon an informed judgment by management regarding the overall adequacy and effectiveness of internal controls based upon available information, that the systems of internal controls are operating as intended.
reporting	Disclosures and measures provided to those inside and outside of the DoD. The measures of performance, other than the traditional assessment of financial performance, including performance results in accordance with Title 31, U.S.C. Measures of performance also may reference index scores, ratios, counts, and other information not presented in the basic financial statements (e.g., the balance sheet, statement of net cost, statement of changes in net position, statement of budgetary resources, and the notes). All information disclosed in the annual report (but outside the main financial statements) about such items are considered non-financial information.
residual risk	Risk remaining following application of defined and documented internal controls. Residual risk is evaluated to determine if the remaining risk may be accepted or must be managed further once an internal control is established to address the original risk.
risk	The effect of uncertainty on objectives.
risk appetite	The amount of risk, on a broad level, an organization is willing to accept in pursuit of its objectives.
risk management	A series of coordinated activities to direct and control threats and opportunities to achieve an organization's goals and objectives.

TERM	DEFINITION
Risk Management Framework	A U.S. Government guideline, standard, and process for risk management to help secure information systems (computers and networks) developed by the National Institute of Standards and Technology.
risk profile	A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks. The profile must identify sources of uncertainty, both positive (e.g., opportunities) and negative (e.g., threats).
risk register	A listing of risks including every risk identified, accompanied by a description of risk impact, probability of occurrence, potential consequences, and any other factor the risk register's owner determines to be involved in assessing the magnitude of risks within the Component. Risk registers may be used to create risk profiles where consequential risks are itemized.
risk tolerance	The acceptable level of variation in performance relative to the achievement of objectives represented by statement(s) reflecting quantification of problem(s) or negative situations determined to be cost-effective to encounter or of insufficient probability to provide resources in countering.
root cause	The most basic cause of a situation usually determined using root cause analysis (see ICOR-O Guidance for detailed methodology).
SAO	A member of senior management or leadership of the DoD, Component, or accountable unit.
SD	A control deficiency or combination of control deficiencies that, in management's judgment, represents SDs in the design or operation of internal controls that could adversely affect Component or DoD ability to meet its internal control objectives and is important enough to merit attention by those charged with governance.
SD in ICOR	An SD that Component or DoD leadership determines is significant enough to affect internal or external decision-making and reports outside of the Component.
service provider	An entity or segment of an entity that provides services to user entities that are likely to be relevant to those user entities' internal control.

TERM	DEFINITION
SMC	A team, composed of or sponsored by senior level executives, that oversees assessing and documenting the effectiveness of internal controls over operations, financials, compliance, and the associated reporting.
SOA	An annual statement, in memorandum format, that provides a leader's explicit level of assurance whether internal controls are effective. The SOA is based on self-assessments and testing of internal controls developed for mission-essential business functions relative to risk and identifies any MWs found during the analysis.
standards for attestation engagements	A statement that reports on controls at a service organization necessary to address examination engagements undertaken by the service organization.
systemic	Of or relating to a system, especially as opposed to a particular part. Spread across, to some degree, the entity being considered and possessing specific factors characterizing the issue as systemic. Concerning enterprise leadership, systemic is defined as an issue within DoD unit or units that has sufficient effect to significantly impact the accomplishment of the DoD mission, as determined by leadership.
timely	Happening at the most suitable time, with suitable time being determined by designated importance or impact and involved scope, resource requirements, complexity, and interrelationships. When viewed from a project standpoint, timely would relate to the time required to complete a project with no interference in resource availability and efforts were focused on completing the project. Timely does not include non-value activities such as wait times in seeking approvals, delays caused by non-performance of required activities, time delays due to not requesting required resources, or any other step not considered contributory to accomplishing the task at hand.

REFERENCES

American Institute of Certified Public Accountants Statement on Standards for Attestation, September 2020

Defense Federal Acquisition Regulation Supplement, current edition

Deputy Secretary of Defense Memorandum, "Defense Business Council Charter," January 18, 2022

Deputy Secretary of Defense Memorandum, "Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues," September 1, 2021

Deputy Secretary of Defense Memorandum, "Governance Structure for Deputy Secretary Managed Processes," August 23, 2023

DoD 7000.14-R, "Department of Defense Financial Management Regulation (DoD FMR)," current edition

DoD Directive 5118.03, "Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense," April 4, 2023

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD's Data Act Quality Control Plan, July 2, 2021[1]

Federal Acquisition Regulation, current edition

Government Accountability Office 14-704G, "Standards for Internal Control in the Federal Government," September 10, 2014 (also known as the "Government Accountability Office Green Book")

Government Accountability Office 15-593SP, "A Framework for Managing Fraud Risks in Federal Programs," July 2015

Office of the Deputy Chief Financial Officer, "Department of Defense Agency Financial Report," current edition[2]

Office of Management and Budget Circular No. A-11, "Preparation, Submission, and Execution of the Budget," current edition

Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control and Enterprise Risk Management," July 15, 2016

Office of Management and Budget Memorandum M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 19, 2017

Office of Management and Budget Memorandum, "Conducting Acquisition Assessments under OMB Circular A-123," May 21, 2008

[1] Available at https://guidanceweb.ousdc.osd.mil/odcfo_afp.aspx#publications
[2] Available at https://comptroller.defense.gov/ODCFO/afr/.

Office of the Performance Improvement Officer/Director of Administration and Management, "DoD Annual Performance Plan," current edition[3]

Office of the Performance Improvement Officer/Director of Administration and Management, "DoD Annual Performance Report," current edition

Office of the Secretary of Defense, "DoD Strategic Management Plan," current edition

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, "DoD Statement of Assurance Execution Handbook," current edition

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, "Financial Improvement and Audit Remediation Governance Board Charter," April 19, 2012

National Defense Strategy, current edition

Public Law 111-352, "GPRA Modernization Act of 2010," January 4, 2011

Public Law 113-283, "Federal Information Security Modernization Act of 2014," December 18, 2014

Public Law 116-117, "Payment Integrity Information Act of 2019," March 2, 2020

Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Guidance on the Assessment of Acquisition Functions under Office of Management and Budget, Circular No. A-123," April 6, 2009

United States Code, Title 5, Chapter 4 (also known as the "Inspector General Act of 1978," as amended)

United States Code, Title 10, Section 153

United States Code, Title 31

United States Code, Title 44

[3] Available at https://dam.defense.gov/Publications/Annual-Performance-Plan-and-Performance-Report/