



# DISA INSTRUCTION 630-125-6

## RISK MANAGEMENT AND INTERNAL CONTROL PROGRAM

---

**Office of Primary Responsibility:** J-8 Office of the Chief Financial Officer  
[disa.meade.rmc.list.rm3-micp@mail.mil](mailto:disa.meade.rmc.list.rm3-micp@mail.mil)

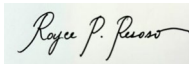
**Effective:** September 12, 2014  
**Change # 1 Effective:** April 7, 2025

**Releasability:** Public Release

**Reissues and Cancels:** DISAI 630-125-6, "Managers' Internal Control Program (MICP)," September 12, 2014

**Approved by:** Frederick A. Henry, Brigadier General, USA, Chief of Staff

**Change #1 Approved by:** Royce P. Resoso, Brigadier General, USA, Chief of Staff

 Digitally signed by  
RESOSO.ROYCE.PATRICK.102  
8338135  
Date: 2025.04.07 14:25:16 -04'00'

**Purpose.** In accordance with the authority contained in DoD Instruction 5010.40, "DoD Enterprise Risk Management and Risk Management and Internal Control Program," December 11, 2024, and DoD Directive 5105.19, "Defense Information Systems Agency," February 15, 2022, this issuance:

- Prescribes policy and assigns responsibility for the Risk Management and Internal Control (RMIC) program for the Defense Information Systems Agency (DISA).
- Advises the Senior Assessment Team (SAT) and identifies and describes the three categories of internal controls used by the Agency for the RMIC Program.

## TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION .....	3
1.1. Applicability .....	3
1.2. Policy .....	3
1.3. IC Categories .....	3
a. Internal Controls Over Reporting for Operations (ICOR-O). ....	3
b. Internal Controls Over Reporting for Financial Reporting (ICOR-FR).....	3
c. Internal Controls Over Reporting for Financial Systems (ICOR-FS) .....	4
1.4. Summary of Changes .....	4
SECTION 2: RESPONSIBILITIES .....	5
2.1. Chief Financial Officer (CFO)/Comptroller, OCFO (J-8) .....	5
2.2. J-Code Directors, Senior Executives, and Commanders.....	5
2.3. Inspector General (IG). ....	6
2.4. Chief Information Officer (CIO).....	6
2.5. Agency RMIC Coordinator .....	6
2.6. AUM .....	7
2.7. SAT .....	7
GLOSSARY .....	9
G.1. Acronyms .....	9
G.2. Definitions .....	9
REFERENCES.....	12

## SECTION 1: GENERAL ISSUANCE INFORMATION

**1.1. APPLICABILITY.** This issuance applies to DISA and other components of the Department of Defense (DoD) over which the agency has been authorized administrative control.

### 1.2. POLICY.

a. The objective of the RMIC program is to establish, evaluate, and correct weaknesses in policies and procedures, provide reasonable assurance that operations are effective and efficient financial reporting is reliable and timely, and ensure the Agency complies with applicable laws and regulations.

b. The focus of the Agency RMIC process will be on continuous monitoring of internal controls (ICs), not on periodic reviews and occasional control exercises. ICs will be integrated into the daily management practices of all DISA managers.

c. The RMIC process will address all significant operations and mission responsibilities and will not be limited to administrative and financial operations.

d. The RMIC evaluation process will, wherever possible, rely on existing information sources such as management and oversight reviews, computer security reviews, audits, and inspections, etc. If existing data does not provide for adequate review of vital internal controls, management should conduct appropriate reviews to make reasonable judgments about the effectiveness of their internal controls.

e. Managers are encouraged to be forthright in reporting material weaknesses in vital internal controls and will not be penalized (at any level of the organization) for reporting a problem as a material weakness.

f. RMIC procedures are applied to the three distinct categories listed below and tailored to each category. These procedures are detailed in OMB Circular A-123 and Agency annual IC guidance. Nonconformance with Federal requirements constitutes a material weakness, which will be reported in the SOA with a corrective action plan and schedule for resolution.

### 1.3. IC CATEGORIES.

**a. Internal Controls Over Reporting for Operations (ICOR-O).** ICOR-O includes all operational and administrative controls relevant to mission essential functions conducted within the organization (excluding financial reporting and financial systems). ICOR-O also includes ICs over acquisition functions and establishes and assesses the ICs used in the ICOR-O process.

**b. Internal Controls Over Reporting for Financial Reporting (ICOR-FR).** ICOR-FR includes all financial reporting functions and establishes and assesses the ICs used in the FMFIA ICOR-FR process. Financial reporting includes reliable, timely, and accurate financial information for managing day-to-day operations and reporting on DISA's financial condition.

**c. Internal Controls Over Reporting for Financial Systems (ICOR-FS).** ICOR-FS includes all integrated financial management systems. ICOR-FS follows procedures to assess, evaluate, and report the conformance of the Agency's integrated financial management systems with Federal requirements.

**1.4. SUMMARY OF CHANGES.** The changes to this issuance update terminology for the RMIC program, clarifies RMIC requirements, assign responsibilities to Agency organizations involved with the RMIC, and advises the SAT.

## **SECTION 2: RESPONSIBILITIES**

**2.1. CHIEF FINANCIAL OFFICER (CFO)/COMPTROLLER, OCFO (J-8).** The CFO, designated by the Director, DISA, as the Senior Responsible Official for the RMIC, will:

- a. Develop guidance that will reasonably ensure Agency RMIC objectives are met and establish a RMIC program to evaluate the design of ICs, assess the operating effectiveness of ICs, and identify and promptly correct ineffective ICs and establish ICs, when warranted.
- b. Annually provide separate explicit levels of assurance in a Statement of Assurance (SOA) addressed to the Secretary of Defense for the three IC assessments of ICOR-O, ICOR-FR, and ICOR-FS, as applicable, based upon the RMIC annual guidance for Director, DISA, signature.
- c. Direct and oversee the RMIC program for the Agency, to include meeting the requirements of Internal Control over Financial Reporting, within Office of Management and Budget (OMB), OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control."
- d. Issue annual guidance to the J-Code Directors, Senior Executives, and Commanders regarding submission requirements for compliance with DoD Instruction 5010.40, (authority document).
- e. Designate a SAT comprised of senior level executives to advise the Director, DISA, on IC matters and ensure the Agency's compliance with the intent and timelines of OMB Circular No. A-123 and Office of the Under Secretary of Defense Comptroller (OUSD(C)) guidance.
- f. Designate an individual to serve as the Agency's RMIC Coordinator who will act as the Agency's point of contact for all matters relating to RMIC.

**2.2. J-CODE DIRECTORS, SENIOR EXECUTIVES, AND COMMANDERS.** These individuals will:

- a. Develop RMIC goals for the directorate that will reasonably ensure Agency RMIC objectives are met.
- b. Segment the organization into Assessable Units (AU) by organization or function, suitable for evaluating ICs. The AU will include all personnel and functions of the organization. An organization with field activities will ensure these activities are included in the inventory.
- c. Assign, in writing, the Assessable Unit Manager (AUM) responsible for each AU.
- d. Ensure AUMs are responsible and accountable for establishing and evaluating ICs in a manner consistent with this issuance.
- e. Ensure internal control weaknesses are promptly reported, and actions taken to correct each weakness.

f. Provide input to the CFO for DISA's annual SOA, in accordance with Agency annual IC guidance.

**2.3. INSPECTOR GENERAL (IG).** The IG will, within the context of its annual audit planning, consider projects that verify corrective actions taken on weaknesses identified by audits and inspections.

**2.4. CHIEF INFORMATION OFFICER (CIO).** The CIO will assess the level of assurance of the ICOR-FS to ensure compliance with the Federal Managers' Financial Integrity Act (FMFIA), in accordance with OMB Circular No. A-123; DoD 7000.14-R, Financial Management Regulation, Volume 1: "General Financial Management Information, Systems, and Requirements," Chapter 3, "Federal Financial Management Improvement Act Compliance;" and the OUSD(C) annual guidance.

**2.5. AGENCY RMIC COORDINATOR.** The Agency RMIC Coordinator will:

- a. Assist the SAT in the design and implementation of the RMIC program.
- b. Work with senior management to rank and prioritize risks to ensure alignment with short- and long-term priorities of the Agency.
- c. Serve as the liaison between the SAT and the AUM to communicate management's mission requirements, ensuring the requirements are incorporated in the review of ICs and associated risks.
- d. Evaluate the effectiveness of management controls and appointment of AUMs and provide technical advice and guidance to AU Administrators and AUMs.
- e. Retain RMIC documentation (e.g., process flows and narratives, including associated risk matrices, control objectives, and control activities; Letter of Assurance from AUMs to support the DISA Letter of Assurance; and listing of AUs and AUMs) at a central repository.
- f. Maintain a list of the AUs and AUMs of the organizations.
- g. Perform studies and prepare recommendations for correcting systemic RMIC weaknesses that cross organizational boundaries.
- h. Monitor and verify corrective actions have been completed on material weaknesses.
- i. Identify and issue annual SOA milestones to the SAT.
- j. Prepare the Agency's annual SOA for the signature of the Director, DISA.

**2.6. AUM.** The AUM will:

- a. Provide training and guidance to AUs regarding program reporting requirements and ensure documentation of operational and financial internal controls within the AU.
- b. Conduct an IC assessment in accordance with the annual OUSD(C) and Agency IC guidance.
- c. Provide an annual Letter of Assurance to the Agency RMIC Coordinator.
- d. Document business processes and procedures to provide recommendations for enhancement, elimination, or implementation of AU internal controls.
- e. Assess risks that may adversely affect the AU's mission, test effectiveness of controls, and identify IC deficiencies and weaknesses.
- f. Upload supporting documentation, such as lists of all AUs, process flow charts, risk assessments and analysis, test plans, test results, and corrective action plans, to the shared workspace for record retention and audit purposes.
- g. Provide status on material weaknesses which address, at a minimum, the risks, test documentation, milestones, and accomplishments, and communicate with the RMIC program manager on Corrective Action Plans, as required, for reporting and resolution of control deficiencies.
- h. Evaluate, in conjunction with the agency RMIC Coordinator, the quality of the organization's implementation of this issuance, including adequate documentation.

**2.7. SAT.** The SAT is comprised of the Agency Senior Executive Service members (or their designated representatives) assigned by the chair (Deputy Director, DISA). The SAT, in accordance with the recommendations in OMB Circular No. A-123, Appendix A, will:

- a. Advise the Director, DISA, on IC matters, to include the identification of IC weaknesses that merit reporting as material weaknesses.
- b. Provide oversight of assessing and documenting the effectiveness of ICs for ICOR-FR, ICOR-FS, and ICOR-O in promoting sufficient, efficient, and effective DoD compliance with applicable laws, regulations, and policies.
- c. Communicate the IC-related objectives throughout the Agency.
- d. Ensure IC assessments are carried out in a thorough, effective, and timely manner.
- e. Validate which operational and financial processes and systems weaknesses are material for reporting purposes and report results and recommend the SOA action to the Director, DISA.

f. Maintain records for each SAT meeting in accordance with guidance in DoD Instruction 5015.02, “DoD Records Management Program,” February 24, 2015, Change 1, August 17, 2017.



## GLOSSARY

### G.1. ACRONYMS.

ACRONYM	MEANING
AU	Assessable Unit
AUM	Assessable Unit Manager
CFO	Chief Financial Officer
CIO	Chief Information Officer
FMFIA	Federal Managers' Financial Integrity Act
FMS	Financial Management Systems
IC	Internal Controls
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
IG	Inspector General
OMB	Office of Management and Budget
OUSDC(C)	Office of the under Secretary of Defense Comptroller
RMIC	Risk Management and Internal Control
SAT	Senior Assessment Team
SOA	Statement of Assurance

### G.2. DEFINITIONS. These terms and their definitions are for the purpose of this issuance.

**Agency RMIC Coordinator.** The primary point of contact for the Agency.

**AU.** An organizational or functional subdivision of DISA required to develop, implement, test, and report on ICs in accordance with this issuance. The AU Administrator provides direction and guidance within their respective AU. Due to the inherently governmental nature of this function, the AU Administrator must be a Government employee (civilian or military).

**AUM.** The head or principal deputy assigned direct responsibility for ensuring the RMIC program is in place and operating effectively within the AU.

**Control Deficiency.** Exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect errors or misstatements on a timely basis.

**Financial Management Systems (FMS).** A unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel, process (manual and automated), procedures, controls, and data necessary to perform financial management functions, manage financial operations of the Agency, and report on the Agency's financial status to central agencies, Congress, and the public.

**Internal Controls.** The organizations, policies, and procedures that help program and financial managers achieve results and safeguard the integrity of their programs by reducing the risk of adverse activities.

**Internal Control Assessment.** A documented evaluation of the effectiveness and adequacy of the controls put in place to meet the mission objectives.

**ICOR-FR.** Relevant to financial reporting functions.

**ICOR-FS.** Relevant to integrated financial management systems conformance with Federal requirements.

**ICOR-O.** Pertains to the overall program, operational, and administrative controls relevant to all mission essential functions, except financial reporting and financial systems.

**Letter of Assurance.** A DISA internal document, signed by each DISA organization's Senior Executive or Senior Manager, providing an assessment and assertion of the organization's internal controls.

**Material Weakness.** A control deficiency that should be communicated to the next higher level because it represents significant weaknesses in the design or operation of internal controls that could impact the organization's ability to meet RMIC objectives. The determination to categorize a weakness as material results from management's judgment about the relative impact of the weakness.

**Modified SOA.** One of the three explicit levels of assurance that a FMFIA ICOR-O, ICOR-FR, and ICOR-FS SOA must take. A modified SOA provides reasonable assurance that ICs are effective except for one or more material weakness(es) of the FMS is not fully compliant with Federal requirements reported. The SOA must cite the material weaknesses in internal management controls that preclude a modified statement.

**No Assurance SOA.** One of the three explicit levels of assurance that a FMFIA ICOR-O, ICOR-FR, and ICOR-FS SOA must take. No assurance provides not reasonable assurance that ICs are effective because no assessments were conducted, the noted material weakness(es) are pervasive across many key operations, or the FMS is substantially noncompliant with Federal requirements. The reporting entity will provide an extensive rationale for this position.

**Reasonable Assurance.** An informed judgment by management based on available information that the ICs in place are effective and operating as intended.

**Risk.** The possibility an event will occur and adversely affect the achievement of the RMIC objectives.

**Significant Deficiency.** A deficiency in the design or operation of ICs that could impact the organization's ability to achieve the objective of the control.

**SOA.** An annual statement, in memorandum format, that provides the AUMs an explicit level of assurance on whether ICs are effective. The SOA is based on self-assessments conducted for mission-essential functions relative to risk and identifies any material weaknesses found during the assessments. The SOA is submitted by the AUM to the next higher level of command unless otherwise specified. The DISA annual SOA is submitted to the Secretary of Defense.

**Unmodified SOA.** One of the three explicit levels of assurance that a FMFIA ICOR-O, ICOR-FR, and ICOR-FS SOA must take. An unmodified SOA provides reasonable assurance that ICs are effective with no material weaknesses reported or that the FMS is in conformance with Federal requirements. Each unmodified statement must provide a firm basis and evidence for that position in the SOA.

## REFERENCES

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

DoD Directive 5105.19, “Defense Information Systems Agency,” February 15, 2022

DoD Instruction 5010.40, “DoD Enterprise Risk Management, and Risk Management and Internal Control Program,” December 11, 2024

DoD Instruction 5015.02, “DoD Records Management Program,” February 24, 2015, Change 1, August 17, 2017

Government Accountability Office Green Book, Standards for Internal Control in the Federal Government, September 10, 2014

OMB Circular A-123, “Management’s Responsibility for Enterprise Risk Management and Internal Control,” and Appendices A, B, C, and D