



# UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES

OFFICE OF THE PRESIDENT  
4301 JONES BRIDGE ROAD  
BETHESDA, MARYLAND 20814-4799  
www.usuhs.edu



July 19, 2022

## SUBJECT: Risk Management Internal Control Program

### Instruction 7004

(OAC)

#### ABSTRACT

This Instruction implements Department of Defense (DoD) requirements for the Risk Management and Internal Control (RMIC) Program under the Federal Managers' Financial Integrity Act (FMFIA) (*Reference (a)*) and as an Executive Agency, the Office of Management and Budget (OMB) Circular A-123 (*Reference (b)*), as well as the Government Accountability Office (GAO) Green Book (*Reference (c)*). To comply, each agency must establish a program of risk management and internal controls to ensure that programs and administrative functions are efficiently and effectively carried out in accordance with applicable laws and management policies, to provide reasonable assurances each year that resources are adequately safeguarded, and provide reliability of financial reporting. The FMFIA, OMB A-123 (*Reference (b)*), and GAO Green Book (*Reference (c)*), include an annual reporting requirement, the Statement of Assurance (SOA), which requires USU to report if it has met the above objectives and/or report on material weaknesses (MWs) and/or significant deficiencies over Financial Reporting, Financial Systems, and Operations.

**A. Reissuance and Purpose.** This Instruction reissues Uniformed Services University of the Health Sciences (USU) Instruction 7004 (*Reference (d)*), and will establish and manage the USU RMIC Program. USU RMIC identifies and manages risks, processes, and controls that may affect the University's ability to achieve its mission, strategic goals, and objectives. Incorporate guidance in DoD Directive 5010.40b. (*Reference (e)*), Title 31 USC, Section 3512c (*Reference (a)*), (also known as the Federal Managers' Financial Integrity Act (FMFIA) of 1982), Office of OMB Circular A-123d (*Reference (c)*), OMB Year-End Internal Control Report, OMB Guidelines for the Evaluation and Improvement of, and Reporting on, Internal Control Systems in the Federal Government; and GAO Standards for Internal Control in the Federal Government (*Reference (c)*) and will establish responsibilities for the USU RMIC Program and for department's and other activity's SOA input.

#### **B. Background**

1. The Office of Accreditation and Organizational Assessment (OAC) is responsible for the implementation of the FMFIA, OMB A-123 (*Reference (b)*), the GAO Green Book (*Reference (c)*), at USU. OAC responsibilities for the overall program of RMIC include performing various management evaluations, establishing internal control systems, coordinating with Office of the Under Secretary of Defense Personnel & Readiness (USD) P&R RMIC and Fraud Group initiatives, and draft the annual SOA regarding adequacy of internal controls in their individual departments/activities.

In addition, OAC is working towards establishing an Enterprise Risk Management governance structure to implement the latest OMB A-123 (*Reference (b)*) instructions. USU departments, schools, programs and centers heads' responsibilities include participating in the annual risk assessment, assuring efficiency and effectiveness of programs and administrative functions under their control following laws and management policies, processing transactions correctly and timely to further the reliability of the financial reporting, and participating in various reviews during the year. OAC coordinates with USU Assessable Unit Manager's (AUMs) to ensure the University is following the GAO Green Book (*Reference (c)*), and adheres to its five components: control environment, risk assessment, control activities, information and communication, and monitoring. AUMs complete annual surveys that assist in determining the effectiveness of internal controls.

**C. References.** *See Enclosure 1.*

**D. Applicability.** This Instruction applies to all USU components.

**E. Definitions.** *See Enclosure 2.*

**F. Policy.** It is USU policy that:

1. USU shall implement a RMIC Program that will provide reasonable assurance that:
  - a. Assets are safeguarded against waste, loss, unauthorized use, and misappropriation.
  - b. Obligations and costs comply with applicable laws.
  - c. Revenues and expenditures applicable to USU operations are recorded correctly to ensure the preparation of reliable financial and statistical reports, and to maintain accountability over the assets.
  - d. Programs and administrative functions are efficiently and effectively carried out in accordance with applicable laws and management policies. The cost of internal controls should not exceed the expected benefits.
2. The USU RMIC shall:
  - a. Meet the "GAO Standards for Internal Control in the Federal Government" (*Reference (c)*) (*see Enclosure 3*), and comply with the policies and documentation requirements prescribed in this Instruction and applicable OMB documents for guidance.
  - b. Be designed, documented, and operated to provide reasonable assurance that specific GAO Green Book (*Reference (c)*) objectives enumerated in Title 31, USC, Chapter 35, Section 3512c (*Reference (a)*) are met.

c. Provide for the assignment of overall responsibility for program design, direction, and implementation to a designated senior management official who is accountable to the President, USU.

d. Involve management at all levels and assign to the manager of each assessable unit responsibility and accountability for internal controls.

e. Address all program and administrative activities involving management of funds, property, and other assets for which managers are responsible, to include non-appropriated fund activities.

f. Implement methods of evaluation such as computer security reviews, financial system reviews, audits, inspections, checklists, investigations, and internal review studies.

3. Each USU Component shall annually submit input for the SOA to the President, based on an evaluation as to whether or not the internal controls meet the program standards, goals, and objectives. These statements will support the annual SOA submitted by the President, USU, through the Director, Defense Health Agency (DHA), to the (USD) P&R.

4. The Defense Finance and Accounting Service (DFAS) shall review the USU accounting system as part of the process for indicating whether the accounting system is in compliance with accounting principles, standards, and related requirements, as established by the GAO.

5. The DHA shall review the USU internal control deliverables to DoD USD (Comptroller), as for quality control purposes. The DHA will also receive and compile the USU responses to internal control inquiries from the external auditors for the annual DHA audit.

6. The DoD USD (Comptroller) shall provide guidance and prescribe required tasks and deliverables related to internal control. Present deliverables include:

- 1) SOA,
- 2) Entity Level Control Matrix,
- 3) Payment Integrity Controls Matrix Template,
- 4) Digital Accountability and Transparency Act (Data)
- 5) Material Weaknesses and Significant Deficiencies Template,
- 6) Risk Assessment Template,
- 7) Testing Focus Area Verification and Validation Template,
- 8) Summary of Management's Approach to Internal Control Evaluation Template,



- 9) Fraud Controls Matrix Template,
- 10) Recovery Audit Template- Commercial Pay,
- 11) Anti-Deficiency Act (ADA) Annual Evaluation Memorandum,
- 12) End to End Process Control Narrative Key Controls Memo,
- 13) Financial Improvement and Audit readiness (FIAR) Governance Board Meeting,
- 14) Agency Financial Report.

**G. Responsibilities.**

1. The President, USU shall:
  - a. Ensure the establishment and the on-going operation of the USU RMIC Program.
  - b. Submit the USU Annual SOA to USD with an evaluation copy to DHA, by complying with timeline of RMIC Events set by the USD (Comptroller) on an annual basis.
  - c. Assign adequate resources to ensure that the provisions of this Instruction are fully implemented.
  - d. Set the tone at the top by written and verbal communication.
2. The Assistant Vice President, Office of Accreditation and Organizational Assessment (OAC) shall:
  - a. Serve as the USU official under OMB Circular A-123 (*Reference (b)*) for policy guidance, direction and coordination with DoD Components and other Federal Agencies on RMIC Program matters.
  - b. Identify and resolve material weaknesses across USU related to Entity Level Controls (ELCs). ELCs represent the overriding management controls that create an environment of management oversight for the financial and non-financial activities.
  - c. Establish the RMIC Program and oversee its implementation and operation throughout the USU.
  - d. Issue applicable guidance to USU component heads by providing annual training on responsibilities and obligations using the USU RMIC Guide, and provide technical assistance to USU components on RMIC matters, including reporting.

e. Monitor any audit or inspection including those performed by the Inspector General (IG), DoD, GAO (*Reference (c)*) or the Defense Logistics Agency (DLA), which discloses a potential weakness in USU RMIC follow-up on the status of agreed-on corrective actions.

f. Monitor implementation of the program and establish follow-up systems to ensure acceptable performance and prompt correction of all material and other weaknesses.

g. Based on risk assessments, periodically perform RMIC evaluations of USU components and functions, including testing.

h. Consolidate and review documentation for submission to USD (P&R) requests and assert that USU controls testing has taken into account the DoD-wide process control narratives (PCNS) and that key supporting documentation, testing results, identification and explanation of control deviations and/or Corrective Action Plan (CAP) have been document.

i. Prepare for the President USU, the SOA, based on the statements of USU department/activity heads, for submission to the USD (P&R) through the Director, DHA, as required by Title 31, USC, Section 3512c (*Reference (a)*) and OMB Memorandum (*References (b)*).

3. The Manager of each Assessable Unit (USU Department and Activity Heads (*see Enclosure 4*), shall:

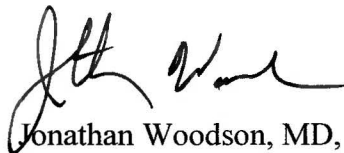
a. Provide the President USU, through the Assistant Vice President, Office of OAC, input for the SOA assessment (*see Enclosure 4*) for their Assessable Unit.

b. Be responsible for implementing the department or activity's RMIC plan, following the procedures as outlined in *see Enclosure 5*.

c. Emphasize prevention and correction of waste, fraud, and mismanagement in all RMIC plans and guidelines.

d. Participate with OAC when conducting an evaluation of their unit and/or with specific internal control testing.

e. Ensure that accountability for the success or failure of RMIC practices is reflected in performance evaluations of civilian and military managers having significant RMIC responsibilities.



Jonathan Woodson, MD, MSS, FACS  
President

Enclosures:

1. References
2. Definitions
3. GAO Standard for Internal Control in the Federal Government
4. Sample Statement of Assurance
5. Management Control (RMIC) Program: Steps for Manager

**REFERENCES**

- (a) Title 31 USC, Section 3512 “Federal Manager’s Financial Integrity Act of 1982” (FMFIA) dated January 7, 2011.
- (b) Office of Management and Budget (OMB) Circular No. A-123“.
- (c) Government Accountability Office (GAO) “Standards for Internal Control in the Federal Government,” (Green Book), September 2014.
- (d) USUI 7004 Managers' Internal Control Program, “dated May 23, 2007 (hereby canceled).
- (e) Department of Defense (DoD) Directive 5010.40, “Managers Internal Control (MIC) Program Procedures,” current edition.
- (f) OMB, “Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government,” 2014 Edition.
- (g) Federal Financial Management Improvement Act of 1996 (FFMIA).
- (h) “Responsibility for Internal Control,” as amended.
- (i) OMB Circular A-134 – Financial Accounting Principles and Standards, as amended.
- (j) OMB Circular A-11, Preparation, Submission, and Execution of the Budget (revised), as amended.
- (k) Government Performance and Results Act (GPRA) Act of 2010.
- (l) Federal Funding Accountability and Transparency Act (FFATA) of 2006, amended by the Government Funding Transparency Act of 2008 (Public Law 110-252).
- (m) Federal Information Security Modernization Act (FISMA) of 2014.
- (n) Digital Accountability and Transparency Act (DATA Act) of 2014, as amended.
- (o) Chief Financial Officers Act of 1990 (CFO Act), as amended.
- (p) DoD 7000.14-R, Volume 6A Chapter 2, Section 020202.1, “DoD Financial Management Regulation (FMRs),” current edition.
- (q) DoD Statement of Assurance Execution Handbook, as amended.

- (r) DoD Internal Control Over Financial Reporting Guide, as amended. DoD Office of the USOD (Comptroller)/Chief Financial Officer, “Financial Improvement and Audit Readiness (FIAR) Guidance”.
- (s) The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), March 27, 2020.
- (t) Memorandum for William M. Roberts, Acting President through Chief of Staff, USU, “Major Expansion of DHP Management Internal Control Program,” dated February 2019.
- (u) “Uniformed Services University of the Health Sciences Management Control Guide,” dated June 2006.



## DEFINITIONS

1. Assessable Unit. Any material organizational, functional, programmatic or other applicable subdivision of an organization that allows for adequate internal control analysis. An assessable unit's functions include the documentation, identification, and insertion of controls associated with a specific sub-function in order to mitigate identified risk. The assessable unit is required to have an appointed and adequately trained assessable unit manager. For USU that includes schools, departments, programs, and centers.
2. RMIC. The plan of organization, methods and procedures adopted by management to provide reasonable assurance that the objectives of FMFIA are met.
3. RMIC Checklist. A document similar to the Risk Assessment designed for evaluating an assessable unit's operations, specifically at USU (also referred to as the (SOA) Annual Self-Assessment Survey).
4. RMIC Evaluation. A detailed evaluation of an assessable unit to determine whether adequate control techniques exist and are implemented to achieve cost effective compliance with FMFIA using the methodology specified in the OMB Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government. All reviews should produce written materials documenting what was done and what was found.
5. RMIC Guide. The material developed for RMIC training at USU.
6. RMIC Guidelines. (*Reference (i)*) presents a suggested approach that may be adapted to meet component needs. Any such adaptation should remain in compliance with OMB Circular No. A-123d (*Reference (b)*) and include testing of controls and documentation.
7. RMIC Program. The formal effort of an organization to ensure that RMIC systems are working effectively through assignment of responsibilities at the policy level, issuance and implementation of guidance, conduct of risk assessments and RMIC reviews, provisions for quality control, and reporting to senior management.
8. RMIC Standards. The GAO Standards for Internal Control in the Federal Government issued by the USD (Comptroller) General for use in establishing and maintaining RMIC systems.
9. RMIC System. The sum of a departments or activity's methods and measures used to achieve the FMFIA and RMIC objectives. It is not a separate system, but an integral part of the systems used to operate programs and functions.
10. Managers with Significant RMIC Responsibilities. This includes top level managers, down through operational managers of all programs and activities in which funds, property, and other assets must be safeguarded against fraud, waste, abuse and mismanagement, and in which resources must be managed efficiently and effectively.

11. Material Weakness. Specific instances of noncompliance with the FMFIA (*Reference (a)*) of sufficient importance to be reported to the next higher level of management. Such weakness significantly impairs the fulfillment of a Component's mission; deprives the public of needed services; violates statutory or regulatory requirements of funds, property, or other assets; or results in a conflict of interest. The final determination to categorize an internal control weakness as material rests with management's judgment about the relative impact of the weakness. For example, scoring each of the following considerations as "significant" or "insignificant" might help a manager in determining whether the absence of, or noncompliance with, a control is a material weakness.

- a. Actual or potential loss of resources.
- b. Sensitive nature of the resource(s) involved.
- c. Magnitude of funds, property, or other resources involved.
- d. Frequency of actual and/or potential loss.
- e. Current or probable media interest (adverse legislative action).
- f. Current or probable Congressional interest (adverse publicity).
- g. Unreliable information causing unsound management decisions.
- h. Diminished credibility or reputation of management.
- i. Impaired fulfillment of essential mission.
- j. Violation of statutory or regulatory requirements.
- k. Impact on information security.
- l. Deprived the public of needed Government services.

## GAO STANDARDS FOR INTERNAL CONTROL IN THE FEDERAL GOVERNMENT

1. **Fundamental Concepts of Internal Control.** Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. It comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives (i.e. operational, reporting and compliance) of the entity. It serves as the first line of defense in safeguarding assets. In short, internal control helps managers achieve desired results through effective stewardship of public resources.

2. **Categories of Objectives:**

- a. Management group's objectives into one or more of the three categories of objectives:
  - 1) Operations - Effectiveness and efficiency of operations.
  - 2) Reporting - Reliability of reporting for internal and external use.
  - 3) Compliance - Compliance with applicable laws and regulations.

3. **The Five Components and 17 Principles of Internal Control**

a. **Control Environment.**

- 1) Control activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out. In other words, control activities are actions taken to minimize risk.
- 2) Principles:
  - a) The oversight body and management should demonstrate a commitment to integrity and ethical values.
  - b) The oversight body should oversee the entity's internal control system.
  - c) Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
  - d) Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
  - e) Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

b. Risk Assessment. A risk assessment is the combined effort of: identifying and analyzing potential events that may negatively impact business objectives, assets, and/or the environment; and making judgments on the tolerability of the risk on the basis of a risk analysis.

1) Principles:

- a) Management should define objectives clearly to enable the identification of risks and define risk tolerances.
- b) Management should identify, analyze, and respond to risks related to achieving the defined objectives.
- c) Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
- d) Management should identify, analyze, and respond to significant changes that could impact the internal control system.

c. Control Activities.

1) Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

2) Principles:

- a) Management should design control activities to achieve objectives and respond to risks.
- b) Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
- c) Management should implement control activities through policies.

d. Information and Communication. Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information.

1) Principles:

- a) Management should use quality information to achieve the entity's objectives.
- b) Management should internally communicate the necessary quality information to achieve the entity's objectives.



c) Management should externally communicate the necessary quality information to achieve the entity's objectives.

e. Monitoring.

1) Finally, ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning.

2) Principles:

a) Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

b) Management should remediate identified internal control deficiencies on a timely basis.

-Sample-

May, 2022

MEMORANDUM FOR PRESIDENT, UNIFORMED SERVICES UNIVERSITY OF THE  
HEALTH SCIENCES

THROUGH: (MANAGEMENT CHAIN)

SUBJECT: Input for 2022 Annual Statement of Assurance under the Federal Managers'  
Financial Integrity Act: *(Name of Assessable Unit)*

The *(Name of Assessable Unit)* provides the information in this memorandum in support of your forthcoming Annual Statement to the Assistant Secretary of Defense (Health Affairs) and the Under Secretary of Defense (Comptroller).

As *(Title of Assessable Unit Manager/Program Manager)*, of the *(Name of Assessable Unit)*:

- a. I am aware that this position has significant management control responsibilities, the execution of which will be measured in my annual performance appraisal.
- b. I am aware of the importance of management controls. I have taken the necessary measures to assure that program and administrative controls have been implemented and are observed within the segment of the University that is within my management responsibility.
- c. I provide reasonable assurance that in the *(Name of Assessable Unit)*, the objectives of management control are being met: 1) obligations and costs are in compliance with applicable law; 2) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and 3) revenues and expenditures are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.
- d. The assets, program responsibilities and mission objectives under my responsibility have been reasonably insulated against fraud, waste, and mismanagement and have not been materially impeded by deficiencies in management controls. I base this assurance on [Note to preparer: Examples include management studies, observations, and initiatives; management knowledge; internal management review/checklists; internal/external reviews; or procedural reviews.]

*I am providing a detailed description of how the Management Control Program has been applied or reviewed for compliance during. October 1, 2021 – June 30, 2022 [Note to preparer: Provide narrative.]*

*I am providing a detailed description of the problems encountered in implementing the Management Control Program, and other considerations (e.g., resource constraints, technological concerns, and operational or mission considerations).*

*Describe assessments that have been conducted by including examples of deficiencies found that do not warrant reporting as a material weakness and the actions taken or planned to resolve these deficiencies during October 1, 2021 – June 30, 2022. [Note to preparer: Provide narrative.]*

- a. Use the following format:

Description of Issue:

Accomplishments:

*Provide a detailed description of restrictions or constraints that limit your ability to correct Management Control Program weaknesses. [Note to preparer: Provide narrative.]*

*As (Title of Assessable Unit Manager), I continue to support the objectives of the Federal Managers' Financial Integrity Act.*

(Name of Assessable Unit Manager)  
(Name of Assessable Unit)

Enclosures:  
As stated

A "**material weakness**" is a systemic problem with significant deficiency, or combination of significant deficiencies that infringe on the accomplishment of the USU mission such as failure of internal control components or a failure caused by error or fraud.

## **RISK MANAGEMENT INTERNAL CONTROL (RMIC) PROGRAM**

### **STEPS FOR MANAGERS**

1. **Setting up an RMIC system.** The purpose of setting up an RMIC system is to effectively and efficiently manage your department's operations, and to protect against fraud, waste, and abuse.

- a. Establish a written departmental mission and functions statement.
- b. Identify short-and long-term goals to support your department's mission.
- c. Determine your department's objectives and techniques to accomplish goals.
- d. Develop written Standard Operating Procedures (SOPs) or manuals for your department's functions and operations, to include departmental policies.

2. **Assessing your RMIC System.** The following should be done annually with the submission of the Annual SOA. However, it is recommended that a semi-annual review be conducted as well. Assistance is available from the Office of Accreditation and Organizational Assessment (OAC).

a. Review and evaluate your department's operations and functions by using either the Risk Assessment or RMIC Checklist, or some other format discussed with the Vice President, Office of Accreditation and Organizational Assessment (OAC).

b. Examine the results of your review to determine if any portion(s) of the department's operations or functions are deficient and/or could use improvement. Also, consider problem areas you feel need management's attention.

3. **Correcting a Problem Area.**

a. Identify those areas in need of revision or improvement and establish a corrective action plan to implement the changes needed.

- 1) Submit this plan to your chain of command with your SOA.
- 2) Review your plan periodically and record completion of steps.
- 3) Report the progress of your plan to your chain of command and the Office of Accreditation and Organizational Assessment (OAC).



**4. Reporting a Continuing Problem Area.**

- a. Discuss with your chain of command if the problem area persists, and improvements are not being accomplished.
- b. If you feel you are not getting management's support to correct the problem, contact the Office of Accreditation and Organizational Assessment (OAC) at 301-295-3681.
- c. The Office of Accreditation and Organizational Assessment (OAC) will conduct an internal review based on the above information and discussions with all parties involved.