DCMA Manual 4301-11, Volume 1

Management Controls: Managers' Internal Control Program

Office of Primary Responsibility	**Stewardship Capability**
Effective:	June 24, 2019
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-INST 4301, "Stewardship," July 18, 2018
Incorporates and Cancels:	DCMA-INST 710, "Managers' Internal Control Program," April 21, 2014
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/ST/SitePages/4301-11v1r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This Manual is composed of several volumes, each containing its own purpose. In accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," this Manual implements policies and procedures as defined in DCMA Instruction 4301, "Stewardship," and incorporates or assigns responsibility for:

- Executing the Managers' Internal Control Program.
- Establishing a formal mechanism for reporting the Agency annual Statement of Assurance to the Office of the Under Secretary of Defense (Comptroller).
- Complying with federal law and other higher-level guidance, primarily with Office of Management and Budget Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control."
- Utilizing the DCMA 360 site for authoritative documentation of program elements.
- Entity-level controls for operational and financial missions.
- Design of the Agency's internal control strategy to include Enterprise Risk Management.
- Adding risk profiles to the annual Statement of Assurance reporting.
- Establishing the roles and responsibilities for the Senior Assessment Team, Assessable Units, and Subs-Assessable Units.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. This issuance will establish and maintain a single authoritative program that DCMA components will use to develop, coordinate, assess, review, and publish reports pertaining to the Managers' Internal Control Program. It further establishes a Managers' Internal Control Program, pursuant to DoD Instruction (DoDI) 5010.40, "Managers' Internal Control Program Procedures;" the Government Accountability Office (GAO), "Standards for Internal Control in the Federal Government," also known and referred to in this issuance as the "Green Book;" and Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control." It is DCMA policy to:

(1) Assess inherent risks in mission-essential processes.

(2) Document and design internal controls.

(3) Test the design and operating effectiveness of existing internal controls.

(4) Promptly prepare, execute, monitor and report corrective action plans.

(5) Monitor and report the status of corrective action plans until resolution of identified deficiencies.

(6) Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DCMA DIRECTOR. The Director retains final authority over this Manual by demonstrating leadership, receiving guidance, and providing decisions as required. The DCMA Director will:

a. Lead the Agency toward achieving its mission, articulate the Agency's vision, set program and budget priorities, approve internal policies and assess Agency performance.

b. Establish a Managers' Internal Control Program to assess inherent risks in mission-essential processes, document and design internal controls, and test the design and operating effectiveness of existing internal controls in accordance with DoDI 5010.40 and OMB Circular No. A-123.

c. Submit the annual SoA to the OUSD(C) as specified in annual guidance.

d. Appoint, in writing, a primary Managers' Internal Control Program Coordinator and Senior Assessment Team Chairperson to oversee the development, documentation, and management of internal controls throughout all aspects of DCMA's mission and reportable activities.

e. Ensure critical elements relative to the Managers' Internal Control Program are developed and included in performance plans for Assessable Unit Managers and the Managers' Internal Control Program Coordinator.

f. Designate, in writing, a Managers' Internal Control Program Coordinator within 90 days of a vacated position.

g. Designate, as necessary, the authoritative Assessable Unit for Managers' Internal Control Program operations.

2.2. EXECUTIVE DIRECTOR, FINANCIAL AND BUSINESS OPERATIONS. The Executive Director, Financial and Business Operations (FB) will:

a. Delegate overall responsibility for management of the Managers' Internal Control Program to the Planning, Programming, and Analysis Division.

b. Ensure Managers' Internal Control Program actions, as required by OUSD(C), are being executed in a timely manner to include SoA submissions and quarterly deficiency corrective action plan (CAP) reporting.

2.3. DIRECTOR, BUSINESS PLANNING, PROGRAMS AND ANALYSIS DIVISION. The Director, Business Planning, Programs and Analysis Division will:

a. Manage the Agency Managers' Internal Control Program effort to include annual SoA and deficiency CAP reporting.

b. Manage internal control operational risk management as defined in OMB Circular No. A-123.

c. Manage Agency internal control deficiency CAP reporting as defined in DoDI 5010.40.

d. Conduct business analysis and support activities for agency-wide financial and resource management activities.

2.4. MANAGERS' INTERNAL CONTROL PROGRAM COORDINATOR. The Managers' Internal Control Program (MICP) Coordinator will:

a. Implement an effective internal control program within the Agency in accordance with guidelines established in DoDI 5010.40.

b. Coordinate with Assessable Unit Managers to ensure proper documentation of end-to-end processes that support operational, administrative, system, and financial events to assess controls and improve efficiency within the Agency. At a minimum, documentation will include processes assigned Internal Control Plans (e.g., process risk assessments, flows, Key Controls, narratives), agency assessments, Certification Statements, and other administrative actions as necessary.

c. Monitor and report deficiency CAP progress to the Senior Assessment Team and report updates to OUSD(C) as required.

d. Ensure the DCMA Director, Senior Assessment Team, and Assessable Unit Managers identify internal control objectives based on risk assessments to effectively support the Agency.

e. When requested, assist in testing and validating conclusions provided by subject matter experts on the effectiveness of internal controls.

f. Assist the Agency Director, Senior Assessment Team, and Assessable Unit Managers in identifying and classifying internal control deficiencies based on internal and external evaluations, assessments, audits, and inspections.

g. Prepare the annual SoA in accordance with OUSD(C) guidance, based upon material weaknesses identified during current and prior fiscal years.

h. Coordinate, with assessable units, updates to DCMA Entity-Level Controls for areas specified by OUSD(C).

i. Maintain a library or access to key MICP documentation and annual deliverables (e.g., process lists, flows and narratives; risk matrices; annual Test Plans; deficiency CAPs; Assessable Unit assessments and certifications; SoA; and key personnel) for a minimum of five years and one month.

j. Develop, implement, recommend, and/or conduct annual Agency MICP training.

k. Coordinate, with assessable units, to populate Agency financial and operational risk profiles and submit to OUSD(C) as required in the annual SoA.

l. Formally task Assessable Units for internal control data.

2.5. SENIOR ASSESSMENT TEAM CHAIRPERSON. The Senior Assessment Team Chairperson will:

a. Establish a Charter detailing membership, objectives, meeting frequency, and other rules and governance.

b. Convene meetings, as necessary, to advise Agency senior leaders on internal control matters, including:

(1) Assessing and monitoring MICP efforts.

(2) Ensuring subject matter experts and field operations assess risks to strategic outputs that may adversely affect the Agency mission or financial performance.

(3) Identifying internal control issues that merit reporting in the annual SoA.

(4) Identify low-value, duplicative, or obsolete activities that can be ended.

(5) Initiating prompt and effective actions to resolve issues with internal controls through Agency Capability Boards or functional subject matter experts.

2.6. ASSESSABLE UNIT MANAGER. The Assessable Unit Manager (AUM), or designated Subordinate AUM (Sub-AUM), is the Executive Director, Director, or Commander of the identified Assessable Unit. The AUM or Subordinate must be a government employee or uniformed service member due to the inherently governmental nature of the work. The AUM will:

a. Appoint Sub-Assessable Units and Sub-AUMs to manage control of processes.

(1) The Sub-AUM will perform the duties of the AUM for their respected organizational business unit code.

(2) The Sub-AUM may designate a Sub-Assessable Unit Administrator to coordinate organizational business unit internal control operations to ensure process efficiency.

b. Appoint an Assessable Unit Administrator to administer the Assessable Unit's MICP.

c. Provide and update the MICP Coordinator with a list of key personnel, designated Sub-Assessable Units, and processes supporting strategic delivery objectives on critical functions annually.

d. Develop, maintain, and monitor an Internal Control Plan for each process owned and assigned by the Agency's Authoritative Process List (APL). AUMs will utilize the Internal Control Plan to:

(1) Establish internal controls to address risks and monitor performance.

(2) Develop and execute annually, a Test Plan, to test the effectiveness of the internal controls.

(3) Identify and assess risks that may adversely affect the Assessable Unit's strategic delivery objectives or other critical mission areas using a Risk Assessment/Risk Register.

(4) Document Process Flows showing all logic gates necessary to start and stop a process.

(5) Document Process Narratives describing each process step and detailing control point process steps as required by the MICP Coordinator.

(6) As necessary, document and execute a process Test Result to ensure process compliance or risk mitigation strategy. Test Results shall include the results of the Test Plan and be conducted by agency Assessments. This can be delegated by the AUM to the designated process subject matter expert as defined by the Agency APL.

e. Identify and classify internal control deficiencies according to the reporting categories.

f. Develop, implement, track, and report deficiency CAP progress to the MICP Coordinator.

g. Provide an annual Assessable Unit Certification Statement with explicit level of assurance to the Agency Director via the MICP Coordinator to support the Agency SoA.

2.7. ASSESSABLE UNIT ADMINISTRATOR. The Assessable Unit Administrator (AUA) or designated Subordinate AUA (Sub-AUA) will:

a. Assist the AUM/Sub-AUM in the implementation of the MICP.

b. Prepare the annual Assessable Unit Certification to the Agency SoA based on findings of internal control effectiveness over Assessable Units/Sub-Assessable Unit operations, and financial and compliance requirements for submission to the MICP Coordinator.

c. Monitor and consolidate quarterly reports of deficiency CAP Milestones to the MICP Coordinator.

d. Identify and coordinate MICP training for Assessable Units.

e. Represent the Agency and Assessable Units by actively participating in monthly Oversight Panel for Managers' Internal Controls meetings.

f. Upload all Assessable Unit MICP documents (e.g., narratives, risk matrices, completed assessments, certifications, plans, etc.) to the DCMA MICP 360 site for validation by the MICP team.

2.8. SUBJECT MATTER EXPERT. A DCMA employee that knows and understands the process, how the process works, and who does what and when during the process is considered a subject matter expert (SME). The SME will complete a process Internal Control Plan for each process owned.

2.9. DCMA EMPLOYEES. DCMA employees who identify control deficiencies will elevate them to the AUM to reasonably assure that programs achieve their intended results; the risk of loss of life and/or loss of public trust is mitigated; the use of resources is consistent with the Agency's mission; programs and resources are protected from fraud, waste, and abuse; laws and regulations are followed; and that reliable and timely information is obtained, maintained, reported, and used for decision making.

SECTION 3: PROGRAM OBJECTIVES AND FUNCTIONS

3.1. INTERNAL CONTROLS. Internal controls may consist of policies, procedures, and other mechanisms that minimize the risk of Assessable Units not achieving their goals and objectives. Each Assessable Unit will ensure, with cognizance of the appropriate AUM, an evaluation of internal control activities and associated processes has been accomplished, is maintained, and remains current.

a. AUMs evaluate internal controls for their assigned Assessable Units and determine which internal controls are to be tested based on consideration of:

(1) Frequency. Controls that occur less frequently but mitigate the same risks as other controls may be prioritized to increase efficiency due to a smaller population of samples.

(2) Materiality. The magnitude of an omission or misstatement of an item in a financial or operations report that, in light of surrounding circumstances, makes it probable that the judgement of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item.

(3) Risk Level. The likelihood of occurrence within a monitoring period (frequency), which would interfere with successfully achieving a specified objective and/or facilitate the occurrence of a disruptive event.

b. Internal controls are not unique to the DoD or financial realm. Resources are available to assist personnel in evaluating and improving their internal control programs. Key source guidance for internal control documents are:

(1) DoDI 5010.40 incorporates internal controls over operations due to the Federal Managers Financial Integrity Act of 1982, and directly encompasses DoD Financial Statement Audit Guide methodology, to include internal controls over financial reporting and internal control over financial systems. DoD directs agencies to establish a MICP to evaluate and report on the effectiveness of internal controls throughout the Agency and make corrections when necessary. Assessable Units must use the MICP methodology, modified as required, along with organizational assessments, evaluations, and other contributing information (e.g., performance metrics, internal controls, external audits and inspections, etc.) as forms of monitoring internal controls.

(2) OMB Circular No. A-123 emphasizes management's responsibility to implement, integrate, and coordinate risk management. Strong and effective internal controls is an integral part of managing the Agency's business activities and necessary to strengthen documentation, monitoring, and reporting requirements.

(a) Enterprise Risk Management (ERM) and internal controls are components of a governance framework. ERM provides an enterprise-wide, strategically aligned view of organizational challenges that improve insight on how to more effectively prioritize and manage risks to mission delivery. Through adequate risk management, agencies can concentrate their

efforts towards key points of failure and reduce or eliminate the potential for disruptive events. The internal control process is affected by an entity's oversight body, management, and other personnel. Internal controls provide reasonable assurance that the objectives of an entity will be achieved.

(b) Establishing Entity Level Controls is another primary step in operating an effective system of internal controls. Entity Level Controls are defined as controls that have a pervasive effect on an entity's internal control system and pertain to multiple components. Entity level controls also include controls related to the entity's use of service organizations, management override of internal controls, disruption/disaster response, and fraud.

(3) The GAO describes federal government and international methods and standards of internal controls. While potentially complex, all internal control systems must address five components: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communications, and (5) monitoring activities. The design, operation, and documentation of the Agency's MICP will provide reasonable assurance that these components are addressed.

(4) The annual OUSD(C) SoA guidance specifies format, content, submission dates, and coordination procedures for the Agency SoA. It changes annually and requires careful study when issued.

c. The internal control cycle consists of five phases with detailed activities and outputs that are required for each phase. The phases provide guidance to implement an effective internal control cycle that is assessed and monitored continuously throughout the year.

(1) Evaluation Phase. Includes a review of all documentation that pertains to the design, implementation, and operating effectiveness of an internal control system. During this phase, unresolved notice of findings and recommendations received from external auditors will be reviewed.

(2) Planning Phase. Includes determining which internal controls will be tested throughout the year and developing a timeline for testing for SoA reporting.

(3) Testing Phase. Executes internal control testing across Entity Level Controls, financial reporting, and system controls to assess the design and operating effectiveness of control activities within Assessable Units.

(4) Reporting Phase. Includes management review of the internal control testing results and deficiencies identified, the determination of the level of assurance that will be presented based upon the test results and deficiencies identified, determination of the overall status of Internal controls within the Assessable Units, and submission of the SoA.

(5) Corrective Action Phase. Encompasses development and implementation of deficiencies identified. Requirements to mitigate deficiencies in control activities or supporting documentation are defined and solutions are designed to strengthen and execute control

activities, processes and/or systems and policies. This phase is ongoing and may span the entire internal control cycle.

3.2. ASSESSABLE UNITS.

a. Organization. Assessable Units represent all DCMA components that report directly to the Agency Director. The AUM of each Assessable Unit establishes and assesses internal controls. A sample list of Assessable Units is provided in Table 1. Sample List of Assessable Units and the list of DCMA Assessable Units can be found on the MICP Resource Page.

Table 1. Sample List of Assessable Units

Assessable Unit	Code
Business Operations	BO
Contracts Directorate	CO
Human Capital	HC
Inspector General	IG

b. Assessable Unit Actions. The MICP Coordinator will task Assessable Units for annual MICP due outs via email and/or an Agency-level tasking memo. Annual due outs include:

(1) Sub-AUAs and AUAs. The AUM validates and maintains a current list of Assessable Units and Sub-Assessable Units, AUMs and Sub-AUMs, and AUAs and Sub-AUAs on the DCMA MICP 360 site.

(2) Process Inventory. The APL will serve as the MICP process inventory. Assessable Units will ensure that all processes and sub-processes are developed with appropriate risks, materiality, flows, and narratives cross-referenced to the APL. The APL requires consideration or key data for each process:

(a) Significant or unique processes are documented in an Internal Control Plan, which identifies an assigned Headquarters-level point of contact, and documents the process with a minimum requirement of a risk register, Process Narrative, flow, and key control activity.

(b) DCMA issuances, sub-processes, business practices, or other formal guidance (e.g., Defense Federal Acquisition Regulation Supplement (DFARS)) are cited and cross-referenced with the narrative.

(c) Each process is documented with a Test Plan in accordance with the DoD Financial Statement Audit Guide, and assessed for inherent risk and materiality using a MICP matrix. This will be accomplished when the process is first established or significantly changes.

(d) Capability Boards providing oversight of the process are identified, as well as the internal control reporting category, and any other list data as applicable.

(3) Internal Controls. All internal controls will consist of a process Risk register, Narrative, Process Flow, Test Plan, test results, and applicable deficiency CAPs.

(4) Critical Measures. The goal of MICP is to have a complete system of critical measures to successfully analyze and improve operational efficiency and compliance. Assessable Units will prioritize their process documentation to achieve an optimal balance of internal controls, critical process metrics, red flag indicators (documented by a yellow triangle on flows), and performance measures:

(a) SMEs will develop Process Narratives, Process Flows, and identify Key Controls to monitor all strategic or unique processes in accordance with DoDI 5010.40, OMB Circular No. A-123, and the DoD Financial Statement Audit Guide.

(b) Assessable Units will identify critical process metrics or other means of assessing process effectiveness and efficiency and the forum in which they will be monitored (e.g., performance reviews, capability boards, etc.).

(c) In a few exceptional cases, process success cannot be measured by red flags or discovered failures because the process itself does not directly control behavior or ability. Examples include Equal Employment Opportunity complaints, actual fraud reports, and individual training failures. For these processes, the Assessable Unit must establish a means to monitor materiality thresholds and reporting procedures.

(d) If risks and materiality are undefined, they will be considered "high risk" and "high material" until fully evaluated and Key Controls are established.

(5) Internal Control Test Plans. Each Assessable Unit will produce an annual Internal Control Test Plan. At minimum, the plan will include measures that:

(a) Discuss, assess, and test Process Flows and Key Controls.

(b) Ensure all documentation is up-to-date and accurate.

(c) Ensure all risks and controls are still valid.

(d) Ensure all references are up-to-date (including DoD and Manual references).

(e) Identify the strategic objectives the Assessable Unit supports.

(f) Verify Sub-Assessable Unit structure, process inventory, and risk analysis is current.

(g) Include internal control areas targeted for improvement, training and planned testing.

(h) Include internal/external assessments scheduled for the fiscal year.

(6) Deficiency CAPs. Deficiency CAP status' will be updated quarterly to the Senior Assessment Team via the MICP Coordinator.

(7) SoA. Assessable Units must review and consolidate their Sub-Assessable Unit Certification Statements into a single format to enable the MICP Coordinator to prepare the annual SoA Certification for submission to the Agency Director. At a minimum, the annual Certification Statement submission must include:

(a) For current fiscal year, an assertion of Unmodified, Modified, or Statement of No Assurance that Assessable Unit internal control systems are in place and function effectively.

1. Unmodified Assurance. No material weaknesses have been identified or reported. The SoA provides firm basis for justification or assertion in a cover memorandum.

2. Modified Assurance. One or more material weaknesses were reported. There are corrective actions to address all identified material weaknesses.

3. Statement of No Assurance. No assessments were conducted or noted material weaknesses are pervasive. The AUM must provide an extensive rationale for this position.

(b) Review of Internal Control Plan success and/or significant changes.

(c) Top level recap of assessments, audits, exams, inspections, and overall results.

(d) List of new and continuing material weaknesses and systemic deficiencies with all associated data and a developed deficiency CAP.

3.3. SENIOR ASSESSMENT TEAM. The Senior Assessment Team (SAT) will meet at minimum once annually. However, it is recommended the team meet quarterly to discuss progress on reported material weaknesses, significant deficiencies, and control deficiencies and to discuss potential new material weaknesses, significant deficiencies, control deficiencies, and risk management.

3.4. REPORTING PERIOD.

a. The DCMA SoA reporting period will follow the 1 October to 30 September fiscal year calendar structure.

b. Since preparation of the SoA occurs during the fourth quarter of the fiscal year, it is strongly advised not to assign milestone completions during this period. It is difficult to accurately report and update fourth quarter milestones once the preparation of the SoA begins. For this reason, it is advised to schedule milestone completions prior to the fourth quarter. If the completion date of a milestone must fall after August 1st of the current fiscal year, it is recommended to identify and assess the process in the first quarter of the next fiscal year. This will allow adequate time to confirm completion of the milestone and report to the AUM for approval and coordination with the MICP Coordinator.

3.5. OPERATIONAL REPORTING CATEGORIES. The Assessable Unit will designate each operational internal control deficiency into one of the reporting categories according to the description of the functional operation:

a. 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.

b. Communications. 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.

c. Contract Administration. 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 federal government.

d. Force 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.

e. 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. This includes computers, ancillary equipment, software, firmware and similar services and related resources whether performed by in-house or by contractor, intra-agency or intergovernmental agency resources or personnel.

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

g. Manufacturing, Maintenance, and Repair. Management of operation of in-house and contractor-operated facilities performing maintenance and repair or installation of modifications to materiel, equipment, and supplies. It also includes depot and arsenal-type facilities as well as intermediate and unit levels of military organizations.

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

i. Personnel and Organizational Management. Authorizations, recruitment, training, assignments, and the use, development, and management of military and civilian DoD personnel.

Also includes the operations of headquarters' organizations. Contract personnel are not covered by this category.

j. Procurement. Decisions to purchase items and services with certain actions to award and amend contracts (e.g., Acquisition Review Board approval, contractual provisions, type of contract, invitation to bid, independent government cost estimate, technical specifications, evaluation and selection process, pricing, and reporting).

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

l. Research, Development, Test, and Evaluation. The basic project definition, approval, and the 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 such as Procurement and Contract Administration.

m. Security. Plans, operations, systems, and management activities for safeguarding classified resources (not peripheral assets and support functions covered by other reporting categories). It also covers the DoD programs for protection of classified information.

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

o. Supply Operations. Supply operations at the wholesale (depot and inventory control point) level from the initial determination of material requirements through receipt, storage, issue reporting, and inventory control (excluding the procurement of materials and supplies). It also covers all supply operations at retail (customer) 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).

p. Support Services. All support service functions financed from appropriated funds not covered by the other reporting categories such as health care, veterinary care, and legal and public affairs services. Every non-appropriated fund activity is also covered by this category.

3.6. FINANCIAL REPORTING CATEGORIES. The Assessable Unit will designate each financial reporting internal control deficiency into one of the financial reporting categories according to the description of financial reporting:

a. Budget-to-Report. Business functions necessary to plan, formulate, create, execute, and report on the budget and business activities of the entity and updates to the general ledger. It also includes all activities associated with generating and managing the internal and external

financial reporting requirements of the entity, to include pre-closing and post-closing entries related to adjustments, reconciliations, consolidations, eliminations, etc.

b. Hire-to-Retire. Business functions necessary to plan for, hire, develop, assign, sustain, and separate personnel in the Agency.

c. Order-to-Cash. Business functions necessary to accept and process customer orders for services or inventory. This includes managing customers, accepting orders, prioritizing and fulfilling orders, distribution, managing receivables, and managing cash collections.

d. Procure-to-Pay. Business functions necessary to obtain goods and services. This includes requirements identification, sourcing, contract management, purchasing, payment management, and receipt of debt management.

e. Acquire-to-Retire. 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.

f. Plan-to-Stock. Business functions necessary to plan, procure, produce, inventory, and stock materials used both in operations and maintenance, as well as for sale.

3.7. ASSESSABLE UNIT ASSESSMENTS. Assessable Unit assessments are performed using the approved Managers' Internal Control Assessment (MICA) template. Annually, the AUM will determine what assessments will be performed by the Assessable Unit. The MICA template can be accessed through the DCMA MICP site.

3.8. ANNUAL CERTIFICATION STATEMENT.

a. Actions. Information regarding internal controls, to include control deficiencies and control-related accomplishments, is collected through two main venues, self-reporting and audits.

(1) The MICP Coordinator will compile and prepare the Agency's annual SoA for submission to the OUSD(C).

(2) AUMs review internal control certification statements from their Sub-Assessable Units and in turn submit certifications to the Agency Director via the MICP Coordinator. The self-reporting of control deficiencies enable the AUMs to demonstrate their control environments and activities, as well as indicate the findings of the control assessments.

(3) AUMs will use external audit reports (GAO, DoD Inspector General, etc.), internal audit reports (Inspections and Evaluation Team (IET), Internal Audit Team (IAT), etc.), performance reviews, input from Continuous Process Improvement activities, and Lean Six Sigma to help identify material control deficiencies throughout the year.

(4) AUMs will work closely with the IET and IAT to review audit reports on a quarterly basis and utilize a systemic method to determine materiality and potential inclusion in the annual SoA.

(5) AUMs will work to develop, document, and monitor corrective actions and milestones in accordance with DoDI 5010.40 and applicable guidance for both self-reported issues and those stemming from audit reports or other sources.

(6) The MICP Coordinator must reference any systemic weaknesses identified by the AUMs during the MICP Certification process and report material weaknesses in the Agency SoA.

b. Financial Reporting Assessment. The Agency will develop a financial improvement plan incorporating deficiency CAPs for identified internal control deficiencies, as required by the DoDI 5010.40 and the DoD Financial Statement Audit Guide. Summaries of the CAPs will be reported in accordance with the DoD Financial Statement Audit Guide and OUSD(C)/Chief Financial Officer guidelines.

c. Financial Systems Assessment. Assessable Units will use the DoD Financial Statement Audit Guide methodology to assess, evaluate, and report compliance of the Integrated Financial Management System (IFMS) with federal requirements in accordance with DoDI 5010.40; Section 3512 of Title 31, United States Code (U.S.C.), "Executive Agency Accounting and Other Financial Management Reports and Plans;" OMB Circular No. A-123; OMB Circular No. A-127, "Financial Management Systems;" DoD 7000.14-R, Volume 1, "General Financial Management Information, Systems and Requirements," and the DoD Financial Statement Audit Guide.

(1) Nonconformance with federal financial management system requirements constitutes a material weakness, which must be reported in the SoA and accompanied by a Root Cause Analysis and deficiency CAP summary for resolution.

(2) DCMA's designated role as Service Provider of the IFMS is to provide testing of material controls by an auditor as part of the Service Provider Agreement to enable the Agency to assess the reliability of the overall IFMS in accordance with OUSD(C) /Chief Financial Officer, DoD.

d. Statement Preparation. The submission of the MICP Certification Statement must include:

(1) Information (Info) Memo. Document addressed to the MICP Coordinator and signed by the AUM and provides the AUM's assessment as to whether there is a reasonable assurance that internal controls are in place and operating effectively. The AUM must certify to the number of internal control assessments that were scheduled for the reported fiscal year.

(2) Accomplishments. A brief summary of the most significant actions and accomplishments to strengthen internal controls that were taken by the AUM during the current fiscal year. The accomplishments must be in order of significance with the most significant listed first.

(3) Deficiency CAP Details. A separate deficiency CAP summary for each uncorrected material weakness, significant deficiency, and control deficiency. The summary must contain detailed narrative descriptions including the plans and schedules for the corrective action(s).

SECTION 4: DOCUMENTATION STANDARDS

4.1. INVENTORY OF ASSESSABLE UNITS AND PROCESSES.

a. Assessable Units are designed to provide a reasonable span of control to conduct MICP assessments of processes. A Sub-Assessable Unit can be any organization, function, program, or subdivision capable of being evaluated using internal control assessment procedures. A Sub-Assessable Unit must have clear limits or boundaries and be identifiable to a specific responsible manager. Further, it must be small enough to provide reasonable assurance of adequate management controls but large enough that any detected material weakness has the potential to impact the mission of the Agency.

b. Assessable Units must constitute the entire Agency. This means every part of the Agency must be represented by one of the Assessable Units in the Agency's Inventory of Assessable Units.

c. Assessable Units are structured by organization. AUMs will identify Sub-Assessable Units to better document process assessments or to establish and document standard processes for Assessable Unit mission execution. At a minimum, the Inventory of Sub-Assessable Units must include the name of the Sub-Assessable Unit and the responsible manager, identified by name and title, as seen in Table 2. Sample Inventory of Sub-Assessable Units.

Table 2. Sample Inventory of Sub-Assessable Units

Assessable Unit: FB	
Sub-Assessable Unit Name	**Sub-AUM**
1. Budget Operations	J. Doe, Director
2. Accounting Services	K. Smith, Director
3. Financial Planning	T. King, Director
4. Manpower Operations	C. Jones, Director
5. Financial Systems	D. James, Director

4.2. ANNUAL TEST PLANS. The Annual Test Plan is an executive summary of each AUM's MICP that captures their approach to implementing an effective internal control program. The consolidation of each AUM's Annual Test Plan serves as the first resource to the Agency's MICP.

a. Annual Test Plans will assist in the transition from one AUM and AUA to another by establishing in writing, how the Assessable Unit is implementing the relevant guidance. New AUMs will use the Plan to learn the specific approach and vision of the MICP within their Assessable Units.

b. Annual Test Plans will be updated by the AUMs at least annually and forwarded to the MICP Coordinator. The Plan may take any form but must identify the key elements:

(1) Fiscal year associated with the Test Plan.

(2) Identification of the AUA.

(3) Overview of the MICP within the Assessable Unit addressing all five elements of the Green Book standards.

(4) Description of how accomplishments will be documented.

(5) Description of how deficiency CAPs will be documented and monitored.

(6) Schedule of documented training.

(7) Description of what will be assessed, including the identification of all processes owned, process risk rating, materiality rating, date of scheduled process review, and the date of completion for deficiency CAPs (if applicable).

4.3. MATERIALITY. Materiality is based on management's judgment of an item's impact, influence, value, and the circumstances in which it occurs. It is difficult to apply a strict formula or test to determine whether something is or is not material. There are, however, important questions that can be asked to help management determine if an issue is considered a material weakness.

a. Is the issue control-related? Consider whether the issue is related to internal controls. If a control deficiency has been identified through the risk assessment process, this will be clear. If the issue was identified through other sources, such as an audit, it may not be clear. Not all problems are control-related. There could be a significant exposure to risk and/or a potential for loss of significant financial resources that result from informed management decisions, not from a control deficiency. Issues must be control-related to be included in the MICP Certification Statement.

b. Does the issue meet the general criteria for materiality? The concept of materiality can be financial or take on qualitative factors that affect success to mission, health, safety or image.

(1) Threat to Mission. Consider whether the control deficiency presents a risk to achieving the operational mission of DCMA. Threats to mission include but are not limited to:

(a) Impaired fulfillment of essential mission or operations.

(b) Unreliable information causing unsound management decisions.

(c) Violations of statutory or regulatory requirements.

(d) Impact on information security.

(e) Depriving the public of needed Government services.

(2) Threat to Resources. Consider whether the control deficiency is a threat to physical, financial or human resources. Both actual loss and potential for loss of resources will be considered along with the magnitude and frequency of the loss. When a control deficiency has a clear dollar value associated with it, the general standard used for materiality is a one percent threshold. Whereas, anything greater than one percent of the Agency's budget would be considered material.

(3) Threat to Image. Consider the impact on the Agency's reputation. A control deficiency may not pose a threat to the mission or be a material threat to resources, but it may bring substantial negative publicity. These control deficiencies could be material even if they do not meet the first two criteria. Threats to image include but are not limited to:

(a) Sensitivity of the resources involved (e.g., drugs, munitions).

(b) Current or probable congressional or media interest.

(c) Diminished credibility or reputation of management.

c. How does the issue affect DCMA's mission? Once it is determined that an issue threatens or impacts DCMA's mission, resource or reputation, it is helpful to perform a risk assessment and create a Matrix of Materiality to determine the issue's full impact, as seen in Table 3. Sample Matrix of Risk and Table 4. Sample Matrix of Materiality.

Table 3. Sample Matrix of Risk

Likelihood of Occurrence	Consequence of Impact To Organization				
Almost Certain	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Remote	Low	Low	Low	Medium	Medium
	Insignificant	Minor	Moderate	Major	Catastrophic

Table 4. Sample Matrix of Materiality

A. Impact/Severity Rating Scale				
Organizational Impact of Occurrence	**Rating**	**1**	**3**	**5**
	Financial Impact	**Low** financial impact resulting in a loss of < 1%	**Medium** **Moderate** financial impact resulting in a loss of 5% - 10%	**High** **and/or** **Extreme** financial impact resulting in a loss > 10%
	Reputational Impact	**No likely impact** on reputation.	Could result in a **moderate negative impact** to reputation	Could result in a **sustained negative impact** to reputation and / or national / global media coverage (e.g., front page of Washington Post).
	Operational Impact	**Not likely** to result in any operational impact.	Could result in **moderate** operational damage.	Could result in a **catastrophic** operational impact.
B. Likelihood Rating Scale				
Likelihood of Occurrence	**Rating**	**1**	**3**	**5**
	Frequency	once/1 - 3 Yrs	once/qtr	> once/mo
	Probability	< 25%	25 - 50%	51 - 100%
C. Control Effectiveness Rating Scale				
Residual Risk (Control Design & Implementation)	**Rating**	**1**	**3**	**5**
	Control Effectiveness	Controls are fully implemented and are highly effective in all instances	Partially implemented and/or effective	Control(s) do not exist or are not implemented

4.4. RISK ASSESSMENT DOCUMENTATION. The identification, assessment, and management of Assessable Unit risks is an essential part of an effective internal control system. Risks are future events or conditions that may prevent or negatively impact the Agency's achievement of its mission and objectives.

a. AUMs must implement risk management practices that are:

(1) Forward-looking to proactively identify existing and potential risks.

(2) Designed to assist the Agency Director with better decision making to manage existing and potential threats and identify opportunities to improve efficiency and effectiveness of government business process operations.

(3) Based on relationships to financial systems/reporting, business operations, and objectives established to drive performance and improvement.

b. Each of the risks identified in a mission and/or business process, control activity, or combination of control activities will be identified and documented in the risk assessment. The Green Book identifies the three types of risk:

(1) Inherent. The original susceptibility to a potential hazard or material misstatement, assuming there are no related specific control activities. For example, human error in data entry of figures.

(2) Control. The risk that a hazard or misstatement will not be prevented or detected by the internal control. For example, the control activity to prevent data entry error is to include a reconciliation total. The control to mitigate risk is that the reconciliation total will not prevent a misstatement.

(3) Combined. Also known as residual risk, it is the likelihood a hazard or material misstatement would occur and not be prevented or detected on a timely basis by the Agency's internal control. For example, combined risk remains if the transposition of numbers in the data entry process results in the total transactions matching the reconciliation total. In this case, the reconciliation total would not mitigate the inherent risk. The risk that remains is known as the combined risk.

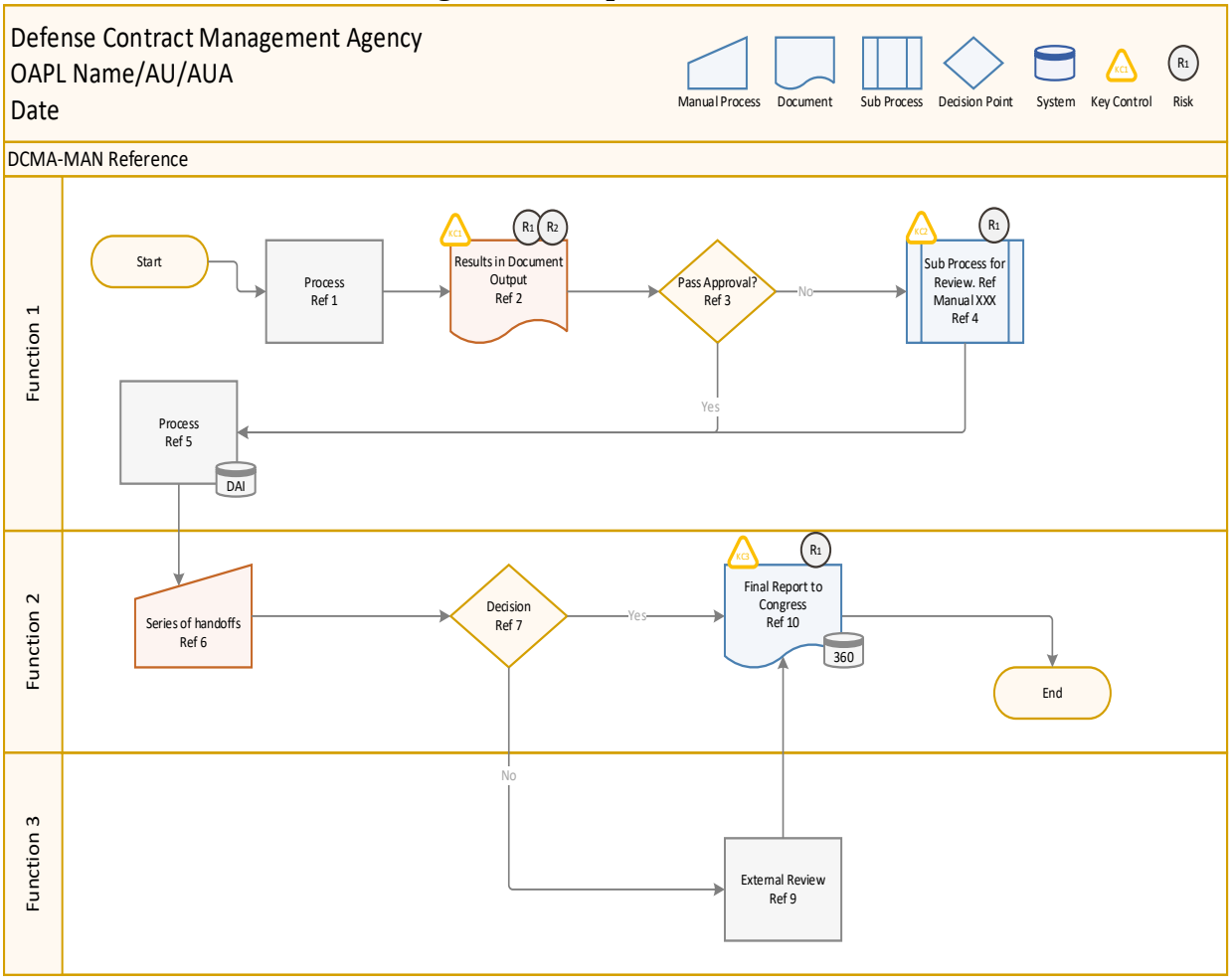
c. The MICP Coordinator and the AUM will review Internal Control Plans (Process Risk Assessments, Flows, Key Controls, and Narratives), Agency Assessments, Certification Statements, and other administrative actions as necessary to verify that the Assessable Unit Inventory includes operational, administrative, system, and financial events.

(1) Process Narratives are written descriptions of the Process Flows, and explain what actions are being taken in each step. In some instances, issuances may document the process steps and serve as a Process Narrative.

(2) Process Internal Control Plans will accompany significant Agency processes, to include those processes identified within the APL, DCMA issuances, essential operations, and any others deemed necessary for proper internal control operations. A process, as seen in Figure 1. Sample Process Flow, and narrative will identify the key processes and related control activities over information processing, physical control over vulnerable assets, segregation of duties, and accurate and timely recording of transactions and events.

(3) The MICP Coordinator may waive (in writing) the requirement for Process Flows or specific requirements in the Internal Control Plan for unique circumstances at the request of the AUM. The waiver will be incorporated into the Internal Control Plan documentation.

Figure 1. Sample Process Flow



4.5. CONTROL ASSESSMENT DOCUMENTATION. Once internal controls are in place, management is required to actively monitor the controls to ensure they are functioning correctly and effectively, and mitigate the associated risk. Control assessments can include both an internal review of the controls and evaluations from external organizations such as audit organizations or evaluations from the offices of the Inspector General.

a. Individual documented controls will initially be rated as having a low, moderate, or high control risk. Usually a control risk would be rated high if the control has not been implemented or if the control is not effective in either design or operation. A deficiency CAP must be developed for all high risk rated controls to decrease the risk of vulnerability or failure within the process.

b. Controls with low or moderate control risks are to be tested to see if the controls are effective. If the control is assessed to be ineffective, the control will be reclassified as having a high control risk. A deficiency CAP must be developed for those controls reclassified as having a high control risk.

c. Significant control deficiencies must be reported to the MICP Coordinator via the next higher level of authority as either a significant deficiency or material weakness. The level of deficiencies range by the likelihood of a misstatement:

(1) 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 satisfactorily accomplish their assigned functions or inhibits the prevention or detection of misstatements in a timely manner.

(2) Significant Deficiency. A control deficiency, or combination of control deficiencies, that adversely affects the ability to initiate, authorize, record, process, or report financial data reliably. There is more than a remote likelihood that a misstatement will not be prevented or detected.

(3) Material Weakness. Must be reported in the Agency SoA to OUSD(C). A material weakness is a type of significant deficiency or combination of significant deficiencies resulting in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

d. The DCMA MICP 360 site contains best practice documentation which is strongly suggested for use. The goal is to maintain internal control assessment documentation. A sample Control Assessment Overview is provided as a template on the DCMA MICP Resource Page, giving the AUMs information to establish and improve internal controls within their Assessable Unit.

4.6. CORRECTIVE ACTION PROCESS. Assessable Units must develop and implement deficiency CAPs to remediate identified deficiencies. The monitoring of internal controls must include policies and procedures for ensuring the findings of audits and other reviews are promptly resolved. Please refer to the resource page for template guidelines.

a. A completed deficiency CAP must include:

(1) Title and description of issue.

(2) Year identified.

(3) Original targeted completion date.

(4) Updated targeted completion date/scope to include any adjusted dates from prior year reports.

(5) Current target date for completion.

(6) If applicable, document scope creep and reason(s) for changes in targeted completion date.

(7) A step by step timeline on planned actions to improve internal controls.

(8) Validation of how actions are producing desired result.

(9) No CAP is required for localized performance issue deficiencies.

b. AUMs must accomplish activities in a timely and effective manner:

(1) Promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate Agency operations.

(2) Determine proper actions in response to findings and recommendations from audits and reviews.

(3) Complete, within established timeframes, all actions that correct or otherwise resolve the matters brought to the AUMs attention.

c. Deficiency CAPs for all material weaknesses, significant deficiencies, and control deficiencies must be included as an enclosure to the MICP Certification Statement.

d. The MICP Coordinator and AUMs must prioritize remediation of deficiency CAPs based on:

(1) The materiality level assigned to the deficiency.

(2) The impact on Assessable Unit financial statements in comparison with other existing deficiencies and deficiency CAPs by material weakness, significant deficiency, and control deficiency.

e. Deficiency CAPs must be implemented by the person performing the control. A well-developed CAP will contain detailed steps required to implement the corrective actions.

f. Deficiency CAPs must be monitored by the MICP Coordinator or responsible AUM to ensure it is being implemented as written and detailed milestones are being met.

g. Once a deficiency CAP has been implemented, the Assessable Unit must complete testing and/or other activities detailed in the CAP to verify it is achieving the desired milestones and final targeted results to remediate the internal control deficiency.

h. The SAT will conduct regular meetings to discuss and assess internal control deficiencies identified during the current fiscal year as well as the status of outstanding deficiency CAPs and remediation efforts. The SAT will provide recommendations to the AUM to assist with concluding whether or not corrective actions taken have been effective.

i. The SAT will review, verify, and oversee deficiency CAPs documented by the AUMs to remediate internal control deficiencies.

j. The corrective action process is only considered complete when appropriate corrective action has been implemented to correct the deficiency, when it produces intended and sustainable improvements, and when it demonstrates the findings and recommendations do not warrant further action.

4.7. ACCESSIBILITY AND RETENTION.

a. Accessibility. Internal control documents must be accessible upon request. DCMA utilizes a Sharepoint webpage to store this documentation. All DCMA employees have access to review documents stored on the DCMA MICP 360 site. DCMA AUMs and AUAs also have access to contribute their Assessable Unit documents to the site.

b. Retention. Federal entities must follow record retention requirements in accordance with Chapter 31 of Title 44, U.S.C., "Records Management by Federal Agencies," and guidelines set forth by the National Archives and Records Administration, General Records Schedules 5.7, Agency Accountability Records, which defines the retention requirements for internal control related records as seen in Table 5. Internal Control Documentation Retention Periods.

Table 5. Internal Control Documentation Retention Periods

Document	Retention Period
Policy, procedure, and guidance files	1 year
Management control plans	1 year
Risk analyses	1 year
Annual reports and assurance statements	1 year
Tracking files	1 year
MICP Documentation – MICP Office	5 years 1 month

GLOSSARY

G.1. DEFINITIONS

Annual Test Plan. An executive summary of each AUMs MICP that captures their approach to implementing an effective internal control program.

Annual Test Result. A document which describes the result, annually, of a process evaluation/ assessment. This document will be maintained and verified by the process owner according to the APL. The format and outline will follow OUSD (C) guidelines. This document should be a part of a Process Internal Control Plan.

APL. A list of all major DCMA processes. Once published, this list will be the Agency's internal control standard for assessing, testing, and reporting internal controls on the SoA.

Assessable Unit. A subdivision (organization, functional, programmatic or other) of the Agency's total MICP, as designated by the Director, which allows for adequate internal controls of the subdivision to include analysis, documentation, identification, and insertion of controls in order to mitigate risk.

AUA. Coordinates the MICP for their AUM. Communicates with MICP Coordinator on policy and annually coordinates the Assessable Unit Certification and quarterly updates for AUM approval.

AUM. Head of the Assessable Unit and responsible for MICP requirements. Appoints and oversees the AUA in the conduct of the Assessable Unit MICP effort. Appoints and oversees the Sub-Assessable Unit. The AUM must be a government employee to prevent inherently governmental functions from being performed by contracted employees.

CAP. Written document that identifies specific activities necessary to resolve a deficiency (e.g., deficiency, material weakness) and includes targeted milestones and completion dates.

Control Activities. Policies and procedures that help ensure necessary actions are taken to address risks related to the achievement of the program's objectives.

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 achieve control objectives and address related risks.

Control Environment. Influences the sustainability of an organization's effective internal controls.

Control Risk. Controls in place that may fail to prevent/detect identified inherent risks.

DoDI. A DoD issuance implementing the policy, or prescribing the manner of a specific plan or action for carrying out the policy.

Entity Level Controls. Controls with a pervasive effect on an entity's internal control system and designed to provide reasonable assurance that objectives related to the entity as a unit are met.

ERM. Agency-wide 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 individually.

Flow Chart. A graphical representation of a process. It is highly recommended to be developed in Microsoft Visio utilizing either vertical or horizontal swim lanes and be in compliant with DCMC Flow Chart Standards. This document should be a part of a Process Internal Control Plan

IFMS. 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.

Inherent Risk. Conditions that exist which could negatively impact mission objectives, assuming no controls are in place.

Internal Control. Process providing reasonable assurance that the Agency's mission and objectives will be achieved.

Internal Control Assessment. Documented evaluation on the effectiveness and adequacy of the internal control framework to meet mission objectives.

Internal Control Over Financial Reporting. Process designed to provide reasonable assurance regarding the reliability of financial reporting.

Internal Control Plan. A formalized strategy that is a single source for an executed process (may or may not include sub-processes). The plan shall contain a Risk Register, Flow, Narrative, Test Plan, and will document annual test results.

Levels of Assurance. Explicit finding provided by the AUM or Agency Director as to the status of internal controls in a reported element. One of three findings (unqualified, qualified, or no assurance) that must be reported in the Assessable Unit Certification and the Agency SoA.

Localized Performance Issue. A concern that may only be contained within a business unit that reflects a way the Sub-Assessable Unit does business and conducts its processes.

Material Weakness. Significant deficiency, or combination of significant deficiencies, resulting in more than a likelihood that a material misstatement of the financial statements will not be prevented or detected.

Materiality. Represents the magnitude of an omission or misstatement of an item in a financial report that in light of surrounding circumstances, making it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item.

MICP. Established by Public Law 97-255, the Federal Managers Financial Integrity Act (FMFIA) and enacted to ensure efficient and effective management of government resources to protect against fraud, waste, and abuse.

MICP Coordinator. Program manager of the MICP that administers the Agency-wide program to include policy, tools and training; maintains Agency Assessable Unit Inventory; supports AUM and AUA in the conduct of their efforts; coordinates with OUSD(C) and the Under Secretary of Defense for Acquisition & Sustainment on policy and administrative matters; and annually prepares the Agency SoA and quarterly updates for approval.

Modified Assurance. Provides reasonable assurance that internal controls are effective with the exception of one or more material weakness, or the IFMS is not in conformance with federal requirements.

Narrative. A document which describes, in detail, each process step in an executed process. The format and outline will follow OUSD (C) guidelines. This document should be a part of a Process Internal Control Plan

Oversight Panel for Managers' Internal Control. Serves as a monthly working group advisory board and the forum that facilitates working-level, cross coordination during the development of MICP requirements for Agency processes.

Residual Risk. Includes risks that still exist after management responds and modifies controls already in place, resulting in a need to potentially incorporate additional controls.

Risk. Possibility that an event will occur and adversely affect the achievement of the Agency's mission and objectives.

Risk Assessment. Internal management process for identifying, analyzing, setting risk tolerances, and managing risks relative to the Agency's mission and defined objectives.

Risk Register. A document that outlines and ranks risk according to OUSD (C) guidelines. This document should be a part of a Process Internal Control Plan

Root Cause Analysis. A systematic approach to getting to the true root cause of a problem. The root cause is the fundamental breakdown or failure of a process which, when resolved, prevents a recurrence of the problem.

SAT. Senior leader executives that provide oversight of assessing and documenting the effectiveness of internal controls for financial reporting and financial systems.

Significant Deficiency. Control deficiency or combination of control deficiencies, that in

management's judgment, present a significant impact in the design or operation of internal controls that could adversely affect the component's ability to meets its internal control objectives.

SoA. Agency's informed judgment as to the overall adequacy and effectiveness of internal controls within the Agency related to operations, reporting, and compliance.

Statement of No Assurance. Unable to provide reasonable assurance because no assessments were conducted or the noted material weaknesses are extensive and/or pervasive.

Sub-AUA. Coordinates the MICP for the Sub-AUM; communicates with AUA on policy; annually coordinates the Sub-Assessable Unit Certification and quarterly updates for Sub-AUM approval.

Sub-AUM. The primary responsible manager of the Sub-Assessable Unit as designated by the AUM.

Subordinate Assessable Unit. A sub-component of an Assessable Unit identified to better document process assessment or to better establish documentation of standard process for Assessable Unit execution.

Systemic Weakness. Specific instance of a failure in a system of control or lack of control that is pervasive within the Agency and materially affects internal controls across organizational and program lines, usually affecting more than one Assessable Unit.

Test Plan. A document which describes, in detail, how each process or Key Control, or risk will be tested. The document will be part of a Process Internal Control Plan and the format and outline will follow OUSD (C) guidelines.

Unmodified Assurance. Provides reasonable assurance that internal controls are effective with no material weaknesses reported.

GLOSSARY

G.2. ACRONYMS.

APL	Authoritative Process List
AUA	Assessable Unit Administrator
AUM	Assessable Unit Manager
CAP	Corrective Action Plan
DCMA-INST	DCMA Instruction
DODI	DoD Instruction
ERM	Enterprise Risk Management
FB	Financial and Business Operations
GAO	Government Accountability Office
IAT	Internal Audit Team
IET	Inspections and Evaluation Team
IFMS	Integrated Financial Management System
MICA	Managers' Internal Control Assessment
MICP	Managers' Internal Control Program
OMB	Office of Management and Budget
OUSD(C)	Office of the Under Secretary of Defense, Comptroller
SAT	Senior Assessment Team
SME	Subject Matter Expert
SoA	Statement of Assurance
Sub	Subordinate
Sub-AUA	Subordinate Assessable Unit Administrator
Sub-AUM	Subordinate Assessable Unit Manager
U.S.C.	United States Code

REFERENCES

DoD Financial Statement Audit Guide, May 2018
DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013
DoD 7000.14-R, Volume 1, "General Financial Management Information, Systems and Requirements," current edition
Office of Management and Budget Circular No. A-123, "Managements Responsibility for Internal Control," December 21, 2001, as amended
Office of Management and Budget Circular No. A-127, "Financial Management Systems," July 23, 1993, as amended
Public Law 97-255, "The Federal Managers Financial Integrity Act of 1982," September 8, 1982
United States Code, Title 31, Section 3512, "Executive Agency Accounting and Other Financial Management Reports and Plans"
United States Code, Title 44, Chapter 31, "Records Management by Federal Agencies"
United States Government Accountability Office "Standards for Internal Control in the Federal Government," GAO-14-704G (also known as "Greenbook"), September 2014