ADS Chapter 596

Management's Responsibility for Enterprise Risk Management and Internal Control

Partial Revision Date: 03/09/2023
Responsible Office: M/CFO/FPS
File Name: 596_030923

Functional Series 500 – Management Services
ADS 596 – Management's Responsibility for Enterprise Risk Management and Internal Control
POCs for ADS 596: Lydia Nylander, lnylander@usaid.gov; Charleta Dixon, cdixon@usaid.gov

Table of Contents

ADS 596 – Management's Responsibility for Enterprise Risk Management and Internal Control

596.1 OVERVIEW

Effective Date: 09/22/2022

This chapter describes the policy directives and required procedures on management's responsibilities for USAID's Enterprise Risk Management and Internal Control (ERM/IC) program pursuant to the **Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (OMB Circular A-123)** and the **Federal Managers' Financial Integrity Act (FMFIA), as amended**. This chapter provides implementation guidance to USAID assessable units (AUs) to:

1. Integrate risk management and internal control to enhance strategic planning, ensure performance of key objectives, and manage risk; and

2. Improve accountability and effectiveness of programs and operations through awareness and implementation of ERM practices by establishing, maintaining, and assessing internal control effectiveness.

The **Fraud Reduction and Data Analytics (FRDA) Act of 2015** requires agencies to: (1) establish financial and administrative controls to identify and assess fraud risks; and (2) design and implement control activities to prevent, detect, and respond to fraud. USAID defines fraud as "obtaining something of value through willful misrepresentation." Fraud jeopardizes Missions by diverting resources from their intended purpose. Management's responsibility for fraud risk is meant to facilitate achievement of the program's broader mission and strategic goals by helping to ensure that funds are spent effectively, services fulfill their intended purpose, and assets are safeguarded. USAID's ERM/IC program provides guidance and resources for fraud risk management and required internal control activities consistent with **ADS 596sac, USAID Anti-Fraud Plan**.

596.2 PRIMARY RESPONSIBILITIES

Effective Date: 09/22/2022

a. The **Administrator (A/AID)** ensures USAID's commitment to an appropriate system of internal control and enterprise risk management, to include anti-fraud, that is incorporated into governance, strategy, and mission performance. The A/AID:

- Leads in establishing the amount of risk USAID is willing to accept in pursuit of its mission;

- Facilitates the achievement of results and safeguards the integrity of USAID programs; and

- Submits the USAID annual Statement of Assurance to the President and Congress, and publishes the statement in USAID's Financial Report in accordance with **OMB Circular A-123** and **Sections 2 and 4 of FMFIA**.

b. The **Deputy Administrator (DA/AID)** communicates to the Administrator management's responsibility for the ERM/IC program; and chairs USAID's Executive Management Council on Risk and Internal Control (EMCRIC).

c. The **Chief Risk Officer (CRO)** serves as an advisor to the EMCRIC chair(s) and the Risk Management Council (RMC). The CRO:

- Provides senior leadership oversight for USAID's risk management needs;

- Oversees the development and implementation of an integrated risk management framework; and

- In conjunction with the ERM Executive Secretariat, ensures the function of the risk management framework, continuously reviews and responds to critical USAID risks, and confirms the appropriate risk culture is established and communicated throughout USAID.

d. The **Executive Management Council on Risk and Internal Control (EMCRIC)** is chaired by the DA for Management and Resources, or their designee(s), and recommends the Administrator's approval of the USAID annual Statement of Assurance, the Agency's Risk Profile, and proposed corrective measures and risk response. The membership consists of:

- The Agency Counselor,

- Assistant Administrators (AAs) of Bureaus and Heads of Independent Offices,

- Statutory Officers of the Agency, and

- The Inspector General (as an observer).

The EMCRIC provides oversight for USAID's ERM practices and internal control systems; and reports to the Administrator, who provides final approval on the EMCRIC's recommendations.

e. The **Senior Assessment Team (SAT)** is chaired by the Chief Financial Officer (CFO) and membership consists of Agency Statutory Officers and selected Bureau/Independent Office (B/IO) Deputy Heads. The SAT is responsible for:

- Oversight and management reporting of deficiencies in financial internal control, as identified through the FMFIA certification process, Government Management Reform (GMRA) Act of 1994, and any other related functions;

- Assessing, monitoring, and/or proposing appropriate corrective measures;

- Reviewing significant internal control deficiencies and reporting deficiencies deemed to be material weaknesses to USAID as a whole -- which must be included in the Agency's Risk Profile (ARP) and USAID's annual Statement of Assurance; and

- Providing SAT results that may include any financial risks to the RMC for inclusion, as appropriate, in the ARP.

f. The **Risk Management Council (RMC)** is co-chaired by Deputy Assistant Administrators (DAAs) from the Bureau for Management (M) and the Bureau for Policy Planning and Learning (PPL) and membership consists of DAAs or Deputy Heads of all B/IOs and Deputies of the Agency's Statutory Officers (see ADS 101saa, Statutory, Regulatory, and Other Mandated Management Officials). The RMC assesses the roll-up of enterprise risks and non-financial internal control input from Mission and B/IO level Management Councils on Risk and Internal Controls (MCRICs) and financial internal control from the SAT. The RMC reviews the ARP and deliberates on any proposed new risks for review and approval by the EMCRIC.

g. The **ERM Executive Secretariat** consists of the ERM/IC staff in M/CFO. The ERM Executive Secretariat:

- Carries out the responsibilities in the Governance Charter for ERM and Internal Control at USAID (see **ADS 596mab**);

- Provides technical assistance, training, and guidance to Missions, B/IOs, and all Agency management in developing a common vision, definition, and strategy for managing risk and internal control; and

- Ensures the RMC, EMCRIC co-chairs, and USAID Principals are knowledgeable about relevant risk topics impacting USAID to facilitate constructive meetings/discussions.

Under the Governance Charter responsibilities, the ERM Executive Secretariat establishes protocols and procedures for escalation of significant risk events; and tracks, solicits, and monitors votes, decisions, and follow up actions during meetings.

h. The Agency's **Chief Financial Officer (CFO)** and the **Bureau for Management, Office of the Chief Financial Officer (M/CFO)** carries out the statutory responsibilities of the **Chief Financial Officers Act of 1990** and heads the ERM Executive Secretariat for the following ERM governance bodies: EMCRIC, RMC, and SAT.

The CFO is USAID's **Senior Accountable Official (SAO)** for Enterprise Risk Management. As head of the ERM Executive Secretariat, the CFO facilitates the efforts of the ERM governance bodies by advancing risk awareness, risk expertise, risk mitigation actions, and maintaining ERM governance bodies' documents and records. The CFO recommends activities and processes to ensure compliance with **FMFIA**, **OMB Circular A-11**, and **OMB Circular A-123** (Appendices **A**, **B**, **C**, and **D**).

i. The **Chief Information Officer (CIO)** is designated by the Administrator as the **Senior Agency Official for Risk Management (SAORM)** and has Agency-wide responsibility and accountability for ensuring the implementation of USAID's cybersecurity risk management activities is aligned with USAID strategic, operational, and budgetary planning processes. The SAORM works closely with EMCRIC and participates as a member of the SAT to monitor and report on the testing and documentation of information technology controls.

j. **Assessable Units (AUs)** is an organizational unit within USAID that submits an annual Statement of Assurance (to the next supervisory level on the status of internal control) and an organizational Risk Profile. All Missions and B/IOs are designated as AUs. Lower-level organizational units, such as divisions or offices within Missions or B/IOs, may be considered AUs as designated by the responsible Mission or B/IO.

k. **USAID Managers in Missions/B/IOs** ensure OMB Circular A-123, FMFIA, and **GAO Standards for Internal Control in the Federal Government (GAO Green Book)** criteria are incorporated into the strategies, plans, guidance, and procedures that achieve USAID's program goals and objectives. Managers are responsible for:

- Risk identification, risk assessment, and risk mitigation; and
- Ensuring AUs are properly established and identified and all Missions and B/IOs are designated as AUs.

l. **USAID/W Bureaus and Independent Offices (B/IOs):**

- Review/coordinate subordinate units' annual certifications for internal control and submission of the units' Risk Profile;
- Consolidate the annual OMB Circular A-123, FMFIA certification, and the GAO Green Book based on compliance documentation for the B/IO using information submitted by subordinate units' and their own AUs information;
- Designate a **Risk Management Liaison (RML)** for their respective B/IO;
- Ensure risks are operationalized, identified, and managed by B/IO technical experts for their respective discipline and environment as part of the AU's risk assessment process for developing the AU's Risk Profile and the Risk Appetite Statement (RAS); and

- Ensure technical experts have risk resources (e.g., funding, staff, time, and capacity) that serve to inform Agency Task Force priorities and ERM Governance Councils on identified risks in their area of expertise and environment.

USAID/Washington (USAID/W) B/IOs have the flexibility to designate lower-level organizational units as AUs or use an alternative means of ensuring a comprehensive report on the status of controls in the B/IO is prepared.

m. Management Councils on Risk and Internal Control (MCRICs) provide management and oversight for ERM and internal control at the Mission and B/IO level and at the Mission/Washington office level. Each MCRIC manages risks and internal control deficiencies faced by its AUs and prepares and submits its FMFIA certification and Risk Profile to the RMC and/or the SAT. In addition to assessing their own risks and internal control, Mission and B/IO level MCRICs also assess the FMFIA certification of their subordinate AUs and submit a composite FMFIA certification and Risk Profile that provides a Mission or B/IO level portfolio view of risk to the RMC and/or SAT.

n. Risk Management Liaisons (RMLs) facilitate communication between the ERM Executive Secretariat and their respective B/IO, and any Missions in their region. RMLs facilitate USAID's annual Risk Profile process. Missions and B/IOs are required to designate a RML and have the option to designate multiple RMLs at their discretion.

596.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 09/22/2022

USAID's ERM/IC program fosters a risk aware culture and ensures that senior leadership can effectively address inherent and emerging risks. The goal is to neither control nor avoid all risk, but rather to take advantage of opportunities while reducing or mitigating threats to achieve USAID's mission and objectives. The ERM/IC program provides a holistic approach in identifying, assessing, and managing risks to support strategic decision-making.

USAID defines risk as the effect of uncertainty on the Agency's objectives, where risk may present negative outcomes or potential opportunities that can impact, threaten, or enhance the likelihood of achieving a set of objectives. To better understand and address risk, USAID developed **ADS 596mad, USAID Risk Appetite Statement** to provide broad-based guidance on the level and type of risk the Agency is willing to accept—based on an evaluation of opportunities and threats—to achieve the Agency's mission and objectives. **ADS 201, Program Cycle Operational Policy** outlines practical steps, including risk management, for making evidence-based decisions for key strategic, programmatic, and operational priorities for planning, delivering, assessing, and adapting development programming.

Per OMB A-123, risk management can be described as a coordinated activity to direct opportunities and control challenges or threats to achieving an organization's goals and objectives. Missions and B/IOs share information on the major risks facing their organization in a Risk Profile to inform senior leadership of decisions that may have an impact on operations.

596.3.1 Relationship Between Enterprise Risk Management and Internal Control

Effective Date: 09/22/2022

ERM and IC processes contribute to USAID's risk management in different, but complementary ways. Using an enterprise-wide, strategically aligned portfolio view of organizational challenges provides better insight into how to most effectively prioritize resource allocations to ensure successful mission delivery. ERM allows USAID to examine risks to shape their impact on objectives and promotes an approach to management measures taken, rather than those taken in silos.

The IC process provides reasonable assurance that the objectives of an entity will be achieved and includes involvement from management and other personnel. At USAID, ERM and IC work together to achieve strategic, operational, reporting, and compliance objectives. ERM and Internal Control are integral parts of the overall governance process and in strategy setting, communicating with USAID stakeholders, and measuring performance.

596.3.2 Management's Responsibility for Enterprise Risk Management and Internal Control

Effective Date: 03/09/2023

A. Governance and Implementation

The top-down component of governance within the ERM program provides the following:

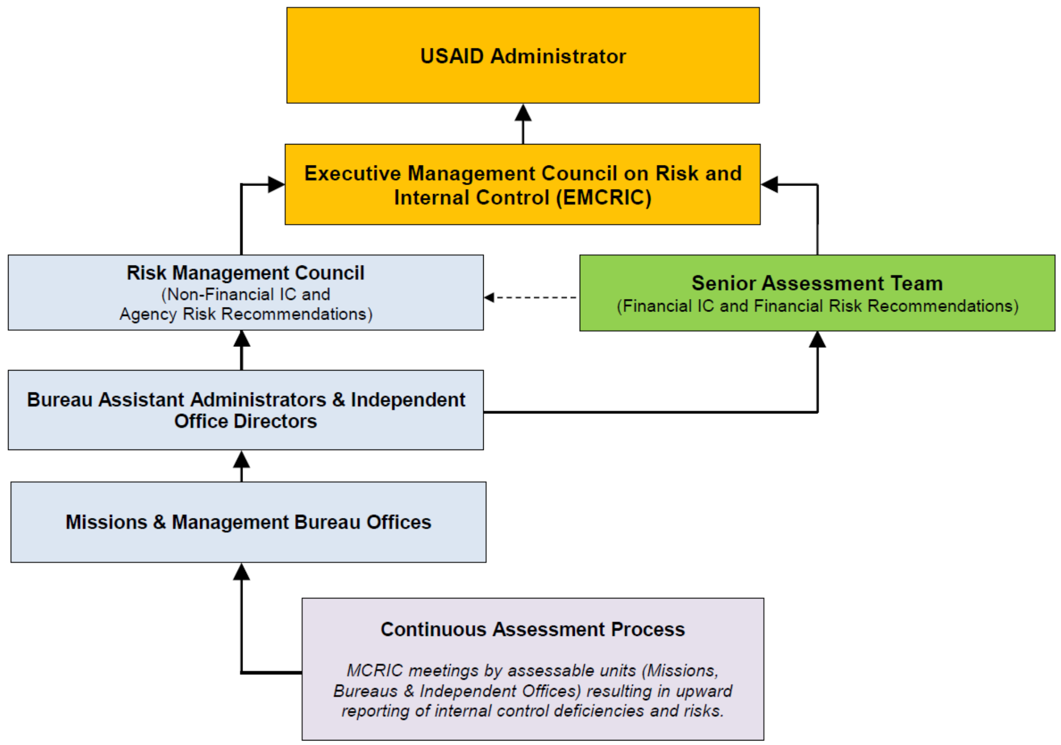
- Leadership or those charged with governance as the person(s) or organization(s) with responsibility and accountability for identifying, managing, and monitoring enterprise risk for USAID;

- Fostering and promoting an environment for risk transparency, promoting collaborative and timely risk decision-making; and

- Enabling a risk-aware culture within USAID.

The bottom-up component of the ERM governance process actively provides input into risk identification; understands and utilizes ERM terms, tools, and techniques; and acts in accordance with top-down guidance on specific risk responses. See the figure below for **USAID's ERM and Internal Control governance structure**:

Governance Structure for ERM and Internal Control Systems


USAID Administrator
Executive Management Council on Risk and Internal Control (EMCRIC)
Risk Management Council
(Non-Financial IC and Agency Risk Recommendations)
Senior Assessment Team
(Financial IC and Financial Risk Recommendations)
Bureau Assistant Administrators & Independent Office Directors
Missions & Management Bureau Offices
Continuous Assessment Process
MCRIC meetings by assessable units (Missions, Bureaus & Independent Offices) resulting in upward reporting of internal control deficiencies and risks.

The specific guiding principles of ERM at USAID are:

- ***Tone from the Top*** fosters a fully transparent risk management culture and ensures leadership accountability.

- ***A Whole-of-Mission Approach*** requires an appropriate understanding of Mission and country-level issues to make informed decisions to mitigate risks, seizing opportunities, and achieving strategic and operational objectives.

- ***Leverage Existing Processes*** that reflect the risk management culture and integrate continuous risk monitoring of the organization.

- ***The USAID Risk Appetite Statement*** sets the parameters for the type and level of risks that the Agency is willing to accept to achieve objectives based on the identification of key threats; and opportunities to leverage or enhance USAID programming or operations.

Management of risk must be regularly monitored for effectiveness and consideration must be given to changes in the risk profile. Through the ERM governance structure, monitoring is conducted, and key documents are produced such as:

- The RAS, which is approved by USAID's senior leadership; and

- The ARP, which is informed by an AUs Risk Profile, to assess and manage risk.

B. USAID's Risk Appetite Statement

Risk appetite is the broad-based concept of the amount of risk an organization is willing to accept at an aggregate level and for specific types of risk in pursuit of its mission/vision. It is led and established by the USAID Administrator along with senior leadership and serves as the guidepost to set strategy and select objectives. The concept of "risk appetite" is key to achieving effective ERM and is essential for determining risk responses. Risk appetite can be considered qualitatively and/or quantitatively and must be factored into the process of balancing risks and opportunities. Identifying the appropriate amount of risk an organization is willing to accept in pursuit of a specific objective must be directly linked to the value derived by managing to that level of risk. More information detailing USAID's risk appetite can be found in **ADS 596mad, USAID Risk Appetite Statement**.

C. Agency Risk Profile

While the AUs may be tracking several risks at any given time, only key risks are elevated for reporting in the ARP. Collectively, all AU risk profiles create the Bureau Risk Profile to inform creation of the ARP. The profiles provide senior leadership with an up-to-date set of enterprise risks facing the organization, as informed by the USAID RAS, and enables proactive decision-making and maintains compliance with OMB Circular A-123.

All AUs must submit their Risk Profile annually through the Agency Secure Image and Storage Tracking System (ASIST)/Consolidated Audit and Compliance Systems (CACS). Missions and B/IOs compile and analyze the AUs Risk Profile and inform the USAID Risk Profile by:

- Determining the aggregate level and types of risk that all agency management need to consider to achieve its business objectives;

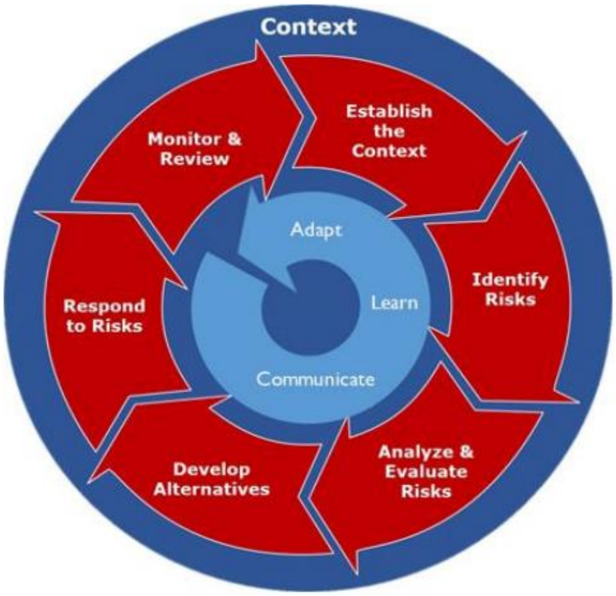
- Evaluating fraud risk and using a risk-based approach to design and implement financial and administrative control activities to mitigate identified material fraud risks; and

- Identifying sources of uncertainty, both positive (opportunities) and negative (threats), and the need to consider fraud risk.

More information on how to prepare the Risk Profile is available via the **Office of the Chief Financial Officer/ERM/IC resource webpage**.

D. Risk Management Framework

USAID has adopted the seven-step risk management process defined in, and adapted from, OMB Circular A-123. The risk management process is not meant to be a stand-alone activity, rather, it is a framework or approach to inform decision-making. To build risk awareness at USAID, the following seven steps must be performed in sequential order to properly address risk.



Step 1: Establish the Context

Step 2: Identify Risks

Step 3: Analyze and Evaluate Risks

Step 4: Develop Alternatives

Step 5: Respond to Risks

Step 6: Monitor and Review

Step 7: Communicate, Learn, and Adapt

E. Risk Assessment

A precondition to risk assessment is the establishment of clear, consistent objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving objectives, such as those defined in USAID's strategic and annual performance plans and forms a basis for determining how risks must be managed.

As part of the AU's risk assessment process in completing the AU's Risk Profile, management needs to comprehensively identify risk and consider all significant interactions between the organization and other parties, as well as internal factors at the activity level. Risk identification may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits, customer surveys/feedback or other assessments.

Once risks have been identified, they must be analyzed for their possible effect. Risk analysis includes estimating the risk's significance, assessing the likelihood of its occurrence and its impact, and deciding how to manage the risk and what actions must be taken.

F. Fraud Risk Management

The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and impact of fraud (see **GAO-15–593SP**). USAID defines fraud as “involves obtaining something of value through willful misrepresentation.” USAID management is responsible for mitigating fraud, waste, abuse, misconduct, and fraudulent payments in USAID programs and operations. This is a part of a holistic approach to fraud prevention, detection, and response efforts and integrates the **Governance Charter for Enterprise Risk Management and Internal Control at USAID** and the overall Risk Assessment process.

Fraud risk management and the **USAID Anti-Fraud Plan** provides a strategic implementation approach that protects USAID’s operations and programs against fraud, ensures USAID can work effectively, and is an integral part of our Enterprise Risk Management program.

As USAID implements the Anti-Fraud Plan, entity-wide fraud risk assessments must address the risk of fraudulent financial reporting, fraudulent non-financial reporting, asset misappropriation, and other illegal acts. The results will help USAID:

- Identify fraud schemes, fraud risks, and exposures;
- Estimate the likelihood and impact of each fraud scheme and risk;
- Identify existing fraud controls and assess their design;
- Assess the effectiveness of existing controls; and
- Document USAID’s fraud risks.

The plan needs to address possible fraud risks reported annually as **Top Management Challenges** by USAID’s **Office of Inspector General (OIG)** and published in the **Agency Financial Report (AFR)**.

596.3.3 Guidance for Establishing Internal Control

Effective Date: 03/09/2023

A. The Requirements

In the GAO **Green Book**, internal control is defined as “a process effected by an entity’s oversight body, management, and other personnel that provides reasonable assurance that the objectives of an organization are achieved.” Reasonable assurance refers to a satisfactory level of management confidence that internal control is adequate and operating as intended. Inherently a management decision, reasonable assurance recognizes that acceptable levels of risk exist that cannot be avoided because the cost of absolute control would exceed the benefits derived. The GAO Green Book prescribes the standards of internal control that Federal managers must use in designing, implementing, and operating in an effective system of internal control. USAID managers and staff must develop and implement appropriate, cost-effective internal control that produces results and ensures ERM and internal control work together. ERM and internal control must reasonably verify:

- Effectiveness and efficiency of operations including the use of USAID resources;
- Reliability of reporting for internal and external use; and
- Compliance with applicable laws and regulations to include safeguarding of assets (fraud awareness and prevention).

OMB Circular A-123, Appendix A, Management of Reporting and Data Integrity Risk provides an updated methodology for management to assess, document, and report on internal control over reporting (ICOR). Reporting focuses on the expansion of internal control over financial reporting (ICOFR) to all reporting objectives (e.g., strategic, operations, reporting, and compliance) to ensure the efforts of ERM and internal control are reflected in the ARP and the RAS. Management must also consider all reporting objectives using an external and internal view. For example, external objectives consider statutory requirements or the need for accountability and transparency. Internal objectives factor in daily reporting and budgeting for programs.

To establish an effective internal control system, USAID follows the GAO Green Book to balance controls and risk. The GAO Green Book is organized by five components of internal control and 17 required principles as shown below:

Components of Internal Control	Principles
Control Environment	1. Demonstrate Commitment to Integrity and Ethical Values 2. Exercise Oversight Responsibility 3. Establish Structure, Responsibility, and Authority 4. Demonstrate Commitment to Competence 5. Enforce Accountability
Risk Assessment	6. Define Objectives and Risk Tolerances 7. Identify, Analyze, and Respond to Risk 8. Assess Fraud Risk 9. Analyze and Respond to Change
Control Activities	10. Design Control Activities 11. Design Activities for Information Systems 12. Implement Control Activities

Information and Communication	13. Use Quality Information 14. Communicate Internally 15. Communicate Externally
Monitoring	16. Perform Monitoring Activities 17. Remediate Deficiency

B. Internal Control Assessment

To demonstrate compliance with the requirements of FMFIA and to support the Administrator's annual Statement of Assurance published in the AFR, each AU must perform an internal control assessment. This assessment requires a FMFIA certification letter generated by ASIST/CACS; the completion of the Uniform Risk and Internal Control Assessment tool (**URICA**); and corrective action plans (CAPs) for all identified deficiencies - control deficiencies (CDs), significant deficiencies (SDs), and/or material weaknesses (MWs).

The ASIST/CACS generated certification letter must include:

1. A statement that there is reasonable assurance that internal control is achieving the intended objectives;

2. A description of SDs and MWs that could adversely affect the AUs ability to meet its internal control objectives; and

3. CAPs with Specific, Measurable, Achievable, Realistic, and Time-bound (SMART) milestones and target completion dates.

Management is responsible for the inputs in the URICA tool. Those inputs are meant to assess/evaluate the entity-level identification and prioritization of risk and internal control and to decide if deficiencies have a pervasive effect on the organization. Risks identified in URICA are internal control risks that threaten operational objectives (relating to efficient and effective operations of internal business processes and capabilities; reliability of reporting; and compliance with laws and regulations). Once concerns or events have been identified and documented as risks, management will use URICA to calculate an internal control deficiency score, using inputs such as: likelihood of the event, magnitude of impact, effectiveness of controls, and documented testing.

ERM risks are broader and focus on strategic goals and objectives and must be reported on the AU Risk Profile. AUs must consider all risks in both contexts, operational objectives, and strategic objectives, before reporting in URICA and completing the annual Risk Profile exercise. AUs are responsible for the compilation of a Risk Profile. There are additional fraud awareness statements (safeguarding of assets) in URICA that require evaluation along with the standard assertion statements. Annually, Missions and B/IOs must review risk for any potential risk changes due to changes in process, personnel, or applicable regulatory requirements. A good rule for determining the desired frequency of risk review/evaluation of business processes is:

- High Risk - Review business processes every year,
- Medium Risk - Review business processes every two years, and
- Low Risk - Review business processes every three years.

CAPs must be created and monitored for all identified deficiencies: control (CD), significant (SD), and material weaknesses (MWs). Once identified, a CAP must be created in ASIST/CACS for all deficiencies.

Additionally, management is responsible for a self-evaluation using the GAO Green Book (5) components and 17 principles. The evaluation promotes awareness of the unit's internal control maturity level and improvements that can be made and conducted by the office coordinating the FMFIA review, with results presented for discussion at the unit's MCRIC.

C. Other Internal Control Assessment OMB A-123 Reviews

USAID ERM/IC staff conducts internal control assessments of selected Missions and USAID/W B/IOs annually based on analytical reviews/data. The reviews of Missions and USAID/W B/IOs are conducted on Appendix A, B, C and D based on management comments, challenges, OIG reviews, justifications of circumstances (e.g., Covid-19 funding distributions, governmental situations, etc.), and other relevant factors.

The assessments are conducted using OMB A-123 requirements, GAO Green Book, the Automated Directives System (ADS), and other applicable laws and regulations. The objective is to evaluate key controls (in scope) of business processes to provide reasonable assurance on whether the controls are suitably operating as intended. The ERM/IC completes a final results report that includes any noted items and/or identified deficiencies and CAPs are created in ASIST/CACS. The ERM/IC reports significant deficiencies and/or material weakness in the FMFIA certification and/or SAT if not completed and closed timely. The Missions and USAID/W B/IOs receive a copy of the results reports after CFO management reviews and provides clearance.

596.3.4 Management's Responsibility to Continuously Monitor, Assess and Improve Internal Control

Effective Date: 03/09/2023

A. Certification Process

The FMFIA Certification Process requires a five-step process. The AUs RML coordinates and completes this process. The five-steps are:

1. Assess risk and internal control activities,

2. MCRICs conduct reviews and make final deficiency determinations,

3. Prepare CAPs,

4. Generate and submit FMFIA certification in ASIST/CACS, and

5. Upload supporting documentation in ASIST/CACS.

Additional information on the certification process can be found on the Office of the Chief Financial Officer webpage under FMFIA guidance.

B. Documentation Requirements

Documentation is required to demonstrate the design, implementation, and operating effectiveness of an organization’s internal control system. The level and nature of documentation can vary based on the size of the organization and the complexity of the operational processes the organization performs. Management must choose the appropriate level of documentation needed to support its internal control. The GAO Green Book provides documentation requirements that are a necessary part of an effective internal control system (see **ADS 502, The USAID Records Management Program**).

C. Identifying Deficiencies

The absence or ineffectiveness of a key internal control can constitute a deficiency or weakness that must be corrected by a CAP. Management evaluates whether the weakness or deficiency, based on supporting data, rises to the level of significant or material which is then reported to the next level of management. Managers must keep the next level of management informed of sensitive problems and issues. Even if a weakness or deficiency can be corrected at one level, it does not exclude reporting it to the next level.

USAID staff are encouraged to identify deficiencies, as this reflects positively on USAID’s commitment to recognizing and addressing management issues. Failing to report a known material weakness or significant deficiency reflects adversely on USAID and places the Mission at risk. To decide if internal control weaknesses and/or deficiencies are material, consider the following:

- Material misstatement in the financial statements,

- Current or probable congressional interest,

- Impairment of mission, and/or

- Unreliable information causing unsound management decisions.

Each significant deficiency/material weakness reported must include a CAP and a milestone plan that tracks and validates that the corrective action(s) have in fact resolved the weakness and/or deficiency and must be reviewed by the next level of management/supervision. Significant deficiency/material weakness will not be closed until this validation milestone is completed. The AU must make supporting documentation available for review upon request.

D. Responsibility for Monitoring

Using a variety of information sources, USAID managers are primarily responsible for assessing and monitoring controls and using applicable data, sources, and/or documentation. To continuously assess and improve the effectiveness of internal control for USAID programs and operations, management should look at ways to monitor controls including the following examples:

- Management reviews conducted specifically for the purpose of assessing internal control or for other purposes with an assessment of internal control as a by-product of the review.

- Annual performance plans, reports, strategic reviews, and program evaluations pursuant to GPRA Modernization Act of 2010 and OMB Circular A-11, Section 200, Federal Performance Framework.

- Audit of financial statements conducted pursuant to the CFO Act, as amended.

- Office of the Inspector General (IG) audit inspections, reviews, investigations, or hotline complaints and GAO reports or audits.

- Payment Integrity Information Act of 2019 (PIIA).

- Single Audit reports for grant-making agencies.

- Audit reports for non-U.S. recipient contracted audits.

- Federal Information Security Modernization Act (FISMA 2014) audits.

- Mission Management Assessments.

- Customer surveys and feedback.

- Internal control checklists developed and maintained centrally as well as control activities.

Internal control is designed to ensure that ongoing monitoring occurs during normal operations, performed continually, and is ingrained in operations. Monitoring of internal control includes policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. USAID managers are responsible for promptly evaluating findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate USAID operations; determining proper actions in response to findings and recommendations from audits and reviews; and completing, within established timeframes, all actions that correct or otherwise resolve the matters brought to management's attention.

Ongoing monitoring of internal control and ERM are facilitated by semi-annual MCRIC meetings. Missions and B/IOs prepare information to meet the unit's MCRIC requirements and timeline. Agreement needs to be reached on identifying material weaknesses and significant deficiencies requiring reporting to the next supervisory level in the FMFIA certification process (see **ADS 596mab**).

596.3.5 Correcting Internal Control Deficiencies

Effective Date: 03/09/2023

AUs must develop CAPs for their own identified internal deficiencies and ensure that the weakness is corrected. CAPs and milestones are generated from the results of the internal control and risk assessments. Each milestone represents an activity or activities marking significant improvement toward the remediation of the deficiency through treating the root cause. Identifying and developing an understanding of the principal cause of deficiencies is management's responsibility. AUs must periodically assess progress against the CAP and report to the next management level through ASIST/CACS.

Management must take timely and effective action to improve or correct internal control deficiencies in accordance with the CAPs. To be effective, CAPs must:

- Address the root cause of the condition(s) in the deficiency,
- Include milestones to design and implement internal control,
- Produce evidentiary artifacts to demonstrate that the internal control is operating effectively,
- Address one or more deficiencies,
- Target a completion date, and
- Validate that the corrective actions performed have resolved the deficiency.

Milestones must be actionable and measurable to properly document remediation progress and provide management with objective evidence that the deficiency is being corrected. USAID managers must track the progress of the CAP to ensure timely and effective results. It is management's responsibility to determine if a deficiency has been corrected by considering the sufficiency of the corrective actions and the results achieved.

M/CFO monitors the CAPs and closure of significant deficiencies and material weaknesses. M/CFO informs the EMCRIC of progress made towards implementing CAPs. AUs are responsible for implementing corrective actions for their control deficiencies that are not significant or material that is not reported upward.

596.3.6 Annual Reporting

Effective Date: 09/22/2022

FMFIA and OMB Circular A-123 requires the USAID Administrator to annually submit to the President and the Congress (i) a statement on whether there is reasonable assurance that controls are achieving their intended objectives; and (ii) a report on material weaknesses and significant deficiencies (see **FMFIA** and **OMB Circular A-123**).

The USAID Administrator's annual Statement of Assurance includes an evaluation of USAID's accounting systems and administrative controls for compliance with laws, regulations, and reporting standards in the **AFR**, in the section titled *Analysis of Entity's Systems, Controls and Legal Compliance*. FMFIA requires management to provide a signed statement by September 30 of each fiscal year. The reporting requirements are:

a. **Reporting Pursuant to Integration of Enterprise Risk Management and Internal Control**. Assurance is based on USAID's process to identify risk and establish controls or integrate existing controls to the identified risk. (Continued reporting to OIG and/or a private accounting firm is required until full implementation of an ERM process.)

b. **Reporting Pursuant to OMB Circular A-123, Appendix A**. Assurance is based on USAID's assessment, documentation, and reporting on ICOR.

c. **Reporting Pursuant to OMB Circular A-130, Appendix I**. Assurance is based on USAID implementing information security and privacy controls.

d. **Reporting Pursuant to Section 2, 31 U.S.C. 3512(d)(2)**. Assurance represents USAID's informed judgment as to the overall adequacy and effectiveness of internal control related to operations, reporting, and compliance and a report on material weaknesses in agency controls.

e. **Reporting Pursuant to Section 4, 31 U.S.C. 3512(d)(2)(B)**. Assurance represents USAID's financial management systems that comply with government-wide requirements.

596.3.6.1 Reporting by Assessable Units

Effective Date: 09/22/2022

To support the Administrator’s annual Statement of Assurance, AUs must provide an annual certification, to the next management level, on the overall adequacy and effectiveness of its internal control. AUs must consider information from various sources to assess the status of controls. The certification must include:

a. A statement that there is reasonable assurance that internal control is achieving the intended objectives;

b. A description of control deficiencies that are significant in the design or operation of internal control, and those that adversely affect the AUs ability to meet its internal control objectives. Categorize these deficiencies as significant and have USAID managers internally track and monitor them; and

c. A CAP and accompanying target completion dates with realistic milestones for significant deficiencies*.*

USAID encourages managers and staff to identify deficiencies. This not only reflects positively on USAID’s commitment to recognize and address management problems, but also promotes good government practices with emphasis on accountability and effectiveness. AUs must maintain documentation supporting management decisions in support of the annual certification that are easily accessible and available for internal/external review and audit.

596.3.6.2 Bureau/Independent Office Certification

Effective Date: 09/22/2022

AAs and Independent Office Directors must review certifications submitted by subordinate AUs to determine:

- The relative importance of each deficiency identified; and

- If identified deficiencies are significant and need to be included in the Mission and B/IO certification to the Administrator. Internal control deficiencies that are classified as material weaknesses or significant deficiencies must be included in the certification.

In the case of a significant deficiency or material weakness, each AA and Independent Office Director must submit a certification to the Administrator that indicates such a deficiency, using the format described in section **596.3.6.1**.

596.3.6.3 Review of Deficiencies

Effective Date: 09/22/2022

The EMCRIC must review the deficiencies reported by AA’s and Independent Office Directors. The EMCRIC then recommends to the Administrator which deficiencies are deemed to be material to USAID as a whole and must be reported as material weaknesses in the Administrator’s annual Statement of Assurance published in the

AFR. Then, the EMCRIC concludes if a significant deficiency is also a USAID material weakness by considering if the deficiency demonstrates the following characteristics:

a. Significant impairment in USAID's ability to achieve its objectives;

b. Use of resources is inconsistent with USAID's mission;

c. Violation of statutory or regulatory requirements;

d. Significant lack of safeguards against waste, loss, unauthorized use, or misappropriation of funds, property, or other assets;

e. Impairments in the ability to obtain, maintain, report, and use reliable and timely information for decision making;

f. Improper ethical conduct; and

g. Conflict of interest.

While identifying and assessing the relative importance of significant deficiencies and material weaknesses, consideration must be given to the independent opinion of the USAID OIG from the Agency's annual GMRA audits. The EMCRIC carefully considers if systemic weaknesses exist that adversely affect internal control across organizational or program lines.

596.3.6.4 The Administrator's Report on Management Responsibility for Internal Control and Enterprise Risk Management

Effective Date: 09/22/2022

A. The Report

M/CFO prepares the Administrator's annual Statement of Assurance (based on the Administrator's approval of EMCRIC decisions) for the **AFR**. The report must encompass program, operational, and administrative areas, as well as accounting and financial management. The report must include the following:

1. A statement that there is reasonable assurance that USAID's controls are achieving their intended objectives (the annual Statement of Assurance),

2. A summary of material weaknesses and significant deficiencies found in USAID's internal control, and

3. A summary of CAPs developed to address USAID's material weaknesses.

B. Management Assurance

The Administrator’s annual Statement of Assurance represents their informed judgment about the overall adequacy and effectiveness of internal control within USAID. The annual Statement of Assurance must take one of the following forms:

i. **Unmodified** statement (no material weaknesses reported);

ii. **Modified** Statement of Assurance, considering the exceptions explicitly noted; or

iii. Statement of **No Assurance** (no internal control processes in place or there are pervasive material weaknesses).

596.3.7 Staff Performance on Internal Control Responsibilities

Effective Date: 09/22/2022

Job descriptions should clearly indicate the degree of authority and accountability delegated to each position and the responsibilities assigned. Job descriptions and performance evaluations need to contain specific references to internal control-related duties, responsibilities, and accountability.

596.4 MANDATORY REFERENCES

596.4.1 External Mandatory References

Effective Date: 09/22/2022

a. **Chief Financial Officer’s (CFO) Act of 1990, Public Law 101-576**

b. **Federal Financial Management Improvement Act of 1996 (FFMIA) (P.L. 104-208)**

c. **Federal Information Security Modernization Act (FISMA 2014) (P.L. 113-283, 44 U.S.C. 3554)**

d. **Federal Managers’ Financial Integrity Act (FMFIA) of 1982 (P.L. 97-255)**

e. **Fraud Reduction and Data Analytics Act of 2015 (FRDAA)**

f. **Government Accountability Office’s (GAO) Standards for Internal Control in the Federal Government (GAO Green Book)** 2014

g. **Government Performance and Results Act (GPRA) Modernization Act of 2010 (P.L. 111-352)**

h. **OMB Circular A-123, Management's Responsibility for Enterprise Risk and Internal Control (2016) and its Appendices:**

- **OMB Circular A-123, Appendix A, Management of Reporting and Data Integrity Risk**

- OMB Circular A-123, Appendix B, A Risk Management Framework for Government Charge Card Programs

- OMB Circular A-123, Appendix C, Requirements for Payment Integrity Improvement

- OMB Circular A-123, Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996

i. OMB Circular A-130, Management of Federal Information as a Strategic Resource

j. Payment Integrity Information Act of 2019 (PIIA) (P.L. 116-117)

596.4.2 Internal Mandatory References

Effective Date: 09/22/2022

a. ADS 201, Program Cycle Operational Policy

b. ADS 502, The USAID Records Management Program

d. ADS 596mab, Governance Charter for Enterprise Risk Management and Internal Control at USAID

e. ADS 596mad, USAID Risk Appetite Statement

596.5 ADDITIONAL HELP

Effective Date: 12/13/2022

a. ADS 101saa, Statutory, Regulatory, and Other Mandated Management Officials

b. ADS 596sac, USAID Anti-Fraud Plan

c. ADS 596sad, Anti-Fraud Field Guide: Implementing the USAID Anti-Fraud Plan

d. Chief Financial Officers Council (CFO) and Performance Improvement Council (PIC) Playbook: Enterprise Risk Management for the U.S. Federal Government (ERM Playbook)

e. Committee of Sponsoring Organizations of the Treadway Committee (COSO) Framework

f. COSO Guidance on Enterprise Risk Management

g. **GAO Framework for Managing Fraud Risk in Federal Programs**

h. **USAID Enterprise Risk Management webpage**

i. **U.S. Government Accountability Office (GAO) Financial Audit Manual**

596.6 DEFINITIONS

Effective Date: 03/09/2023

See the **ADS Glossary** for all ADS terms and definitions.

Agency Financial Report (AFR)
An alternative to the Performance and Accountability Report as allowed by OMB Circular A-136. Together, the AFR, the annual Performance Report, and the Summary of Performance and Financial Information provide performance and financial information that enables Congress, the President, and the public to assess the performance of a Federal agency relative to its mission and the stewardship of the resources entrusted to it. (**Chapter 596**)

Assessable Units (AUs)
An organizational unit within USAID, i.e., Mission, Bureau, or Independent Office, that is required to submit an annual Statement of Assurance on the status of internal control and a Risk Profile to the next management level. All Missions, Bureaus, and independent offices are AUs. Additionally, lower-level organizational units can be AUs, as designated by the responsible Bureaus/Independent Offices/Missions. (**Chapter 596**)

Agency Secure Image and Storage Tracking System (ASIST)/Consolidated Audit and Compliance System (CACS)
A worldwide Web-based management information system which 1) provides for a repository of information, including FMFIA certifications, validity of obligations and review of unexpended balances certifications, and audit-related documentation that can be accessed and/or updated worldwide and 2) is used to track actions, the status of FMFIA material weaknesses and deficiencies, OIG management and performance challenges, A-123 and audit recommendations, and corrective action plans; submit requests for final action (closure); upload supporting documentation; and print reports. (**Chapters 591, 593, 596, 621**)

Control Deficiency
A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A design deficiency exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met. An operation deficiency exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively. (**Chapter 596**)

Control Environment
The organizational structure and culture created by management and employees to sustain operational support for effective internal control. (**Chapter 596**)

Corrective Action Plans (CAPs)
Management's plan of action that describes an internal control deficiency and provides a schedule, including milestones and target dates, to remediate the deficiency. Corrective actions must be cost-beneficial to implement. (**Chapter 596**)

Enterprise Risk Management (ERM)
Is a discipline that deals with identifying, assessing, and managing risks and is a component of a governance framework. It requires Federal leaders and managers who are responsible for establishing and achieving goals and objectives, to find opportunities to improve effectiveness and efficiency of operations. An enterprise-wide, strategically aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocation to ensure successful mission delivery. (**Chapter 596**)

Executive Management Council on Risk and Internal Control (EMCRIC)
Co-chaired by the Deputy Administrator for Management & Resources and Deputy Administrator for Program & Policy Oversight, or their designee, and is charged with reviewing and providing approval of USAID's FMFIA assurance statement, risk profile, and proposed corrective measures and risk response. Provides oversight for USAID's ERM practices and internal control systems. Reports to the Administrator, who provides final approval on the council's recommendations. (**Chapter 595 and 596**)

Fraud
Obtaining something of value through willful misrepresentation. Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk. (**Chapter 596**)

Internal Control
The organization, policies, procedures, and tools used to determine reasonable assurance that (a) programs achieve their intended results; (b) resources are used in accordance with the mission; (c) programs and resources are protected from waste, fraud, and mismanagement; (d) laws and regulations are followed; and (e) reliable and timely information is obtained, maintained, reported, and used for decision making. (**Chapter 596**)

Internal Control Over Reporting (ICOR)
Assessment category that includes financial (internal and external) reporting requirements as well as non-financial (internal and external) reporting requirements. (**Chapter 596**)

Internal Control Standards
The standards provide criteria for assessing the design, implementation, and operating effectiveness of internal control in Federal Government entities to determine if an internal control system is effective. (**Chapter 596**)

Management Accountability
The expectation that managers are responsible for the quality and timeliness of program performance, increasing productivity, controlling costs, mitigating adverse aspects of USAID operations, and assuring that problems are managed with integrity and in compliance with applicable law. (**Chapter 596**)

Management Councils on Risk and Internal Control (MCRIC)
A group of senior officials at the mission, bureau, or independent office level who provide oversight and assistance for the management control program and audit management issues. (**Chapter 595** and **596**)

Material Weakness
FMFIA overall: A significant deficiency, or combination of significant deficiencies, that is significant enough to report outside of the agency, such as the Office of Management and Budget and Congress. Generally, such a weakness would a) significantly impair the organization’s ability to achieve its objectives; b) result in the use of resources in a way that is inconsistent with USAID mission; c) violate statutory or regulatory requirements; d) result in a significant lack of safeguards against waste, loss, unauthorized use, or misappropriation of funds, property, or other assets; e) impair the ability to obtain, maintain, report, and use reliable and timely information for decision making; or f) permit improper ethical conduct or a conflict of interest. (**Chapter 596**)

Nonconformance
Instances in which financial management systems do not substantially conform to established financial systems requirements. Financial management systems include both financial and financial-related (mixed) systems. (**Chapter 596**)

Risk
The effect of uncertainty on entity objectives. (**Chapter 596**)

Risk Appetite
Provides broad-based guidance on the level and type of risk the Agency is willing to accept-based on an evaluation of opportunities and threats-to achieve the Agency’s mission and objectives. (**Chapter 596**)

Risk Assessment
An internal management process for identifying, analyzing, and managing risks relevant to achieving the objectives of safeguarding assets, compliance with relevant laws and regulations, and reliable financial reporting. (**Chapter 596**)

Risk Management
A process that aims to minimize the impact of unfortunate events or to prevent those events from occurring while also identifying opportunities to improve programs and operations. (**Chapter 596**)

Risk Profile
A prioritized inventory of an organization's most significant risks. Organizations use a risk profile to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. (**Chapter 596**)

Significant Deficiency
A deficiency or a combination of deficiencies in internal control that in management's judgment, need to be communicated to the next level of management because they represent significant weaknesses in the design or operation of an administrative, programmatic, operational, accounting, or financial internal control that could adversely affect overall internal control objectives. (**Chapter 596**)

Statement of Assurance
Represents USAID's informed judgment as to the overall adequacy and effectiveness of internal control related to operations, reporting, and compliance. (**Chapter 596**)

596_083123