



Governance Charter for Enterprise Risk Management and Internal Control at USAID

A Mandatory Reference for ADS Chapter 596

Full Revision Date: 08/24/2017
Responsible Office: M/CFO
File Name: 596mab_082417

TABLE OF CONTENTS

1. INTRODUCTION	3
1.1 Purpose	3
1.2 Objective	3
1.3 Authority	3
2. GOVERNANCE STRUCTURE	3
3. EXECUTIVE MANAGEMENT COUNCIL ON RISK AND INTERNAL CONTROL	4
3.1 Meetings	4
3.2 Membership	5
3.3 Decision-Making	5
3.4 Roles and Responsibilities	5
3.5 Executive Secretariat	6
4. RISK-MANAGEMENT COUNCIL	6
4.1 Meetings	6
4.2 Membership	6
4.3 Decision-Making	6
4.4 Roles and Responsibilities	6
4.5 Executive Secretariat	7
5. SENIOR ASSESSMENT TEAM	7
5.1 Meetings	7
5.2 Membership	7
5.3 Decision-Making	7
5.4 Roles and Responsibilities	8
5.5 Executive Secretariat	8
6. MANAGEMENT COUNCILS ON RISK AND INTERNAL CONTROL WITHIN BUREAUS AND INDEPENDENT OFFICES AND MISSIONS	8
6.1 Roles and Responsibilities	8
7. DEFINITIONS	9
ANNEX A: Governance Structure for ERM and Internal Control Systems	11

GOVERNANCE CHARTER FOR ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL AT USAID

1. INTRODUCTION

1.1 Purpose

This Governance Charter (Charter) expands the scope, responsibilities, and membership of the governance structure that oversees internal control at the U.S. Agency for International Development (USAID), to include enterprise risk-management (ERM). This Charter also establishes a new Risk-Management Council (RMC) responsible for overseeing implementation of the policies, processes, and procedures through which ERM governance occurs.

1.2 Objective

The objective of this Charter and its associated governance structure is to improve the accountability and effectiveness of USAID programs and support operations through implementation and support of ERM practices and internal control systems. This Charter emphasizes a holistic approach to risk management that is not only integrated and coordinated across the Agency, but goes beyond fiduciary and compliance risk to include strategic, programmatic and other risks, to optimize the Agency's overall risk-management performance. Successful implementation of this Charter will engage all Agency management, beyond the traditional ownership of internal control by the Chief Financial Officer, to enable the Agency to make better decisions, alleviate threats, and identify opportunities.

1.3 Authority

This Charter is issued under the authority of the Federal Managers' Financial Integrity Act (FMFIA) of 1982, as codified in [31 USC 3512](#), and the Government Performance Results Act (GPRA) Modernization Act, [Public Law 111-352](#). It is also issued pursuant to [OMB Circular No. A-123](#), as updated in 2016, which requires that Federal Departments and Agencies integrate ERM with internal control systems.

2. GOVERNANCE STRUCTURE

The governance structure described in this mandatory reference is designed to facilitate open, candid, and collaborative governance, so information flows both up and down the Agency, and across its organizational structures, to improve knowledge sharing and, ultimately, the quality of decision-making. This structure includes the following management and oversight bodies (see **Annex A: Governance Structure for ERM and Internal Control Systems at USAID**, at the end of this reference, for a graphic that depicts the relationships between these management and oversight bodies).

- The **Executive Management Council on Risk and Internal Control (EMCRIC)**, chaired by the Deputy Administrator, or designee, is the most senior body

charged with reviewing and providing penultimate approval of the Agency's FMFIA assurance statement, Risk Profile, and proposed corrective measures or risk response; and generally providing oversight for the Agency's ERM practices and internal-control systems. Both the Risk-Management Council (RMC) and Senior Assessment Team (SAT) report directly to the EMCRIC. The EMCRIC reports to the Administrator, who provides final approval on the EMCRIC's recommendations.

- **The Risk-Management Council (RMC)**, co-chaired by Deputy Assistant Administrators (DAAs) from the Bureau for Management (M) and the Bureau for Policy Planning and Learning (PPL), is responsible for assessing the roll-up of enterprise risks and "non-financial internal control", based on input from Bureau and Independent Office (B/IO) level MCRICs across the Agency, as well as "financial internal control" (see **Section 7: Definitions**), based on input from the SAT. The RMC evaluates the composite profiles and develops an Agency Risk Profile that presents an Agency-level "portfolio view of risk" (see **Section 7: Definitions**), coupled with proposed risk response, where appropriate, to the EMCRIC for its review and approval.
- The **Senior Assessment Team (SAT)**, chaired by the Agency's Chief Financial Officer (CFO), is responsible for taking an Agency-wide view of deficiencies in financial internal control, as identified through the FMFIA certification process, audit program, and any other related functions, and assessing, monitoring, and/or proposing appropriate corrective measures. The SAT reports financial internal-control deficiencies deemed to be material weaknesses to the Agency as a whole -- which will be included in the annual FMFIA assurance statement. It also provides SAT results to the RMC for inclusion, as appropriate, in the Agency Risk Profile (see **Section 7: Definitions**).
- **Management Councils on Risk and Internal Control (MCRICs)** provide management and oversight for ERM and internal-control. Each MCRIC is responsible for managing risks and internal control deficiencies faced by its "assessable unit (AU)" (see **Section 7: Definitions**), and preparing and submitting its FMFIA certification and Risk Profile to the RMC. There are two levels of MCRICs: one at the B/IO-level and one at the Mission/Washington office-level. In addition to assessing their own risks and internal controls, B/IO level MCRICs also assess the FMFIA certifications and Risk Profiles of their subordinate AUs and submit a composite FMFIA certification and Risk Profile that provide a B/IO-level portfolio view of risk to the RMC.

3. EXECUTIVE MANAGEMENT COUNCIL ON RISK AND INTERNAL CONTROL

3.1 Meetings

The Deputy Administrator or his/her designee will chair the EMCRIC. The Chair will call and preside over EMCRIC meetings, which take place at least semi-annually, generally in the Spring and Fall. On voting issues, the Chair will have one vote.

3.2 Membership

In addition to the Chair, the Committee must consist of the following members:

- The Agency Counselor;
- Assistant Administrators (AAs) of Bureaus and Heads of Independent Offices;
- Statutory Officers: Chief Financial Officer (CFO), Chief Information Officer (CIO), and Chief Acquisition Officer/Procurement Executive (CAO);
- Director, M/MPBP; and
- Inspector General (IG) (non-voting observer).

On voting issues, each member will have one vote (except for the Inspector General).

3.3 Decision-Making

Most issues should be settled by consensus facilitated by the Chair. On issues requiring a vote (as determined by the Chair), voting will require a quorum. A quorum is defined as a simple majority of the voting members (or their designees). Issues will be decided by a simple majority of voting members. The EMCRIC's decisions are binding, unless overruled by the Administrator.

3.4 Roles and Responsibilities

- Provides oversight and responsibility for the identification, assessment, and treatment of the Agency's key enterprise risks;
- Approves and communicates the Agency's overall ERM strategy and approach, including the Agency's risk appetite to serve as a guidepost for the assessment, treatment, and monitoring of key enterprise risks across the Agency;
- Reviews the Agency Risk Profile, including proposed risk responses, presented by the RMC, and recommends the final Agency Risk Profile to the Administrator;
- Provides oversight and responsibility for the identification, assessment, correction, and monitoring of internal-control and audit deficiencies;
- Reviews recommendations from the SAT regarding whether the Agency has corrected a significant deficiency or material weakness has been corrected; and recommends approval or disapproval to the Administrator; and
- Reviews recommendations from the SAT regarding deficiencies deemed to be material weaknesses to the Agency as a whole that should be included in the

annual FMFIA assurance statement, and recommends approval or disapproval to the Administrator.

3.5 Executive Secretariat

M/CFO, with assistance from M, PPL, and others across the Agency, as needed, will support the EMCRIC. The Secretariat will maintain an archive of EMCRIC decisions, minutes, and other documents, and provide support for communications and follow-up.

4. RISK-MANAGEMENT COUNCIL

4.1 Meetings

Deputy Assistant Administrators (DAAs) from the M Bureau and PPL will co-chair the RMC. The co-chairs will call and preside over the RMC meetings, which must take place at least semi-annually. On voting issues, the co-chairs will each have one vote.

4.2 Membership

In addition to the co-chairs, the Council must consist of the following members:

- DAAs or Deputy Heads of B/IOs; and
- Deputies to the Statutory Officers (Deputies to the CFO, CIO, and CAO) (non-voting).

On voting issues, each B/IO member will have one vote.

4.3 Decision-Making

The Council should settle most questions by consensus, facilitated by the co-chairs. On issues requiring a vote (as determined by the co-chairs), voting will require a quorum. A quorum is defined as a simple majority of the voting members (or their designees). Issues will be decided by a simple majority of voting members. RMC decisions are binding, unless overruled by the EMCRIC.

4.4 Roles and Responsibilities

- Reviews and clears core policies and procedures with respect to ERM, including overseeing a process to define and iteratively update the Agency's Risk Appetite and risk tolerance (balancing risk with opportunities), and establishing a strong reporting and analysis system to enable effective portfolio views of risk;
- Reviews and approves briefing materials, issue papers, presentations, memoranda, reports, and other formal documents on the Agency's ERM and non-financial control activities;

- Prioritizes and evaluates submitted risks by B/IO level MCRICs and any significant risks identified through audits; identifies aggregate risk levels, concentrations of risk, and/or risks that could have a significant impact on the mission-level outcomes of the Agency; ensures that current risk levels are consistent with any thresholds established in the Agency's Risk Appetite and Tolerance; and proposes options for addressing the most significant risks, where appropriate;
- Establishes or updates the Agency's Risk Profile at least semi-annually, or as needed; and
- Submits the Agency Risk Profile, including options for addressing the most-significant risks to the Agency, to the EMCRIC for its review and approval; and elevates any other critical issues or decisions related to ERM to the EMCRIC in a timely manner.

4.5 Executive Secretariat

M/CFO, with assistance from M, PPL, and others across the Agency, as needed, will support the RMC. The Secretariat will maintain an archive of RMC decisions, minutes, and other documents, and provide support for communications and follow-up.

In addition, each B/IO, or their designee, must designate a Risk-Management Liaison (RML), and inform the Secretariat of this appointment. The RML will also support the Secretariat, as needed.

5. SENIOR ASSESSMENT TEAM

5.1 Meetings

The CFO will chair the SAT. The Chair will call and preside over SAT meetings, which must take place at least semi-annually. On voting issues, the Chair will have one vote.

5.2 Membership

In addition to the Chair and the other Statutory Officers (CIO and CAO), the CFO will identify each B/IO deputy head required to participate in the SAT, based on the financial internal-controls issue the team will address.

5.3 Decision-Making

The SAT should settle most questions by consensus facilitated by the Chair. On issues requiring a vote (as determined by the Chair), voting will require a quorum. A quorum is defined as a simple majority of the voting members (or their designees). Issues will be decided by a simple majority of voting members.

5.4 Roles and Responsibilities

- Determines the scope, design, and methodology of the [OMB Circular A-123 Appendix A](#) assessment;
- Ensures clear communication throughout the Agency of the objectives of the financial reporting assessment according to [OMB Circular A-123](#);
- Ensures the completion of the financial-reporting assessment in a thorough, effective, and timely manner;
- Identifies and ensures the Agency makes available adequate funding and resources for internal-control assessments;
- Ensures that senior staff effectively manage audit follow-up responsibilities;
- Makes recommendations to the EMCRIC regarding which internal control deficiencies are deemed to be material weaknesses to the Agency as a whole, and should therefore be included in the annual [Federal Managers' Financial Integrity Act \(FMFIA\)](#) assurance statement and reported in the agency's Annual Financial Report (AFR) ([OMB Circular A-136 Federal Financial Reporting](#));
- Makes recommendations to the EMCRIC when the Agency has taken sufficient action to declare that it has corrected a significant deficiency or material weakness; and
- Reports its major findings and recommendations to the RMC for consideration in the Agency Risk Profile.

5.5 Executive Secretariat

M/CFO staff will support the SAT and its members. The Secretariat will maintain an archive of SAT decisions, minutes, and other documents, and provide support for communications and follow-up.

6. MANAGEMENT COUNCILS ON RISK AND INTERNAL CONTROL WITHIN BUREAUS AND INDEPENDENT OFFICES AND MISSIONS

Each B/IO and Mission MCRIC should establish its own governance structure and rules of engagement, in accordance with the overall Charter established herein and the roles and responsibilities set forth in **Section 6.1**. For Missions and Regional Missions/Platforms, the next management level is respective Regional Bureaus.

6.1 Roles and Responsibilities

- Identify key risks and internal control deficiencies by using a structured and systematic approach;

- Analyze and evaluate risks and internal control deficiencies, considering the causes, sources, probability of the risk, the potential positive or negative outcomes; and prioritize the results of this analysis;
- Systematically identify and assess a range of risk response options, guided by the Risk Appetite (see **Section 7: Definitions**) and tolerance thresholds approved by the EMCRIC;
- Respond to risks and prepare and execute the selected response strategy;
- Monitor and review risk performance to determine whether the implemented risk management options achieved the stated goals and objectives;
- Prepare and submit the B/IO or Mission Risk Profile and FMFIA certification;
- Regularly review risk to monitor whether or not the B/IO or Mission Risk Profile has changed; and make provisions for alerting the appropriate level of management in Washington and at Post to new or emerging risks, as well as changes in already identified risks; and
- In addition to the above roles and responsibilities, MCRICs at the B/IO level will review and assess FMFIA certifications and Risk Profiles of their subordinate AUs and submit a composite FMFIA certification and Risk Profile that provides a B/IO's portfolio view of risk to the RMC.

7. DEFINITIONS

Assessable Unit (AU)

An organizational unit within USAID required to submit a statement of assurance on the status of internal control and an organizational Risk Profile to the next management level. All B/IOs and Missions are AUs. In addition, lower-level organizational units, such as divisions or offices within B/IOs or Missions, may be AUs, as designated by the responsible B/IO or Mission.

Enterprise Risk Management (ERM)

An 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 only within silos.

Financial Internal Controls

Internal controls primarily focused on effective and efficient financial operations, and financial reporting and compliance.

Non-Financial Internal Control

Internal controls primarily focused on effective and efficient non-financial operations, and non-financial reporting and compliance.

Portfolio View of Risk

Insight into all areas of organizational exposure to risk (such as reputational, programmatic performance, financial, information technology, acquisitions, human capital, etc.) to increase the Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the operating environment.

Risk

The effect of uncertainty on objectives.

Risk Appetite

The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision.

Risk Management

A series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives.

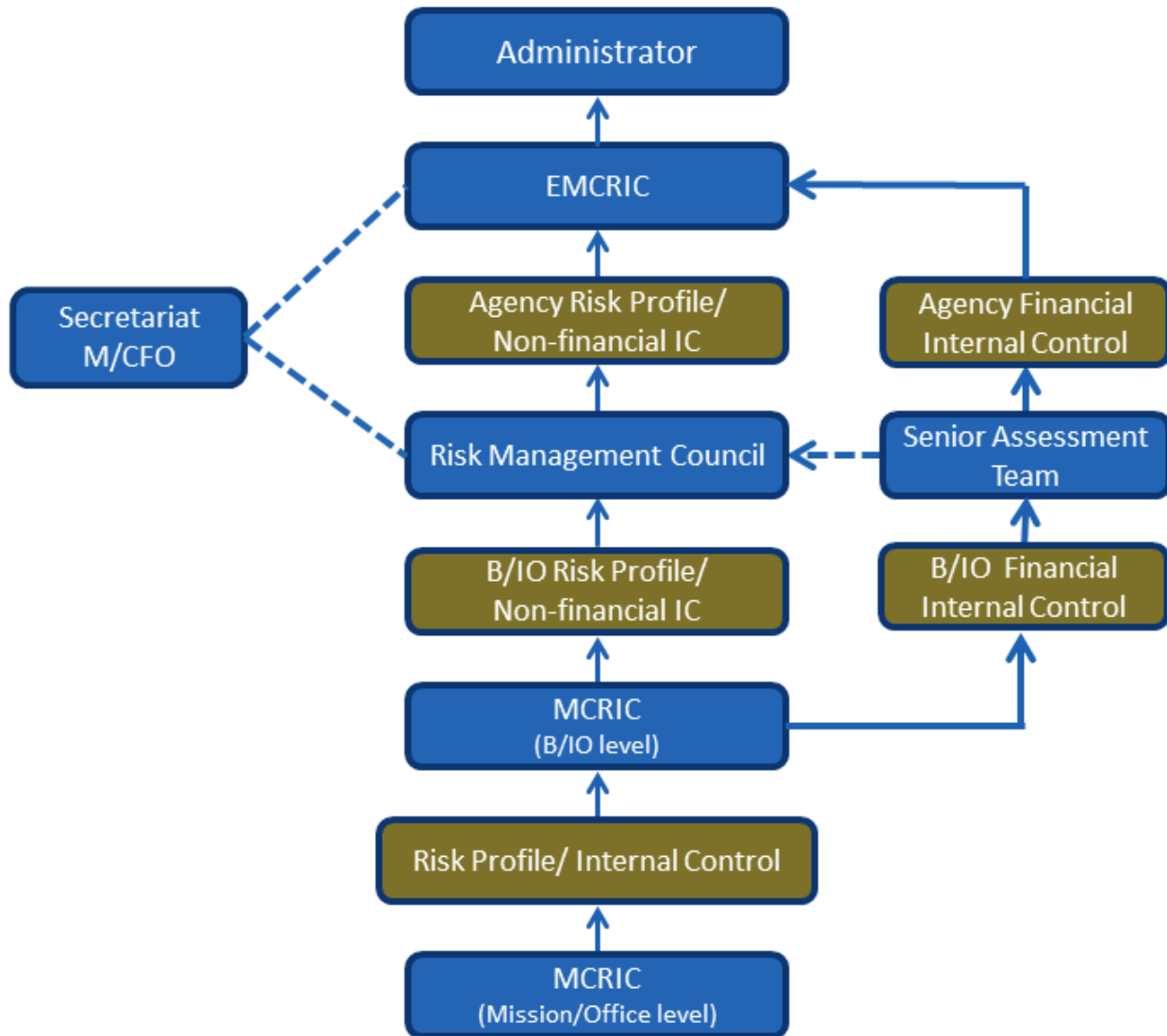
Risk Profile

According to OMB Circular A-123 Section II (B), a document that provides thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives that arise from its activities and operations, and appropriate options for addressing significant risks.

Risk Tolerance

The acceptable level of variance in performance relative to the achievement of objectives, with special consideration to the relative importance of related objectives. Risk tolerance must align with risk appetite.

ANNEX A: Governance Structure for ERM and Internal Control Systems



NOTE: The above diagram is intended to reflect the upward decision-making process of prioritization and treatment of risks through the risk profile and internal control processes. However, the EMCRIC, under the guidance of the Administrator and supported by the RMC, will provide downward communications and guidance on risk appetite and the balance among objectives, resources, and risks.