

Capacity Statement

Risk Management

SUMMARY

Catholic Relief Services (CRS) defines risk as a limitation that affects enterprise ability to carry out its mission. Risk is mitigated using preventive, detective, and management controls.

Preventive controls are measures that aim to prevent or reduce the likelihood of adverse events or incidents occurring. They are based on industry specific and general good practices, as well as on the analysis of identified risks and incidents that have affected or could affect CRS. Preventive controls also consider the operating environment and geographies where CRS operates and accommodate local conditions and challenges. CRS extends preventive controls to its subrecipients by assessing their risks and then deploying monitoring activities that correspond to the risk exposure. These preventive controls are defined and prescribed in CRS policies, procedures, and other standards, which CRS employees are oriented and trained in. CRS employees also acknowledge/accept their respective responsibilities and are held accountable for adherence to any applicable policy and/or standard.

Detective controls are integral aspects of CRS systems and routine activities which are designed to identify and respond to problems or incidents that may affect the organization's ability to carry out its mission. These controls include regular internal audits and compliance monitoring, as well as external audits by independent third parties. CRS also encourages and protects whistleblowing as a way of reporting any suspected fraud, ethical misconduct, or non-compliance. These mechanisms help CRS to ensure that its policies and procedures are followed and that any deviations are detected and corrected promptly.

Management controls involve the implementation of standards-based activities that enable CRS to respond quickly and efficiently to risk generating incidents before they escalate and have significant consequences for the agency and affected parties. These controls are manifested in CRS' robust, policy-driven system for managing incidents reported by internal and external parties. Incident management is a key aspect of CRS operations that ensures that reported incidents are addressed in a timely and effective manner, while adhering to the agency's standards of ethical conduct. CRS' incident management practices and outcomes are subject to a rigorous ethics program that ensures accountability and transparency via monitoring and evaluation of the agency's incident management practices and outcomes.

ORGANIZATION

Risk management is organized in accordance with CRS' governance frameworks and processes, and corresponds to the following structure:

- I. **Board level**, managed by Audit Risk Management (ARM) Committee of the Board.
- II. **Executive and Global Levels**, represented by the ELT and the Global cross-functional bodies.
- III. **Division and cross-divisional level**, represented by respective divisions covering functional areas.
- IV. **Project level**, managed by Project and Country Program Management Teams.
- V. **Audits**, represented and managed by Internal and External Auditors.





EXTENDED DESCRIPTION

I. Audit and Risk Management Committee (ARM) of the Board

The ARM, composed of independent Directors (board members), was delegated by the Agency's full Board of Directors to serve as its oversight and governance mechanism that will advise and hold management accountable for effective risk management (financial management, audit, compliance, technology, legal, security and ethics) to best affect the uses of resources to demonstrate the stewardship and good governance necessary for the Agency to execute its mission. The ARM convenes quarterly, coordinates its activities with other board committees, and escalates critical matters to the full Board.

II. Executive and Global level

1. The **Agency's President & CEO** is the ultimate risk owner. Per policy, organizational structures, and/or other delegations, the CEO assigns responsibilities and accountability for risk management to the Executive Leadership Team, Division leadership, and select cross-functional bodies charged with risk strategy, compliance oversight, financial stewardship, and operational excellence (*see more under sections II.2.a and III*).
2. Global cross-functional bodies charged with oversight, support, and/or advisory responsibility that informs Executive Leadership and Board decision making are:
 - a. The **Enterprise Risk Management (ERM) Council** is made up of twelve cross-division risk champions, chaired by the Senior Director of GRC & ERM, who identify and evaluate strategic risks, and monitor management's risk response progress for such risks that impact threats and opportunities which influence achieving strategic objectives. The ERM Council also provides oversight for the risk appetite policy and confirms management recommendations for the use and maintenance of the Agency's net asset reserves. These resources are utilized (per the Board approved protocols) to address extraordinary risks and opportunities (financial or programmatic) which are largely outside of management's control to plan for via routine operating cycles.
 - b. The **Compliance Council**, chaired by the Sr Director GRC & ERM provides systematic analysis and management action planning/ learning to affect adherence to applicable compliance requirement and regulatory standards. It serves as a dedicated advisory body to help the Senior and the Executive VPs for Overseas Operations resource, identify, assess, and resolve global compliance risks.
 - c. The **Fraud Allegation Management (FAM) Council** (also known as FAM Steering Group) is a dedicated body whose main function is to provide advice to the Director of Fraud Operations on fraud allegations pertinent to Overseas Operations and enable cross-divisional transparency, internal control improvement, sharing and learning.
3. The **Global Risk & Compliance (GRC) Team**, led by Sr Director for GRC & ERM, is responsible for: a) Providing strategic direction and oversight to OverOps global compliance systems, internal and external, and b) Managing global risk and compliance programs and portfolios, and implementation of compliance & risk strategy for overseas operations.
4. The **Fraud Oversight Team**, led by Fraud Operations Director, is responsible for the agency's Fraud Allegation Management (FAM) system. The team monitors and analyzes the fraud risks and controls across the business units and functions and provides guidance and recommendations to mitigate them. The team also conducts investigations and audits on suspected or reported fraud cases and reports the findings and outcomes to the senior management and external stakeholders. The team works closely with other internal and external parties, such as the legal, compliance, risk, audit, to coordinate the fraud response and recovery efforts.
5. The **Safeguarding Team** function, led by the Safeguarding Director, is to protect the welfare and well-being of children and vulnerable adults who are involved in CRS activities or services. The safeguarding team is responsible for ensuring that all staff and volunteers are trained and vetted according to CRS policies and procedures, and that any concerns or allegations of abuse are reported and handled appropriately. The safeguarding team also provides advice and guidance to staff and volunteers on how to prevent and respond to safeguarding issues and works with external agencies and partners to promote a safe and supportive environment for everyone.

III. **Divisional Risk Management Frameworks**

The divisional risk management framework is based on the identification, assessment, and mitigation of CRS' global risks related to accounting & finance, supply chain, knowledge & information management, people resources, and operations. Divisional leadership ensures that the risk mitigation standards and processes, including internal controls, are documented in applicable policies and procedures. These policies and procedures are checked for compatibility with applicable U.S. Federal Government, Global Fund, and other major donor requirements, deployed worldwide, and supported by periodic training activities and robust compliance programs. The responsible departments provide periodic assurance for the implementation of these policies and procedures and produce reports where applicable. The responsibility and accountability related to various aspects of the divisional policies are assigned to the relevant stakeholders, both in the field and headquarters. These documents are published, updated, and disseminated periodically.

IV. **Project-level**

Project-level risk management activities normally start with preliminary risk identification and assessment activities, followed by determining and implementing risk mitigation options and strategies (see Appendix). The risk-identification processes and tools vary by project and are optimized to donor requirements,, third-party (sub-recipient and vendor) risks, and the local environment (compensating controls), and integrate both cross-divisional and division-centric risks as well as internal and external assurances as applicable (audits). Project-level risk management custodians are the project managers or chiefs of party, under the leadership and targeted oversight of the country senior management teams, normally comprised of the Country Representatives, the Heads of Operations, the Heads of Programs, and other senior personnel.

V. **Audits**

CRS' internal audit function provides an independent in-house opinion regarding the implementation of the agency's internal controls. In addition to the in-house opinion, CRS hosts an external auditor to conduct an annual assessment of CRS operations funded by U.S. Federal Government. The same auditor produces CRS' annual audited financial statements. Internal Audit provides assurance on the implementation of the policies and procedures. The auditors survey the application and provide their independent opinion on compliance. On a quarterly basis, the Director of Internal Audit reports out to the Audit and Risk Management Committee on the implementation of the annual audit plans audit findings trends, implementation of audit recommendations, and other audit related matters that are of importance to the committee. Internal audits of overseas programs include regular visits to high risk implementing partners to assess internal control capacity. The Sr Director of Internal Audit also works closely with the Agency's external auditor who receives all copies of internal audit reports completed during the period covered by the external audit. Every September, the Sr Director of Internal Audit presents a risk based internal audit plan to the Audit and Risk Management Committee for approval. The CRS Internal Audit Department conducts an average of 17 internal audit engagements per year of overseas country programs and headquarter operations. CRS' internal audit function regularly undergoes Quality Assurance Reviews (QAR) per the International Standards for the Professional Practice of Internal Auditing (Standards). Every year, the Department conducts a quality assurance self-assessment, which is validated by an independent quality assurance reviewer every five years.



APPENDIX: PROJECT LEVEL RISK MANAGEMENT BY DESIGN CYCLE



Design

Risk prediction in planning
(Project activities are designed by taking into consideration the probable project specific risks. In this phase it's critical to make weighted decisions regarding activities, scope and partnership by using the risk management principles of avoidance, transfer, mitigation and acceptance. The risk mitigation planning should include both high-level risks as well as project activity specific mitigation activities and strategies.)



Start-up

Risk prediction and mitigation, validation and adjustment. (The mitigating activities and risk acceptance predicted in the design stage are validated or readjusted. This is a unique opportunity to revisit the activities and identify the opportunities for risk avoidance or transfer.)

- Risk validation, adjustment, analysis and new risk planning (if not already covered in design phase),
- Setting-up risk management systems (establishing risk tolerances, escalation procedures, and project boards/governance systems).



Implementation

Risk mitigation monitoring and reporting. (The PM/Designate monitors the implementation of risk mitigation plan/activities and tracks the accepted risks. The new risks and risk incidents are reported.)

Risk tracking and handling. (Materialized risks and incidents are tracked and responded; risk register is updated.)

Learning/systems Improvement, local and/or global. (Internal systems and project activities are improved based on incidents and other learning.)



Closeout

Learning/systems Improvement, local and/or global. (Internal systems and project activities are improved based on incidents and other learning.)