CAPACITY STATEMENT | RISK MANAGEMENT

SUMMARY

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

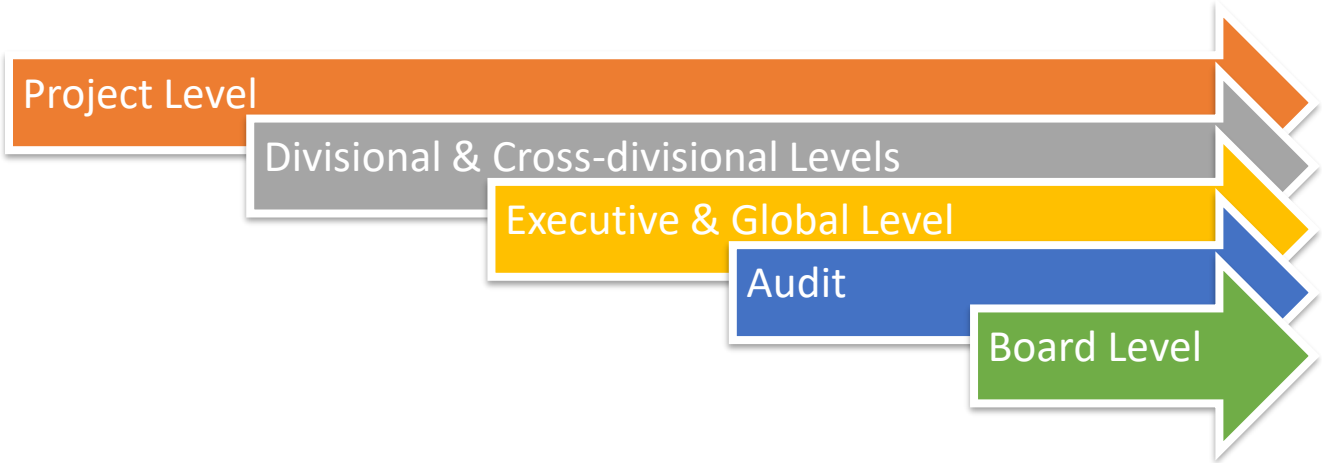
Preventive controls are established in accordance with industry specific and general good practices and are informed by previously identified risks and prior incidents, while considering the operating environment and geographies where CRS operates. These controls extend to CRS subrecipients; CRS assesses its subrecipients to determine risks and then deploys monitoring activities that correspond to the risk exposure. These preventative controls are described in CRS policies, procedures, and other standards. CRS employees are oriented and trained in them, accept their respective responsibilities, and are held accountable.

Detective controls are an integral part of CRS systems and routine activities. They are reflected in the required segregation of duties as well as independent and transparent verification of activities and decisions by in-country, regional, and headquarters personnel (including internal and external auditors). CRS has a response mechanism in place for reactive-detective controls that address suspicions and allegations identified by beneficiaries, communities, subrecipient and partner staff via CRS internal and external whistleblowing channels.

CRS' management controls are manifested in its robust system for managing incidents reported by internal and external parties. Senior personnel representing relevant divisions and departments oversee that management of reported incidents. The management controls include investigation, reporting and system improvement processes through which new internal controls and compensating controls are established.

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 level**, managed by the CEO and global councils
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. **Independent 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 audit, compliance, technology, legal, and tax) to best affect the uses of resources to demonstrate the stewardship and good governance necessary for the Agency to execute is 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 and 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 stewardships, 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 Head of Internal Audit & Enterprise Risk, 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 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 Director for Global Compliance & Risk, 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 Vice President for Overseas Operations resource, identify, assess, and resolve global compliance risks.

    c. The **Fraud Allegation Management (FAM) Steering Group** is a dedicated body whose main function is to provide advice to Director of Risk Management & Security on fraud allegations pertinent to Overseas Operations and enable cross-divisional transparency, internal control improvement, sharing and learning.

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, human resources, and operations. Division 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[1], 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 a Country Representative, a Head of Operations, a Head 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 as well as an annual opinion on each of CRS' Global Fund PR grants. 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 to discuss recent internal audits, trends, implementation of audit recommendations, and fraud allegations. Internal audits of overseas programs include regular visits to high risk implementing partners to assess internal control capacity. The Director of Internal Audit also works closely with the Agency's external auditor (currently RSM). RSM receives all copies of internal audit reports. Every September, the 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 20 internal audits per year of overseas country programs and headquarter operations. In addition, the Internal Audit Department conducts capacity training and education and technical assistance projects on proper control systems, business process improvement for risk control, participates in the investigation of fraud allegations, administers, with the Human Resources department, the Agency Whistleblower hotline, and serves in various working groups within the Agency. 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 year.

[1] CRS will use the Global Fund's Risk and Controls Matrix Template as the risk register and management tracking tool for its Global Fund programs.

APPENDIX: PROJECT LEVEL RISK MANAGEMENT BYDESIGN CYCLE

Design

Risk prediction and 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 partnerships 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 re-adjusted. This is a unique oportunity to revisit the activities and identify the oportunities 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.)*