RISK MANAGEMENT IN USAID

PROPOSED DEFINITION AND CONCEPTUAL FRAMEWORK

E5 LLC

NOVEMBER 2014

This document was produced for review by the support of the U.S. Agency for International Development (USAID) under the Knowledge-Driven Agricultural Development (KDAD) project, implemented by Insight Systems Corp. The views expressed are those of the author and do not represent the views of the United States Agency for International Development or the United States Government.

INTRODUCTION

As part of the USAID Forward reform process, new attention is being given to the Agency's policies and systems for addressing risks that might undermine the achievement of USAID's priority development goals. The Local Systems Framework has identified three areas in which USAID needs to improve risk management practices, which are summarized here:

- Create opportunities to think about risks comprehensively and comparatively;
- Consider risks and rewards in setting program goals; and
- Calibrate risk mitigation measures to the risks faced in a given country or project.

The first phase of FIRM comprises an assessment of the risk landscape in which USAID operates, beginning with a review of its existing risk management practices including Sustainability Analysis, PFMRAF Stage 1 and Stage 2, Organizational Capacity Assessments, Pre-Award Surveys, the USAID Program Cycle, and risk training offered by the Agency. This document summarizes some definitions and approaches to risk management currently used in the private and public sectors, and proposes a conceptual framework for understanding how current USAID practices map against contemporary standards and practices.

1. Risk Management Background

The term "risk" is subject to different interpretations around the world and therefore different definitions have been applied to the practice of risk management. Managers make daily decisions involving some form of risk by applying their judgment based upon experience and professional training, while in other cases formal risk policies or guidelines may be applied and monitored by specialized staff. Concepts such as Integrated Risk Management (IRM) and Enterprise Risk Management (ERM) have evolved in part because of business failures which prompted the search for measures which could mitigate such occurrences in the future (well-known examples include Enron, AIG, Lehman Brothers, among others). The insurance industry and the accounting profession have been two of the most prominent sources of training and development of standards and other tools for risk management. Much of the ERM literature focuses on the design and operation of internal controls to ensure that management's risk mitigation strategies and policies are properly carried out and respond appropriately to new information. In the United States, this has been given additional prominence as a result of the Sarbanes-Oxley Act of 2002 (Public Law 107-204) which requires the top management of publicly-held companies to individually certify the accuracy of financial information. Sarbanes-Oxley also increased the oversight role of boards of directors, the independence of external auditors who verify the accuracy of financial statements, and greatly increased penalties for fraudulent actions by management and for retaliation against whistleblowers.[i] Over time the range of issues being addressed under the rubric of risk management has grown: business continuity and IT security are two areas of current focus in ERM, for example. Also, the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 (Public Law 111-203) has introduced a significant number of new requirements which are intended in part to reduce risks across the U.S. banking and financial services sector.

One widely used international standard is ISO 31000 which defines risk as "the effect of uncertainty on objectives" and defines risk management as "coordinated activities to direct and control an organization with regard to risk." ISO Guide 73 "Risk Management Vocabulary" clarifies that the effect of risk may be positive, negative, or a deviation from the expected; risk is often described by "an event, a change in circumstances or a consequence;" related is ISO 31010 "Risk Assessment Techniques" which describes several tools for risk assessment in different situations.[ii] Unlike some other ISO standards, such as ISO 9000 on Quality Assurance, ISO 31000 is not intended as a certification standard but is a flexible standard which can be adapted by private or public sector organizations to their specific needs. ISO 31000 is very similar to the British Standard BS31100, and was largely based on the Australian and New Zealand Standard AS/NZS HB4360 with additional inputs provided by Switzlerland, France, and Brazil, and implementation guidelines based on documents from Australia, New Zealand and Canada.[iii] In 2004 the UK Government published the "Orange Book – Management of Risk" (M_o_R) and a series of guidance documents which are specifically aimed at public agencies, including an analysis which maps the contents of M_o_R against ISO 31000.[iv] To date there is not a similar framework in the US which focuses on risk management within public agencies.

In the United States, one of the most widely used approaches to risk management is sponsored by COSO (the Committee of Sponsoring Organizations) which resulted from the National Commission on Fraudulent Financial Reporting (the Treadway Commission) whose 1987 report identified recommendations and good practice standards for financial reporting in public companies.[v] In 2004 COSO published a framework for enterprise risk management (ERM) which it defines as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[vi] The COSO framework gives particular emphasis to the responsibility of the board and its members, which is helpful in focusing senior management attention on understanding risk as a strategic topic, not simply a matter for lower-level processes and compliance functions. COSO represents a number of associations of financial professionals, including the American Accounting Association, the American

Institute of Certified Public Accountants, Financial Executives International, Association for Accountants and Financial Professionals in Business, and the Institute of Internal Auditors.

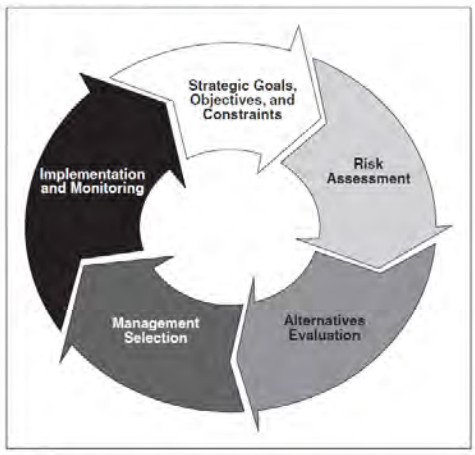
The Federation of European Risk Management Associations (FERMA) represents risk management and insurance associations, and defines risk management as "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities."[vii] FERMA is largely similar to COSO and ISO 31000 in calling for a continuous process of monitoring the performance of risk management processes. Whereas COSO is primarily identified with the private sector, FERMA includes the UK-based National Forum for Risk Management in the Public Sector.

Other standards also exist, such as the "Red Book" published by the Open Compliance and Ethics Group (OECG) which promotes risk management under the label of "GRC" – governance, risk management and compliance (see www.oceg.org); the regulatory standard "Solvency II" which came into effect in 2012 and which applies to insurance companies operating in the European Union; the Basel II and Basel III regulatory standards for banks, and the 2010 Dodd-Frank Act in the US which addresses many aspects of the US financial services sector. These are not considered here as they have little direct relevance to the mission or structure of USAID.

One body of guidance which directly applies to USAID is OMB Circular A-123, which applies to all US Executive Branch bodies. In Appendix A, OMB defines risk management as "an internal management process for identifying, analyzing and managing risks relevant to achieving the objectives of reliable financial reporting, safeguarding of assets and compliance with relevant laws and regulations."[viii] As with of the other frameworks described above, A-123 primarily addresses internal controls and fiduciary responsibilities and does not directly address operational or programmatic risks. Some efforts have been made to identify elements of ERM which are relevant to public sector entities, while ISO 31000 is intended to be applicable to both private sector and public sector organizations.

The GAO has proposed a risk management framework for the Department of Homeland Security which draws from private sector approaches such as COSO, but notes that application of such risk management tools is handicapped by lack of consensus on definitions or risk, and also notes that Congressional authorizing and funding of federal agencies is a significant constraint on how managers approach risk management.[ix]

Figure 1: GAO Risk Management Framework



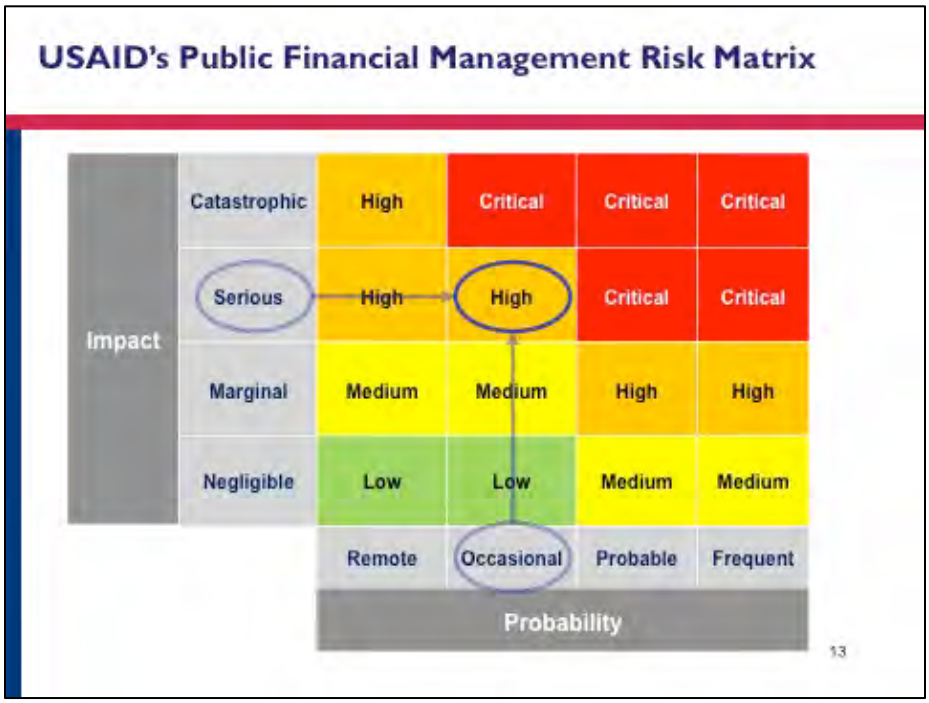
Source: GAO.

2. Common Risk Management Factors

Risk management frameworks often refer to the need for management to establish an "appetite" or degree of tolerance for risk as part of the overall responsibility for institutional governance. Mitigation of risk may be done in various ways, for example through insurance coverage, portfolio balancing (combining riskier and less risky

business lines or locations), and pricing of risk though market mechanisms. The corporate internal control process monitors how well these mechanisms are operating, and assesses whether indicators of risky behavior or situations are being appropriately communicated to senior management. In regulated industries such as banking, "stress tests" may periodically be undertaken by external authorities to ensure that appropriate reserve requirements are in place to mitigate the risk of unexpected market losses. COSO workshops are another mechanism for verifying that internal control procedures are operating effectively, and that staff are aware of risk management policies and feel empowered to raise issues with senior management.

Risk management frameworks usually include metrics for estimation of (i) the likelihood of a risk materializing, and (ii) the degree of severity of consequences if this happens, frequently illustrated in the form of a matrix or "heat map" (see example from USAID PFMRAF, below). Corporate managers may assign different weights to risks in one category, for example an unsuccessful product launch or supply chain interruption which loses money for the firm, compared with another risk such as non-compliance with a law or regulation which exposes the firm to possible legal sanctions and reputational harm, or unethical behavior which attracts negative publicity and damages the company's "brand." The concept of "risk appetite" acknowledges that not all risk can be avoided, and highlights that there can be legitimate potential to reap higher returns from riskier ventures, provided that this is done consciously and with effective oversight from senior management and the board.



For Federal agencies, OMB Circular A-123 provides guidance to managers on internal controls and management of risks but does not address the concept of "risk appetite" in the use of public funds or potential for misuse or loss. This is an important difference: OMB A-123 specifically addresses financial reporting, while the ERM literature describing the upside potential of accepting risk is not suggesting that managers take risks with fiduciary or statutory responsibilities, but that they need to balance risk and reward potential in various aspects of their business operations. Current ERM literature emphasizes that organizations exist for the purpose of creating value – whether financial or in other forms – and therefore risk management should be understood as something which involves consciously weighing the risks of negative events against the potential benefits from a particular activity.

"Tolerate" is not an option for managing risk at USAID.

PFMRAF Training Manual

The concept of consciously accepting a policy of tolerance for risk is much more readily accepted in the private sector than in the public sector, which delivers public services which are financed by appropriated funds. However, the OECD has proposed a typology of risk to be used by donor agencies operating in fragile or transitional environments. This model explicitly recognizes that the "business" of development assistance is inherently risky and concludes that donor agencies need better instruments with which to identify and manage risks. The OECD framework includes three categories of risk:

- contextual risk, which arises from factors within the country or setting in which aid is delivered;
- programmatic risk, which results from the implementation of the agency's assistance interventions; and
- institutional risk, related to fiduciary losses or management failures which potentially harm the organization's reputation or domestic political support.

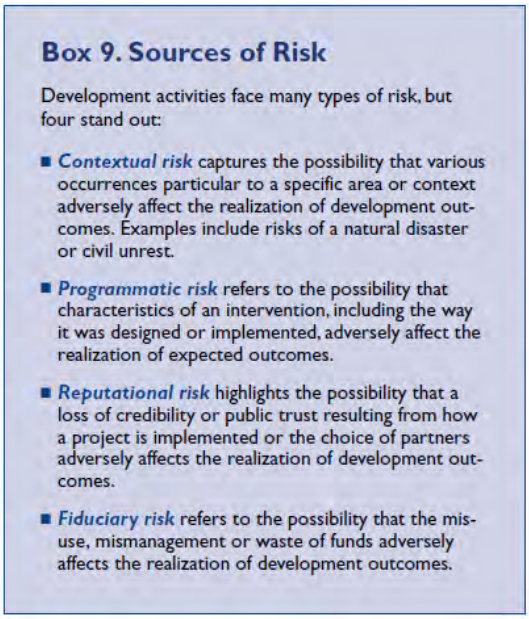
As shown in the graphic below, these categories are not homogenous but contain a degree of overlap—for example, local political instability may undermine program effectiveness and delivery of results, while environmental or other harm caused by a project may result in reputational damage to the aid agency. What sets this model apart from most risk management frameworks is its inclusion of operational risk arising from an agency's projects and programs, including country and political risks within the operating context, as well as risk that projects and programs may not achieve their objectives. The OECD typology was developed for aid donors working in the context of fragile or transitional settings, and is appropriate for USAID which operates in many such situations–in fact, the OECD report mentions the USAID Office of Transition Initiatives as an example. The OECD model specifically addresses risks associated with new or innovative approaches, including the failure to innovate, as well as risks and opportunities arising from using local systems—an important element of the USAID Forward initiative. OECD states that "risk management is not just about risk reduction: it is also about rebalancing risk and opportunity in such as way as to ensure the best overall outcome."[x]

Box 1.1. Categories of risk

- ***Contextual*** (or country, situational or external) risk: the range of potential adverse outcomes that could arise in a certain context: the risk of political destabilisation, a return to violent conflict, failure to develop, a humanitarian crisis and so on. It includes the risk of harm spreading beyond the country's borders.
- ***Programmatic*** (or intervention) risk relates to the risk of programme failure, *i.e.* the potential for interventions not to achieve their objectives or to exacerbate contextual risk.
- ***Institutional*** (or internal) risk relates to the range of potential adverse consequences of intervention for the implementing organisation and its staff. These consequences could range from management and fiduciary failure to reputational or political damage.

THE PRICE OF SUCCESS? AID RISKS AND RISK TAKING IN FRAGILE AND TRANSITIONAL CONTEXTS – © OECD 2011

USAID has slightly revised the OECD framework by dividing the third category, Institutional Risk, into two separate categories: (i) Reputational Risk, and (ii) Fiduciary Risk, as shown in the box below, resulting in a typology with four categories in all [xi] In other respects the USAID framework is fully consistent with the OECD approach, notably in emphasizing the need to consider both the potential benefits as well as potential threats when weighing development investments. It should also be kept in mind that there are many different ways of framing risk typologies–what is most important is that the selected approach lends itself to rigorous and comprehensive thinking about possible sources of risk as well as ways of avoiding or mitigating these. The OECD/USAID framework is consistent with the industry-standard approaches described previously, and has the additional advantage of being specifically designed for application to delivery of development assistance, often in fragile contexts and increasingly through country systems.



Box 9. Sources of Risk

Development activities face many types of risk, but four stand out:

- ***Contextual risk*** captures the possibility that various occurrences particular to a specific area or context adversely affect the realization of development outcomes. Examples include risks of a natural disaster or civil unrest.
- ***Programmatic risk*** refers to the possibility that characteristics of an intervention, including the way it was designed or implemented, adversely affect the realization of expected outcomes.
- ***Reputational risk*** highlights the possibility that a loss of credibility or public trust resulting from how a project is implemented or the choice of partners adversely affects the realization of development outcomes.
- ***Fiduciary risk*** refers to the possibility that the misuse, mismanagement or waste of funds adversely affects the realization of development outcomes.

Source: USAID 2014

In order to help USAID to better understand the risk landscape in which the Agency operations, the FIRM research team will use the modified OECD/USAID typology to map existing USAID control and oversight processes in terms of how adequately they cover (i) Contextual risks, notably in the countries in which USAID operates; (ii) Programmatic risks, related to the achievement of development outcomes of USAID interventions; (iii) Reputational risks, which may result in loss of domestic political support or funding, and (iv) Fiduciary risks which may result from misuse or lack of oversight of funds.

The team will identify areas in which USAID practice is currently appropriately aligned with industry good practice in each of these areas, as well as gaps which need to be addressed. The team will also seek to identify ways in which risk monitoring activities in various parts of the Agency are reported up to Management, and any mechanisms which may be in place for synthesis of risks across the portfolio. The team will specifically identify industry-standard references from ERM, ISO 31000, COSO etc. in its mapping of USAID risk management procedures; where USAID's development activities do not have a specific counterpart within these industry frameworks, the OECD typology will be used to provide a consistent analytical framework in order to structure the team's findings.

---

[i] *http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act*

[ii] ISO 31000 and ISO/Guide 73:2009(en); *http://www.iso.org*

[iii] A comparison of risk management standards is available from the Risk Insurance and Management Society (RIMS): "An Overview of Widely Used Risk Management Standards and Guidelines," *http:www.rims.org*

[iv] HM Treasury. *https://www.gov.uk/government/publications/green-book-supplementary-guidance-risk*

[v] National Commission on Fraudulent Financial Reporting. 2007. *Report of the National Commission on Fraudulent Financial Reporting*.

[vi] Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management–Integrated Framework*. 2004, p.2; *http://www.coso.org*

[vii] FERMA. *A Risk Management Standard*. *http://www.ferma.eu*

[viii] Implementation Guide for OMB Circular A-123, *Management's Responsibility for Internal Control*, Appendix A, *Internal Control over Financing Reporting*. OMB: July 2005, p.19

[ix] GAO-06-91 *Risk Management*. Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. Dec. 2005.
[x] OECD. 2011. *Managing Risks in Fragile and Transitional Contexts – the Price of Success?* *http://www.oecd.org/dac/incaf/48634348.pdf*
[xi] See USAID. *Local Systems: a Framework for Supporting Sustained Development*. April 2014; and *Country Systems Strengthening: Implications for Risk and Risk Management*. March 2013.