How to implement risk management to drive development impact

Lessons learned in implementing risk appetite frameworks

June 2020

Building a better working world

Lessons learned in implementing risk appetite frameworks

We have entered the final decade of global efforts to achieve ambitious 2030 Sustainable Development Goals (SDGs). The international development community and multilateral organizations are focused on marshalling, deploying and targeting their resources to maximize their contribution to the SDGs and drive up development impact.

In recent years, there has been a growing recognition that strengthening risk management within development agencies is a key component of driving up impact. In simple terms, the better the agencies identify, measure, manage and mitigate risks, the better risk decisions they can make. This means agencies can conduct more innovative, more complex or larger activities in more challenging environments and circumstances. In so doing, they will have more impact on the SDGs. The importance of effective risk management has never been so top-of-mind for development agencies, given the need to mobilize resources quickly in response to the evolving COVID-19 pandemic. Agencies need to determine the impact of the crisis on partner governments and on existing projects, as well as carefully monitor risks in emergency response activities.

Development agencies manage risks on a day-to-day basis, in some ways, better than anyone. Yet, their formal risk management capabilities are often not sufficiently mature. Organizations, such as the United Nations (UN), recognize the need to chart a road to mature risk management, so have started issuing guidance to support risk modernization. First, through its risk management taskforce under its High-Level Committee on Management (HLCM), the UN published its reference model for risk management[1] to help agencies – and others beyond the UN universe – to benchmark themselves across a range of areas, such as enterprise risk management, governance, processes, systems and tools, and risk culture.

Second, the UN HLCM risk management taskforce has begun issuing guidelines on enhancing certain aspects of risk management, initially its *Risk Appetite Statement Guidelines*.[2] The development and implementation of a risk appetite framework (RAF) and risk-specific risk appetite statements (RASs) is a critical starting point for development agencies.

Developing a RAF can be daunting, especially for organizations with nascent risk management. To help, this report outlines 10 lessons learned from the work of EY teams in supporting the efforts of public and private-sector organizations globally implementing a RAF and associated RASs. We believe these lessons learned will drive progress, through a pragmatic approach, tailored to development agencies.

---

1 https://www.unsystem.org/content/reference-maturity-model-risk-management-38th-session-oct-2019

2 HLCM Cross-Functional Task Force on Risk Management. (2019). *Risk Appetite Statement Guidelines https://www.unsceb.org/CEBPublicFiles/2019.HLCM_.26%20-%20Guidelines%20on%20Risk%20Appetite%20Statements%20-%20Final_1.pdf*

Ten key lessons learned

1. Good governance and leadership are critical to making risk appetite drive day-to-day change
2. An inclusive approach to risk appetite development helps to achieve necessary buy-in across the organization
3. Considering a range of benchmarks can support risk appetite development, although it still needs to be tailored
4. A common language surrounding risk must be established to unify and standardize risk management across the organization
5. Pragmatism is key in developing and refining risk appetite
6. Building an effective risk dashboard linked to thresholds and triggers enables risk oversight
7. Risk must be embedded in decision-making processes to bring about the desired change in behaviors
8. Build risk appetite into the broader ERM program/project
9. Communicate, communicate, communicate (and train)
10. Risk management is a journey

Key definitions[3]

Risk appetite: The aggregate amount (level and types) of risk an organization wants to assume in pursuit of its strategic objectives (and mission).

Risk appetite framework: The risk appetite framework is the approach through which: risk appetite is established, communicated, monitored and aligned to the organization's strategy; material risks to the organization are considered.

Risk appetite statement: A document that articulates the current risk appetite of an organization in various areas or levels.

Risk appetite scale: The defined levels of risk appetite that an organization can assign to different types of risk.

Risk tolerance: Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives; or put another way the boundaries of risk taking outside of which the organization is not prepared to venture in the pursuit of its long-term objectives.

[3] With exception of the definition for a risk appetite framework, these definitions are drawn from the HLCM Cross-Functional Task Force on Risk Management. (2019). Risk Appetite Statement Guidelines https://www.unsceb.org/CEBPublicFiles/2019.HLCM_.26%20-%20Guidelines%20on%20Risk%20Appetite%20Statements%20-%20Final_1.pdf

1 | Good governance and leadership are critical to making risk appetite drive day-to-day change

Effective risk management requires a strong, organization-wide governance structure that makes risk considerations a priority of the board and senior management. Without such leadership and commitment, efforts to enhance risk management may be perceived as a bureaucratic "compliance exercise" required by headquarters, as distinct from an important component of enabling more risk-taking and delivering more development impact.

Strong governance is at two levels:

- **Board governance:** Board oversight and engagement in risk management is essential, but even more so in many development agencies and international financial institutions (IFIs) because board members typically represent donor and beneficiary member governments or other partners. Those representatives appreciate that strong risk management is required to enable effective deployment and use of donor funds and operations in riskier environments. A RAF supports strong governance because it helps bring transparency and alignment between the board and senior management on the scale and type of risks that are being taken to achieve the desired development objectives.
- **Senior management accountability:** Senior leadership has to be woven into oversight and management of risk; risk can't be divorced from strategy execution. The senior leadership team has to remain accountable for bringing all the risks together across the firm, supported by a well-functioning management (sub)committee structure. The development and implementation of the RAF should be embedded in existing – or new – management committees or other such structures so there is accountability across the entire organization.

2 | An inclusive approach to risk appetite development helps to achieve necessary buy-in across the organization

A risk appetite framework cannot be developed in a management silo – it must be easily understood and supported by all levels of the organization. So, senior management should involve stakeholders from across the organization early in the process and empower operational staff to contribute to and own the initiative. The culture in development agencies makes these issues even more important, where broad-based stakeholder engagement is commonplace.

An inclusive approach to risk appetite development and implementation should:

- **Engage a broad range of internal stakeholders:** Ultimately, the framework has to be understood and used by those in the field. It should be developed and informed by a diverse mix of perspectives and knowledge from across the organization, which collectively provide an organization-wide view of risks. That said, management should strike a balance between gathering input from a representative group of cross-functional stakeholders and creating a cumbersome feedback loop that stalls progress.
- **Educate the workforce on risk matters:** Operational staff actively manage risks throughout their day-to-day operations, but these efforts are often not recognized by staff as "risk management" practices, nor are those efforts necessarily structured or done consistently. As a more formalized approach to risk management is developed, the organization should make sure staff receive education on risk management, including the relevant risk concepts, terminologies and leading practices. This is critical at the outset of developing a RAF so that participants involved in its development have a sense of:
  - Why are we developing a RAF? What is the rationale?
  - How will it affect me and the organization?
  - How can I determine low from high risks? What do we mean by residual risk?
  - How will this be embedded in our project approval and review processes?

Ongoing risk education will then be important after the RAF is developed and to help foster a common risk language, encourage transparency, and help staff throughout the organization understand what risks they are taking, how these risks are changing, how these risks can and should be managed, and when issues need to be escalated.

3 | Considering a range of benchmarks can support risk appetite development, although it still needs to be tailored

Every RAF must be tailored to the needs and circumstances of each organization. This is especially important for development agencies, given the distinct nature of the mission, objectives and operating model. Risk has to be set within the context of development impact, not financial return.

Although agencies are different, they can learn from others. As they look for learnings and practices that might be relevant to inform and support progress, they should think broadly:

- **Public sector:** Development agencies can leverage information from other development and international financial organizations, most of which operate across a spectrum of risk management maturity levels. Institutions in this sector are typical keen and open to share lessons learned in the pursuit of common objectives and often publish guidance or thought leadership on topics related to risk management.
- **Private sector:** Private sector organizations (particularly financial institutions) can be viewed as a model for more mature risk management. Practices in these institutions have evolved significantly over the past decade, and they have accrued a lot of lessons learned as they have strengthened their approach, including in implementing RAFs. Financial services firms have honed their core risk management capabilities and know how to embed them across the organization into key decision-making processes, including capital and resource-allocation, and in the management of nonfinancial risks.

4 | A common language surrounding risk must be established to unify and standardize risk management across the organization

Establishing an organization-wide, common risk language is fundamental to successfully managing risk. Every member of an organization has a role in risk management and must be able to understand and communicate risk concepts and terminology in a consistent manner.

A common language is supported by:

- **Organization-wide risk taxonomy:** A taxonomy helps enable a standardized approach to risk management, effective risk conversations, and clearer comparisons of risk types and levels across the organization. It is a hierarchical categorization of risks and should be comprehensive in nature and avoid overlap across categories. The structure is relatively straight forward:
  - Major risks: So-called Level 1 risks are the top level – the 4-5 key risks facing the organization. In agencies, these are often strategic, financial, operational and those related to achieving the development outcomes of programs and projects. There may also be cross-cutting risks, like legal and reputational risks.
  - Sub-risks: Level 2 risks are major risks under each level 1; think of credit and liquidity risks, under financial risks.
  - Risk drivers: Level 3 risks are risk drivers. When organizations see worrisome trends at this level it can indicate future issues with level 2 – or even level 1 – risks. Risk drivers can help enable risk dialogues about risk trends and potential proactive measures earlier in the process. As a result, these drivers serve as early warning risk indicators.
- **Consistent rating scales:** Organizations often have multiple rating scales being used across the enterprise, and they are rarely consistent or comparable. An enterprise-wide rating scale is essential for a RAF to work, and it needs to be linked directly to the risk taxonomy. The levels of the scale (e.g. low, medium, substantial and high) should be clearly defined, communicated and easily understood by everyone and serve as the basis for risk management and reporting. While the scale may be adapted to serve different purposes in parts of the organization, it must be sufficiently standardized so that a rating of "high" risk, for example, carries the same meaning across all risk areas.
- **Consistent policies, and guidance:** Policies, procedures and guidance across that organization that govern or influence risk management should be aligned to the risk taxonomy, so that it is built into the fabric of everyday operations and decision-making.

Risks in development outcomes

A distinct feature of development agencies and IFIs, as compared to the private sector, is how they manage risks that can affect their development outcomes – in a sense, the risks to successfully implementing their programs and projects from the perspective of the desired outcomes. This risk has three distinct elements:

Managing risks to development outcomes is a shared responsibility between the development agency and host governments/recipients: Typically, organizations focus on risks they can manage, not on the ones of their customers and hosts. In the case of risks to development outcomes, agencies sometimes have more direct supervision of the programs, but often the direct supervision is undertaken by host governments or recipients. This places emphasis on having a common understanding of the inherent and residual risks; mitigating measures and how they are being performed and a common commitment to open communications as issues arise. The main impact on agencies of this dual risk management responsibility is they are constrained in their ability to manage down residual risks directly.

The risk has a varied set of risk types: The sub-risks underneath this risk are fairly eclectic: some relate to the external environment (including the governmental and political landscape), and the ability to mitigate them is limited; others relate more to the implementing agency and program and project design and supervision, where more mitigants can be designed; some are more like operational risks (such as around project procurement, financial management and environmental impact) where oftentimes tried-and-tested mitigating measures can be implemented; and some relate to stakeholders, where initial identification and ongoing engagement (directly and indirectly) become important mitigants.

This risk is heavily influenced by other risk domains: Albeit these risks are discrete, they are interwoven with the other risk domains. For example, the amount and type of development-outcome risk an agency can take is directly influenced by: the ability to target resources on the agency core mission (strategic risk); the availability to attract sufficient funding (a financial risk); and the availability of a sufficient number of staff to monitor the operations safely on the ground (operational risks). Thus, development outcome risk should be managed in the context of monitoring how these other risks are developing, and vice versa.

5 | Pragmatism is key in developing and refining risk appetite

Developing a formal risk appetite often represents a significant change within an organization, especially those with fairly immature risk management. The task of setting risk appetite levels across all risk types can sound daunting.

The key is to be pragmatic:

- **Start with qualitative risk appetite statements:** A qualitative RAS articulates why the organization is willing to accept a given type and level of risk to achieve its stated objectives. Think of a common one in development agencies:

  The [organization] has zero appetite for fraud and corruption in the context of its operations. The [organization] assesses the risk of fraud and corruption in its host countries and the operations and programs it supports, and designs mitigation measures to address such risks, notably in financial management and procurement. It reviews all complaints, investigates and seek sanctions in line with applicable policies and procedures.

  These statements are typically developed at levels 1 and 2, but can be set at the granular level 3, over time. For each one, stakeholders should identify relevant governing documents (e.g. polices, frameworks) related to managing that risk, articulate risk objectives, and articulate potential impacts associated with the risk materializing.

  For any given risk, stakeholders may identify that there are specific circumstances in which the organization would be willing to take more risk, in pursuit of objectives that are particularly important to the agency's mission – say, in fragile or conflict-stricken states or in the context of an emergency need. In those situations, the agency may articulate what is called a differentiated appetite for operations in those specific states.

- **Establish preliminary appetite level:** The goal of this step is to assign initial quantitative appetites to each level 1 and 2 risk, which reflects the desired level of residual risk exposures. Those involved in setting initial appetites should draw on their understanding of the existing, or inherent, risk environment, on the prevailing appetite for residual risk (type and level) across the organization, and on the perceived overall effectiveness of controls they typically use to manage specific risks. *See Inherent versus residual risk*.

- **Select key risk indicators:** In order to monitor risk appetite, the organization should identify and select a set of risk metrics that is aligned with the risk taxonomy and designed to measure key residual exposures. Each metric should be clearly linked to specific risks, easily aggregated and capture necessary information efficiently. Where possible, these metrics should relate to level-3 risk drivers, so that they form the basis of a solid set of early warning indicators. These metrics will support effective risk reporting and enable effective oversight as to the organization's adherence to established preliminary risk appetites.

- **Assess initial risk profile:** Proposed initial risk appetite levels need to be validated before they are reported to the agency's board, even if positioned as preliminary. The organization will need to determine its current risk profile, evaluate whether existing risk data is consistent with the proposed preliminary levels, and adjust accordingly. The availability of risk data could constrain what risks can be assessed accurately, so organizations should be pragmatic in identifying what kinds of data are currently available. For example, in areas such as program delivery, subjective risk ratings may be the only risk data that can be used, which is fine.

- **Establish risk thresholds:** Agencies should set target levels for each risk metric that establish an acceptable range within which exposure levels can fluctuate – known as the organization's risk tolerance. Within the established tolerance, escalation thresholds should be established that trigger clear procedures for addressing elevated exposure levels. See Figure 1.

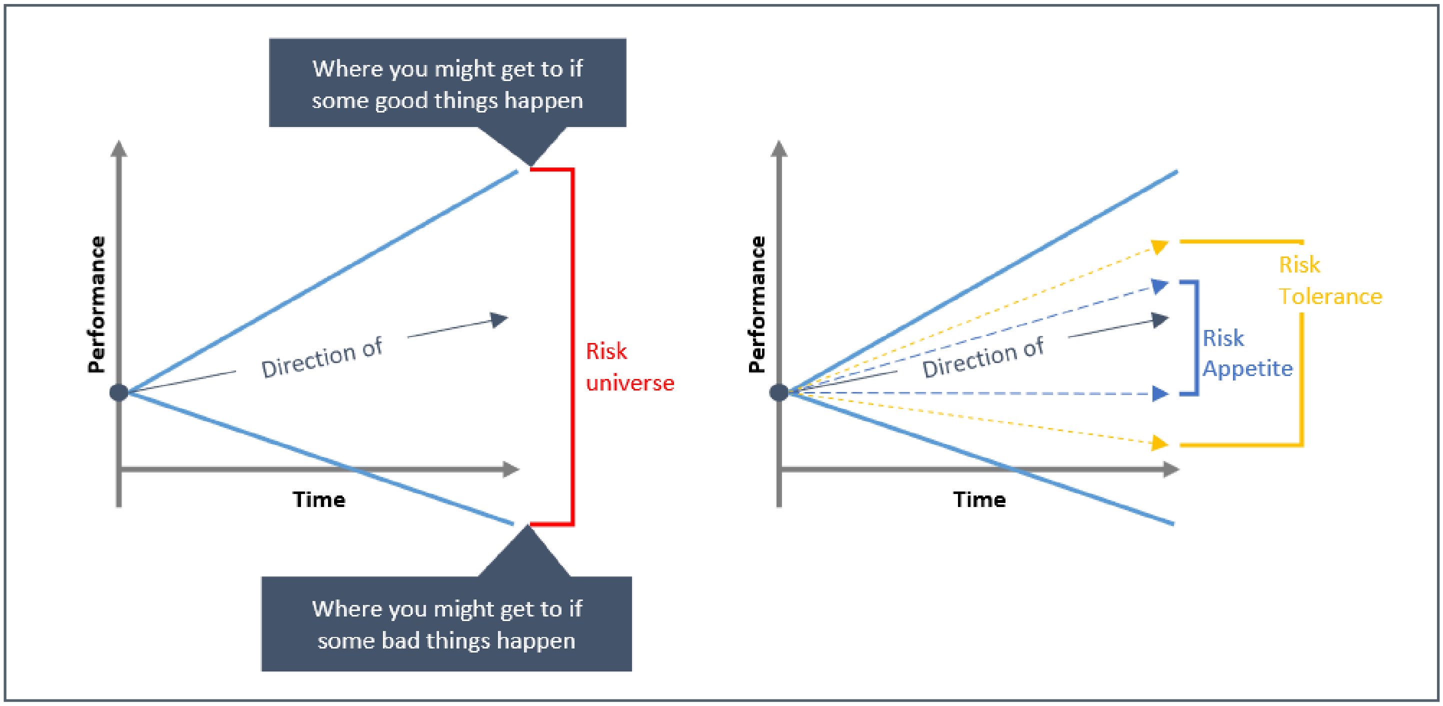


Figure 1: Understanding the relationship between risk appetite and threshold
The Risk Appetite Statement Guidelines published by the UN's HLCM Cross-Functional Task Force on Risk Management illustrate well the relationship between risk appetite and thresholds.[4]

- **Use year-one to learn and adjust:** The first year of implementation will be a learning exercise and monitoring how chosen appetite levels influence risk-taking and behaviors will be essential to confirming risk appetite, in time. Agencies should gather risk data for a full year and assess the organization's performance in managing risk exposures within established appetites and thresholds. After a year, agencies should have enough data to compare how actual risk metric levels performed against target thresholds and, armed with this information, management should review and revise established appetite levels and adjust metric tolerances, as appropriate.

Inherent vs residual risk

It is imperative that stakeholders throughout the organization have a fundamental understanding of concepts of inherent and residual risk, to support effective management of risk and appropriate allocation of resources to mitigation measures and controls throughout the operations. The two concepts are fairly simple:

- **Inherent risk** is the level of risk present in the absence of controls or mitigation measures. In other words, inherent risk is a measure of the level of risk observed if no action is taken by the organization to reduce the likelihood of occurrence or severity of impact of the risk.
- **Residual risk** is the level of risk remaining after controls or mitigation measures have been applied.

All risk decisions, ratings or expressions of appetite should be framed in the context of residual risk exposures.

A simple way of thinking of it is as follows: one starts with a dangerous road, which has a high accident rate. The road is inherently high-risk. To mitigate the risks, one installs road bumps. To the extent those bumps (the mitigation measures) have been shown to be highly effective previously in such settings, the residual risk would be notably lower (because it represents the level of risk after taking into account the positive effects of the bumps). To the extent road bumps are a novel mitigant (i.e., have not been used previously), residual risk may still be high until the bumps have been proven to be effective.

[4] https://www.unsceb.org/CEBPublicFiles/2019.HLCM_.26%20-%20Guidelines%20on%20Risk%20Appetite%20Statements%20-%20Final_1.pdf

6 | Building an effective risk dashboard linked to thresholds and triggers enables risk oversight

Risk dashboards are important to monitor the organization's top and emerging risks, and should be:

- **Linked to risk taxonomy and RASs:** Risk metrics should be linked to each level-3 risk driver and aligned to the risk taxonomy so that the organization can properly measure the risk profile against established appetites for each key risk.
- **Focused on a prioritized set of risks metrics:** Excess information undermines having a clear view of risks and can lead to bad decisions or inaction. While risk priorities may change over time, reflecting the evolving risk environment, it is important to maintain a core set of metrics that are consistently reported to allow for trending analyses and effective benchmarking. Only the most relevant risks metrics should be included in risk dashboards.
- **Tailored to the audience:** Risk dashboards are visual tools used for managing and reporting risks and must be sufficiently versatile to provide the right level of risk information to each level of the organization. The board requires higher-level information to support governance, senior management requires organization-wide information to support portfolio-level decision-making, and staff need risk information for day-to-day decision-making.
- **Well designed and easy to read:** The best dashboards focus on risk impact and importance and present clear, actionable information to the reader. Such dashboards supplement quantitative risk data with qualitative analysis and provide a narrative on driving factors behind emerging trends, top-of-mind considerations, and key takeaways for action. The visual style of the reports is also important: data has to be intuitive and clear, prior ratings (e.g., red, yellow, green) need to be consistently applied, and data visualization has to clearly highlight key points for discussion and action.

7 | Risk must be embedded in decision-making processes to bring about the desired change in behaviors

To be fully effective in enabling the desired level and type of risk-taking, the RAF must be integrated into decision-making processes, including:

- **Strategic planning:** Decisions on the agency's strategy have to be informed by a view on existing and expected levels of residual risk and set in the context of risk appetite. Similarly, risk appetite levels have to capture the agency's strategic aspirations, especially when strategic changes are being considered, such as directing more resources towards achieving SDGs. The risk appetite should feed into strategic planning early in the annual planning process, be accounted for as business unit and organization-wide plans are developed, and be considered as strategic plans are approved.
- **Budgeting and resource allocation:** Risk-based resource allocation, with the context of risk appetites and thresholds, should enable resources to be deployed to help maximize risk-taking to achieve desired development objectives and to help manage key risk exposures. As with strategy planning, risk information should be fed into budget planning across the year; the impact on resource allocation should be ongoing.
- **Portfolio management:** Once an agency has gathered enough organization-wide information, such as on programs and projects, it can aggregate that data at various portfolio levels – i.e., country, regional, practice or global levels. Such information can then feed into decisions on country-level frameworks, and regional and global pipeline planning (including current and future pipeline) and be compared to risk appetite levels at these various levels. Beyond projects, it can inform other types of portfolio-level decisions, such as the loan or technology portfolios.
- **Project and program approval and oversight:** Agencies have to decide how risk appetite will inform program and project approvals and ongoing supervision. In some ways, risk appetite is an aggregate-level tool, so should not constrain or stall individual projects. However, those designing projects should know what corporate risk appetite levels are so it informs the design and helps hone messaging in approval documents. Those approving projects should be aware of how each project compares to appetite levels, so they know if it is out of appetite – when it is, they can challenge if the agency is getting commensurate levels of development outcome for the enhanced level of residual risk, and when approved, they can affirmatively accept that additional risk.

As for live projects, teams should know when residual risk levels exceed those that were approved for the project and manage or supervise risks in that context. When residual risks exceed expected levels, they should appropriately escalate risks sufficiently early (not just when they realize they cannot get the risks back within risk appetite or approved levels). Keeping risk ratings up-to-date is essential to inform portfolio decision-making.

Mobilizing resources for COVID-19 response: the importance of risk in decision-making processes

The COVID-19 pandemic illustrates the need to properly embed risk management in decision making. When resources need to be mobilized quickly in response to high-impact events, such as COVID-19, well-established decision-making processes, which are informed by an up-to-date perspective of the organization's risk profile, support more effective determination of priorities and allocation of resources. The impact of the event on the risk profiles of existing projects can also be determined and monitored, at project and portfolio levels. A well-thought-out organization-wide risk taxonomy can be an invaluable roadmap to quickly identify potential impacts of crises across all risk areas and to determine if residual risk levels have exceeded desired levels as a result of events and what remedial actions, if any, need to be taken.

For example, taking a typical risk domain structure within development agencies – which normally have strategic, financial, operational and development-outcome-related risks – one can identify a number of areas where COVID-19 could impact the risk profile and, thus, help focus management attention on the most important potential risk changes.

Strategic risks	Financial risks	Operational risks	Development outcome risks
‣ Funding cycle impacts ‣ Member country or partner engagement challenges ‣ Flexibility in supporting emergency actions	‣ Lower levels of liquidity or capital (e.g., due to debt forbearance) ‣ Interest rate and foreign exchange movements	‣ Employee health and safety ‣ Cyber security threats ‣ Procurement challenges ‣ Potential conflicts of interest in projects that are fast-tracked	‣ Heightened political or economic instability ‣ Degradation of implementing agency's capacity ‣ Delays in implementing existing projects ‣ Supply chain or procurement impacts ‣ Financial integrity impacts

8 | Build risk appetite into the broader ERM program/project

In the end, the RAF and RASs are tools within the broader risk management framework. That framework and the associated policy(s) include other fundamentals, including the governance and leadership noted above (notably how risk will be overseen and governed by the board and managed by senior management, the frequency and process for risk oversight, and the supporting committee and approval processes).

The three-lines-of-defense risk operating model has been shown to be an effective framework for risk management and implementation of an organization-wide RAF, and has been adopted by the likes of the UN. The model sets out clear roles and responsibilities across all risk types. *See Roles across the three-lines-of-defense.*

Key prerequisites in implementing this model include:

- **Clearly delineating who is in the first line:** Often, in organizations, there is ambiguity regarding who constitutes the first line. In development agencies, this ambiguity is heightened because host governments and external partners are often the ones implementing the development activities (and, thus, in some ways form part of an "extended first line"). For sure, operational staff who design and supervise projects and programs in coordination with external partners are part of the first line, as are country and regional management, and practice management. In addition, functional activities that enable risk taking, such as IT, finance and procurement, are part of the first line.
- **Establishing strong independent risk oversight:** A strong second line of defense is responsible for monitoring and providing credible challenge to first-line risk-taking activities and for monitoring aggregate organization-wide risk exposures. Typically, the second line takes on the role of developing risk-related policies and frameworks, which the first line then implements in standards, guidelines and procedures. Second-line risk management should be a formal group led by an individual, such as a chief risk officer, with the authority and resources, and who has access to the board. In development agencies, any operational policy-making group would also be considered second line.
- **Providing for periodic independent assessments:** The third line of defense — notably internal audit — plays an important role in evaluating levels of adherence to policies and procedures, the effectiveness of risk governance, and the agency's performance relative to industry practices. In development agencies, independent evaluations of development impact are important, so as to inform strategy-setting and program design. These assessments are typically performed by a distinct, independent third-line group (not by internal audit). These third-line groups report independently to the board.
- **Leveraging technology:** There are many instances in which technology can support and enhance risk management, including in determining risk ratings (e.g., on projects and programs), measuring and reporting on risk data, deploying and managing organization-wide risk-and-control assessments, providing a centralized repository for risk and audit data, and for tracking remediation activities. There is a danger agencies and multilaterals focus too early on technology – the trick is determining how risk management will be conducted in a way that suits the organization's distinct needs, and then determining what technology is needed (not the other way around). In some settings, organizations don't need the most advanced technology — more foundational technologies can suit those organizations in the early stages of maturity.

Roles across the three-lines-of-defense

The roles of each line of defense in development agencies is as follows:

1st Line of Defense	2nd Line of Defense	3rd Line of Defense
‣ Work with borrowers / host implementing agencies to design programs and projects ‣ Assess and manage risks ‣ Design and implement controls ‣ Supervision or support supervision of programs and projects ‣ Provide the necessary functional support to operate the business (e.g., IT infrastructure)	‣ Establish risk management frameworks and policies ‣ Monitor and provide challenge to first-line risk-taking ‣ Measure and monitor aggregate risk exposures ‣ Provide an independent risk perspective to senior management and the board	‣ Independently assess risk management and risk governance framework ‣ Conduct internal audits and report findings to the board ‣ Provide assurance over control environment ‣ Evaluate impact of development operations

9 | Communicate, communicate, communicate (and train)

Ultimately, development agencies have to realize that the implementation of a RAF is not simply a technical effort; it is about supporting a cultural change in how risk is identified, measured, managed and mitigated.

However, staff in the field may misinterpret the purpose or militate against the framework and its implementation, viewing it as a distraction. So, communications around the RAF – as it is developed and, more importantly, when it is rolled out – are critical. Key elements include:

- **An organization-wide, top-down communication strategy:** This strategy should be led by the lead executive (e.g., president or secretary general) and management team, overseen and supported by the board, and cover:
  - Rationale for the RAF (notably enabling, versus constraining, risk taking to achieve more development outcomes)
  - Benefits that accrue to each stakeholder (including, for those designing and driving projects and programs, and those in the functional and finance areas)
  - Impact on decision-making and resource allocation

A key objective is making sure staff view it as a tool that they should use on a day-to-day basis and not another organization-driven "compliance"-type exercise. It should help, not hinder, them.

- **Ongoing risk education at all levels of the organization:** Training and education will help individuals at all levels – from staff to the board – understand how risk management and reporting will support decision-making and transparency. While initial trainings should support the design, introduction and implementation of the RAF, continuing efforts need to solidify a common language, encourage candor and transparency across the organization, support decision-making and enable appropriate risk escalation.
- **Disclosures to external stakeholders:** Some development institutions have put high-level elements of their risk management approach into public disclosures and external communications. Top-level RASs, for example, can be particularly effective in creating awareness outside the organization about its s risk appetite in the context of strategic goals and operations.

10 | Risk management is a journey

While the introduction of the RAF may represent a marked shift in the organization's approach to risk management, it is part of a much longer journey. Strategic objectives and risk management priorities evolve over time as the development environment and risk landscape changes.

To support this journey, agencies should:

- **Identify and resolve policy gaps:** As the RAF is developed, management will inevitably identify operational units and risk areas that may be operating at different levels of maturity, and where policies and frameworks are outdated or non-existent, or ineffectively (or only minimally) implemented. The agency should document these gaps and develop a prioritized remediation program as part of its organization-wide risk enhancement program.
- **Implement a policy of policy:** Some organizations find they have not yet implemented a hierarchy of policies – one that distinguishes policies, frameworks, standards, guidelines, working papers, and so on, and for each articulates how they should be drafted, reviewed and approved. Such a policy supports organization-wide consistency and quality, distinguishes organization-wide documentation (e.g., policies) from unit-specific documentation (e.g., guidelines), and makes sure that oversight and approval responsibilities are aligned to the right level of governance (i.e., a board would normally only review and approve policies).
- **Make sure the risk function is adequately resourced:** Few agencies have fully built out a risk management group – indeed some only have part-time roles, not a team. Initial investments in staffing, technology and other resources should focus on implementing the RAF and enhancing the control environment and risk reporting. Over time, additional resources should focus on specific risk areas, working with the first line of defense, such as fraud, technology and cybersecurity, procurement, financial-risk management, legal and so on.

Get started and adjust as you go

For organizations that do not have strong and deep risk management expertise, implementing a RAF can be challenging. It brings with it a coterie of other required items — risk taxonomies, risk/governing documents, risk indicators, etc. — each of which feels like a major piece of work by itself.

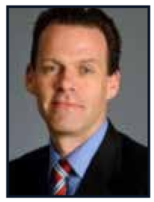
It can be less burdensome, if done pragmatically. There is a vast body of experience on how best to implement such frameworks, in the public and private sector, and those learnings should be leveraged, within the context of each agency's own unique circumstances and strategy. Building on the experiences of others speeds progress and avoids known pitfalls.

It is important to position the RAF as a fundamental part of achieving greater development impact.

A rallying cry could be how implementing the RAF is directly related to achieving the SDGs, recognizing most agencies are considering how best to marshal, deploy and target finite resources on maximizing their development impact. The reality is the SDGs are very ambitious and require a significant focus on specific regions and countries, and within them on the most critical development issues, and taking more risk in doing so. Enhanced risk management allows the organization to manage these higher levels of risk in delivering against the organization's mission.

Contacts

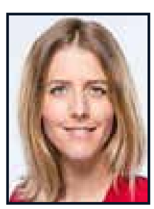
Michael Beaulieu
Managing Director
Global Client Service Partner, UN
michael.beaulieu@ey.com
+1 703 747 1819



Mark Watson
Managing Director
US Regional Coordinating Partner, World Bank Group
Deputy Leader, Financial Services Center for Board Matters
mark.watson@ey.com
+1 617 305 2217

Corbin J. Long
Senior Manager
Financial Services Risk Management
corbin.long@ey.com
+1 703 747 1639

Barry Franck
Partner
UN Lead Partner, Switzerland
barry.franck@ch.ey.com
+41 58 286 57 13



Elise Salaun
Senior Manager
Advisory Risk Services
elise.salaun@ch.ey.com
+41 58 286 4361

EYG no. 001664-20Gbl
BSC No. 2003-3461855

ED None