OLIVER WYMAN

GLOBAL PARTNERSHIP for EDUCATION

RISK FRAMEWORK REVIEW
GAP ANALYSIS AND RECOMMENDATIONS

MARCH 20, 2018

MARSH & McLENNAN COMPANIES

CONFIDENTIALITY

Our clients' industries are extremely competitive, and the maintenance of confidentiality with respect to our clients' plans and data is critical. Oliver Wyman rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of Oliver Wyman.

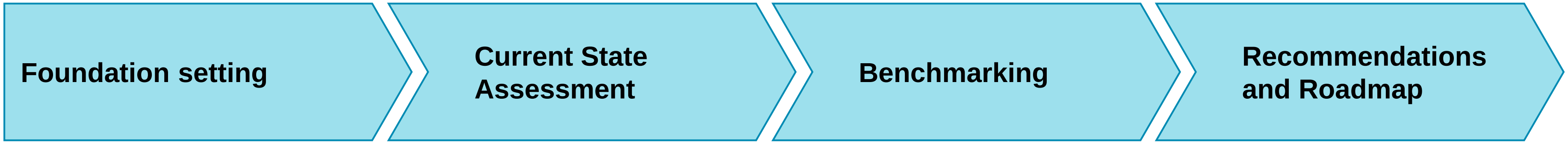
1 | Project objectives, scope & approach

The Global Partnership of Education brought in Oliver Wyman to perform an external review of its Risk Management Framework

Project objectives

- The Secretariat of the Global Partnership of Education engaged Oliver Wyman to review its risk policies and practices with a view to identifying gaps and areas for improvement
- The key objectives for this work were to
  - Review current GPE Secretariat risk policies and practices to assess gaps and areas for improvement
  - Benchmark current GPE Secretariat risk policies and practices against policies and practices of other comparable organizations
  - Make recommendations and propose concrete solutions to help the GPE Secretariat improve its risk assessment methodologies and monitoring of risk mitigation actions
- The core engagement took place over a four week period in February and March of 2018

The project was completed in four steps



Foundation setting

- Initial review of GPE policy documentation and reporting, covering all documents and reports identified in the GPE RFP
- Interviews with selected members of senior leadership and risk management function
- Development of a review framework and assessment dimensions
- High level articulation of GPE risk management goals and objectives
- Preparation and delivery of the inception report to GPE

Current State Assessment

- Detailed review of GPE framework/policy documentation and reporting and historical performance
- Additional interviews with selected members of senior leadership, GPE committees, Grant Agents, and risk management function, as well as selected staff likely to be impacted by risk management policies
- Evaluation of GPE current state, highlighting where current policies and practices do not support risk management objectives and/or impose inefficiencies on the organization

Benchmarking

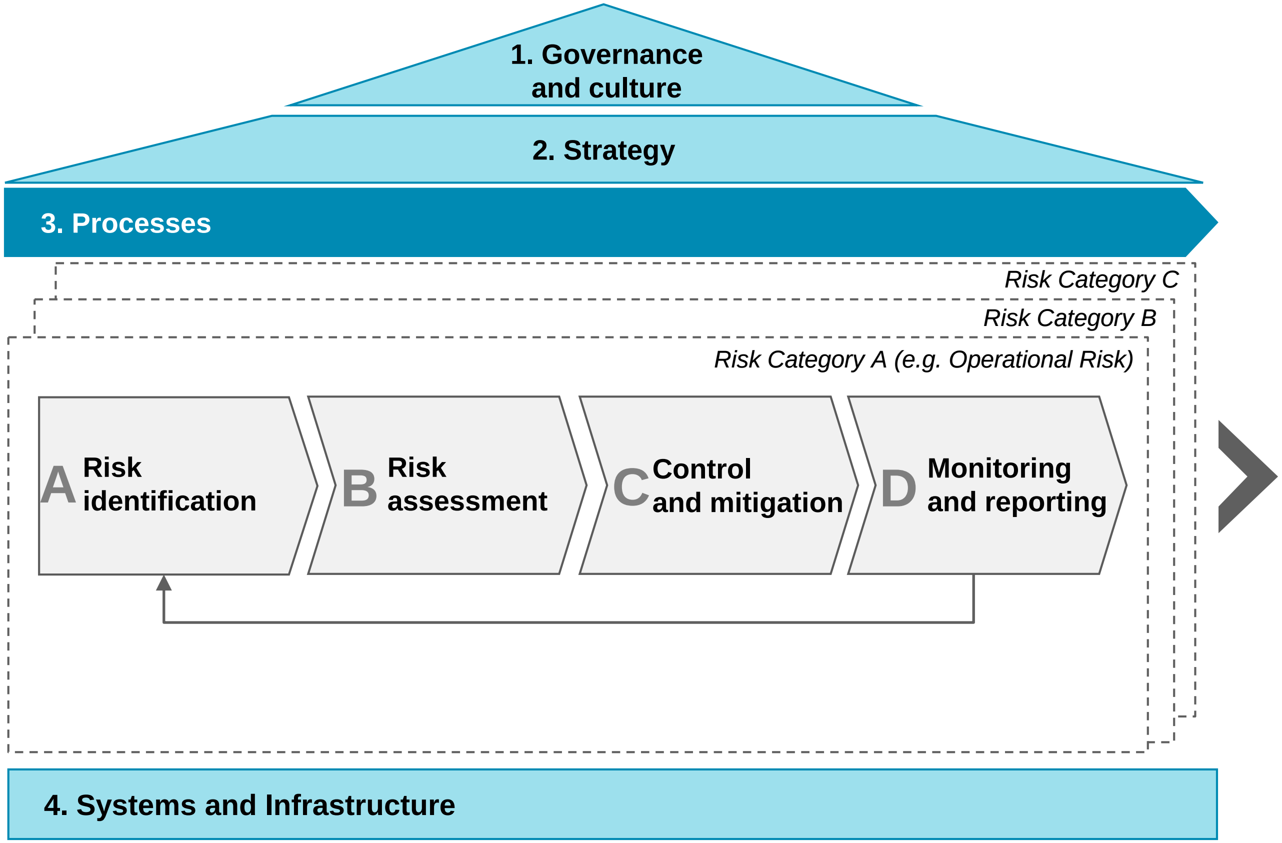
- Identification and agreement of target benchmarking organizations
- Outreach and interviews of benchmarking targets
- Synthesis of market practices, highlighting both ‘standard” best practices and also specific practices of potential interest to and applicability at GPE

Recommendations and Roadmap

- Identification of key gaps between GPE current practices and either GPE desired practices/target state or market best practices
- Identification and evaluation of possible tactics for addressing these gaps based on costs, implementation difficulty, and downside risks
- Development of high-level implementation plan defining recommended initiatives and timing
- Preparation of diagnostic report, including recommendations

The analysis and detailed findings are structured along the dimensions of a typical Enterprise Risk Management Framework

Key components of an Enterprise Risk Management Framework


1. Governance and culture
2. Strategy
3. Processes
Risk Category C
Risk Category B
Risk Category A (e.g. Operational Risk)
A Risk identification
B Risk assessment
C Control and mitigation
D Monitoring and reporting
4. Systems and Infrastructure

1 **Governance:** Oversight structure, risk ownership, roles and responsibilities, risk appetite and culture

2 **Strategy:** Risk management incorporated into strategic decision making

3 **Risk Processes:** Processes for identifying, assessing, controlling/mitigating and reporting/monitoring risks

4 **Systems and Infrastructure:** For supporting ERM framework

Three main sources were used to review GPE's risk landscape including frameworks/polices, interviews with GPE management, and analogue organizations

1 DOCUMENTS REVIEWED

- GPE risk management framework, 2013
- Risk management policy, 2014
- Risk management report #1, May 2015
- Report from the Governance Committee: Risk management report, Nov. 2015
- Report from the Governance Committee: Risk management dashboard, Nov. 2015
- Risk management report #2, December 2015
- Report from the Governance Committee: Risk management report #3, June 2016
- Operational risk framework: Report to the Country Grants and Performance Committee, October 2016
- Risk management report #4, December 2016
- Risk management report # 5. June 2017
- Operational risk framework #2. June 2017

2 INTERVIEWS CONDUCTED

- Finance and Risk Committee
- Grant and Performance Committee
- Grant Agents (World Bank, UNICEF)
- CFO and Secretariat Risk Management
- Country Leads
- GPE Management
  - Alice Albright
  - Margarita Focas Lich
  - Karen Mundy
  - Padraig Power

3 ANALOGUE DISCUSSIONS

Gavi
The Vaccine Alliance

Investing in our future
The Global Fund
To Fight AIDS, Tuberculosis and Malaria

GREEN
CLIMATE
FUND

The remainder of this report is structured in 3 sections

1 **Section 1: Project objectives, scope & approach**
Describes project objectives and scope, approach undertaken to perform the gap assessment, including a list of documents reviewed and employees at GPE and analogue organizations interviewed

2 **Section 2: Summary results and recommendations**
Establishes the context, identifies key gaps vs. aspiration/best practices, and introduces Oliver Wyman's recommendations

3 **Section 3: Summary ERM framework gap assessment findings and roadmap**
Summarizes key gaps identified for each of the ERM framework components (governance & culture, strategy, processes, systems and infrastructure) and suggests a roadmap on how to address these

4 **Section 4: Detailed ERM framework gap assessment findings and recommendations**
Provides a detailed overview of all gap assessment findings for each ERM framework component as well as detailed recommendations on how to address these

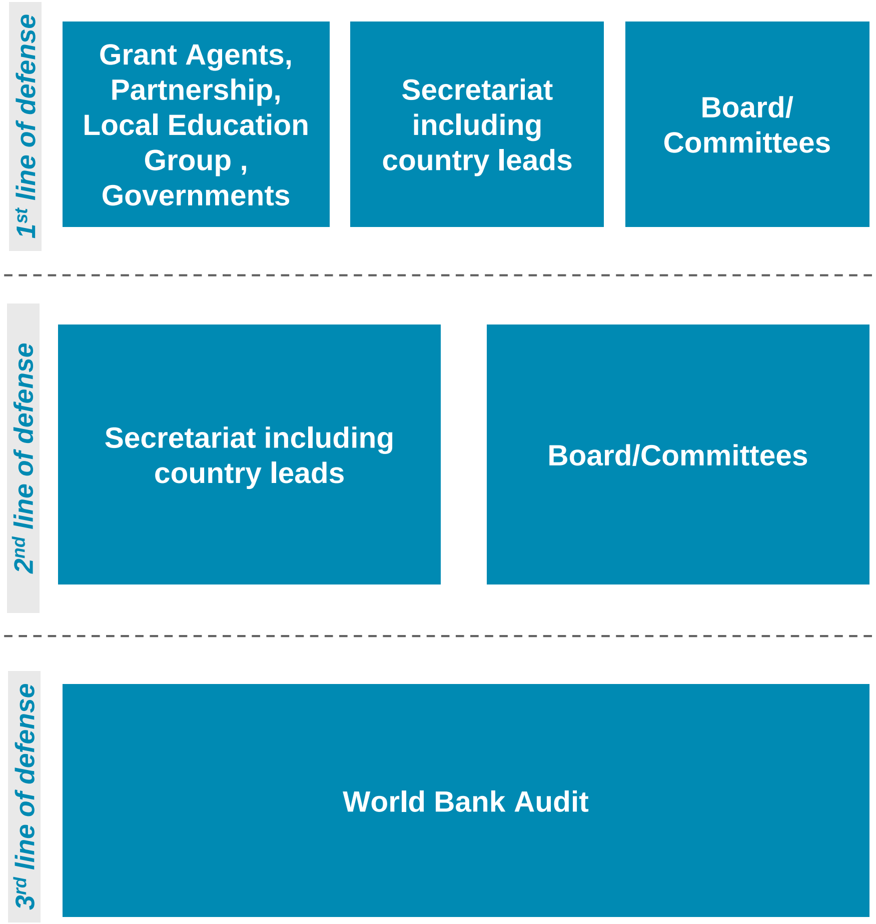
2 Summary results and recommendations

The assessment of GPE's risk management framework needs to be viewed in the context of its unique institutional set-up and governance

- The unique organizational structure of both the Global Partnership for Education and other similar institutions creates challenges for both risk management and other governance related issues
- As a partnership, the organization is composed of multi-stakeholders made up of developing countries, donors, international organizations, civil society, teacher organizations, the private sector and foundations
- Significant risk for the partnership comes from the reliance on Local Education Groups, i.e. low performance from them may lead to GPE not achieving their impact goals as per the Strategy 2020
- To support the partnership, The Secretariat provides administrative and operational support to the partnership and facilitates collaboration with all partners
- The Secretariat is hosted within a larger organization (World Bank) and relies on the World Bank to provide internal and external audit services, which creates operational complexity
- In addition, the Board of Directors which is made up of members of the partnership provides support for the objective of the partnership including resourcing, monitoring of financial resources, advocating for the partnership, and overseeing the secretariat budget and work plan
- These complexities, compared to traditional corporations, create challenges that extend to operational issues and risk management which is what has been explored in this engagement

Among other implications, this has led to confusion around the appropriate allocation of risk management accountability within the 3 LoD framework

Current risk management governance and structure



1st line of defense

Grant Agents, Partnership, Local Education Group , Governments

Secretariat including country leads

Board/ Committees

2nd line of defense

Secretariat including country leads

Board/Committees

3rd line of defense

World Bank Audit

- GPE has no staff on the ground locally; it relies on local third parties (e.g. grant agents, local education sector groups) to identify and manage risks
- At the same time, GPE did not feel comfortable assigning risk ownership to third parties, hence many of the (locally managed risks) are currently owned by the GPE Secretariat (predominantly the Risk Management team) and or its committees
- However, the GPE Secretariat (Risk Management and Country Teams) together with the FRC, GPC and SIC committees are currently also tasked with the 2nd line of defense function
  - GPC is responsible for approval of new grants but also with the risk ownership of the Operational Risk Framework
  - FRC is responsible for GPE strategic and funding risks but owns oversight of the Risk Management processes
  - SIC is responsible for partnership level risks related to strategy and impact as defined by the GPE 2020 strategic plan
- Hence, we see a strong overlap between 1st and 2nd line roles at the moment, which leaves a lot of unclarity around who should be responsible for what and can trigger double work as well as blind spots
- In terms of the third line, GPE does not have its own internal audit function but currently relies on the World Bank's internal audit function which is not customized to the needs of GPE

Many ERM design choices depend on whether GPE is striving for a centralized or decentralized approach

Approaches to risk management and GPE's current positioning

	Decentralized approach	GPE risk management approach	Centralized approach
Governance	• Heavy reliance on local grant agents and other third parties to perform not only first but also second line of defense tasks • GPE secretariat's role is to provide risk policies and guidelines in addition to third party's own policies, but very limited actual challenge and oversight role • Strong reliance on third line (audit function)	• Tendency of GPE Risk Management Team to strive for centralized model and play second line of defense role by challenging and overseeing work performed by the local first line	• Local grant agents and other third parties to perform only first line tasks • GPE secretariat staff to perform second line tasks, providing risk policies and guidelines AND challenging and overseeing the work of the first line • Lower importance of third line than in decentralized model (although still high)
Risk resourcing	• Small Risk Management team at Secretariat level (~ 1 FTE)	• More Risk Management resources available than required in a decentralized model, but not enough to perform the tasks required in a centralized model	• Medium Risk Management Team at Secretariat level (~5-15 FTE)
Analogues	Gavi The Vaccine Alliance	GLOBAL PARTNERSHIP for EDUCATION	The Global Fund To Fight AIDS, Tuberculosis and Malaria GREEN CLIMATE FUND
Considerations	• Fewer FTE costs • Less control over risk management, more reliance on third-parties • Analogues focus on delivery of goods not services		• Higher FTE costs • More control over risk management, less reliance on third-parties • Analogues focus on delivery of services and support direct giving

The choice of model should not be made on the basis of risk management effectiveness alone but rather on the basis of the overall ability to deliver on GPE's mission

The review surfaces six key findings; how, and how effectively, they can be addressed will depend on GPE’s future institutional structure and governance

	Key Risk Management Framework gaps we identified	Analogue practices
1	**Risk appetite statement:** Risk appetite is broadly defined within GPE’s Risk Management Policy. Leading practice is, that this is defined in more detail for the main risk categories with a structured and documented process involving the board. Risk Appetite is not equal to the residual risk	Risk appetite statement either in place or currently being developed by all three analogue organizations
2	**Risk governance:** Overlaps between 1st and 2nd line of defense responsibilities. Greater clarity needed on who challenges and who owns/mitigates risks. Risks should be assigned ownership to staff with operational responsibility and/or co-ownership with e.g. country teams	Predominantly, 1st line defined as a joint responsibility between local third parties and some kind of country team at Secretariat level
3	**Incorporation of risk into business decisions & strategic planning:** Link between risk management framework and business decisions, such as strategic planning and grant allocations could be stronger	Only one out of three analogues describe the link between risk and strategic decisions as strong, others think it still has to be strengthened
4	**Risk taxonomy:** Limited categorization of risks into key risks and sub-risks/risk drivers. Risk taxonomy should be mutually exclusive and collectively exhaustive to ensure full risk coverage without overlapping risk types or categories	Mixed analogue practices. One with a very clear, streamlined taxonomy. Others with room for improvements
5	**Monitoring & Reporting:** No systematic identification and active monitoring of Key Risk and Control Indicators (KRIs/KCIs) that are compiled into reporting. Additionally, no separate reports with differing level of detail and use of dashboard for Committees and Board	Limited use of KRIs/KCIs and visual dashboards, however at one organization currently being developed
6	**Framework and policy documents:** Documents could benefit from greater clarity and simplicity, clear separation between reporting documents and framework/policy documents	Greater clarity at analogue organizations, incl. e.g. version / document administration tracker for policy documents

Based on our review, we have 4 recommendations that can be implemented immediately

- Our review has identified key recommendations to GPE's risk management to allow them to align to their strategic plans and ambitions:
  - Revisions to Risk Appetite Statement including a greater link to strategy and a risk by risk evaluation of partnership-wide risk tolerance
  - Implementation of a risk governance structure with clear role ownership across the three lines of defense to provide a structured approach to risk management, oversight and audit within the organization
  - Simplification of the risk taxonomy at GPE in order to streamline risk management processes
  - Identification of key risk indicators and key control indicators are needed to objectively manage risk
- Addressing the first two recommendations on Risk Appetite Statement and risk governance, would bring GPE in line with analogue practices
- The second two recommendations will create a clear linkage to the strategic ambitions of the partnership with objective and efficient measures of risk which are currently lacking
- In addition GPE should determine if they need to adopt a more centralized approach to risk to provide better controls over risks managed and owned by third parties GPE works with locally, which would likely require an increase in Risk Management staff resources at the Secretariat level

3 Summary ERM framework gap assessment findings, recommendations and roadmap

Summary of ERM framework gap assessment findings (1 of 5)
Governance and culture

	ERM Components	GPE practices in line with analogues	Gaps/potential areas for improvement	Gap	Criticality
1	**GOVERNANCE AND CULTURE**				
1A	**Risk appetite**	• GPE defines the risk appetite for certain key risks and connects these directly to the strategic goals with the Risk Management Policy	• No Risk Appetite Statement in place; Risk Appetite (RA) is not defined at a risk-by-risk or risk category level • RA does not directly set guidance with partnership expectations in mind such as how significant risks could impact the goals and strategy of GPE, no shared understanding of RA	◕	🔺
1B	**Oversight**	• Board and Finance and Risk Committee in place who's main role is to challenge and oversee risks and GPE's Risk Management Framework similar to analogue organizations	• Challenge for the board to provide effective oversight as all risks are presented to them with little prioritization/little focus on higher priority risks • Finance and Risk Committee struggles to provide effective oversight and challenging due to overlap between the 1st and 2nd line of defense responsibilities	◑	⚠
1C	**Roles and Responsibilities**	• Duties of the Board, GPC, FRC, and secretariat are defined with respect to risk management in the Risk Management Policy • Key risks, including the operational risk framework and the corporate risk matrix, have assigned owners responsible ensuring completion and participation from needed parties	• Overlap between the 1st and 2nd LoD responsibilities, some roles appear to be assigned to multiple parties creates unclarity, risk of double-work and/or blind spots • Not enough time is being dedicated to review of risk processes due to competing priorities/responsibilities • The role of audit (to some extent provided by the World Bank audit unit) is not defined in the risk management policy providing scope of their work and associated responsibilities for GPE	◑	🔺

GAP TO BEST PRACTICE

○ Small ◑ Medium ● Large

CRITICALITY OF GAPS

▲ Low ⚠ Moderate 🔺 High

Summary of ERM framework gap assessment findings (2 of 5)
Governance and culture

	ERM Components	GPE practices in line with analogues	Gaps/potential areas for improvement	Gap	Criticality
1D	**Risk ownership**	• Risk owners are assigned for all risks with in both the risk matrix and the operational risk framework • Ownership of risks and the associated responsibilities are aligned with appropriate parties	• Risk ownership often not assigned to those with actual control over the outcomes, esp. third parties at country level such as Local Education Group and grant agents • Process for determining risk ownership is not clearly outlined in the process documents for the operational risk framework and corporate risk matrix	◐	🔺
1E	**Risk culture**	• Risk based principles, which were present at all analogues, of management and a culture of risk awareness are described in the risk management policy • Discussion of communication and risk is described including an emphasis on clear continuous communication between GPE and its partners	• Risk appetite does not set risk level thresholds to allow the organization to understand which risks should be focused on that may impact GPE's strategy • Risk not seen as a priority to majority of staff as many do not see how risk would influence grant allocation, strategy decisions or day-to-day operations	◐	△

GAP TO BEST PRACTICE

○ Small ◐ Medium ● Large

CRITICALITY OF GAPS

▲ Low △ Moderate 🔺 High

Summary of ERM framework gap assessment findings (3 of 5)
Strategy and Processes

	ERM Components	GPE practices in line with analogues	Gaps/potential areas for improvement	Gap	Criticality
2	**STRATEGY**				
2A	**Incorporation of risks into strategic planning**	• Risk and the associated accountability such as monitoring and mitigation are described in the Risk Policy and how they relate to strategy • GPE describes how risk and opportunities are linked due to the organization operating in vulnerable and high-risk areas	• There is no direct link between risk appetite/outcomes and GPE's strategy • No soft link into GPE's strategic plan including information of how risks could impact the plan • No hard link into grant allocation decisions and/or grant pay-outs • Risk mitigations are also not considered in light of costs associated with them and expected return – i.e. prioritization of resources often not sufficiently made	◕	🟥
3	**PROCESSES**				
3A	**Risk Identification**	• A total of 36 risks are assessed through a corporate risk self assessment template • The operational risk template assesses 6 risks, which form a subset of the Corporate Risk Matrix, filled in by local third parties • Users can identify and make suggestions for new risks to be added • It is a forward looking assessment that looks at the next 3 yr. period	• The current taxonomy is too granular and hinders ease of use and effectiveness of risk management • New risks have been added to the corporate risk matrix which has grown the number risks without sufficient discussion or vetting, no regular period reviews in place	◑	🟨

GAP TO BEST PRACTICE

○ Small ◑ Medium ● Large

CRITICALITY OF GAPS

🟩 Low 🟨 Moderate 🟥 High

Summary of ERM framework gap assessment findings (4 of 5)

Processes

	ERM Components	GPE practices in line with analogues	Gaps/potential areas for improvement	Gap	Criticality
3B	**Risk Assessment**	• Each risk in both the corporate risk and operational risk matrix/template are assessed by the 1st LoD, who is responsible for filling in the risk assessment templates, they: • provide a risk assessment rationale • assess probability and impact for each risk based on standardized scores, leading to an overall materiality risk level • Assessments are reviewed by RM team, Country team and FRC	• No systematic use of Key Risk Indicators (KRIs) to monitor and assess risks, which would be needed to trigger mitigating actions and/or a discussion on justification of cost/effort put into mitigations • Risk materiality ratings may not be filled out in a consistent manner and are currently not thoroughly reviewed and challenged • Due to overlap between 1st/2nd LoD (refer to component 1C), potential overlap/blind spots in reviewing risk assessments	◑	▲
3C	**Control and mitigation**	• 1st LoD is responsible for identifying, mitigating, and implementation as part of the RCSA as well as associated owners • Summary of sector and grant risks along with mitigation actions taken for focus contexts are well detailed and provide guidance on the current risk levels	• Some owners of mitigations are not the party responsible for the actual mitigation (e.g. 1st LoD) but are actually 2nd LoD members of the Secretariat that oversee the risk mitigation but do not perform them • Controls/mitigations are not linked to Key Control Indicators (KCIs) to monitor how well the control is implemented; also no assessment of the effectiveness of controls, which creates a risk of time and resources wasted on ineffective controls	◕	▲

GAP TO BEST PRACTICE

○ Small ◑ Medium ● Large

CRITICALITY OF GAPS

▲ Low ▲ Moderate ▲ High

Summary of ERM framework gap assessment findings (5 of 5)
Processes, Systems and infrastructure

	ERM Components	GPE practices in line with analogues	Gaps/potential areas for improvement	Gap	Criticality
3D	**Monitoring and reporting**	• All risk reports currently provide a view of the current risk level across all levels of reporting • Analogue organizations all had risk reporting that is transparent with full outputs of the RCSAs available for review by the board and committees	• No customized reporting to Board and FRC, with different level of detail/focus, little use of dashboards/visualization to help focus on top risks, limited education on risk framework/importance included in reporting, no use of KRIs/KCIs and longer-term trends • Many policy documents are mixed into Board or Committee reports – clear differentiation between reports and policy documents needed to ensure ease of use	◕	🟨
4	**SYSTEMS AND INFRASTRUCTURE**				
4A	**Systems and Infrastructure**	• Current RCSAs are simple excel reports which are in line with all analogues in reporting • Reporting is centralized within the risk department and shows historical changes in risk from the prior assessment	• Operational risk RCSAs need assistance by risk to be filled out properly by the country leads or the results are often stale or not consistent • Current reporting is manual and requires significant additional work to aggregate responses and present them for management, committees, and board of directors	◔	🟩

GAP TO BEST PRACTICE

○ Small ◑ Medium ● Large

CRITICALITY OF GAPS

🟩 Low 🟨 Moderate 🟥 High

We think that the majority of gaps could be addressed within the next ~18 months

Roadmap – assumes current GPE resources w/o external support

	1-2 months	*12-18 months*	*6 months*	*On-going*
	Phase 1: Foundation	**Phase 2: Design**	**Phase 3: Implementation**	**Phase 4: Enhancement**
Governance & culture		- *Develop **Risk Appetite framework** and statement, set appetite per major risk, develop framework governance* - *Develop a clear **risk governance** structure based on the three-lines of defense principles (assign 1st, 2nd and 3rd line roles and responsibilities per risk)*	- *Strengthen **risk culture** by communicating and providing training on revised Risk Management Framework – esp. on the Risk Appetite Framework, new risk governance and how results will impact GPE's strategy*	- *Introduce **periodic review** cycles of Risk Appetite Framework and risk governance* - ***Continue communication and training** efforts*
Strategy		- *Discuss options of how to strengthen the **link between risk and strategy** (soft vs. hard link) and agree on link type*	- *In case a soft link is preferred: Implement soft **link between risk and strategy***	- ***Potentially re-visit** decision to introduce hard link (in case soft link in the first instance)*
Processes	- *Review and simplify **risk taxonomy***	- *Develop initial set of **KRIs, Controls and KCIs** per risk* - *Re-design Risk-Control-Self-Assessment **(RCSA) template** – make use of new taxonomy and initial KRIs, Controls, KCIS* - *Further develop **risk dashboard** into a comprehensive monitoring and reporting tool*	- *Agree **limits for each KRI** in line with Risk Appetite Statement* - *Develop **customized risk reports** for Secretariat Mgmt., Committees and Board based on information contained in Risk Dashboard* - *Create **separate report and policy** documents*	- *Introduce **periodic review** cycles of processes and risk taxonomy*
Systems & Infra.		- *Re-design existing manual risk identification and assessment **tools** to increase ease of use for 1st line users and RM team*		- *Develop/buy software to **automate/system support** manual processes and tools, start with front-end*

For each required step we are suggesting parties responsible for development and implementation and sign-off responsibility (1 of 2)

ERM Component	Sub Component	Key Recommendation	Implementation responsibility	Sign-off
Governance and culture	Risk appetite	Develop Risk Appetite framework and statement, set appetite per major risk, develop framework governance	Risk Management to lead, involving Country Support Teams (CST), Finance and Risk Committee (FRC), Grant and Performance Committee (GPC), the Board, Representatives from Local Education Groups (LEG)/Grant Agents (GA)	Board
	Oversight, roles and responsibilities and ownership	Develop a clear risk governance structure based on the three-lines of defense principles (assign 1st, 2nd and 3rd line roles and responsibilities per risk)	Risk Management to lead, involving CST, FRC, GPC, Board, LEG and GA	Board
	Risk Culture	Strengthen risk culture by communicating and providing training on revised Risk Management Framework – esp. on the Risk Appetite Framework, new risk governance and how results will impact GPE‘s strategy	Risk Management to lead, with involvement/training targeted at all other units	None

For each required step we are suggesting parties responsible for development and implementation and sign-off responsibility (2 of 2)

ERM Component	Sub Component	Key Recommendation	Implementation responsibility	Sign-off
Strategy	Incorporation of risks into strategic planning	Discuss and agree whether to establish a soft or hard link between risk and strategy and in case a soft link is preferred: develop an approach how to embed this within strategic planning mechanism	Risk Management and CST to lead, involving FRC and GPC	Board
Process	Risk Identification	Introduce a simpler risk taxonomy	Risk Management to lead, involving CST	CFO/FRC
		Introduce a periodic review of the risk taxonomy	Risk Management to lead, involving CST	CFO/FRC
	Risk assessment, control and mitigation	Develop initial set of KRIs, Controls and KCIs per risk and agree limits	Risk Management to lead, involving CST, FRC, GPC, LEG and GA	Board
		Re-design Risk-Control-Self-Assessment (RCSA) template – make use of new taxonomy and initial KRIs, Controls, KCIS	Risk Management to lead, involving CST, FRC, GPC, LEG and GA	CFO/FRC
	Monitoring and reporting	Further develop risk dashboard into a comprehensive monitoring and reporting tool	Risk Management	None
		Develop a customized reporting for the FRC, GPC and Board	Risk Management	FRC/Board
Supporting systems and infrastructure	Supporting systems and infrastructure	Consider improvements to existing manual tools to improve ease of use for 1st line users and RM team	Risk Management	None
		Focus on “front-end” (i.e. 1st line/risk owners) system improvements and Software should be able to compile information from all individual RCSAs into one aggregated view/dashboard	Risk Management	CFO/Board

4 Detailed ERM framework gap assessment findings and recommendations

Preliminary hypothesis

1A Governance and culture: Risk appetite

Significant gap with no granular Risk Appetite Statement currently defined

Leading practices observations

- Clearly articulated Risk Appetite Statement at enterprise-level for setting guidance for organization-wide risk management and for setting stakeholder expectations
- The Risk Appetite Statement is linked to the institution’s mandate/strategy and sets clear boundaries and expectations by establishing quantitative limits and/or principle-based qualitative statements
- The statement is simple and easy to communicate to multiple stakeholders
- It is cascaded down to key risk categories
- Allows for risk oversight and risk ownership to be clearly defined:
  - BoD responsible for setting institution-wide risk appetite and reviewing adherence
  - BoD risk committee is responsible for controlling whether the institution has adequate risk management, monitors the implementation of risk strategies, ensuring in particular that they are in line with the defined risk tolerance
  - 1st line/risk owners accountable for ongoing risk assessment, monitoring and mitigation
- Risk Appetite Statement recognizes that risk management is a multi-dimensional problem that involves trade-offs
- Any decisions that will lead to a breach of risk appetite are only acceptable if an exception is granted by the body that issues the risk appetite
- Any unintended breach of risk appetite results in specific action to return risk exposure to an acceptable level

GPE practices in line with analogues

- GPE’s risk appetite articulated at a high level within its Risk Management Policy, defining that the organization’s overall appetite for risks as “moderate”
- GPE defines the risk appetite for two example risks and connects these directly to its strategic goals
  - The appetite for risks related to fraud and misuse of funds is defined as “very low”
  - The appetite for risks associated to work in fragile and conflict-affected states is defined as “moderate to high”

Gaps/potential areas for improvement

- No formal Risk Appetite Statement defined besides what is articulated in the Risk Management Policy because it is lacking guidance for risk limits and does not connect to GPE strategy
- Implicitly, some members of GPE committees and Secretariat staff understand Risk Appetite as the residual risk that cannot be mitigated away
- Risk Appetite is not defined systematically for all key risk categories
- There are no standardized/quantitative risk appetite tolerance levels defined and hence also not part of GPE’s risk monitoring and reporting
- The Board is not involved in setting and monitoring risk appetite on a regular basis
- There is no clear link between the prospect of risk appetite breaches and grant decisions
- Risk appetite breaches have no consequence

Assessment result:	◕ Gap to best practice	▲ Criticality

Work in progress

A well embedded Risk Appetite should define the constraints on strategy by articulating the levels of acceptable risk-taking

Benefits of Risk Appetite Statement

Improved Board awareness and ability to engage

- Board and management have confidence that risk-taking remains within internal and external expectations
- Generates cohesiveness between Board and management regarding Risk

Stakeholder management

- Articulate the key risk areas and appetite levels
- Demonstration to donors that risk-taking is appropriately constrained

Efficient planning and risk management

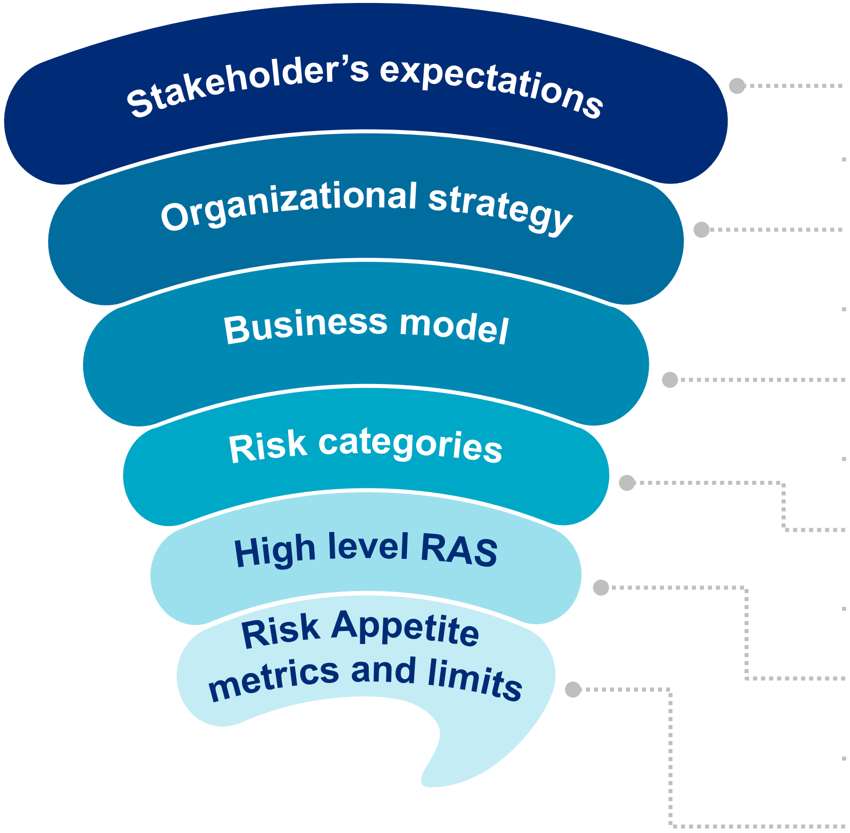
- Strategy and plans are aligned with agreed risk appetite constraints
- Framework for considering new strategies
- Negative trends on metrics drive early plans for remedial action

Better organization-wide understanding of risk issues

- Foundation for risk-adjustments in day-to-day decision making, boundaries are clear
- Supports a robust “risk culture” based of shared understanding of risks that can and cannot be taken

Work in progress

Setting an organization's Risk Appetite entails multiple steps and starts with the identification of its main stakeholders' expectations



DESCRIPTION

Who are the organization's main stakeholders and what are their expectations?

Which strategy enables the organization to meet its shareholders' expectations?

Which business model does the organization need to operationalize to follow its strategy?

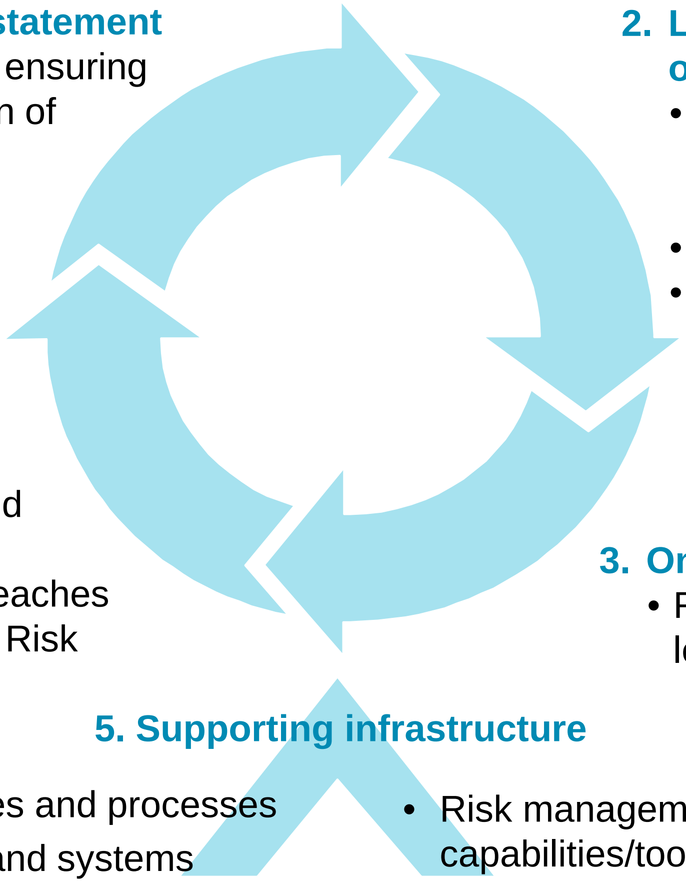
Which types of risks emanate from the organization's chosen business model?

What type and amount of risk is the organization willing to take in the pursuit of its strategy and business model?

Through which metrics and thresholds should the risk appetite statement be cascaded down to operational units (e.g. country levels and other decision takers)?

Work in progress

The Risk Appetite needs to be meaningfully embedded across all stages of the risk “life cycle”



1. **Articulation of Risk Appetite statement** (select metrics, calibrate levels, ensuring link to strategy and incorporation of stakeholder expectations)

2. **Linking Risk Appetite to operations**
   - Embedding in processes and decision-making, e.g. grant allocation, strategic planning
   - Potentially, country-specific RAS
   - Linking to limits and policies

3. **Ongoing reporting and monitoring**
   - Risk appetite thresholds and actual levels included in risk reporting

4. **Governance, oversight and breach management**
   - Committees, accountability and ownership of metrics
   - Mitigation plans in event of breaches
   - Governance around changing Risk Appetite calibration

5. Supporting infrastructure

- Policies and processes
- Data and systems
- Risk management capabilities/tools

Work in progress

Critical success factors to avoid common pitfalls and mistakes

Organizational	• Early and regular Board engagement, oversight and challenge • Senior management need to become risk appetite “literate” – Understand why metrics are important, why levels are right, what implications on institution’s performance and objectives are, etc.
Strategic	• Ensure risk appetite and medium-term strategy are aligned – Refresh Risk Appetite and Strategy in tandem, to ensure continued alignment
Governance	• Ensure clear, named, accountability in the event of a breach of risk appetite – Mitigation plans in place and enforced; implementation plans tracked – Metrics not allowed to remain “red” for any meaningful period of time • Leave some flexibility to management judgment – this should not stifle achieving goals and fostering innovation
Practical	• Conciseness is important – too many metrics/statements blurs the message • Better to have simple Risk appetite metrics that are understood and can be measured, than theoretically perfect ones that can’t • Only cascade what’s important to the places, and to the level, that drives it – this is not a one size fits all problem • Avoid over-engineered and rigid limits framework – a formulaic approach often isn’t needed • Embed into existing reporting and keep it simple, to allow management/the board to focus on the key areas and provide early visibility of actual or potential breaches • Get concepts into existing processes such as grant allocations, strategic planning, performance management

Work in progress

The high level Risk Appetite Statement should set the high level threshold for the organization’s risk profile stemming from pursuing its strategy and business model

Anonymized example: High level Risk Appetite Statement of a multilateral development bank

In pursuit of its strategy and business model the bank accepts to take on credit, market and liquidity risk up to the level where it remains aligned with the following high level risk appetite statement

- **The bank aims to remain compliant with its Statute and public mission**
- **The bank aims to do business in an ethical and fair way with proper regard for anti-money laundering and combating the financing of terrorism**
- **The bank aims to retain its long-term AAA-rating from all the major rating agencies, which is a primary pillar of the bank’s business model**
- **The bank aims for stability of earnings and preservation of the economic value of own funds in order to ensure the self-financing of the bank’s growth in the long term**

As a public institution, the bank does not aim to make profits from speculative exposures to risks. As a consequence, the bank does not consider its treasury or funding activities as profit-maximizing centers and does not engage into trading or arbitrage operations.

The bank does not engage in currency operations not directly required to carry out its lending operations or fulfil commitments arising out of loans raised or guarantees granted by it.

The bank’s ALM policy reflects the expectations of the main stakeholders of the bank in terms of stability of earnings, preservation of the economic value of own funds and the self-financing of the bank’s growth in the long term. The ALM strategy is therefore driven by these medium to long-term objectives and is not influenced by any short term views on trends in interest rates.

Work in progress

To steer and monitor the business, the high level risk appetite is translated into risk appetite metrics to which limits can be assigned

Anonymized non-profit client example: Tolerance levels for risk taking, high level risk appetite statement and translation into metrics and limits

Tolerance levels for risk taking

Zero risk tolerance

- Activities that the organization will not engage in and for which it will have zero risk tolerance

Moderate risk tolerance

- Risk taking based on activities that are a by-product of operating a materially significant fund, to be carefully managed

Considerable risk tolerance

- Risk taken to achieve strategic impact

High level risk appetite statement

- Briefly lays out for each of the appetite levels above, which key risk categories the organization is willing to take or not take (e.g. zero risk tolerance for breaches of international sanctions and willingness to accept considerable uncertainties around investment risks to achieve strategic objectives)

Specification of tolerance levels and risk appetite metrics for one exemplary major risk category

Risk category	Tolerance level	Rationale	Risk appetite metric & limit
Concentration risk	*Moderate risk tolerance*	*To ensure that the organization maintains a diverse portfolio to optimize deployment of its financial resources, it will maintain prudential risk appetite levels on the amount of funding allocated to countries and project types*	*No more than 50% (appetite level)/30% (warning level) of total investable amount into a single country* *No more than 10% (appetite level)/5% (warning level) into a single project type*

Work in progress

The Risk Appetite Framework Governance should follow the three-lines-of-defense principles as presented in the example below

Recommended 3 lines of defense structure for RAF

	Local 1st line of defense	Shadow 1st line of defense	2nd line of defense	3rd line of defense
Party	Grant Agents, Partnership, Local Education Group etc.	Country Team at the Secretariat	Secretariat Risk Management with input from Committees and BoD	E.g. World Bank Audit unit or GPE Internal Audit service (either in-house or outsourced)
Role	Take risk appetite into account in day-to-day operations	Joint risk ownership/supervisory of country and sector risk	Set RAF/Monitor Risk Appetite	Validate Effectiveness of RAF
Responsibilities	• Manage grants and operations in line with operational plans, risk appetite and operational limits • Manage disbursement of funds for grants • Manage and monitor grant and country risks after disbursement • Identification and assessment of risks, controls, KRIs/KCIs via RCSA	• Manage country and sector risks including the risk appetite and operational limits • Coordinate risk control and mitigation activities with Local 1st line of defense • Provide review and input for Identification and assessment of risks, controls, KRIs/KCIs via RCSA for joint risk ownership	• Develop and establish risk appetite framework • Articulate risk appetite statement and set boundaries with input from Board of Directors and relevant committees • Monitor actual risk profile against set appetite • Provide reporting on risk profile vs. risk appetite • Escalate risk appetite breaches and the appropriate mitigation actions	• Assess effectiveness of risk appetite framework and adherence to best business practices • Provide assurance on effectiveness of risk appetite framework to Board of Directors

Governance and culture: Risk appetite
Key recommendations

1

Agree Risk Appetite Framework governance in line with three lines-of-defense principles

- Agree 1st line (who to take risk appetite into account in day-to-day operations), 2nd line (who to develop the framework and monitor risk profile against appetite) and 3rd line (validate effectiveness of RAF) – pg. 31

2

Specify risk tolerance levels, **review risk categories (once in place) in light of GPE mission & strategy**

- Agree ~3-5 levels of risk tolerance for the organization (e.g. zero, moderate, high tolerance)
- Discuss and agree which risks should have a low or high risk tolerance, e.g. low tolerance with regard to breaches of international sanctions, fraud etc. vs. high with regard to program risks

3

Develop high-level organization-wide Risk Appetite Statement

- Max. 1 page length, refer to page 29 and 30 as examples
- Should specify a risk tolerance level for each risk category and lay out rationale (e.g. GPE's strategic objective to promote educational paradigm shift justifies higher tolerance for program/impact risks)

4

Specify risk appetite (incl. KRI metrics and limits) for all key risk categories

- Be as specific as possible in expressing appetite for each risk category (e.g. for FX Risk, explain where FX risk comes from, why it potentially cannot be eliminated 100% due to uncertainty of future outflows…)
- To the extent possible, put key risk indicators (KRIs) in place to measure the level of risk over time and monitor those – e.g. number of adverse publicity/media statements
- For risks where you have defined KRIs, agree quantitative appetite limits (e.g. number of press articles)

5

Agree how to handle breaches

- Agree a process on how limit breaches are dealt with – e.g. immediate reporting to the board, who will have to decide on mitigating actions to be put in place

Preliminary hypothesis

1B Governance and culture: Oversight

Gap over lack of clarity over allocation of risks between oversight layers

Leading practices observations

- Separation of risk-taking, control and oversight to avoid conflict of interest
- “Three lines of defense” structure for risk management and control oversight
  - 1st: Business owners implementing controls/managing risks
  - 2nd: Risk Management and Compliance teams set internal risk policies/standards, monitor and challenge 1st LoD risk assessment as well as adherence to policies/standards and risk appetite
  - 3rd: Independent audit function reviews risk management environment and tests controls
- Risk oversight within large organizations often has the following layers of oversight:
  - Appropriate risk demarcation between layers of oversight – i.e. risks seen by Board are significant enough to warrant senior review and they do not review lower priority risks
  - Working groups (operational level, but may include members of executive management) in place for greater focus on specific risks and allows for greater cross-functional collaboration

GPE practices in line with analogues

- Board and Finance and Risk Committee in place who’s main role is to challenge and oversee risks and GPE’s Risk Management Framework
- Finance and Risk Committee can directly report to the BoD
- World Bank provides audit function for the GPE Secretariat and Grant Agent activities are audited by each Grant Agent’s internal audit department and per external audit arrangements
  - Grant Agents apply their own applicable audit requirements to sub-grantees (Governments and other organizations) when applicable as well

Gaps/potential areas for improvement

- Challenge for the board to provide effective oversight as all risks are presented to them with little prioritization/little focus on higher priority risks
- Overlap between 1st and 2nd line of defense risk management activities
  - FRC, GPC, and SIC are assigned ownership of risks but at the same time supposed to monitor and oversee the risk and control environment
  - The Partnership as well as the Local Education Group is not sufficiently assigned 1st line of defense responsibilities

Assessment result:	◐ **Gap to best practice**	△ **Criticality**

Preliminary hypothesis

1C Governance/Culture: Roles and Responsibilities

Roles lack specific responsibilities to prevent ambiguity and create clear responsibilities

Leading practices observations

- Roles and responsibilities for managing risk are clearly defined including the interfaces between various layers of risk oversight and staff responsible for managing controls/operational staff, specialist functions and internal audit
  - Clear accountability and unambiguous points of contact between various risk classes, business units and internal audit
  - Independence of risk functions from other executive management and operational management
  - Roles and responsibilities allow for clear understanding of how risks spanning multiple business owners/departments are managed
- Generally observed that ultimate responsibility for risk management decision lies on the Board, part of this responsibility is to ensure adequate engagement with key aspects of risk management process

GPE practices in line with analogues

- Board and committees review risk matrix and corporate risks and provide oversight of the risk management process
- Roles and responsibilities of the board, SIC, GPC , FRC, and secretariat are defined with respect to risk management in the Risk Management Policy
- Key risk including the operational risk framework and the corporate risk matrix have assigned owners responsible ensuring completion and participation from needed parties
- Some key risks and mitigation actions ae owned by the board

Gaps/potential areas for improvement

- Overlap of risk ownership and risk oversight is ambiguous due to an overlap between the 1st and 2nd line of defense risk management responsibilities
- Enough time is not being dedicated to review of risk processes due to competing priorities/responsibilities
- The role of audit is not defined in the risk management policy providing scope of their work and associated responsibilities for GPE
- Board and committees review full risk matrix and corporate risks – no prioritization on key issues and risks

Assessment result:	◐ Gap to best practice	▲ Criticality

1D Governance/Culture: Risk ownership

Ownership of risks could be improved through process enhancements for determination of ownership and mitigation

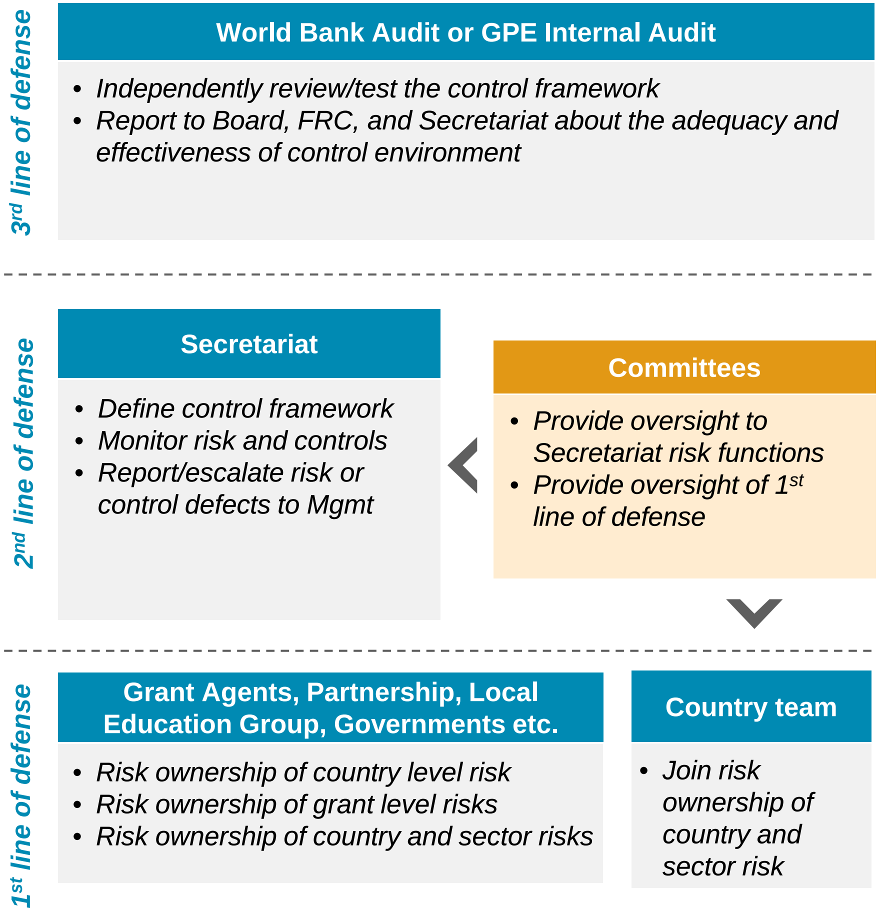
Leading practices observations	GPE practices in line with analogues	Gaps/potential areas for improvement
• Risk ownership and control management is ultimately aligned to staff with operational responsibility (e.g. risks which are relevant to each committee are owned by the specific committee and organization wide risk are centralized and owned by the Secretariat) • Risk ownership is clearly allocated – Risk owners are not allocated more risks than they can be expected to manage effectively – Risks which apply to multiple business/local units/are enterprise wide are centralized in their ownership although may have co-owners to manage mitigants – Responsibilities related to risk ownership are widely understood	• Risk owners are assigned for all risks within both the risk matrix and the operational risk framework • Ownership of risks and the associated responsibilities are aligned with appropriate parties	• Risk ownership often not assigned to those with actual control over the outcomes, esp. third parties at country level such as grant agents, education sector • Process for determining risk ownership is not clearly outlined in the process documents for the operational risk framework and corporate risk matrix • FRC does not have enough time during semi-annual meetings allocated to review/challenge risk ownership

Assessment result:	◐ Gap to best practice	▲ Criticality

Work in progress

Simplification of the governance structure and the associated roles and responsibilities will remediate many gaps

Potential 3 LoDs GPE risk governance structure (illustrative, for discussion)



3rd line of defense

World Bank Audit or GPE Internal Audit

- *Independently review/test the control framework*
- *Report to Board, FRC, and Secretariat about the adequacy and effectiveness of control environment*

2nd line of defense

Secretariat

- *Define control framework*
- *Monitor risk and controls*
- *Report/escalate risk or control defects to Mgmt*

Committees

- *Provide oversight to Secretariat risk functions*
- *Provide oversight of 1st line of defense*

1st line of defense

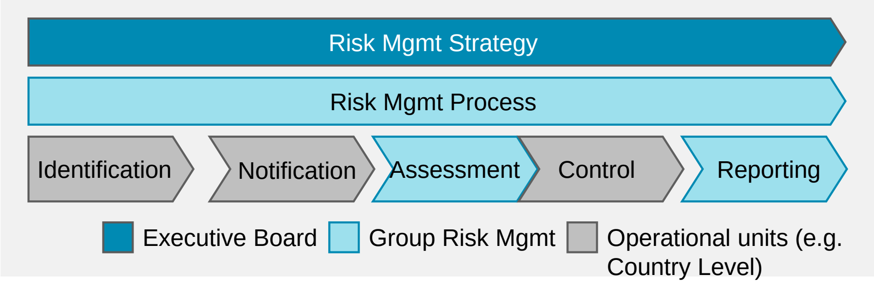
Grant Agents, Partnership, Local Education Group, Governments etc.

- *Risk ownership of country level risk*
- *Risk ownership of grant level risks*
- *Risk ownership of country and sector risks*

Country team

- *Join risk ownership of country and sector risk*

Potential Roles & Responsibilities across risk management, (illustrative, for discussion)



Risk Mgmt Strategy

Risk Mgmt Process

Identification → Notification → Assessment → Control → Reporting

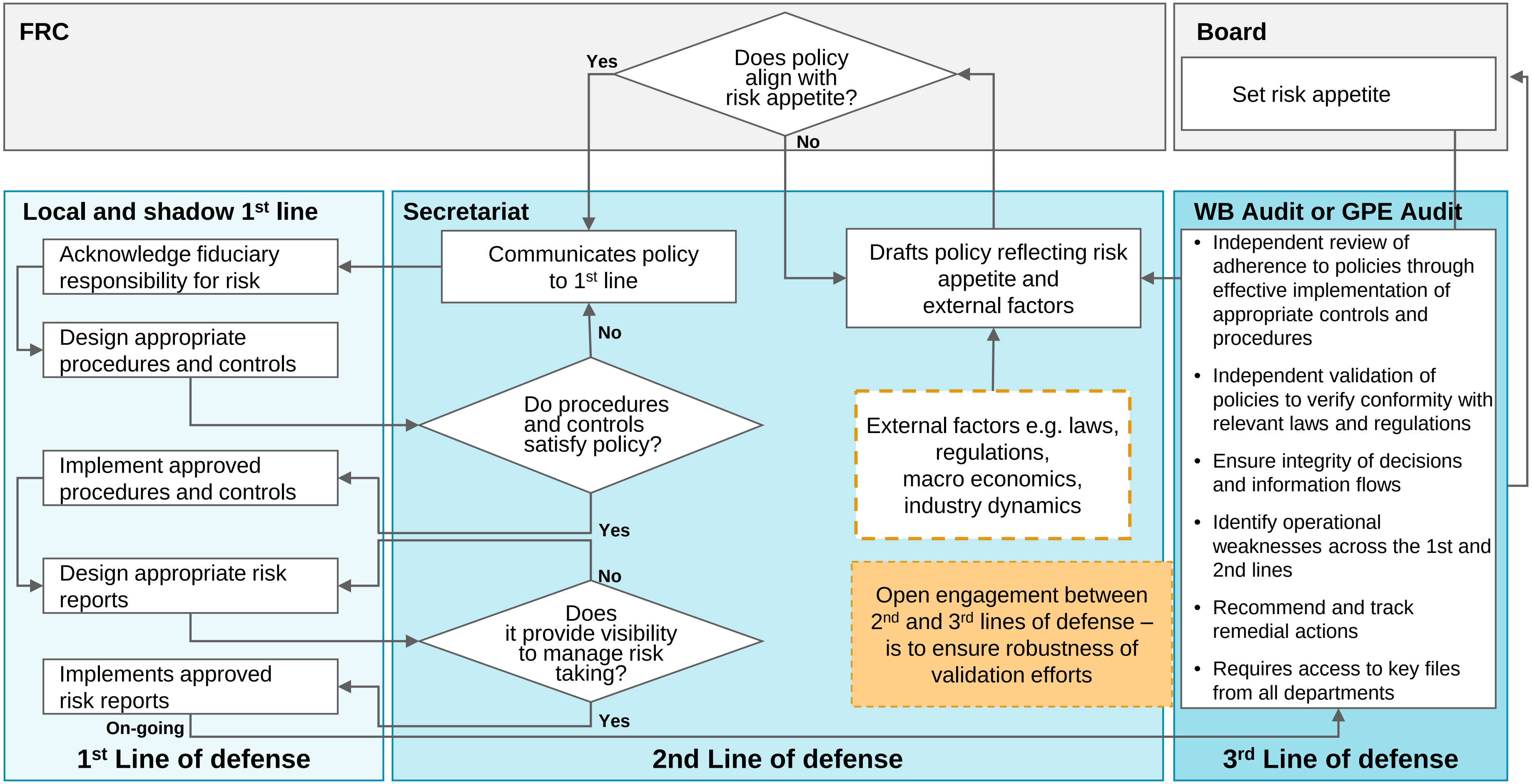
■ Executive Board ■ Group Risk Mgmt ■ Operational units (e.g. Country Level)

	Description	Owner
Risk Mgmt Strategy	• Risk appetite • Risk management principles	Board FRC
Risk Mgmt Process	• Process to implement risk strategy	Secretariat Committees
Identification	• Identify threats, cause of losses/malfunctions	1st line
Notification	• Regularly inform GRM the risks identified	1st line
Assessment	• Assess risks in both quantitative and qualitative manner	Secretariat
Control	• Risk control to minimize risk	1st line
Reporting	• Board is informed of material risks' assessment and countermeasure	Secretariat

Work in progress

Example of clear roles and responsibilities to assist in ensuring the risk appetite cascades through the organization effectively and at all levels

Potential roles and responsibilities for 1st, 2nd and 3rd lines of defense (illustrative, for discussion)



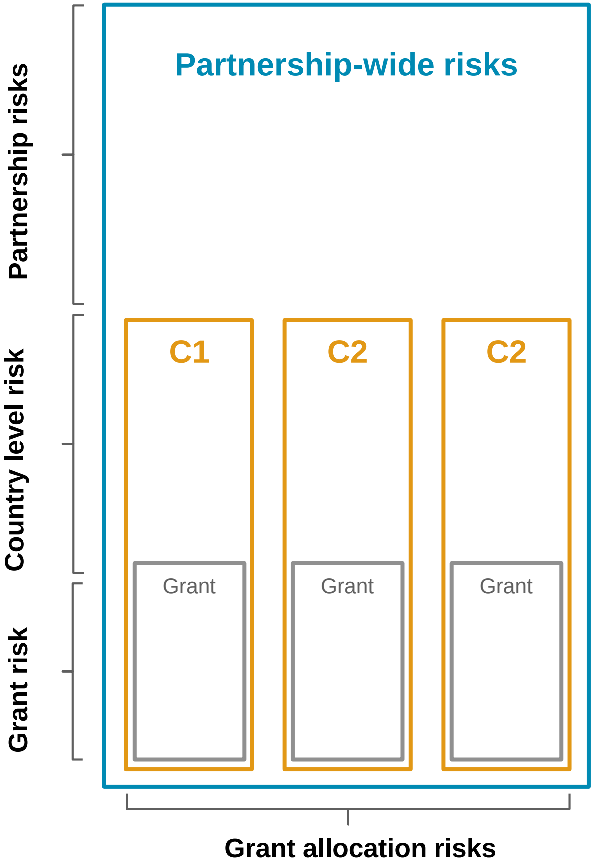
FRC
Board
Set risk appetite
Does policy align with risk appetite?
Yes
No
Local and shadow 1st line
Secretariat
WB Audit or GPE Audit
Acknowledge fiduciary responsibility for risk
Design appropriate procedures and controls
Implement approved procedures and controls
Design appropriate risk reports
Implements approved risk reports
On-going
Communicates policy to 1st line
No
Do procedures and controls satisfy policy?
Yes
No
Does it provide visibility to manage risk taking?
Yes
Drafts policy reflecting risk appetite and external factors
External factors e.g. laws, regulations, macro economics, industry dynamics
Open engagement between 2nd and 3rd lines of defense – is to ensure robustness of validation efforts
1st Line of defense
2nd Line of defense
3rd Line of defense

- Independent review of adherence to policies through effective implementation of appropriate controls and procedures
- Independent validation of policies to verify conformity with relevant laws and regulations
- Ensure integrity of decisions and information flows
- Identify operational weaknesses across the 1st and 2nd lines
- Recommend and track remedial actions
- Requires access to key files from all departments

Work in progress

Key drivers for determining risk ownership are the type of risk and the impact on GPE

Example: Approach to risk ownership by risk type



Description	Example risk	Proposed ownership
Risks which apply to most or all areas of the partnership	**Programmatic risk** – The risk that GPE does not achieve its strategic goals	• Risk could be owned by all 1st line of defense owners with consistent **Partnership** participation • Oversight by the **Secretariat and SIC** is important for partnership level risks with high overall risk levels
Risks which apply to a particular country	**Sector risk** – risks related to ESP quality and implementation as well as domestic financing	• Risks that are related to specific countries could be owned by **Partnership, LEGs, Developing Country Partner Governments, and joint ownership by the Country Leads** oversight by the **Secretariat and FRC**
Risks pertaining to specific grants	**Misuse of funds risk** – GPE funds are diverted from their intended purpose through fraud or other forms of misuse	• Grant level risks could be owned by **Local education group and grant agents** with oversight by the **Secretariat**
Risks pertaining to a grant allocation	**GPE funding risk** – Support to countries: The risk of disruption in country-level processes due to problems in the implementation of the GPE funding model.	• Grant allocation risks could be owned by the **Secretariat** with oversight by the **GPC** and **Secretariat**

Governance and culture: Oversight, roles and responsibilities and ownership
Key recommendations

1

Develop a clear risk governance structure based on the three-lines of defense principles

- Develop a risk governance structure that is aligned with the approach to risk management you choose as an organization (a decentralized approach (Gavi model) or a centralized approach (GF, GCF model))
- The current RM approach raises expectations that cannot be met given the current setup

2

Establish 1st line of defense

- In a decentralized approach: risk ownership would be owned only by the Local Education Group/ Grant Agents with low level of involvement of the Secretariat, LEGs/GAs are responsible for primary risk management functions
- In a centralized approach: Local risk are also owned by LEGs/GAs but in joint ownership with Secretariat Country Teams

3

Establish 2nd line of defense

- In a decentralized approach: Secretariat provides oversight of 1st line of defense however strong reliance on LEGs and grant agents to adhere with the risk management policy and procedures. Focus on standards/policy setting by Secretariat
- In a centralized approach: Secretariat provides stronger oversight and challenge. Works closely with the local teams to ensure policies and standards are met. Additional oversight by the FRC, GPC, and SIC to help monitor and assess risk

4

Establish 3rd line of defense

- For both approaches: Strengthen audit activities by either agreeing a customized audit agenda leading to more dedicated support with the World Bank, mandating external auditors or establishing an independent audit unit at the Secretariat level, who is also tasked to do on-site inspections from time to time. Benchmarking suggests the latter as common and leading practice and given GPE has no local staff, we think a strong internal audit function is crucial for GPE

5

Re-assign risk ownership, ensure efficient oversight

- Assign risk ownership to the extent possible to the 1st line, who has operational responsibilities and manages risks (i.e. Partnerships, Local Education Groups, GPC for grant allocation)
- Differentiate between oversight responsibilities of the board (focus on setting risk appetite and reviewing high impact, high probability risks, reviewing risk appetite breaches and deciding mitigating actions) and of the committees (overseeing the whole risk framework, input on policies and work of the Secretariat)

Preliminary hypothesis

1E Governance/Culture: Risk culture

Strong risk based principles could be improved with enhancements to the risk appetite and stronger links to GPE strategy

Leading practices observations

- Strong understanding of risk by staff at all levels of the organization – particularly risk relevant to each staffs’ area of focus
  - Institutional acceptance that understanding and managing risk is a universal responsibility and a critical component to the organization's core work
  - Culture encourages open and free discussion and full disclosure of risks with staff not feeling that they cannot raise risk issues and discuss openly
  - Common risk language applied across the organization
- Open discussion about risk by management across company communications is evident and frequent
  - Risk management viewed as an opportunity and core competency rather than a compliance culture
  - Risk management elements embedded into performance management culture of organization and staff incentive setting incorporates risk elements
- Board and senior-management are very engaged in risk matters including committee meetings, and significant risk visibility at Board level

GPE practices in line with analogues

- Risk based principles of management and a culture of risk awareness are described in the risk management policy
- Discussion of communication and risk is described including an emphasis on clear continuous communication between GPE and its partners about risk
- Board and committees have visibility on key risks and are involved in mitigation as needed
- Risks are treated with common and consistent language across the organization including the impact, probability and level
- Strong understanding of how risks impact the GPE’s mission and the importance of risk control (e.g. misuse of funds)

GPE gaps identified

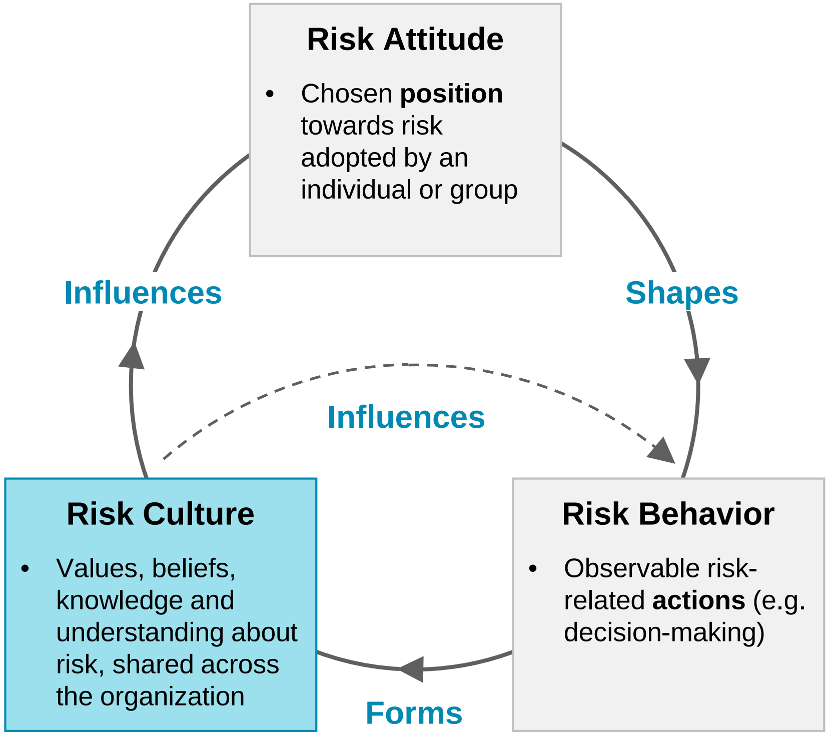
- Risk appetite does not set risk level thresholds to allow the organization to understand which risks should be focused on that may impact GPE’s strategy
- Risk not seen as a priority to majority of staff as many do not see how risk would influence grant allocation, strategy decisions or day-to-day operations

Assessment result:	◔ **Gap to best practice**	▲ **Criticality**

Work in progress

Developing a strong “risk culture” is seen as the “glue” in the ERM framework, a key element to reinforcing risk behavior

Risk Culture influences the attitude and behavior against risk…



Risk Attitude

- Chosen **position** towards risk adopted by an individual or group

Risk Behavior

- Observable risk-related **actions** (e.g. decision-making)

Risk Culture

- Values, beliefs, knowledge and understanding about risk, shared across the organization

Source: IRM

…Hence poor risk culture can undermine the integrity of risk management across the organization

Symptoms of poor risk culture

- **Risk-taking not aligned with risk appetite**
  - Policies and rules poorly adhered to
  - Risk concerns ignored or circumvented
- **Risk avoidance**
  - Paranoia, fear or blame culture
  - Constraint on innovation and change
  - Impact on client relationships
- **Risk control failures**
  - Repeated compliance or policy breaches
  - Operational loss events and reputational damage
- **Dysfunctional relationship between business and control functions**
  - Decisions endlessly debated, revisited or escalated
  - Poor morale and high staff turnover
  - Insights and advice from either side ignored

Governance and culture: Risk culture

Key recommendations

1

Strengthen Risk culture via stronger understanding of Risk Appetite

- Once the Risk Appetite Framework is in place, communicate this very clearly to 1st line and monitor whether risk appetite is taking into account in day-to-day decision making and if limits are breached, escalate to FRC and BoD to agree mitigating actions

2

Strengthen Risk culture via assigning more risk ownership to 1st line/operational staff

- Communicate to 1st line that they are responsible for managing risks and putting controls and mitigating actions in place and that the 2nd line Risk Management function at the Secretariat level is there to support them

3

Strengthen Risk culture via creating direct links between risk and strategy

- Refer to page 44 on Incorporation of risk into strategic planning

2 Strategy: Incorporation of risks into strategic planning
Link between strategy and risk management is not well articulated

Leading practices observations

- At some non-profit organizations, risk is considered in organization-wide strategy planning activities and grant/investment decisions
  - Role of risk management in strategic planning and new initiative development articulated in strategic planning or risk management policies
  - At some organizations, such as GCF, Risk perspectives are a key initial input to project planning and development and grant/investment decisions
  - Risk can be considered for on-going projects (e.g. grants/loans paid out in tranches if performance milestones are achieved and risks are within foreseen limits)
- Risk monitoring and mitigation have a key role in the strategic planning and resource allocation
  - Risk signs off on plan, with a final check of plans vs. risk appetite limits
  - Risk management is seen as a partner to the business and not an obstacle, and is perceived an important participant in the debate on grant strategy

GPE practices in line with analogues

- Risk and the associated accountability such as monitoring and mitigation are described in the Risk Management Policy as they relate to strategy
- GPE describes how risk and opportunities are linked due to its strategy and unique operating conditions of delivering in vulnerable and at-risk areas

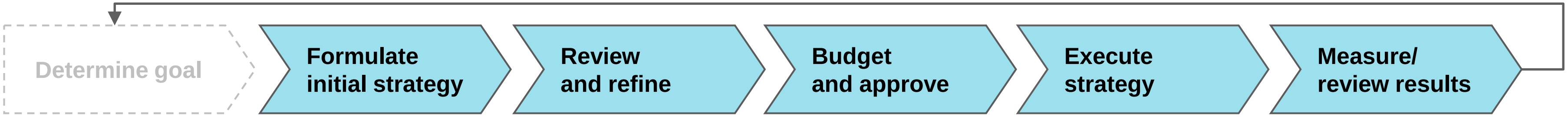
Gaps/potential areas for improvement

- Risk appetite is not directly linked to GPE’s strategic plan including information of how risks could impact the strategic plan
- Policy documents are lacking discussions on strategy and the high risk nature of GPE mission which is important due to vulnerability of countries the partnership works in
- Risk is not factored into the grant allocation formula
- Grants are not paid out in tranches, i.e. independent of interim project milestones and development of risk levels
- Risk mitigations are not directly linked to GPE strategy but are instead only meant to deal with inherent risk and minimize residual risk, i.e.
  - Risk mitigation comes at a cost. Cost is justified if it sufficiently increases expected return (by reducing risk)
  - Lack of deliberate consideration whether mitigations should be undertaken (if cost is justified) or not

Assessment result:	◕ Gap to best practice	▲ Criticality

GPE can establish a soft link between risk and strategy by actively involving risk in strategic planning and – if desired – a hard input into grant allocations

Soft link: Establish role for risk management within the strategic planning cycle and new project evaluations led by Country Support Teams and Grant & Performance Committee



Determine goal

Role & Authority of RM

Formulate initial strategy

- Establish risk baseline based on risk appetite
  - Targets/limits from appetite to guide risk-taking, **e.g. country/concentration limits**
- No direct authority, provide guidelines on risk appetite

Review and refine

- Assess risk implications of proposed strategy/projects
  - Identify/assess potential risks
  - Derive strategic implications
  - Provide risk profile for each strategy
- RM empowered to request changes to aspects of strategic design and additional clarity over risk mitigation

Budget and approve

- Provide final assessment of risk implications of business plan
- Approval of control and monitoring framework proposed for key risks
- Guidance on risk control design
- Provide risk sign-off on plan
- Includes veto rights for new initiatives and right to conditional approval

Execute strategy

- Guidance on risk control implementation
- Enforcement of control implementation

Measure/ review results

- Review and update risk assessments performed
- Flag the risks that have actually occurred/or more likely to occur
- In case situation has changed or unexpected events have occurred, RM should flag these

Hard link: Include risk within grant allocation decisions

- Consider including risk appetite limits and Key risk indicators as an integral part of the grant allocation formula, e.g. maximum amount of funds that can be allocated to certain countries/projects depending on risks associated with the country/project (e.g. level of fraud risk, impact risk etc.)
- Consider to pay out grants in tranches depending on whether project milestones have been achieved and risks associated with a project are within limits
- **Rationale:** Despite GPE’s mission to support educational paradigm shift in high risk countries, which by its nature is associated with high risks, available funds for allocation by GPE are limited. Hence, grants should be allocated to countries where the biggest risk-adjusted return (i.e. impact after risk) is expected.

Strategy: Incorporation of risks into strategic planning
Key recommendations

1

Discuss and agree whether to establish a soft or hard link between risk and strategy

- Facilitate a discussion among GPE Management and the Board about their ambition level of how to link risk management considerations and outcomes to strategic decisions, most notably grant allocations
- Despite GPE's mission to support educational paradigm shift in high risk countries, which by its nature is associated with high risks, available funds for allocation by GPE are limited. Hence, grants should be allocated to projects/countries where the biggest risk-adjusted return (i.e. impact after risk) is expected
- Hence, we recommend to make the link as strong as possible (i.e. Option 2 below), which we think would help GPE to improve its risk culture and understanding of the importance of risk and how it impacts decision making/day-to-day operations. But we also understand from discussions with you that you may prefer are softer link to strategy (i.e. Option 1) given you have just undertaken a review of your grant allocation process

Option 1: Establish soft link

- Review strategic planning process that is led by Country Teams and GPC and evaluate how to best involve Risk Management (in line with typical process steps and responsibilities taken on by RM

Option 2: Establish hard link

- Review grant allocation formula and decide how to make risk appetite and outcomes (KRIs) and integral component of the formula, consider paying grants out in tranches depending on whether programs/projects are on track with interim milestones and risk levels are within limits

3A Processes: Risk Identification

Risk taxonomy is currently too granular and could be simplified to improve the efficiency of other risk processes

Leading practices observations

- Establish a comprehensive inventory of risk types and risks (risk taxonomy)
- Ensure risk identification is forward-looking and considers both financial risks and non-financial risks
- Aggregate risk information from the following sources including but not limited to:
  - Risk and Control Self-Assessment (RCSA)
  - Industry or country-wide emerging risks
  - Risk appetite tracking metrics identified in previous identification processes
  - External research to identify historical risks that have caused damage to analogue organizations
  - Near misses, i.e. risks that had almost materialized
  - Add risks to the risk inventory and remove risks that are no longer relevant
  - Identification of issues found in Audit Reports
  - Project progress reports to identify forward looking risks

GPE practices in line with analogues

- A total of 36 risks are assessed through a corporate risk self assessment template
- The operational risk template assesses 6 risks, which form a subset of the Corporate Risk Matrix, filled in by local third parties
- Users can identify and make suggestions for new risks to be added
- It is a forward looking assessment that looks at the next 3 yr. period

Gaps/potential areas for improvement

- The current taxonomy is too granular and could be simplified to create ease in other risk processes such as assessments
  - Risks are clustered into four main categories (strategic, programmatic, financial and governance) with in total 36 sub-risk types
  - Low number of main risk categories and overlaps between sub-risk types
- New risks have been added to the corporate risk matrix which has grown the number risks without sufficient discussion or vetting
- Operational risk templates are difficult to fill out for members of the country teams and often result in similar outputs each year
- Audit reports performed by grant agents, Results Report, and other tools are not currently feeding in to the risk identification process
- Evidence of the risk identification process is not well outlined in the RAS or risk polices

Assessment result:	◐ **Gap to best practice**	△ **Criticality**

Risk identification processes should be simple but involve stakeholders across all of GPE

The risk identification process should

1

- **Cover all of GPE** including the secretariat, grant agents, and partnership

2

- **Engage the first and second lines of defense**
  - Responsibility for identifying new risks lies with the first LoD, however process is coordinated and results are challenged by the second LoD
  - Country level input is needed to ensure holistic coverage of risks within a country/program (including strategic risk)
  - Risk input is needed to assess risks across all units/countries

3

- **Leverage existing information** wherever possible (i.e. avoid "reinventing the wheel") but go beyond what exists today
  - Avoid overlaps between what the 1st line at a country level does and what the Secretariat does, i.e.

4

- **Be as streamlined as possible** to get the biggest "bang for buck" and ensure the process can be completed efficiently
  - Focus on most major risks to the organization, rather than excessive focus on exhaustiveness
  - Use straightforward risk assessment templates to focus assessments on most relevant information
- Note: the process will serve as foundation for future enhancements, as learnings from the process are incorporated into future iterations

During the risk identification process, there should be a distinction made between risk drivers, risk event types and risk outcomes

Risk drivers

- Risk drivers are specific market/country/external developments that may greatly impact GPE (e.g. exchange rate fluctuations, new governments)
- They may impact several risk types (e.g. state bankruptcy may impact sector risk)
- Risk drivers are needed to be understood to analyze how they would impact GPE
- The focus should therefore be on identifying the most critical drivers rather than a comprehensive list

Risk event types/categories

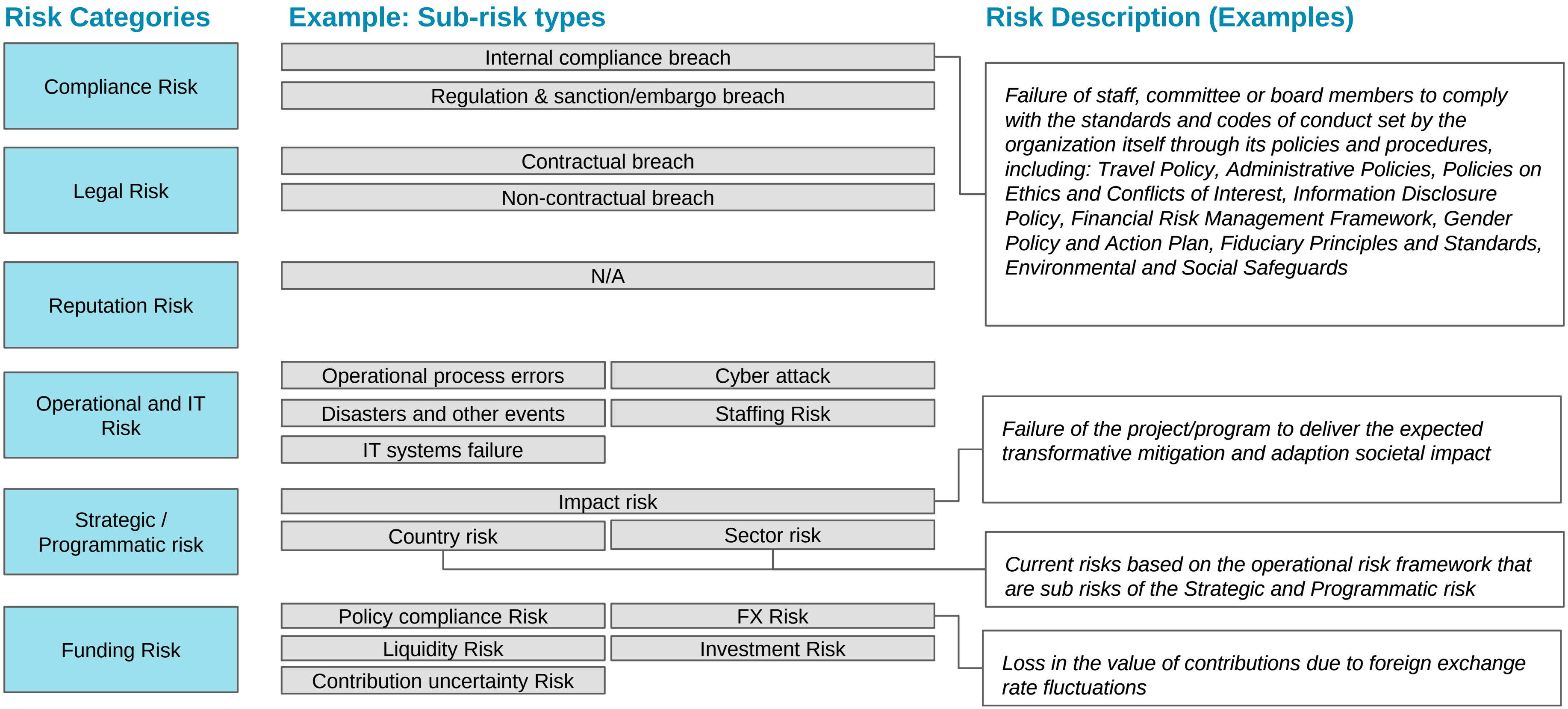
- These are traditional risk types like these identified in the risk framework (e.g. fraud risk)
- However, to ensure full risk coverage, “difficult to quantify” risks must be assessed (e.g. reputational risk)
- Risk management will define risk categories at several levels, e.g. fraud risk (“Level 1”) and can be further broken into misuse of funds risk (“Level 2”)
- Risk categories are generally used to ensure appropriate risk management (e.g. policy, limit-setting and other controls); therefore, they need to be comprehensive in their coverage of risks

Risk outcomes

- Risk outcomes are the impact to an organization that is generated when a risk materializes
- Generally, two types of outcomes are distinguished:
  - Direct (financial) losses
  - Indirect (non-financial) losses (e.g. reputational damage, staff time, opportunity costs)

GPE should create a simplified taxonomy that is “Mutually Exclusive, Collectively Exhaustive” based on high level risk categories linked to their strategy and mission

Possible Risk Taxonomy for GPE



Risk Categories

Compliance Risk

Legal Risk

Reputation Risk

Operational and IT Risk

Strategic / Programmatic risk

Funding Risk

Example: Sub-risk types

Internal compliance breach

Regulation & sanction/embargo breach

Contractual breach

Non-contractual breach

N/A

Operational process errors

Cyber attack

Disasters and other events

Staffing Risk

IT systems failure

Impact risk

Country risk

Sector risk

Policy compliance Risk

FX Risk

Liquidity Risk

Investment Risk

Contribution uncertainty Risk

Risk Description (Examples)

Failure of staff, committee or board members to comply with the standards and codes of conduct set by the organization itself through its policies and procedures, including: Travel Policy, Administrative Policies, Policies on Ethics and Conflicts of Interest, Information Disclosure Policy, Financial Risk Management Framework, Gender Policy and Action Plan, Fiduciary Principles and Standards, Environmental and Social Safeguards

Failure of the project/program to deliver the expected transformative mitigation and adaption societal impact

Current risks based on the operational risk framework that are sub risks of the Strategic and Programmatic risk

Loss in the value of contributions due to foreign exchange rate fluctuations

Processes: Risk identification
Key recommendations

1

Introduce a simpler risk taxonomy

- Review current risks included in the Corporate and Operational Risk Matrix in terms of completeness and overlaps. Some initial observations for consideration:
  - Overlaps: Many strategic/impact risks seem to granular and should be rather considered as risk drivers. See page 43 as an analogue example
  - Completeness: Ensure meaningful main risk categories are in place, e.g.:
    - Consider combining strategic and programmatic Risks be into one category "Risk of Program Failure"
    - Consider adding a "Reputational Risk" and a "Legal & Compliance Risk" Category? Expanding Governance into "Governance, Operational and IT"?
- Agree key risk categories to be monitored and sub-risk types. Benchmarks from for-profit and non-profit organizations suggest that about 5-10 main risk categories ensure sufficient granularity to make them meaningful while ensuring manageability
- Risk Management to propose and suggest risk categories to the FRC and Board

2

Introduce a periodic review of the risk taxonomy

- Agree an (e.g. annual) review of the risk taxonomy, led by the Risk Management team at the Secretariat with input from Country Teams and sign-off by the FRC and Board
- Audit findings should be reviewed by the Secretariat for new risks that have potentially emerged

3B Processes: Risk assessment

Current risk assessment lacks systematic use of KRIs/KCIs and input from a variety of participants to improve coverage within the partnership

Leading practices observations

- Conduct interviews with identified subject matter experts and stakeholders regarding what data can feasibly be gathered and which metrics will provide the most insight into risk
- Evaluate and challenge identified metrics
  - Identify which KRIs serve as the best predictors of the risks which can be used for risk appetite/reporting metrics
  - Select the most useful metrics as KRIs for reporting
- Identify people/committees to survey about risks
- Aggregate risk data from 1st line units through workshops, interviews, process analyses, key risk indicators, data tracking (process administered by the Risk function)
- Have a risk-self assessment (RCSA) template in place and ensure that the RCSA asks about the following topics:
  - Risk-creating actions undertaken by the front line units
  - Risk limits and acceptable levels of variance (both above and below the limit)
  - Risk prevention and mitigation strategies
- Ensure risk assessments and impact/likelihood ratings assigned by first line of defense are reviewed and challenged by the second line of defense and risk type committees
- Assign each risk a materiality rating from the risk assessment performed by the risk owners

GPE practices in line with analogues

- Each risk in both the corporate risk and operational risk matrix/template are assessed by the 1st LoD, who is responsible for filling in the risk assessment templates, they:
  - provide a risk assessment rationale
  - assess probability and impact for each risk based on standardized scores, leading to an overall materiality risk level
  - identify mitigating actions
- Variety of participants from the first line participate in risk assessment including country leads
- Assessments are reviewed by RM team, Country team, GPC, and FRC

Gaps/potential areas for improvement

- No systematic use of KRIs to monitor and assess risk levels, which would be needed to trigger mitigating actions and/or a discussion on justification of cost/effort put into mitigation actions/risk controls
- Risk materiality ratings may not be filled out in a consistent manner and are currently not thoroughly reviewed and challenged though they are reviewed by the FRC prior to dissemination to the board
- Refer to gaps associated with ERM component 1C – Overlap/blind spots of 2nd LoD responsibilities in terms of reviewing risk assessments
- Interviews with partnership stakeholders are not currently included in the risk assessment process
- Audit reports are produced by third parties due to lack of internal unit or from grant agents and are often delayed, hence limiting their use

Assessment result:	◐ **Gap to best practice**	▲ **Criticality**

3C Processes: Control and Mitigation

Individual risks are missing limits and tolerances to connect them to monitoring and control processes

Leading practices observations

- Establish risk limits and tolerances in line with the risk appetite which is the type and level of risk the organization is willing to accept in achieving medium and long-term strategic goals
- Ensure risk limits are reviewed by the management risk committees and the Board
- Determine response procedures and ownership for any risk limit breaches or risk limits likely to breach
- Establish risk control mechanisms based on tools such as the RCSA which should help identify control/mitigating action mechanisms and assess their effectiveness
- For any risk breach, one of the following actions should be taken, the reasoning should be explained and documented, and the decision on the action item should be approved by the Board or the relevant management committee:
  - Accept: If the risk is outside the risk appetite and management seeks to accept the breach, approval from the Board or related oversight bodies is necessary
  - Avoid: Action is taken to remove the risk or identify a response that would reduce the impact of the risk to an acceptable amount of severity
  - Pursue with mitigating factors: Actions are taken to reduce the severity of the risk
- Use of KCI's to manage the effectiveness of controls and mitigations actions

GPE practices in line with analogues

- 1st LoD is responsible for identifying, mitigating, and implementation as part of the RCSA as well as associated owners
- Summary of sector and grant risks along with mitigation actions taken for focus contexts are well detailed and provide guidance on the current risk levels
- Board risk reports contain a review of all risks and their current risk level along with associated mitigations

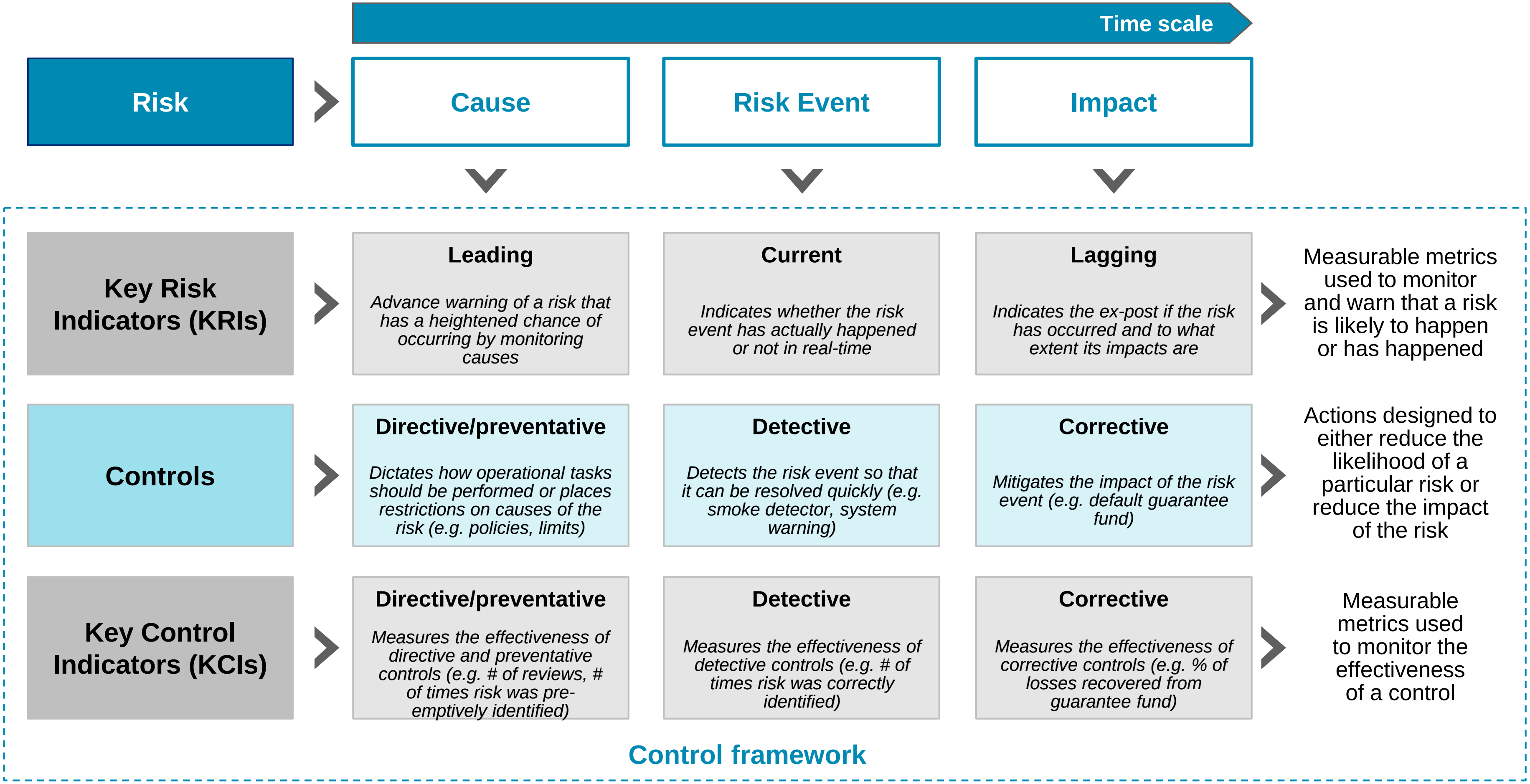
Gaps/potential areas for improvement

- Some owners of mitigations are not the party responsible for the actual mitigation (e.g. 1st LoD) but are actually 2nd LoD members of the Secretariat that oversee the risk mitigation but do not perform them
- Controls/mitigations are not linked to Key Control Indicators (KCIs) to monitor how well the control is implemented
- No assessment of the effectiveness of controls, which creates a risk of time and resources wasted on ineffective controls
- Risk levels and residual risks are reviewed by the board but “risk limits” are not nor are the responses and procedures

Assessment result:	◕ Gap to best practice	🔺 Criticality

A robust risk mitigation/control framework based on global best case practices consists of three core elements

Example of robust KRI/KCI framework



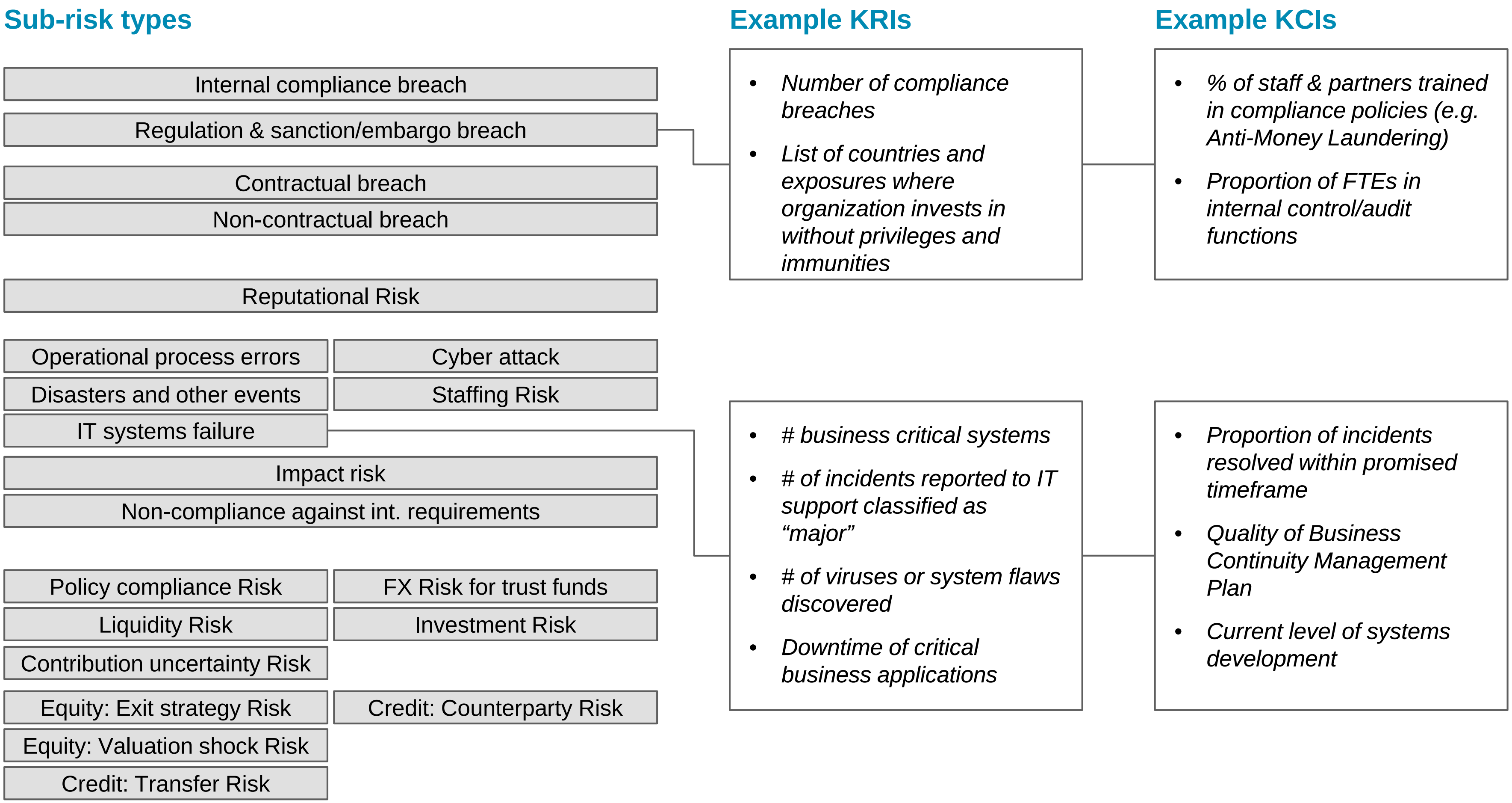
Time scale

Risk	Cause	Risk Event	Impact	
Key Risk Indicators (KRIs)	**Leading** *Advance warning of a risk that has a heightened chance of occurring by monitoring causes*	**Current** *Indicates whether the risk event has actually happened or not in real-time*	**Lagging** *Indicates the ex-post if the risk has occurred and to what extent its impacts are*	Measurable metrics used to monitor and warn that a risk is likely to happen or has happened
Controls	**Directive/preventative** *Dictates how operational tasks should be performed or places restrictions on causes of the risk (e.g. policies, limits)*	**Detective** *Detects the risk event so that it can be resolved quickly (e.g. smoke detector, system warning)*	**Corrective** *Mitigates the impact of the risk event (e.g. default guarantee fund)*	Actions designed to either reduce the likelihood of a particular risk or reduce the impact of the risk
Key Control Indicators (KCIs)	**Directive/preventative** *Measures the effectiveness of directive and preventative controls (e.g. # of reviews, # of times risk was pre-emptively identified)*	**Detective** *Measures the effectiveness of detective controls (e.g. # of times risk was correctly identified)*	**Corrective** *Measures the effectiveness of corrective controls (e.g. % of losses recovered from guarantee fund)*	Measurable metrics used to monitor the effectiveness of a control

Control framework

GPE should create a simplified taxonomy that is “Mutually Exclusive, Collectively Exhaustive” based on high level risk categories linked to their strategy and mission

Anonymized non-profit client example: KRIs and KCIs per risk sub-type



Sub-risk types

- Internal compliance breach
- Regulation & sanction/embargo breach
- Contractual breach
- Non-contractual breach
- Reputational Risk
- Operational process errors
- Cyber attack
- Disasters and other events
- Staffing Risk
- IT systems failure
- Impact risk
- Non-compliance against int. requirements
- Policy compliance Risk
- FX Risk for trust funds
- Liquidity Risk
- Investment Risk
- Contribution uncertainty Risk
- Equity: Exit strategy Risk
- Credit: Counterparty Risk
- Equity: Valuation shock Risk
- Credit: Transfer Risk

Example KRIs

- *Number of compliance breaches*
- *List of countries and exposures where organization invests in without privileges and immunities*

- *# business critical systems*
- *# of incidents reported to IT support classified as “major”*
- *# of viruses or system flaws discovered*
- *Downtime of critical business applications*

Example KCIs

- *% of staff & partners trained in compliance policies (e.g. Anti-Money Laundering)*
- *Proportion of FTEs in internal control/audit functions*

- *Proportion of incidents resolved within promised timeframe*
- *Quality of Business Continuity Management Plan*
- *Current level of systems development*

KRIs and KCIs lay at core of effective risk reporting and monitoring

KRIs/KCIs are indicative metrics to ‘measure’ the correspondent ‘risk’ and ‘control effectiveness’

Definition of KRIs/KCIs

__KRI__ (Key Risk Indicator) is a measurable metric indicating whether the risk event happened or not, and/or how ‘material’ the risk event is, in terms of likelihood and/or impact

__KCI__ (Key Control Indicator) is a measurable metric indicating how ‘effective’ a certain risk control is, in terms of reducing the likelihood, or detecting the risk event, or mitigating the impact

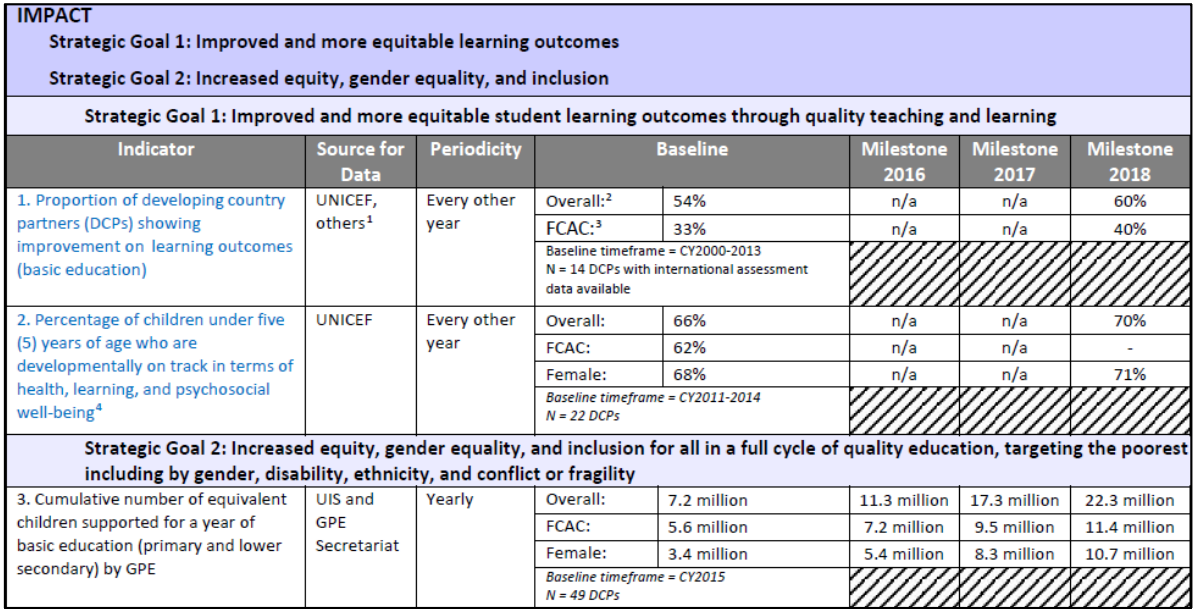
Characteristics of good KRIs/KCIs

1	**Effective**	• Applicable to at least one specific risk or activity • Reflect objective measurement rather than subjective judgment where possible • Measurable at specific point in time • Provide useful management information
2	**Comparable**	• Quantified as an amount, a percentage, or a ratio • Values are comparable over time and across units
3	**Easy to use**	• Available on a timely basis • Cost-effective to collect data • Can be readily understood and communicated

- A single risk event may have multiple KRIs and a certain control may have multiple KCIs as well
  – E.g. KRIs for ‘Grant Execution Risk’ can for example be 1) # students in primary education 2) # textbook purchases 3) Domestic funding for education
  – E.g. KRIs for ‘people risk’ can for example be 1) # of complaints on employee behaviour 2) Employee turnover rate 3) Employee vacancy rate
- A single metric can be both a KRI and a KCI for a certain risk event
  – For: ‘Grant Execution risk’, Domestic funding for education’ can be a KRI indicating how often the risk event happens, and it can also be a KCI by comparing before and after the control is implemented
  – For: ‘people risk’, ‘# of complaints on employee behaviour’ can be a KRI indicating how often the risk event happens, and it can also be a KCI by comparing before and after the control is implemented

The GPE Results Framework provides a set of indicators that can be integrated in processes as KRIs and KCIs

GPE Results Framework snapshot



IMPACT Strategic Goal 1: Improved and more equitable learning outcomes Strategic Goal 2: Increased equity, gender equality, and inclusion							
Strategic Goal 1: Improved and more equitable student learning outcomes through quality teaching and learning							
Indicator	**Source for Data**	**Periodicity**	**Baseline**		**Milestone 2016**	**Milestone 2017**	**Milestone 2018**
1. Proportion of developing country partners (DCPs) showing improvement on learning outcomes (basic education)	UNICEF, others[1]	Every other year	Overall:[2]	54%	n/a	n/a	60%
			FCAC:[3]	33%	n/a	n/a	40%
			Baseline timeframe = CY2000-2013 N = 14 DCPs with international assessment data available		▨	▨	▨
2. Percentage of children under five (5) years of age who are developmentally on track in terms of health, learning, and psychosocial well-being[4]	UNICEF	Every other year	Overall:	66%	n/a	n/a	70%
			FCAC:	62%	n/a	n/a	-
			Female:	68%	n/a	n/a	71%
			Baseline timeframe = CY2011-2014 *N = 22 DCPs*		▨	▨	▨
Strategic Goal 2: Increased equity, gender equality, and inclusion for all in a full cycle of quality education, targeting the poorest including by gender, disability, ethnicity, and conflict or fragility							
3. Cumulative number of equivalent children supported for a year of basic education (primary and lower secondary) by GPE	UIS and GPE Secretariat	Yearly	Overall:	7.2 million	11.3 million	17.3 million	22.3 million
			FCAC:	5.6 million	7.2 million	9.5 million	11.4 million
			Female:	3.4 million	5.4 million	8.3 million	10.7 million
			Baseline timeframe = CY2015 *N = 49 DCPs*		▨	▨	▨

Integration into risk processes

- The results framework provides for the collection of 37 indicators on a yearly/bi-yearly basis
- The collected data, provided by partnership members and other external sources, are based on global strategic objectives of GPE
- For use in risk processes, the indicators could be linked to specific risks and used as KRIs and KCIs
- Many of these indicators could additionally be adapted (when the data is available) to determine country level risks as well
- GPE is well positioned to begin objectively measuring risk due to the data collection used to help the partnership monitor its progress against the goals and objectives of the GPE 2020 strategic plan

Controls should be assessed in terms of their effectiveness and only effective controls should reduce gross risk levels

Example control assessment criteria

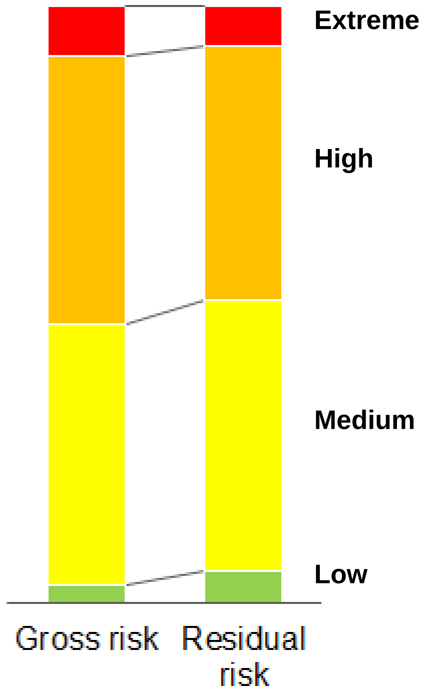
Score	Effectiveness	Control Type	Control Execution	KRI/KCIs
4	**Very effective**	All elements of (3) plus: • 1 of each of a Preventative/Directive, detective and corrective control where possible • "Control sheet" formally completed • Control type has been verified by risk management	All elements of (3) plus: • Proven track record where possible • "Control sheet" formally completed • Control execution has been audited/verified by risk management and shown evidence of control execution	All elements of (3) plus: • At least 1 leading, 1 current AND 1 lagging effectively defined KRI, although preferably 2-3 leading, AND 1-2 current • At least 1 of each of a Preventative/Directive, detective AND corrective KCI where possible • "Control sheet" formally completed • KRIs/KCIs verified by risk mangment
3	**Effective**	• Clearly pre-emptive where possible; **AND,** • Automated where possible	• Control owner clearly designated; **AND,** • Incorporation in SOPs/SLAs; **AND,** • Evidence of the control being actively implemented, through documented monitoring and actions being taken	• At least 1 current KRI AND 1 detective AND 1 preventative OR directive KCI which are effectively defined and properly monitored
2	**Partially effective**			
1	**Not Effective**			
NA	**Uncontrollable**			

Gross risk is only reduced if a control is either "very effective" (residual risk is 2 levels below gross risk) or "effective" (residual risk is 1 level below gross risk)

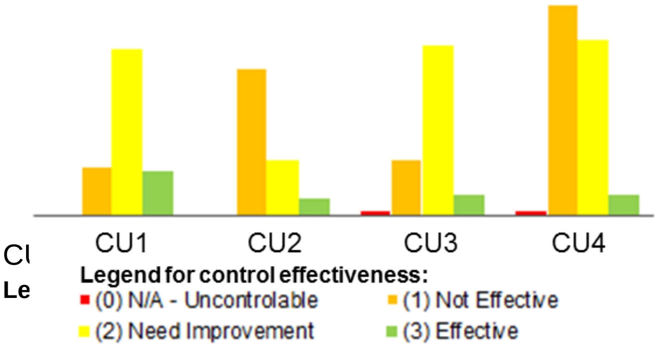
Significant control gaps exist driven especially by KRIs and KCIs which must be addressed for risks to be effectively managed and mitigated

Risk profile
Number of risks

Total risks number [X], with [X] "extreme" residual risks and [X] "high" risks

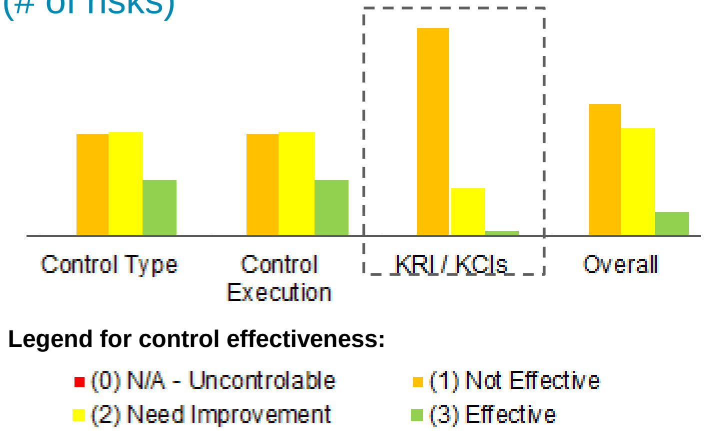


Control effectiveness by business line
(# of risks)



- Only [X] controls received an "effective" rating, and none are "very effective"
- Relatively, support units had the largest share of "not-effective" controls

Control effectiveness by type of control
(# of risks)

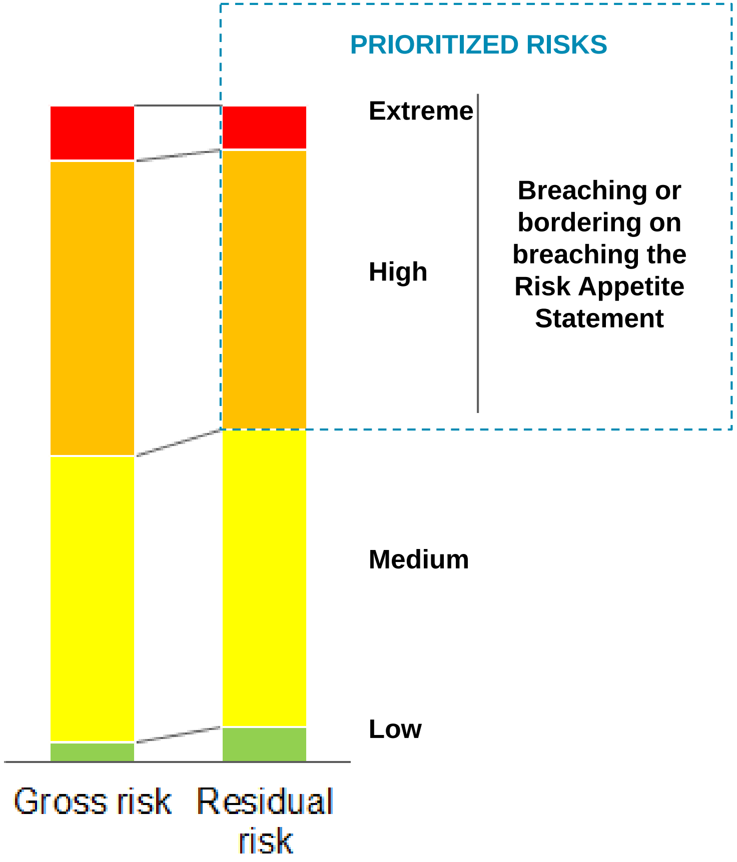


- Low control effectiveness driven by a lack of Key Risk Indicators and Key Control Indicators
- Only certain risks had "effective" KRI/KCI controls
- Other key issues included controls being the same as their risks, controls not relating to their risks, and controls using same sources as their risks

Control framework will help prioritize the partnerships risks with a focus on "extreme" and "high" risks

Control implementation prioritization

Example risk profile (# of risks)

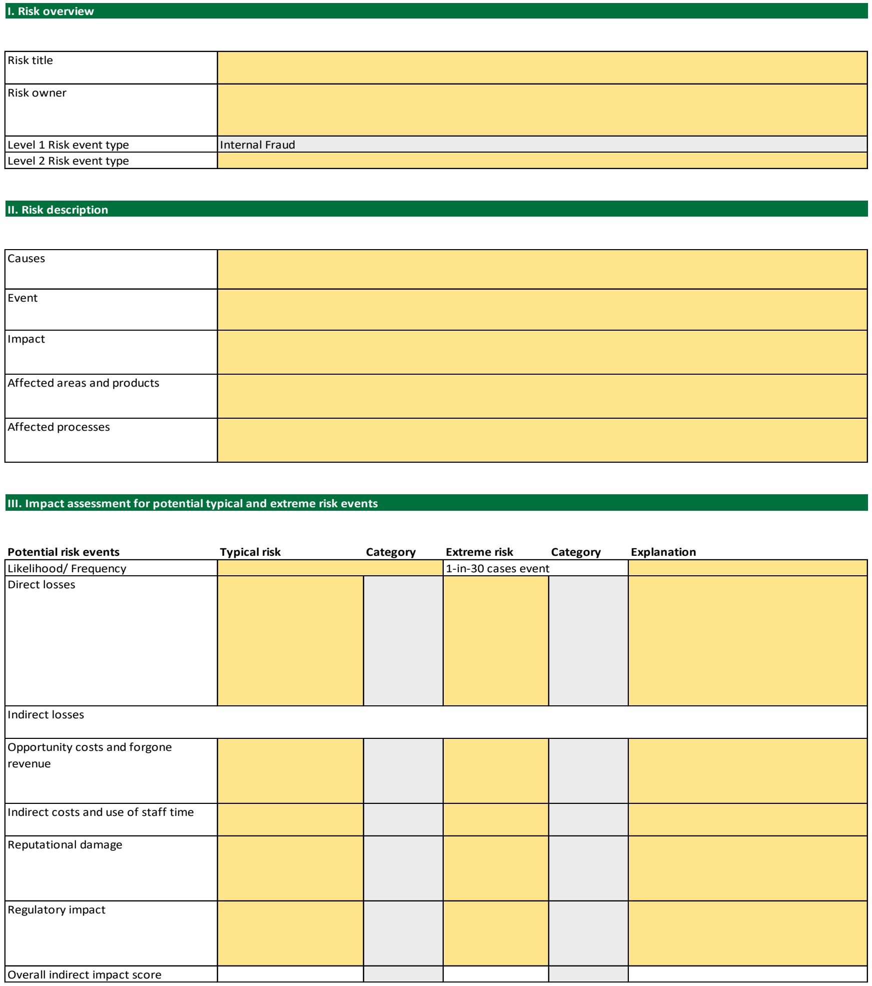


Control implementation enablers

- **Many risks already have "informal" controls in place**, which require formalization through documentation and KRIs/KCIs to become at least "effective"
- **Many KRIs and KCIs can be obtained through existing regular reporting** and require limited efforts to formalize thresholds and documentation
- **Potential KRIs need to be proposed for top risks**
- **Risk control training sessions** should be held to controls processes for risks
- **Detailed ERM Manual** including a procedures manual for control implementation should be provided

Risk and Control Self-Assessment (RCSA) templates should contain specific components to provide enough information for managing risks effectively

Example: Risk and Control Self-Assessment template



I. Risk overview

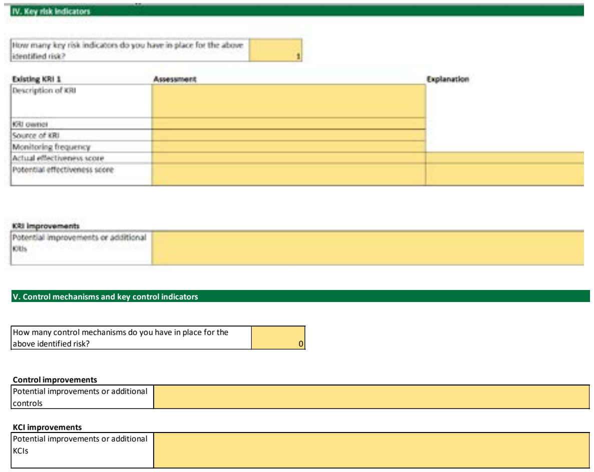
Risk title	
Risk owner	
Level 1 Risk event type	Internal Fraud
Level 2 Risk event type	

II. Risk description

Causes	
Event	
Impact	
Affected areas and products	
Affected processes	

III. Impact assessment for potential typical and extreme risk events

Potential risk events	Typical risk	Category	Extreme risk	Category	Explanation
Likelihood/ Frequency			1-in-30 cases event		
Direct losses					
Indirect losses					
Opportunity costs and forgone revenue					
Indirect costs and use of staff time					
Reputational damage					
Regulatory impact					
Overall indirect impact score					



IV. Key risk indicators

How many key risk indicators do you have in place for the above identified risk?	1

Existing KRI 1	Assessment	Explanation
Description of KRI		
KRI owner		
Source of KRI		
Monitoring frequency		
Actual effectiveness score		
Potential effectiveness score		

KRI improvements

Potential improvements or additional KRIs	

V. Control mechanisms and key control indicators

How many control mechanisms do you have in place for the above identified risk?	0

Control improvements

Potential improvements or additional controls	

KCI improvements

Potential improvements or additional KCIs	

The RCSA template should have the following components

- Descriptions of causes, events, impacts, affected areas/processes
- An estimation of likelihood and estimation of possible impact including direct and indirect losses
- Key risk indicators should be identified/described, including any potential additional or improvements to KRIs
- Control mechanisms and KCI's should also be identified including protentional additional or improvements to KCIs
- KRIs, Controls and KCIs should assessed in terms of their actual and potential effectiveness (referring to suggestions how to improve)

Processes: Risk assessment, control and mitigation
Key recommendations

1

Determine KRIs and KCIs for key risks

- Key risk indicators and key control indicators should be identified for risks within the risk taxonomy with an emphasis on critical and high risks
- Existing information and data should be leveraged as far as possible, e.g. impact metrics from GPE 2020 strategic plan and other internally/externally available sources

2

Revise RCSAs

- Risk control self-assessments templates for corporate and operational risks should be revised to include:
  - Identification and effectiveness assessment of KRIs, controls and KCIs
  - “Blank fields” to suggest improvements (e.g. new KRIs, controls, KCIs or changes to existing ones)
  - Reflection of the new risk taxonomy

3D Processes: Monitoring & reporting

Monitoring and reporting lacks both customization for different audiences and use of risk metrics

Leading practices observations

- Targeted content: Risk reporting should be focused on issues and information relevant to the target group, i.e. different level of detail for different audiences such as Secretariat Senior Management, Committees and Board
- Clear linkage to risk appetite to ensure relevance
- Reports should prioritize issues and prompt actions
- Should include clear summary of key KRIs and KCIs where possible
- Should include risk trends over time
- Reports are easy to read, i.e. use of dashboards, clear color coding of severity/importance
- Appropriate frequency of reports, e.g. every two months/quarterly to Secretariat Risk Management, and every 6 months to Committees and the Board
- Transparency of risk reporting across all layers of staff within the organization to promote risk awareness and understanding
- A more detailed reporting to the Board may be justified if the Board members are lacking Risk Management know-how and will be educated on Risk Management practices and its importance via the reporting

GPE practices in line with analogues

- Reporting frequency for corporate risks to the Committee and Board (every 6 months) in line with analogue practice but only annually for operational risk framework
- All risk reports currently provide a view of the current risk level across all risk types
- Risk reporting is transparent with full outputs of the RCSAs available for review by the board and committees
- The analysis of the current risk levels and discussion of controls are a core element in reports presented to board and committees
- Changes in risk levels are reported also for the previous assessment cycle

Gaps/potential areas for improvement

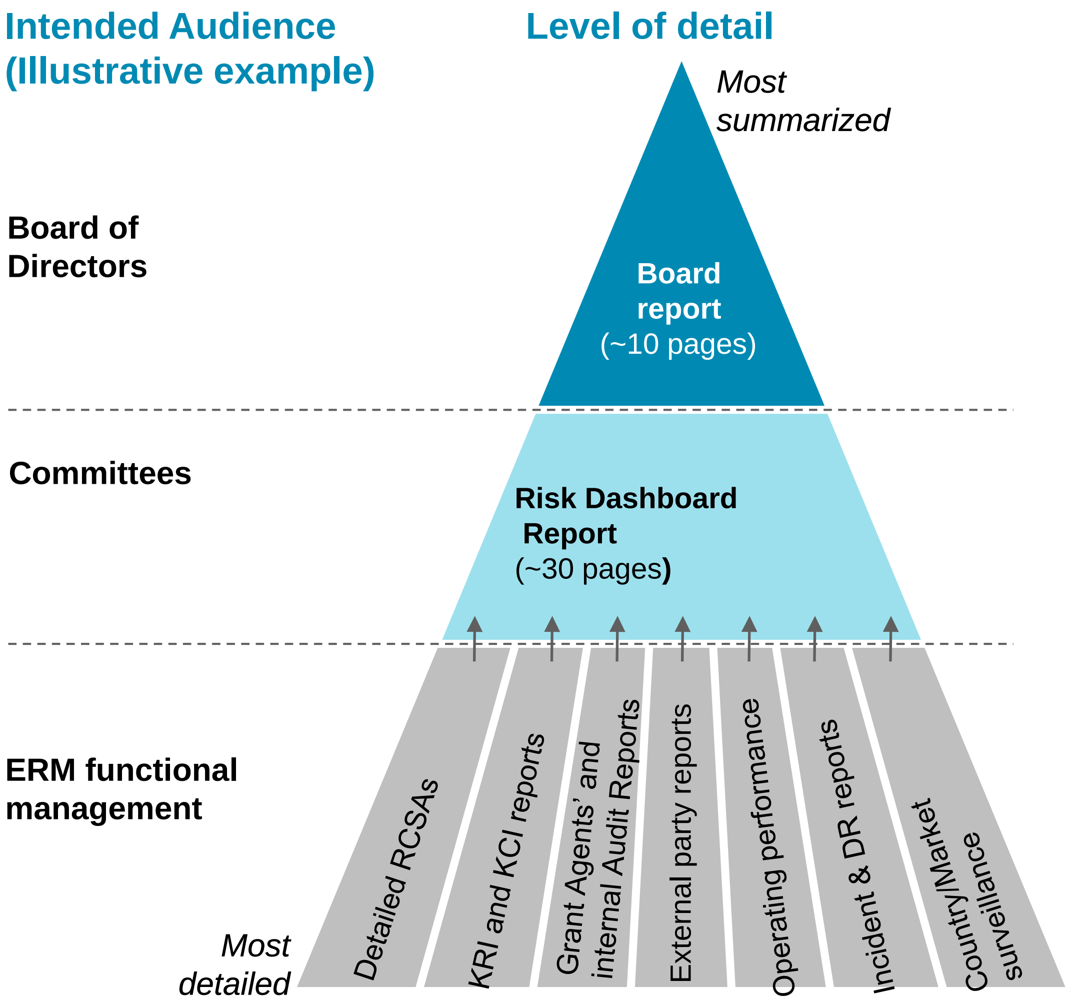
- Board and Committee Reporting does not differ significantly in terms of content/detail - Board receives reporting that may contain too much detail to efficiently review important risks
- Many policy documents are mixed into Board or Committee reports – clear differentiation between reports and policy documents needed to ensure ease of use
- Reporting is rather “wordy”, with little use of dashboards and limited prioritization of key issues/top risks and suggested actions
- No “education” of the board in terms of Risk Framework components, practices and their importance
- No use of KRIs/KCIs in risk monitoring and reporting
- Risk monitoring is only on a semi-annual basis for all reports which may not be frequent enough
- Ideally, longer-term trends of how risk levels evolve should be shown

Assessment result: ◕ **Gap to best practice** △ **Criticality**

The aim of a best practice risk reporting framework is to provide an effective and efficient update of the institution’s risk profile, especially at the higher management levels…

Key principles of effective risk reporting		**Common pitfalls**
Comprehensive and tailored to audience	• All risk reporting should be focused on issues and information relevant to the target group • Presentation of the right level of detail (not too little, but definitely not too much) and use of dashboards for effective summaries • Clear linkage to risk appetite to ensure relevance	• Overly burdensome material to read, absorb and challenge • Limited prioritization, with details obscuring headline issues and most significant changes to the risk profile
Value added-commentary	• A good report uses qualitative data where possible to provide a comprehensive yet concise, forward looking view of the group’s risks	• No significant thought is applied to the meaning of the values, figures or charts presented (identification of the “so what?”) • Limited or unhelpful context and commentary
Drill-down capability and completeness	• A good reporting framework should enable to drill down into details when appropriate, without overwhelming the reader • Includes clear summary of key KRIs and KCIs where possible • Covers all relevant material risk themes and significant external parties	• Metrics and methods of presentation require deep risk specific technical expertise (particularly challenging for non-executives) • Use of technical terms, jargons or institution-specific acronyms increase opacity • Often misses risks external to the organization
Consistent set of tables and charts	• Consistency of charts should be strived for between reports to avoid duplication and confusion for readers • A consistent set of figures/charts allows trend tracing and makes important or worrying developments much easier to spot	• Report reflects the sum of previous requests for changes, not an assessment of the whole
Prompt action	• Reports should prioritize issues and suggest actions on the most important risks, enabling earlier detection, and thus mitigation of threats to the organization • Actions to take should be clearly stated and have embedded follow-up mechanisms • Transparent reporting	• Reported issues contain no link to action or decision

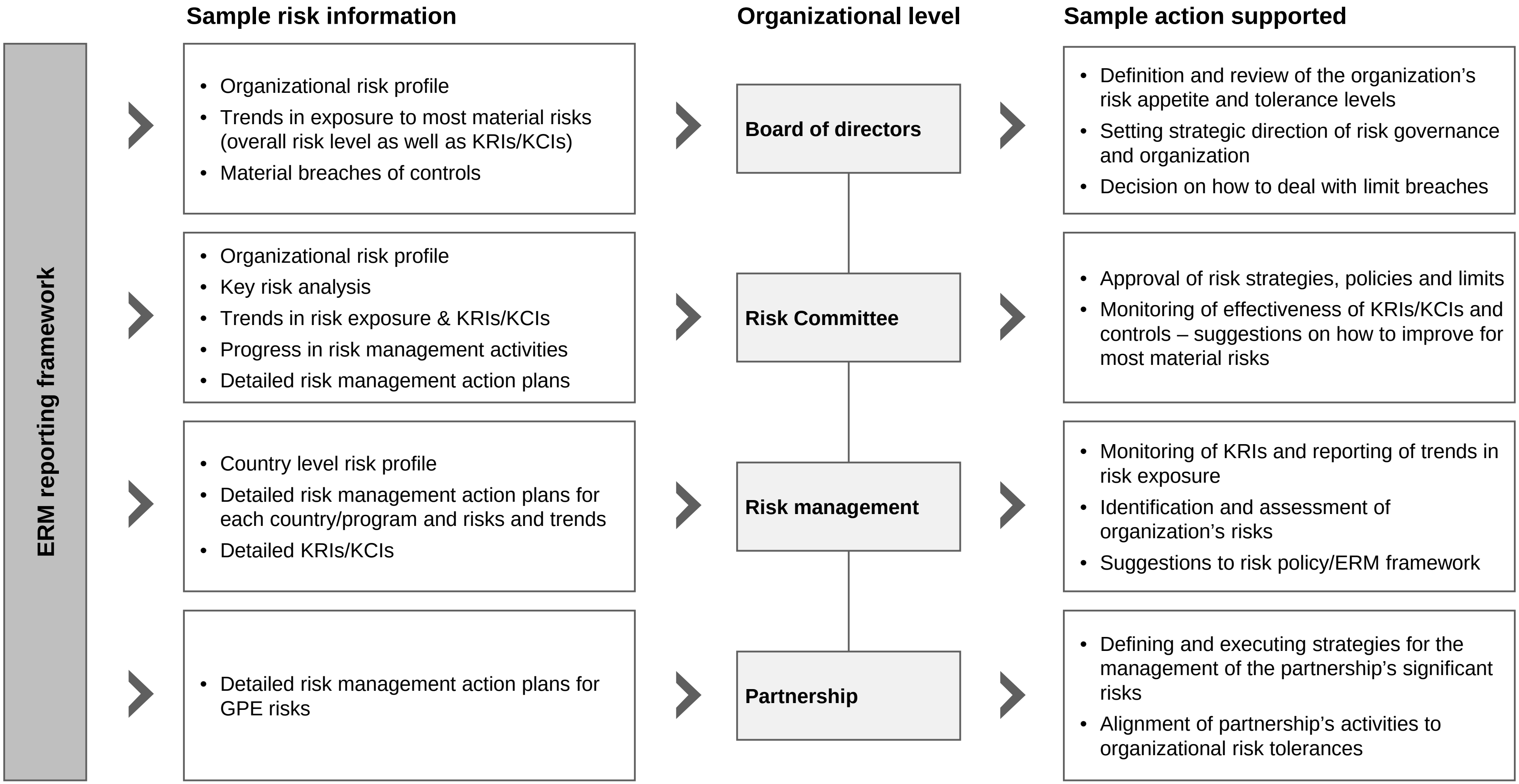
Reporting should follow a pyramid structure summarized in dashboards which helps to ensure that only relevant information is reported upwards



- Reporting should **follow a pyramid structure -** each management forum should have a risk report **tailored to their needs**
  - Allows for each management layer to **focus on specific types of risks** (e.g. focus leveraged for highest priority items)
  - Drill downs of any specific area are possible on request
  - **Higher level reports should be largely synthesized versions** of lower level reports
- **Risk management at the Secretariat acts as a "clearing house" for the numerous risk reports** generated across the organization and for managing the risk reporting framework

…and generate actionable, relevant and informative risk information at every level of the organization

Overview of best-practice reporting by type of audience



	Sample risk information	Organizational level	Sample action supported
ERM reporting framework	• Organizational risk profile • Trends in exposure to most material risks (overall risk level as well as KRIs/KCIs) • Material breaches of controls	**Board of directors**	• Definition and review of the organization's risk appetite and tolerance levels • Setting strategic direction of risk governance and organization • Decision on how to deal with limit breaches
	• Organizational risk profile • Key risk analysis • Trends in risk exposure & KRIs/KCIs • Progress in risk management activities • Detailed risk management action plans	**Risk Committee**	• Approval of risk strategies, policies and limits • Monitoring of effectiveness of KRIs/KCIs and controls – suggestions on how to improve for most material risks
	• Country level risk profile • Detailed risk management action plans for each country/program and risks and trends • Detailed KRIs/KCIs	**Risk management**	• Monitoring of KRIs and reporting of trends in risk exposure • Identification and assessment of organization's risks • Suggestions to risk policy/ERM framework
	• Detailed risk management action plans for GPE risks	**Partnership**	• Defining and executing strategies for the management of the partnership's significant risks • Alignment of partnership's activities to organizational risk tolerances

There are multiple reporting styles utilized for ensuring an effective action-orientated understanding of the organization's risk profile

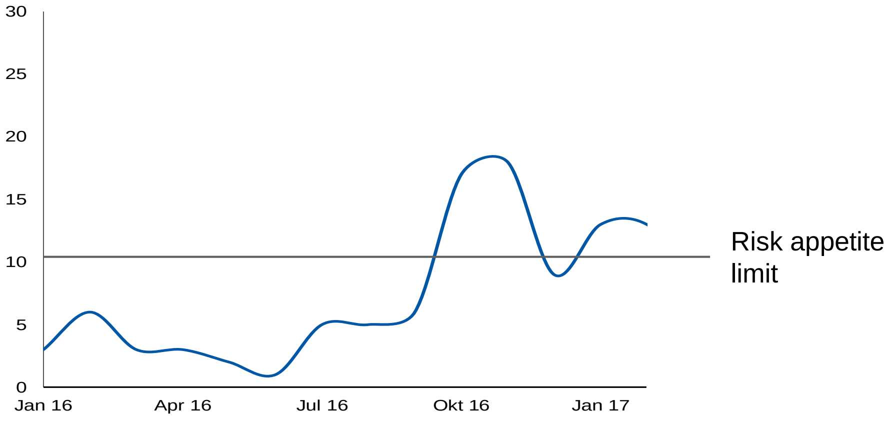
Examples of key reporting styles used

Example: Risk appetite monitoring
(e.g. taxonomy-based)

	RAS vs. KRI thresholds					
Risk appetite statement	Overall (Q1)	Overall (Q2)	KRIs	KRI (Q1)	KRI (Q2)	KRI threshold
"We have zero tolerance for internal compliance breaches"	🟩	🟩	XX	🟩 119	🟩 128	136
…	🟩	🟩	XX	🟥 XX	🟥 XX	XX
…	🟩	🟩	XX	🟩 XX	🟩 XX	XX
…	🟥	🟥	XX	🟧 XX	🟧 XX	XX
Overall Group	🟧	🟧		🟧 XX	🟧 XX	XX
Actual as % threshold	🟩 Green	0-95%	🟧 Amber	95%-100%	🟥 Red	100%+

Example: Trends analysis of key risk indicators

# of negative press statements (monthly)



Focus on analyzing trends to identify new/emerging risks

We think the existing GPE risk dashboard is a good starting point, but should be expanded by adding missing elements (such as risk appetite levels, KRIs/KCIs) and better visualization for ease of use

Effective board reporting should be concise but highlight important risks to the overall strategy of GPE and critical areas that warrant board discussion

Examples of board risk reporting

Risk appetite monitoring (e.g. taxonomy-based))

Risk appetite statement	NFR RAS vs. KRI thresholds Overall (Q1)	Overall (Q2)	KRIs	KRI (Q1)	KRI (Q2)	KRI threshold
Misuse of funds	🟩	🟩	XX	🟩 1	🟩 1	5
…	🟩	🟩	XX	🟥 XX	🟥 XX	XX
…	🟩	🟩	XX	🟩 XX	🟩 XX	XX
…	🟥	🟥	XX	🟧 XX	🟧 XX	XX
Fraud Risk	🟧	🟧		🟧 XX	🟧 XX	XX

Actual as % threshold	Green	0-95%	Amber	95%-100%	Red	100%+

Top identified risks

	Sept 16	Sept 17
Yemen	🟧	🟥
…	🟧	🟥
…	🟥	🟥
…	🟧	🟧

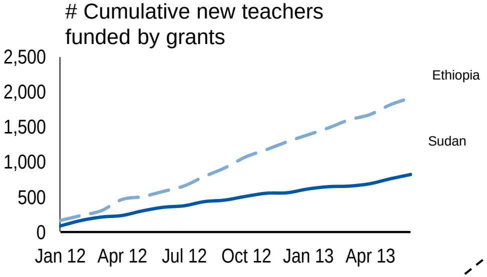
Grant Risk factors

Grant Agent oversight	Critical
Risk that grant objectives are not achieved	Critical
Risk that significant GPE funds are diverted	Critical

Sector Risk factors

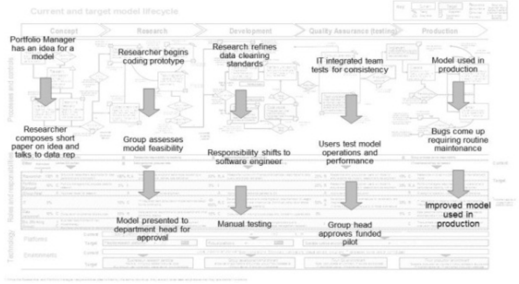
Risk GPE does not leverage capacities	Critical
Risk that GPE does not support planning	High
Risk GPE developing partners fail to increase expenditures	Critical

Trends analysis of key indicators



Focus on analysing trends to identify new / emerging risks

Process based monitoring of risks / controls



Current and target model lifecycle
Concept
Research
Development
Quality Assurance (testing)
Production
Portfolio Manager has an idea for a model
Researcher composes short paper on idea and talks to data rep
Researcher begins coding prototype
Group assesses model feasibility
Model presented to department head for approval
Research refines data cleaning standards
Responsibility shifts to software engineer
Manual testing
IT integrated team tests for consistency
Users test model operations and performance
Group head approves funded pilot
Model used in production
Bugs come up requiring routine maintenance
Improved model used in production
Processes and controls
Roles and responsibilities
Technology
Platforms
Environments

Focus on monitoring and controls along with key KRIs/KCIs identified for top identified risks and key risk appetite measures

Action point tracking & key projects

Action point tracking

Action	Status	Review
Pro		
…		

Key projects

	Description	Owner	Status	Delivery date
1	Project 1	e.g. Board member, senior manager	Amber	01/2006
2	Project 2		Green	01/2007

Action point agenda

- Identification of Board responsibilities
- Tracking of key risk project statuses

Focus on tracking issues / control gaps in processes

Processes: Monitoring & reporting
Key recommendations

1

Take the current risk dashboard as the basis to develop a comprehensive risk reporting at the most granular level for the Secretariat Risk Management team and add missing components

- For each risk
  - Add risk appetite limits
  - Add KRIs and KCIs (description and outcomes)
  - Add effectiveness assessments for mitigation measures, KRIs and KCIs
  - Visualize risk level and trends, e.g. showing development of KRIs for e.g. past 5 reporting periods in relation to risk appetite levels
  - Update this at least on a quarterly basis, consider more frequent updates for critical risks

2

Develop a customized reporting for the FRC, GPC and Board

- Use the expanded risk dashboard as per above as the basis, but use most of this as an “appendix”
- For the main section, select high priority risks (rated as critical or high) and focus attention on those where risk appetite limits are breached and control effectiveness is assessed as low
- Add commentary: Focus the discussion on actions to be taken for those risks, esp. additional controls to be put in place, more resources to be deployed, higher frequency of monitoring/reviews and potentially also implications for future grant allocations
- For the committees; in addition to above, provide also information on framework and policy developments and progress on risk management activities
- For the board (and if needed also for the committee), given the fast membership turnover rate, provide additional educational information on GPE’s risk management framework (key components and processes and their overall importance for GPE as well as the board’s role and expectations from them)

3

Clearly separate Reporting and Policy documents

- Have a repository for framework and policy documents as well as reports that go to the Board and Committees
- Framework and policy documents should have an “owner” and changes to those documents that have been agreed and signed-off should be tracked over time

4 Supporting systems and infrastructure
Systems are inline with analogues for reporting of risk

Leading practices observations

- No use of ERM software solutions and low degree of automation of risk management processes among analogues we interviewed for this project
- Risk identification and assessment as well as analysis, aggregation, monitoring and reporting is largely performed manually, using MS office tools (Excel, Word, PPT)
- However, two of the three have mentioned that they are planning to invest into better system support in the medium term (~3-5 years), with a focus on improving systems available to the first line for risk identification and assessments
- Long-term visions can be described as:
  - Key risk management processes built into software requiring no manual collation, sorting and analysis. Typically includes four areas:
    - Tracking of risks and controls
    - Document repository
    - Workflow management tool including automatic escalation of risks
    - Reporting platform
  - Systems are usually a centralized, well-controlled document repository and data warehouse with storage of historical data and data dictionaries, in order to provide flexibility in model development and testing and allow for efficient ad hoc querying
  - Automated report generation (e.g. all RCSA inputs compiled into dash-boards on-demand, with KRIs/KCIs generated from most recent data and included)

GPE practices in line with analogues

- Current RCSAs are simple excel reports which are in line with analogues
- Aggregation of results and risk analysis is performed in excel workbooks which is in line with analogues
- Reporting is centralized within the risk department and consists of a manual compilation of data from different sources for different reporting recipients

GPE gaps identified

- Operational risk RCSAs need assistance by risk to be filled out properly by the country leads or the results are often stale or not consistent
- Current reporting is manual and requires significant additional work to aggregate responses and present them for management, committees, and board of directors

Assessment result:	◔ **Gap to best practice**	▲ **Criticality**

Generally, there are three potential options to consider for ERM software solution design

Options for ERM solutions

	Options	Description	Cost[1]	Suitability[1]
1	**Off the shelf, reputable platform from “Industrial” systems vendor**	• Reputable solution marketed globally by international vendors such as Open Pages, Cura, BWise, SAS, Cognos and Algorithmics • Generally designed for much larger organizations with highly complex data feeds and risk analytics requirements (e.g. used by most major banks) • Customizable with prices heavily variant and dependent on business requirements and negotiation • May be too complex and sophisticated for GPE’s requirements	○	◑
2	**Custom made solution from “local” vendor or smaller vendor**	• Local vendors and potentially smaller vendors not from the US • Likely to have either significantly less sophisticated systems, but covering basics, or build custom-made solutions fitted to needs • Likely to be more cost-effective in delivery of simpler solutions which may be more aligned to GPE’s needs	◑	◕
3	**Build in-house**	• Depending on functionality required, an in-house developed solution may be able to address all needs adequately • May be higher potential for development/implementation risks • Depends on GPE’s IT capabilities and resources in-house (assessment wasn’t in scope of our review) • Potentially more cost effective than option #2	◕	◕

Legend: ● Attractive ○ Unattractive

[1] Initial high-level estimates

Processes: Supporting systems and infrastructure
Key recommendations

1

For the near term: Consider improvements to existing manual tools to improve ease of use for 1st line users and RM team

- Focus on “front-end” (i.e. 1st line/risk owners) improvements
  - Improve current excel-based corporate and operational RCSA by providing more guidance to users on how to fill in the required fields (e.g. example best practice answers)
  - Continue use of drop down menus/standardized options for answers to select from to simplify aggregation and analysis
  - Create a master sheet which can automatically draw data from individual RCSA templates and increase use of formulas/automate aggregation and analysis – to decrease risk of manual compilation errors

2

For the medium term: As analogues are in the process of upgrading their system capabilities, we recommend GPE to also consider the following steps for the medium term:

- Focus on “front-end” (i.e. 1st line/risk owners) system improvements
  - Move from excel-based RCSA to a software based tool to identify and assess risks, KRIs/KCIs and controls (once RCSA has been revised and all currently missing information fields have been added)
- Software should be able to compile information from all individual RCSAs into one aggregated view/dashboard

Appendix

While reviewing each component of the ERM Framework and associated policies, we kept three main assessment dimensions in mind

Assessment dimensions for Risk framework and policies

Dimension	Factor	Assessment of frameworks	Assessment of policy documents
Comprehensiveness	Completeness	Does the framework cover the entire risk landscape?	Are policies in place for key risks laid out in the risk management framework?
	Appropriateness	Are the framework components appropriate for the organization, i.e. in line with its ambition level?	Do the risk policies contain appropriate level of risk management?
	Detail	Is the level of detail provided in the framework appropriate for its audience?	Do policies contain the needed detail to execute the risk management objectives outlined?
Clarity	Simplicity	Does the framework communicate its content with simple language in a format that is easy to understand?	Are the policies designed simplistically to allow for them to be executed consistently and effectively?
	Assignment	Are individuals and groups that will be accountable for implementation, compliance, and amendments approvals clearly defined?	Do the policies provide accountable individuals in groups for risk tools and procedures?
	Implementable	Does the framework outline activities that meant to be implemented?	Do the policies contain activities that can be readily implemented?
Consistency	Regularity	Are policies consistent across the framework? Are interactions and interdependencies well defined and overlaps avoided?	Are the risk management tools and procedures consistent across policies and do not create inefficiencies?
	Frequency	Is the framework updated and reviewed in a timely fashion?	Is the timing recommended appropriate? (e.g. reporting intervals, periodicity of reviews)
	Leveling	Does the framework provide accountability at the appropriate level? Is it too lenient or constraining?	Are the required procedures (e.g. reporting and monitoring) appropriate for the level of risk?
	Standardization	Does the framework adopt a consistent measure across Country Levels and facilitate roll-up to Global level?	Are the policies consistent with treatment of risks across different levels?

CONFIDENTIALITY

Our clients’ industries are extremely competitive, and the maintenance of confidentiality with respect to our clients’ plans and data is critical. Oliver Wyman rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of Oliver Wyman.