INTERNAL AUDIT REPORT

ENTERPRISE RISK MANAGEMENT
January 2020

Gavi
The Vaccine Alliance

Conclusion

The approach to risk management adopted by Gavi's Board covers strategic, operational, programmatic and corporate risks. The original Enterprise Risk Management ('ERM') framework design, following the 2013 internal audit of ERM and DFID's 2015 recommendations, was based on a well-structured approach, as part of a tailored 'Three Lines of Defence' model. The Risk function has taken a pragmatic approach to implementing this design, proportionate to Gavi's level of maturity, with limited resources (1 FTE intermittently assisted by three successive short-term consultants) and in a challenging environment.

This has yielded positive results in the areas of most strategic importance and created a solid foundation on which to build the next stage of its development. Those areas which have benefited from sustained investment by the Risk function tend to operate most effectively – notably, processes related to strategic and mission-critical risks.

Successful ERM needs to evolve to reflect changing business objectives, structures and operational activities and requires management commitment and resource across the organisation. Recognising the need to revisit the mandate, resource levels and adequacy of its approach for Gavi 5.0, the Risk function already has plans in place for a full review of ERM needs and the 3 Lines of Defence model, to be conducted later in 2019 and 2020. Our review of the initial planning for this Risk 'vision' exercise confirmed that almost all audit issues are already within its scope. Audit recommendations have, nevertheless, been made, in order to ensure that appropriate priority is given to their resolution and to ensure that acceptable timelines for implementation are set and respected.

The key risks to Gavi's future ERM development identified by the audit relate to operational and programmatic risk management which have been given less attention so far. Similarly, the Three Lines of Defence model has yet to fulfil its potential to contribute to Gavi's operational risk management. In addition, there is a need to ensure that ERM implementation plans take into account the key prerequisites for success, including resource requirements, change ownership, cultural factors and optimal systems/tools. The role of the Risk Committee in the overall risk management process should also be revisited and made more explicit. These and other audit observations are explored in more detail below and in the summary of findings section.

Key Internal Audit Issues Summary

Issue Description	Rating
Underdeveloped areas of the current Risk Management approach	
There is a need to review the current risk management approach to prioritise underdeveloped areas including:	
• Operational Risk Management (Secretariat functions)	**M**
• Country Risk Management/Programmatic risk	**M**
• Role of Partners in Risk Management	**M**
Prerequisites for successful implementation of ERM	
There is a need to ensure that ERM implementation plans take into account wider organisational factors including resource requirements, change ownership, cultural factors and optimal systems/tools.	**M**
Governance and Oversight of ERM activities	
The role of the Risk Committee in the overall risk management process should be revisited and made more explicit.	**M**

Contents

Audit Objective

Our audit assessed the design and operating effectiveness of the key controls in relation to Gavi's Enterprise Risk Management ('ERM') processes.

Audit Scope and Approach

We adopted a risk-based audit approach informed by an initial review of the structures, methodologies and processes used for ERM. This preliminary assessment included the review of documents posted on the Risk function's Intranet site, relevant Board and Audit and Finance Committee papers, the report from DFID's 2014 Assurance Review and observations from previous Internal Audit work in related areas. Based on this, the controls over the most significant risks were assessed, through discussion with relevant Secretariat staff, review of supporting documentation and, where appropriate, sample testing evidence of risk management procedures.

The audit is part of the 2019 Annual Internal Audit Plan approved by the Audit and Finance Committee of the Gavi Board. The fieldwork took place during May and June 2019.

This audit was designed to assess the:

- Design and operating effectiveness of the key controls;
- Economy and efficiency of the utilisation of resources;
- Quality of implemented governance and risk management practices; and
- Compliance with relevant policies, procedures, laws, regulations and donor agreements.

The scope of the audit covered the key controls in the following principal areas:

- Development and approval of the ERM strategy, policy and implementation plan (including infrastructure requirements – people, processes, systems);
- Implementation of the ERM strategy; and
- Governance and oversight of ERM activities.

Please note the following exclusions from the audit scope:

- An assessment of the outcomes achieved in applying the risk management processes;
- Risk management processes operated by Alliance partners or in-country. While the scope covered risk management across the Alliance, including Secretariat, countries and partners, as a key controls audit, only those processes operated at the Geneva Secretariat were reviewed and only Geneva Secretariat staff interviewed.

Reference was made during the audit to recognised ERM standards including ISO31000, COSO and IRM guidelines and the experience of other risk management frameworks, where relevant. However, there is no single right approach to risk management. Its purpose is to contribute to the achievement of an organisation's objectives; it should be a continuous and developing process to ensure alignment with changing strategic and operational needs.

Background

Gavi's current ERM strategy was developed in response to recommendations from the 2013 Internal Audit and the 2014 DFID Risk & Assurance review which provided detailed recommendations for the development of a risk management framework appropriate for Gavi's needs at the time. Certain elements of the ERM approach were established before the creation of a dedicated Risk function – the Risk Policy, Board paper risk sections and Secretariat risk registers – but significant progress has been made since the recruitment of a Head, Risk in mid-2015, tasked with development of ERM processes and, shortly after, with co-ordination of the Three Lines of Defence model, a core element of DFID's recommended approach.

The ERM framework now features several elements which may be considered consistent with best practice. These include:

- Regular engagement with the AFC and Board on strategic risks and the development of the ERM framework;
- A Risk Appetite Statement, mapped to each of Gavi's strategic goals, which serves as a reference point for senior management and Board-level discussions and decision-making;
- A well-established process for the identification, assessment, monitoring and reporting of those 'Top Risks' considered to

be most critical to the achievement of Gavi's mission;
- A systematic approach to engaging senior management in 'deep dive' reviews of mission-critical risks and cross-cutting issues (the Risk Committee);
- Increasing integration between risk, strategic and performance management, through the Team Performance Management ('TPM') process in the Secretariat and integrated into strategy progress updates to the Board;
- Commitment by the Risk function to ongoing communication, both to Gavi staff (through the Intranet and other training and information sessions) and to external stakeholders, through the website. This includes the comprehensive annual Risk & Assurance Report; and
- Regular self-assessment to identify opportunities for development, in a quest for continuous improvement.

DFID monitored Gavi's ERM progress until December 2016 when it concluded that the Risk Management and Assurance framework had been 'transformed'. However, it also highlighted risks associated with the pace and scale of change which may result in impaired delivery. These were explored in the audit and conclusions are presented below.

A comprehensive internal review of the design and implementation of the ERM model was performed by the Risk function in 2017, with results reported to the Risk Committee and, in summary form, to the AFC. It concluded that the model was broadly fit for purpose, with roles and tools established and enhanced risk awareness across the Secretariat. Opportunities for improvement were identified in several areas including:

- Partner engagement;
- Linkage between risk management and performance management;
- Clarity of 2nd Line of Defence roles; and
- Risk management culture.

Initiatives were undertaken to enhance these and other areas, including a change management and communication plan intended to increase risk awareness and integrate risk management more fully into key processes and thinking.

Having achieved a much higher level of maturity, the Risk function now intends to review all aspects of the ERM framework to develop a long-term vision and roadmap for Gavi's next strategic period. The Three Lines of Defence model will also be revisited to help clarify roles and responsibilities for risk management and oversight across the Alliance. The results of this audit will serve as an input to this important process of defining the next phase of the ERM journey.

We will continue to work with management to ensure that these audit issues are adequately addressed and required actions undertaken.

We take this opportunity to thank all teams involved in the audit for their assistance during the review.

Head, Internal Audit

Summary of Findings

Our audit identified three medium-rated audit issues. A summary of the issues identified, along with the agreed management actions, is provided below.

There is a need to review the current risk management approach to prioritise underdeveloped areas including operational risk management, country/programmatic risk management and the role of partners

A comprehensive ERM system involves top-down and bottom-up identification and assessment of risk, and consideration of cross-cutting themes and initiatives. It requires regular updates of risk registers by risk owners to identify mitigating actions in accordance with risk appetite. There is, however, no single 'best practice' approach to ERM, which must evolve to remain aligned with business needs and to remain proportionate to the size of the organisation. The Risk function has demonstrated commitment to continuous improvement and keeps abreast of latest ERM developments. The intention is to keep a balance between best practice, pragmatism and effective use of resources – always with the aim of supporting achievement of Gavi's strategic goals.

Since the 2013 Internal Audit of ERM and the 2015 DFID Assurance Review there has been significant progress in implementing ERM, in particular in respect of mission-critical 'Top Risks' and the definition of Risk Appetite. These processes are well designed and operate effectively, following considerable investment in Board engagement and senior management buy-in. Operational and programmatic risk management are less well developed at this stage of the ERM 'journey' and will be an area of focus in the upcoming review of the ERM vision.

Operational Risk Management (Secretariat functions)

A more operational risk management approach may achieve greater ownership and engagement in day-to-day Secretariat business activities, while providing bottom-up input to the TPM and Top Risk processes.

This would, however, require further investment in training and facilitation until fully embedded. The short-term cost of this would need to be weighed against the longer-term benefit of a more risk aware workforce and more comprehensive risk coverage.

Country Risk Management

In response to the 2013 internal audit of ERM and recommendations from the 2015 DFID Assurance Review, a well-structured approach was conceived for the management of grant-related risks. The 'Country Risk Matrix' ('CRM') was central to a number of processes intended to systematically identify, assess and manage risk and to provide assurance over the mitigating controls. Operational Guideline 3.17 sets out the respective roles and responsibilities for country risk management and the use of the Country Risk Matrix. The audit concluded that today's country risk management practices do not reflect all those set out in the OG; nor has it been updated. Following efforts to embed the CRM, a number of new risk management mechanisms have been introduced by Country Support management. However, these tools are not yet being consistently used and there is currently no reliable approach to ensure systematic identification, assessment and management of risks related to Gavi's core grant management activity.

The Risk function intends to use the opportunity of a new MD, Country Programmes to clarify the respective roles and responsibilities of the Risk and Country Support teams in respect of the definition and implementation of ERM for Country Risk Management with a view to developing an effective, fit-for-purpose approach to Country Risk Management.

Role of Partners in Risk Management

The nature of the roles and responsibilities, and supporting processes for partners in-country are not well-defined. Mixed views were expressed during the audit about the scope for partner engagement. Some managers cited examples of positive, transparent approaches to monitoring risk; others felt that there is a challenge in defining and agreeing the role of partners as Gavi's 'eyes' and 'ears' on the ground.

Efforts have been made to engage partners, for example, through participation in Risk Committee meetings or other staff communication sessions but little progress has been made to date in

Summary of Findings

integrating Alliance partners into the ERM framework.

In the April 2019 Report to the AFC and Board, the Risk function acknowledged the need to address this under-served area. The audit recommends that the role of partners in risk management in-country is clarified and formalised as part of the 3LOD rethink.

There is a need to ensure that ERM implementation plans take into account all prerequisites for success, including wider organisational factors

Successful implementation of the ERM strategy depends on wider organisational factors which may be outside the Risk function's direct sphere of influence. These include the tone at the top, oversight, culture, communication processes, performance management systems as well as infrastructure requirements (people, processes, systems and tools).

Significant effort was devoted to designing the ERM framework in 2014-2015 following recommendations from the DFID Assurance Review. DFID's follow-up report in 2015 highlighted risks to implementation including resourcing, change ownership and accountability. Four years on, despite the many developments in Gavi's structures, systems, people and processes, and in the quality of its risk management, these and other prerequisites for success still present significant challenges to efficient, effective ERM implementation.

We identified the following key areas for attention:

- Resource requirements both within the Risk function (1 FTE intermittently assisted by three successive short-term consultants) and wider Secretariat to achieve ERM goals;
- Responsibilities for the implementation of an effective 3 Lines of Defence and its ongoing co-ordination and oversight;
- Knowledge management issues within and across teams resulting from silo-based working and system deficiencies, especially in relation to grant management and country support (i.e. lack of a centralised grant management system).
- Cultural issues, as well as unstructured, undocumented working practices, limited collaboration within and between teams and communication issues and sharing of knowledge which affect the quality and reliability of team risk registers and attitudes towards ERM. Such issues were identified in the 2017 internal Risk Review and led to a new focus on change management by the Risk function. Some signs of progress were noted, but such changes require broad management support.

In defining the new ERM Vision, all relevant organisational factors should be analysed, to ensure that achievable goals are set, with the right accountabilities and a realistic implementation plan.

The role of the Risk Committee in the overall risk management process should be revisited and made more explicit

In many organisations a management 'Risk Committee' plays a crucial role in the ERM process by bringing together a cross-disciplinary group of managers to take an enterprise view of risks and to engage those same individuals to promote risk awareness and sound risk management practices across the organisation. The purpose, organisational status and activities of the Risk Committee may include:

- Oversight of risk appetite and risk tolerance and monitoring compliance;
- Processes and systems for identifying and reporting risks and risk-management deficiencies;
- Specification of management and employees' authority and independence regarding risk management roles and responsibilities;
- Integration of risk management and control objectives in management goals; and
- Effective and timely implementation of corrective actions to address risk management deficiencies.

Gavi's Risk Committee originally acted as a steering body for implementation of the Board-approved plan following the DFID Assurance Review recommendations but its role has evolved and the focus over the last two years has been to review the Top Risks and related mitigating actions.

Summary of Findings

The Risk function looks to the Committee for guidance and endorsement of its approach but its remit in respect of ERM governance and oversight is not clear. The Risk Committee has no documented Terms of Reference.

The purpose and functionality of the Risk Committee, including its composition, should be reviewed, to ensure that it maximises its contribution to Gavi's ERM process and establishment of a positive risk culture. This should be formalised in a Terms of Reference and communicated to stakeholders.

Appendix: Summary of Performance Ratings and Distribution List

Summary Performance Ratings on Areas Reviewed

For ease of follow up and to enable management to focus effectively in addressing the issues in our report, we have classified the issues arising from our review in order of significance: High, Medium and Low. In ranking the issues between 'High', 'Medium' and 'Low', we have considered the relative importance of each matter, taken in the context of both quantitative and qualitative factors, such as the relative magnitude and the nature and effect on the subject matter. This is in accordance with the

Committee of Sponsoring Organisations of the Treadway Committee (COSO) guidance and the Institute of Internal Auditors standards.

Rating	Implication
High	Address a fundamental control weakness in relation to internal controls, governance and/or risk management that should be resolved as a priority
Medium	Address a control weakness in relation to internal controls, governance and/or risk management that should be resolved within a reasonable period of time
Low	Address a potential improvement opportunity in relation to internal controls, governance and/or risk management

Distribution

Head, Risk
Chief of Staff
Managing Director, Country Programmes
Director, Country Support

For Information

Chief Executive Officer
Deputy Chief Executive Officer
Managing Director, Audit & Investigations
Executive Team
Director, Legal
Director, Programme Capacity Assessment