**Report to the**
# GAVI Alliance Board
21-22 November 2013

| | |
|---|---|
| **Subject:** | **Risk Management: Internal Audit: Audit of Enterprise Risk Management** |
| **Report of:** | Simon Lamb, Managing Director of Internal Audit |
| **Authored by:** | Simon Lamb |
| **Agenda item:** | 11b |
| **Category:** | For Information |
| **Strategic goal:** | Affects all strategic goals |

## Section A: Overview

### 1 Purpose of the report

1.1 This paper presents the results of Internal Audit's audit of Enterprise Risk Management (ERM).

### 2 Recommendations

2.1 Various recommendations are included in the audit report relating to the further development of the risk management processes at the Secretariat.

### 3 Executive summary

3.1 As noted in the report, the ERM framework established in GAVI is effective and operates well; many of the processes and methods are consistent with best practice. ERM is a process which should be continually reviewed and enhanced as an organisation grows and matures, and certain findings are made which would strengthen the framework of risk identification and management.

### 4 Risk implication and mitigation

4.1 The audit work undertaken is intended to be an evaluation of the existing processes of risk management; once recommendations are implemented, GAVI's risk management processes will be enhanced.

### 5 Financial implications: Business plan and budgets

5.1 None

## Section B: Content

### 6 Internal Audit's report

6.1 The attached paper presents a description of the audit undertaken, conclusions arising, and agreed actions.

## Section C: Implications

### 7 Impact on countries

7.1 There is no impact on GAVI-eligible countries.

### 8 Impact on GAVI stakeholders

8.1 There is no impact on stakeholders.

### 9 Impact on Secretariat

9.1 On implementation of recommendations, the Secretariat's risk management processes will be enhanced.

### 10 Legal and governance implications

10.1 There are no legal or governance implications.

### 11 Consultation

11.1 No consultation was considered necessary external to GAVI; internally, all conclusions and actions were reviewed and agreed with relevant management in the course of finalising the audit.

### 12 Gender implications

12.1 There are no gender implications associated with this policy.

Internal Audit

Final Report: Enterprise Risk Management

Report Number: 2013-01

Audit Period: 01 May - 31 July 2013

**Contents:**


I. Audit Objective and Scope ..... 2

II. Management Summary ..... 2

III. Detailed Findings and Recommendations ..... 4

IV. Remediation ..... 6

V. Action Plan ..... 8

VI. Appendix ..... 11


**Distributed to:**

Seth Berkley

Helen Evans

**cc.** Executive Team

Adrien de Chaisemartin

Ciara Goldstein

## I. Audit Objective and Scope

Audit Objective

The objective of the audit was to evaluate the process by which risks are identified, evaluated, reported and managed in the GAVI Secretariat ("GAVI"). The audit focus was primarily on the structures and processes used rather than being an assessment of the outcomes achieved in applying the risk management processes.

Audit Scope

Risk may be described as the uncertainty about events and/or their outcomes that could have a material effect on the achievement of an organisation's goals. Enterprise Risk Management (ERM) is the set of processes and associated structures, policies, and methods which enable an organisation to understand and manage its risks so as to achieve its goals with an acceptable level of variation.

The scope of the audit encompassed all of GAVI's activities and the associated risk management processes. There are many elements which make up the ERM framework; a chart, prepared in the course of the audit, sets out the key components of GAVI's ERM Framework, and is shown in the Appendix, section VI.

The audit was undertaken using as a reference point the industry standard, the International Organisation for Standardization (ISO) 31000, 'Risk Management – Principles and Guidelines'. This sets out a recognised best-practice framework which is used to help organisations develop and enhance their risk management processes.

## II. Management Summary

The ERM framework established in GAVI is effective and operates well. At its core is a risk register and associated processes which management reviews and updates quarterly; items considered to be of high risk and newly emerging risks are reviewed by the Executive Team (ET) and routinely reported to the Board, and these are discussed at Board meetings.

The means by which GAVI sets and monitors its objectives (mission, strategic goals, and corporate goals) is highly structured and monitoring metrics have been established by which the achievement of goals and objectives can be assessed. These are essential components in an effective risk management process.

The risk management process has a number of features which are consistent with best practice; key amongst them are that the risk register very formally links to the organisation's goals, and that there is a structured process of regular review, update, discussion, and reporting of risk which is well-integrated into management processes.

Many of the practices around the establishment and monitoring of corporate objectives, and the identification and management of risks within the risk register and associated processes are consistent with best practice; key elements of the existing processes are:

- There is engagement of a broad set of functions right across GAVI. Risks are identified by managers on a bottom-up basis by those close to the relevant departments and functions. This maximises the likelihood that relevant risks will be identified and brought into the scope of the risk management process through their inclusion in the risk register.
- There is effective process around the operation of the risk register which ensures that identified risks are analysed appropriately, mitigating actions are prioritised, and responsible management is identified.
- There is participation of partners (WHO, UNICEF) in providing input to the risk identification and evaluation process. While GAVI does not have staff involved in overseeing execution in-country, the involvement of Alliance partners who act as GAVI's 'eyes and ears' on the ground in the risk identification process increases the likelihood of bringing relevant risks into the scope of the risk management process.
- The risks identified in the risk register are mapped against GAVI's strategic goals. This ensures that risks are clearly associated with the possibility of failing to achieve key objectives of the organisation.

- There is quarterly review and discussion of the risk register at ET meetings. This helps validate and socialise the identified risks, and helps achieve buy-in at senior levels of management both to the process of risk management, and the relevance of the risks identified.
- The risk register is updated quarterly. The risk environment and the emerging risks are highly dynamic and it is important that there is a process of regular review.
- A risk paper describing new risks emerging and setting out the highest risks is prepared and presented to the Board regularly.
- The Key Performance Indicators, KPIs, which are prepared and monitored quarterly, include metrics relating to risk specifically, and also more generally, in that they help maintain oversight on the achievement of corporate goals.

ERM is a process which should be continually reviewed and enhanced as an organisation grows and matures and certain findings are made which would strengthen the framework of risk identification and management in the medium term. These are set out in summary, following.

## III. Detailed Findings and Recommendations

### (1) Development of a risk policy

Although elements of risk management are encapsulated in many GAVI policies (covering a variety of programmatic policies, finance-related policies, and policies and guidelines of a cross-cutting nature) there is no overarching statement of management's approach to risk management. As with any organisation, there are aspects of risk management which are subjective in nature, and would benefit from articulation. In particular, it would strengthen risk management if there was a policy setting out, amongst other things:

- a description of what is meant by risk and risk management in GAVI,
- a definition of risk tolerance and a description of how the organisation applies this in a practical way,

- a statement on the willingness to accept risk, and a determination of how that should be defined in terms of trade-offs against objectives.

The finalisation of a risk policy would create a common understanding of what risk is and how it is represented at GAVI, and help establish a common language that can be used to facilitate discussion and agreement with the Board on matters of risk management and risk tolerance.

**(2) Establishing processes to identify and manage mission-critical risks and operational risks**

Risk management should be comprehensive in covering all aspects of risk which may challenge the ability of the organisation to achieve its goals: this includes mission-critical risks, strategic risks, and operational risks. While the classification of these different risk types is not always clear as there is some overlap amongst them, the risk register tends to focus on risks associated with the achievement of the strategic goals and corporate goals. Benefit would be obtained by more formally identifying and evaluating other risks:

- Mission-critical risks. These are the higher-level risks which potentially jeopardise an organisation fulfilling its core mission. This would require the development of a mechanism by which mission-critical issues are identified, and then the establishment of a process by which they are evaluated and options for managing them are agreed.
- Operational risks. These are the risks of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risks are managed as a matter of routine every day; however, if there are failures of an operational risk nature, they can have profound effect on an organisation especially if multiple failures occur and compound their impact, as can happen when a major failure occurs. Operational risks are routinely managed across the organisation but there is no mechanism by which they are identified and evaluated in a structured way so as to ensure that all relevant risks have been identified, evaluated, and managed as appropriate.

### (3) Establishing a country-risk profile

At the heart of GAVI's risk management are the challenges posed by supporting 73 of the world's poorest countries. The achievement of GAVI's mission will be crucially affected by successful execution in a relatively small number of large and critical countries; there will also be common factors across the portfolio of countries which may benefit from common assessment and management. This would require that GAVI evaluates risk across the country portfolio as a whole; although country-by-country plans are being developed for the most significant countries, this does not offer a risk assessment across the whole range of countries in a way which would allow a country-sensitive risk management programme to be put in place.

### (4) Enhance certain processes used to capture, manage and track remediation of risks in the register to improve the rigour and consistency of approach

In addition, certain areas of potential enhancement were identified which would improve the mechanics of the existing process. None are considered of primary importance and they are not summarised here.

## IV. Remediation

Management has agreed to progress these recommendations and responsible Managing Directors have agreed to sponsor each of these main developments. A number of initiatives are already underway which will be leveraged to develop appropriate solutions:

- The development of the 2016-2020 strategy will be used as an opportunity to identify and plan for the identification and management of critical risks (the consideration of mission-challenging risks is a natural component of the strategic process) (to be sponsored by Helen Evans, Deputy Chief Executive).
- A country risk assessment process will be established as part of the Grant Application and Monitoring and Review process (to be sponsored by Hind Khatib-Othman, Managing Director of Country Programmes).

Other initiatives will need to be newly established:

- The development of a process to map and create an inventory of operational risks will be piloted in Finance and Operations where many, but not all, of the operational risks reside (to be sponsored by Barry Greene, Managing Director, Finance and Operations). This will then serve as a model by which other parts of the organisation can map and inventory their operational risks.
- The development of a risk policy will be taken forward by the Policy and Performance Team (to be sponsored by Nina Schwalbe, Managing Director, Policy and Performance).

Detailed action plans are set out in the following section.

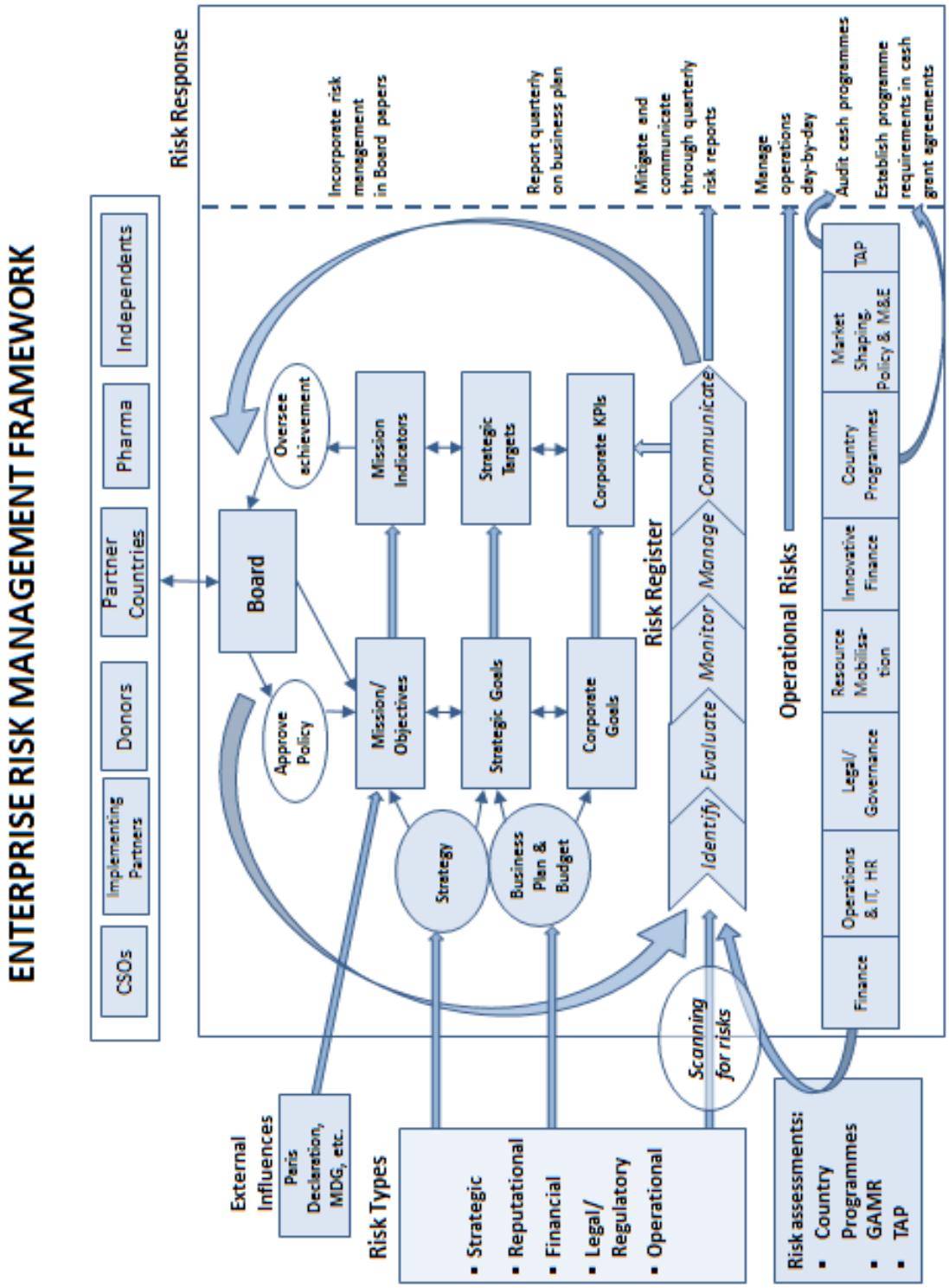
## V. Action Plan

| Issue No. | Issue | REC No. | Recommendation | Recommend-ation Priority | Action Date | Responsible ET member | Responsible Manager | Responsible Function |
|---|---|---|---|---|---|---|---|---|
| 01 | Development of a risk policy | 01 | Prepare a risk policy covering key elements of management's risk management approach (including a description of what is meant by risk at GAVI, key responsibilities in managing risk, and a description of risk tolerances and how they are described and managed). | High | 30.09.2014 (Board presentation, 11.12.2014) | Nina Schwalbe | Aurelia Nguyen | Policy and Performance |
| 02 | Establishment of processes to identify and manage mission-critical and operational risks | 01 | Review and identify a small number of risks which might be considered to be potentially mission-challenging if they were to crystallise. Evaluate their significance for GAVI, and determine if additional actions should be taken to remediate and manage the risk. | High | 30.06.2014 | Helen Evans | Adrien de Chaisemartin | Executive Office |
| 02 | Establishment of processes to identify and manage mission- | 02 | Review and document the key operational risks. Identify the actions in place to manage those risks, and assess whether any are | Medium | 31.03.2014 | Barry Greene | Tony Dutson and Andy Mends | Finance and Operations |

| Issue No. | Issue | REC No. | Recommendation | Recommend-ation Priority | Action Date | Responsible ET member | Responsible Manager | Responsible Function |
|---|---|---|---|---|---|---|---|---|
| | critical and operational risks | | not appropriately managed within the risk tolerances that management are willing to accept. | | | | | |
| 03 | Establishment of a country-risk profile | 01 | Establish a process of risk assessment covering the risks that GAVI incurs in supporting countries, differentiated by country. This should facilitate a risk-weighted, pro-active management by Country Support. | High | 30.06.2014 | Hind Khatib-Othman | Charlie Whetham | Country Programmes, GAMR |
| 04 | Enhancement of certain processes used to capture, manage and track remediation of risks in the register to improve the rigour and consistency of approach. | 01 | Certain aspects of the risk register process could be enhanced: introduce definitions for 'impact' and 'likelihood' to improve the consistency of application across the contributing management team; consider the residual risk both in the current state and post-mitigation - evaluate whether the timescale to achieve the mitigated state is sufficiently long to suggest that additional mitigation actions | Medium | 31.12.2013 | Nina Schwalbe | Adrien de Chaisemartin | Policy and Performance |

| Issue No. | Issue | REC No. | Recommendation | Recommend-ation Priority | Action Date | Responsible ET member | Responsible Manager | Responsible Function |
|---|---|---|---|---|---|---|---|---|
| | | | should be considered in the interim; ensure that all relevant functions are feeding into the risk register (aspects of risk of certain functions were found not to be included in the risk register in the course of the audit). | | | | | |
| | | | | | | | | |

## VI. Appendix


ENTERPRISE RISK MANAGEMENT FRAMEWORK
CSOs
Implementing Partners
Donors
Partner Countries
Pharma
Independents
Risk Response
Board
Approve Policy
Oversee achievement
Mission/ Objectives
Strategic Goals
Corporate Goals
Mission Indicators
Strategic Targets
Corporate KPIs
Strategy
Business Plan & Budget
Risk Register
Identify
Evaluate
Monitor
Manage
Communicate
Scanning for risks
Incorporate risk management in Board papers
Report quarterly on business plan
Mitigate and communicate through quarterly risk reports
Manage operations day-by-day
Audit cash programmes
Establish programme requirements in cash grant agreements
Operational Risks
Finance
Operations & IT, HR
Legal/ Governance
Resource Mobilisa-tion
Innovative Finance
Country Programmes
Market Shaping, Policy & M&E
TAP
External Influences
Paris Declaration, MDG, etc.
Risk Types
Strategic
Reputational
Financial
Legal/ Regulatory
Operational
Risk assessments:
Country Programmes
GAMR
TAP