

# INTERNAL AUDIT REPORT

Risk Culture  
March 2024



**Table of Contents**

	<b>Conclusion</b>	<b>3</b>
	<b>Summary of Key Audit Issues</b>	<b>3</b>
<b>1.</b>	<b>Summary of Issues</b>	<b>5</b>
<b>2.</b>	<b>Background</b>	<b>6</b>
<b>3.</b>	<b>Objectives and Scope</b>	<b>7</b>
<b>4.</b>	<b>Annexes</b>	<b>8</b>

## Conclusion

Our audit procedures were designed to assess the risk culture within Gavi and the extent to which the risk culture assists or impedes the risk management approach within the organisation.

Following recommendations by the former Department for International Development (DfID) of the UK Government, Gavi developed an approach to Enterprise Risk Management (ERM) and in particular focused on the implementation of the Three Lines of Defence (3LoD). ERM was the responsibility of the Head of Risk with the support of one and occasionally two individuals. The principal focus of the small ERM group was the development of the Risk and Assurance Report which is submitted annually to the Audit and Finance Committee of the Board and to the Board itself. This represents a major piece of work on the strategic risks as perceived at the higher levels of the organisation. In addition, the Head of Risk was instrumental in developing an approach to ERM, in running risk workshops and being an advocate for risk management across Gavi. Inevitably, there is a limit to what essentially one or two people could achieve in an organisation the size and complexity of Gavi.








The overall conclusion that is drawn from the internal audit is that ERM is at a relatively immature state in Gavi. This is despite a high level of sophistication of individuals across the organisation, many of whom have come from organisations with much more sophisticated approaches to risk management, and a general sense of willingness to take part in a structured risk management approach.










To summarise: risk is a well understood construct amongst managers and above within Gavi, which provides a great foundation on which to develop further the approach to ERM and to mature the Risk Culture. However, currently as practised at Gavi, ERM operates at a very high strategic level, but there is no effective approach to ERM beneath the annual Risk and Assurance Report. This needs to be seen in the context of an enormous amount of success within Gavi. The budget has grown from \$7.8bn (Gavi 3.0) to \$10.1bn (Gavi 5.0), while the headcount has increased from 137 in 2013 to 397 in 2022. Gavi has also successfully weathered the impact of Covid-19 and the challenges that that global pandemic entailed for the organisation.

Since the audit work was performed, Gavi has appointed a Chief Ethics, Risk and Compliance Officer, who has prepared an Ethics, Risk and Compliance Charter which was adopted by the Gavi Alliance Board in December 2023.

The audit issues identified within six key themes are provided below. In order to mitigate the issues identified, this report brings three recommendations – the first one being an over-arching recommendation encompassing consideration of all the audit issues.

## Summary of Key Audit Issues

Ref:	Description	Rating*
<b>1.1 Theme 1: Outlines of a risk culture</b>		
1.1.1	<i>Does risk inform strategic, programmatic and operational thinking?</i> Risk management as currently practised in Gavi is only effective at the strategic and governance level. ERM is not embedded throughout the organisation.	
1.1.2	<i>Does risk form part of the business conversation?</i> Gavi has a risk-averse culture where people defend the status quo, risk conversations are well structured at the executive level, however, raising risks to superiors is seen as troublemaking.	
1.1.3	<i>Is risk balanced?</i> Risk management within Gavi is significantly more focused on the avoidance of problems rather than on facilitating risks to be taken in the achievement of objectives	
<b>1.2 Theme 2: The factors that shape and inform a risk culture</b>		
1.2.1	<i>Leadership and tone from the top:</i> Senior leaders need to be seen to be active in leading risk management	
1.2.2	<i>Risk appetite and its application:</i> The Risk Appetite statement is a well-articulated document. However, the implementation is poor and there is no guidance for its use in the day-to-day work of Gavi.	
1.2.3	<i>Organisational structure:</i> The 3LoD has been implemented rigidly and is driving uncooperative behaviours which impact collaboration and is restricting the discussion of risks across the organisation.	
1.2.4	<i>Risk team/function:</i> The risk team does not have the resources to be effective in an organisation the size of Gavi.	

Ref:	Description	Rating*
1.2.5	<i>Stakeholders:</i> Gavi needs to make sure that its response to the expectations of key stakeholders regarding risk management is proportionate and tailored to the needs of the organisation	
1.2.6	<i>Societal norms:</i> Some senior people-managers from more hierarchical cultures actively discourage the raising or discussion of risks.	
<b>1.3 Theme 3: The outcomes from a good risk culture</b>		
1.3.1	<i>Better control structures:</i> Gavi has a heavily bureaucratic approach to its work, which is preventing agility in dealing with new and emerging issues.	
1.3.2	<i>More confident risk taking and appropriate risk avoidance:</i> Gavi people view risk as something to be avoided or mitigated. Very few people view risk as a means to take better managed risk in pursuit of objectives.	
1.3.3	<i>Multiple inputs to resolve complex problems:</i> Interviewees referred frequently to a rigid hierarchy that prevents discussion of risks either up the hierarchy or across departmental boundaries.	
1.3.4	<i>Appropriate consultation:</i> Rigid and hierarchical structures hinder effective communication and decision-making.	
1.3.5	<i>Fewer risk incidents and a reduced “herd mentality”:</i> Challenging the status quo and asking hard questions about risks is not happening due to the fear of raising risks upwards.	
<b>1.4 Theme 4: Avoiding the detriments from a bad risk culture</b>		
1.4.1	The Gavi Board and the senior leadership team should have a clear view of the risk culture to which they aspire for Gavi and promulgate this to the rest of the staff.	
1.4.2.	Rigid departmental boundaries prevent wide ranging discussions.	
1.4.3.	A significant proportion of staff fear raising their heads above the parapet by raising risks to their supervisors.	
1.4.4.	We did not identify a sense that the long-term future and the needs of today were actively balanced at Gavi.	
1.4.5	There is a high degree of caution and risk aversion in Gavi; people focus much more on control than risk management.	
1.4.6.	Some interviewees indicated that some individuals in senior roles actively block risks from being raised.	
1.4.7.	Some managers actively discouraged staff, particularly in the First Line, from discussing risks.	
<b>1.5 Theme 5: How to measure a risk culture</b>		
1.5.1	The risk culture should be assessed on a regular basis.	
<b>1.6 Theme 6: How the risk culture fits within the Alliance ecosystem</b>		
1.6.1	There is little explicit consideration of the ecosystem as being a logical level at which to consider risk and its management at Gavi.	
1.6.2	Risk runs through the ecosystem, however scant regard appears to be paid to risk management outside the constraints of the Gavi secretariat.	

## 1. Summary of Issues

Our overall conclusion is that ERM is at a relatively immature state in Gavi. The consequences of this relatively immature approach to risk management are that there is no consistent risk culture across Gavi and as a result risks may be missed, and opportunities may go unheeded. The evidence that emerged in this audit would suggest that with a more mature approach to risk management and a more consistent risk culture, Gavi will be able to face into new growth and to further challenges such as a new pandemic, with more confidence.

Through our audit procedures, we have identified issues across six key cross-cutting and interlinked themes and developed [three recommendations](#).

### Theme 1: Outlines of a risk culture

An effective risk culture informs strategic, programmatic (or tactical) and operational thinking. Risk forms part of the business conversation and risk is balanced.

Risk management as currently practised in Gavi is only effective at the strategic and governance level. Enterprise Risk Management (ERM) is not embedded throughout the organisation. While Gavi Secretariat people were broadly aware of the ERM process, or the concept of ERM, very few actively participated in it or used any tools, techniques or approaches from the ERM approach. This was principally because the risk process was actively designed to address the top-level risks via the creation of the annual Risk and Assurance Report.

The lack of a broad ranging ERM programme means that there is no consistency in the way in which risks are discussed across the organisation, there is little or no risk aggregation and next to no risk reporting from the bottom of the organisation upwards. Consequently, risks are managed in ways which may be sub-optimal to Gavi as a whole, and indeed management may not be aware of risks that are being identified but not reported at lower levels of the organisation.

In 2023, Gavi established the Ethics, Risk and Compliance Office, and the Secretariat presented a Charter for Ethics, Risk and Compliance to the Board in December 2023. This Charter sets the foundations for the implementation of Gavi's ERM programme.

*In response to recommendation 1, management has agreed to put in place a valid, actionable and resourced plan to re-evaluate the ERM programme with a view to ensuring that appropriate policies, tools, techniques, practices, and culture are built and implemented across Gavi so that it reaches across all material aspects of the organisation. In recognition of the fact that this should not be under-estimated in terms of time-frame, resources and change management, and will require careful reflection in order to build the right risk culture and enable appropriate risk management (not too much but not too little) throughout Gavi efficiently and effectively, the detailed section of this report provides a series of issues and suggestions, with a particular focus on risk culture, which management has agreed will be taken into account in developing the plan.*

### Theme 2: Factors that shape and inform a risk culture

Risk culture is shaped and informed by leadership and tone from the top; risk appetite and its application; the organisational structure; the risk team or function, the regulators or stakeholders; the ecosystem; and by societal norms.

One of the cornerstones of risk management which shapes and informs the risk culture is an explicit statement of Risk Appetite. Gavi's Risk Appetite Statement, approved by the Board, is well-articulated and clear about the levels of risk that are acceptable to Gavi. However, as we interviewed people for the audit, it was evident that most people had little or no knowledge of the contents of the Statement however believed that it broadly expressed a low appetite for risk in any context. As a consequence, many risks were being incorrectly challenged both by staff and managers which led to a failure to embrace some opportunities.

*In response to recommendation 2, management has agreed that the risk appetite approach be extended to address the needs of the people within the business so that there is clarity as to the implementation of the risk appetite statement, and that this will be supplemented with appropriate guidance and with a risk-based delegation of authorities.*

The Gavi Alliance is by definition an ecosystem. However, there does not appear to be any significant effort to explicitly manage risks across the ecosystem. The ERM programme operates within the confines of the Gavi Secretariat and yet the risks that are being managed within Gavi cross the entirety of the Alliance. In addition, there are frequently different approaches, cultures, and appetites for risk across Alliance members. The fact that risks pass from one part of

the Alliance to another without a consistent sense of the risk being managed is likely to lead to tension, the possibility of risks being dropped, and contradictory actions being taken which may well cancel out the benefit of any risk management actions.

*In response to recommendation 3, management has agreed to initiate a programme to review how risk is managed across the entirety of the ecosystem.*

### **Theme 3: The outcomes from a good risk culture**

Key outcomes from a good risk culture are better control structures; more confident risk-taking and appropriate risk avoidance; multiple inputs to resolve complex problems; appropriate consultation; fewer risk incidents; and a reduced “herd mentality”.

### **Theme 4: Avoiding the detriments from a bad risk culture**

Key detriments to be avoided are significant deviations from the board-espoused values; silo-based functioning; layered management reporting; excessive short-termism; control management instead of risk management; individually obstructive nodes; and black holes.

### **Theme 5: How to measure a risk culture**

The report discusses the three main tools for assessing the risk culture: surveys; interviews and understanding risk conversations, and proposes that the culture be reviewed again after an appropriate period.

### **Theme 6: How the risk culture fits within the Alliance ecosystem**

A risk culture operates across the ecosystem (the Gavi Alliance) when interests are aligned; relative power is recognised and understood; incentives are allocated; regulatory influences are taken into account; and the extent of shared values and societal views is known.

## **2. Background**

Internal Audit undertook an audit of the ERM function in 2019. One of the recommendations from that review was a follow up audit of Risk Culture, which is the subject of this report. Risk culture is considered to be an important part of an effective risk management programme in any organisation, although it is notoriously difficult to define. There is a high degree of focus on risk culture in risk management circles, including from regulators such as the PRA and FCA in the UK and their equivalents around the world. There is also reference to Risk Culture in Corporate Governance Codes and in guidance to Directors. However, there is remarkably little consensus amongst risk professionals as to what Risk Culture means.

The Internal Audit team, including a high-level risk management expert, conducted 36 interviews of 35 people (one individual was interviewed for planning and then also as part of the fieldwork) and ran a survey amongst all Gavi employees, in response to which it received 88 responses.

### **Key Definitions:**

#### **Culture**

The culture of the organisation is an accretion of the behaviours, beliefs, attitudes, activities, and ethical responses of the individuals in the organisation and determines how those individuals will respond to issues in the “here-and-now”. It is influenced by the tone from the top, incentives, and the social and regulatory environment.

#### **Risk Culture:**

The risk culture of the organisation is about how individuals tackle the complexity of the multiple futures that face them in dealing with issues today. It is about “tomorrow” rather than the “here-and-now”. It is what gives an organisation the resilience to tackle difficult decisions today while having an eye on the impact tomorrow.

### 3. Objectives and Scope

#### 3.1 Audit Objective

The objective of the audit was to assess the risk culture within Gavi and to assess the extent to which the risk culture assists or impedes the risk management approach within the organisation. The audit focused on four key areas: (i) the extent to which staff and contractors recognise the importance of risk and control behaviour and comply with any policies or procedures; (ii) the extent to which staff and contractors stop to consider risk in their daily activities or while they are developing plans for future activities; (iii) the extent to which staff recognise the explicit trade-offs between decisions for today and the impact on tomorrow; and (iv) whether conversations about risks (if any) go outside individuals' own business areas.

#### 3.2 Audit Scope and Approach

The scope of the audit included all business areas and teams across the Gavi Secretariat, and we addressed both senior management across the business and staff at all levels in a sample of business areas.

We focused primarily on the issue of risk culture within the Secretariat rather than across the entirety of the Alliance. However, as part of our interviews with Gavi Secretariat staff, we also considered the issue of risk culture linkages across alliance partners.

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

We take this opportunity to thank all the teams involved in this audit for their on-going assistance.

Director, Internal Audit

## Annexes

### Annex 1 – Methodology

Gavi’s Audit and Investigations (A&I) audits are conducted in accordance with the Institute of Internal Auditors’ (“the Institute”) mandatory guidance which includes the Core Principles for the Professional Practice of Internal Auditing, the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing (Standards). This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the audit activity’s performance. The Institute of Internal Auditors’ Practice Advisories, Practice Guides, and Position Papers are also adhered to as applicable to guide operations. In addition, A&I staff adhere to A&I’s standard operating procedures manual.

The principles and details of the A&I’s audit approach are described in its Board-approved Terms of Reference and Audit Manual and specific terms of reference for each engagement. These documents help audit staff to provide high quality professional work, and to operate efficiently and effectively. They help safeguard the independence of the A&I’s staff and the integrity of their work. The A&I’s Audit Manual contains detailed instructions for carrying out its audits, in line with the appropriate standards and expected quality.

In general, the scope of A&I’s work extends not only to the Secretariat but also to the programmes and activities carried out by Gavi’s grant recipients and partners. More specifically, its scope encompasses the examination and evaluation of the adequacy and effectiveness of Gavi’s governance, risk management processes, system of internal control, and the quality of performance in carrying out assigned responsibilities to achieve stated goals and objectives.

### Annex 2 – Definitions: audit rating and prioritisation

#### Issue Rating

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
<b>High</b>	<p>At least one instance of the criteria described below is applicable to the issue raised:</p> <ul style="list-style-type: none"> <li>• Controls mitigating high inherent risks or strategic business risks are either inadequate or ineffective.</li> <li>• The issues identified may result in a risk materialising that could either have: a major impact on delivery of organisational objectives; major reputation damage; or major financial consequences.</li> <li>• The risk has either materialised or the probability of it occurring is very likely and the mitigations put in place do not mitigate the risk.</li> <li>• Fraud and unethical behaviour including management override of key controls.</li> </ul> <p>Management attention is required as a matter of priority.</p>
<b>Medium</b>	<p>At least one instance of the criteria described below is applicable to the issue raised:</p> <ul style="list-style-type: none"> <li>• Controls mitigating medium inherent risks are either inadequate or ineffective.</li> <li>• The issues identified may result in a risk materialising that could either have: a moderate impact on delivery of organisational objectives; moderate reputation damage; or moderate financial consequences</li> <li>• The probability of the risk occurring is possible and the mitigations put in place moderately reduce the risk.</li> </ul> <p>Management action is required within a reasonable time period.</p>
<b>Low</b>	<p>At least one instance of the criteria described below is applicable to the issue raised:</p> <ul style="list-style-type: none"> <li>• Controls mitigating low inherent risks are either inadequate or ineffective.</li> <li>• The Issues identified could have a minor negative impact on the risk and control environment.</li> <li>• The probability of the risk occurring is unlikely to happen.</li> </ul> <p>Corrective action is required as appropriate.</p>