INTERNAL AUDIT REPORT

Internal Audit on Data Protection and Privacy
April 2025

Gavi
The Vaccine Alliance

Table of Contents

1. Conclusion

Our audit procedures were designed to provide assurance to management and the Gavi Board on the design and effectiveness of the key controls related to data handling, storage, access, retention, and breach response, as well as assessing compliance with best practices to protect personal and confidential business information.

Remediation has been agreed on the issues which were identified during this audit and the resolutions are in the course of implementation by management.

2. Background

Prior to 2021, data protection was implicitly covered in data governance and cyber security initiatives. Following a presentation to the Risk Committee in June 2022, the mandate for information and data protection was assigned to the Data Governance and Analytics team under the Data Protection Office.

Gavi has a low-risk appetite for critical information systems or data being compromised. Therefore, Gavi aims to align with international best practice in data protection and privacy ensuring that it maintains the confidence of stakeholders, including Gavi personnel and donors who play a vital role in its mission. Data Protection and Privacy at Gavi focuses on protecting the information and data that poses a high risk to the organisation if mishandled or disclosed without authorisation.

3. Objectives and Scope

3.1 Audit Objective

The objective of this audit was to provide reasonable assurance to management and the board on the adequacy and effectiveness of the organisation's practices, policies, and systems in ensuring compliance with data protection and privacy regulations. The audit involved evaluating the design and operating effectiveness of controls related to data handling, storage, access, retention, and breach response, as well as assessing compliance with best practices to protect personal and confidential business information.

3.2 Audit Scope and Approach

Our audit approach was risk-based, informed by our understanding of Gavi's business, governance, risk management processes and internal control systems, as well as our assessment of the risks associated with this area.

Our approach included:

- Review of relevant documentation to understand and walkthrough the key processes, risks and mitigations.
- Assessment of the design of the key processes/controls that manage the key inherent risks.
- Testing (on a sample basis) the operationalisation of key processes.
- Assessment of the quality of implemented governance and risk management processes; and
- Reporting on any observations, good practices and opportunities for improvement.

The following key areas were reviewed:

- Implementation of the Data Protection/ Privacy Initiative
- Governance and Accountability for Data Protection/Privacy
- Identification and Protection of Gavi data
- Detection, Response to and Recovery from data incidents.

We will continue to work with management to ensure that all identified audit 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

4. Annexes

Annex 1 – Methodology

Gavi's Audit and Investigations (A&I) audits are conducted in conformance with the Global Internal Audit Standards of the Institute of Internal Auditors. These Standards constitute 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' Global Guidance is also adhered to as applicable to guide operations. In addition, A&I staff adhere to A&I's Audit Manual.

The principles and details of 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 our auditors to provide high quality professional work, and to operate efficiently and effectively. They help safeguard the independence of the A&I's auditors and the integrity of their work. The Audit Manual contains detailed instructions for carrying out audits, in line with the appropriate standards and expected quality.

In general, the scope of A&I's work extends not only to the Gavi 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: opinion, audit issue rating

A. 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
High	At least one instance of the criteria described below is applicable to the finding raised: • Controls mitigating high inherent risks or strategic business risks are either inadequate or ineffective. • 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. • 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. • Fraud and unethical behaviour including management override of key controls. Management attention is required as a matter of priority.
Medium	At least one instance of the criteria described below is applicable to the finding raised: • Controls mitigating medium inherent risks are either inadequate or ineffective. • 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 • The probability of the risk occurring is possible and the mitigations put in place moderately reduce the risk. Management action is required within a reasonable time period.
Low	At least one instance of the criteria described below is applicable to the finding raised: • Controls mitigating low inherent risks are either inadequate or ineffective. • The Issues identified could have a minor negative impact on the risk and control environment. • The probability of the risk occurring is unlikely to happen. Corrective action is required as appropriate.