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.

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.

In this audit, we identified one high risk issue relating to lack of a defined governance framework for the Data Protection and Privacy Initiative and three medium risk issues as summarised below. To address the risks associated with these issues, the audit team raised six recommendations of which two were rated as high priority.

Summary of key audit issues

Ref	Description	Rating*
Governance and Accountability for Data Protection and Data Privacy		
2.2.1	Lack of a defined governance framework including oversight, job descriptions, roadmap and reporting arrangements	
2.2.2	Inadequate management of data protection and privacy risks within Gavi	
2.2.3	There is lack of regular review of Data Protection and Privacy and related policies and no formal documentation of processes and controls for data validation.	
Identification and Protection of Gavi data		
2.2.4	Incomplete Records of Processing Activities (ROPA)	

** The audit ratings attributed to each section of this report, the level of risk assigned to each audit finding and the level of priority for each recommendation, are defined in annex 2 of this report.*

2. Executive Summary

2.1 Good practices

A designated Data Protection Office has responsibility to lead Gavi's data protection effort, including its implementation and operationalisation. Approved policies and procedures outline Gavi's commitment to safeguarding confidential information and personal data.

Mandatory training was rolled out in January 2024 for all staff and consultants on Gavi Data Protection and Privacy which provided information and guidance to Gavi personnel on the general principles of data protection and privacy as well as key practices to adopt.

Privacy considerations are embedded into project planning and development phases to identify and mitigate potential privacy risks early in the process. Privacy notices are provided to data subjects to inform them of how their personal data is collected, used, stored, and shared, as well as their rights regarding this data. There are approved guidelines and processes for handling Data Subject Access Requests related to personal data processed by Gavi.

Robust mechanisms are in place for detecting security incidents and established reporting channels for employees to report potential breaches. Post-Incident reviews are performed to identify lessons learned and improve future response efforts.

A Business Continuity Planning policy ensures that Gavi can continue operations during and after a disruptive event while maintaining the confidentiality, integrity, and availability of sensitive data. There is a Disaster Recovery policy that focuses on ensuring the continued availability, integrity, and confidentiality of critical data after a disruptive event such as a natural disaster, cyberattack, or hardware failure.

2.2 Summary of Issues

Through our audit procedures, we identified one high and three medium risk-rated issues relating to data protection and privacy within Gavi. The issues are summarised below.

High priority issue

2.2.1 Lack of a defined governance framework including oversight, job descriptions, roadmap and reporting arrangements

The Data Protection and Privacy Initiative was set up following a presentation made to the Gavi Risk Committee meeting on data protection and privacy risks on 9 June 2022. However, there was no clear documentation on the formal approval of the business case that detailed the approved deliverables, project plan, or a high-level timeline specifying key milestones, project phases, or estimated timeframe for implementation.

In addition, there were various gaps in the set-up of the initiative. The oversight function for the delivery of the Data Protection and Privacy Initiative was not clearly defined or documented and there was no RASCI (Responsible, Accountable, Supporting, Consulted and Informed) matrix outlining the roles, responsibilities, accountabilities, and interdependencies for the delivery of the initiative. There were no job descriptions or clearly defined skill sets specified for the roles of the Data Protection Officer (DPO) (who is the Head of Data Governance and Analytics) and the Manager of Data Governance to support the effective delivery of data protection and privacy responsibilities for Gavi. The only job description available was for the Data Protection Analyst.

Regarding the roadmap, it was not documented at the inception of the initiative and there was no schedule with clearly defined milestones, deadlines, or documentation specifying the commencement and delivery dates of the initiative.

There was no formal reporting arrangement to track and report the progress of the Data Protection and Privacy Initiative to an oversight mechanism.

The absence of defined and documented governance arrangements and documented RASCI matrix may result in unclear roles and responsibilities, leading to inconsistencies, inefficiencies and delays in decision-making and risk of misalignment with organisational objectives.

In addition, lack of clearly documented roles and responsibilities for the key personnel may lead to inconsistencies in approach, confusion, overlap, or gaps in responsibilities, potentially impacting the effectiveness of the initiative. This could also hinder accountability, making it difficult to hold individuals responsible for specific tasks or outcomes.

Medium priority issues

2.2.2 Inadequate management of data protection and privacy risks within Gavi.

There is no comprehensive Operational Risk Register (ORR) for data protection and privacy risks linking each risk with its respective Risk Owner and associated mitigations. Monitoring and reporting on these risks is not formalised in alignment with the Standard Operating Procedure for Operational Risk Management. Examination of the risk register revealed that there was only a single risk - *'Leakage of personal and sensitive data may lead to reputational damage'* recorded.

In addition, there is no requirement to obtain assurance reports (such as ISAE 3402 or SOC2) from non-IT vendors handling data – such reports would contain information on the adequacy and effectiveness of the service organisations' internal controls and also provide assurance on the robustness of their processes and controls to protect critical information.

Without a comprehensive risk register for data protection and privacy, Gavi faces the risk of failing to systematically identify, assess, and mitigate potential vulnerabilities related to the handling of sensitive information.

2.2.3 There is lack of regular review of Data Protection and Privacy, and related policies and no formal documentation of processes and controls for data validation.

We noted through a review of Data Protection and Privacy Policy and related documents that they were last updated or approved more than a year ago with one policy (Access to Information Policy) having no evidence of review and update since 2015. In addition, there is no formal documentation of the processes and controls relating to data validation.

Lack of periodic review of Data Protection and Privacy Policy and related documents could make them outdated, incomplete or misaligned with Gavi's business needs. Implementation of Gavi's recent Policy on Policies, effective 1 March 2025, should mitigate this risk.

2.2.4 Incomplete Records of Processing Activities (ROPA)

The Records of Processing Activities (ROPA) is ongoing and not complete. Developing a comprehensive ROPA requires a clear understanding of data processing activities across the organisation.

The absence of a completed ROPA means that critical data protection risks are not being adequately identified or mitigated. This could result in unaddressed vulnerabilities, particularly around sensitive data categories, increasing the likelihood of privacy incidents.

3. 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.

4. Objectives and Scope

4.1 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.

4.2 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: Assessing the implementation of Gavi's data protection and privacy roadmap, examining the business case, project organisation and governance, and the effectiveness of the project plan. Evaluating the progress of the initiatives to ensure alignment with key milestones.
- Governance and Accountability for Data Protection/Privacy: Assessing the data governance framework to ensure effective management of data protection and privacy risks. Evaluating monitoring, tracking, and training efforts to promote accountability and ensure all stakeholders are aligned with data privacy requirements.
- Identification and Protection of Gavi data: Assessing Gavi's practices for data identification and protection, including arrangements for data security.
- Detection, Response to and Recovery from data incidents: Assessing the effectiveness of Gavi's detection, response, and recovery processes for data incidents, focusing on security incident management and business continuity/disaster recovery practices.

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 the teams involved in this audit for their on-going assistance.

Director, Internal Audit

5. 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.