INTERNAL AUDIT REPORT

Audit of Cybersecurity
December 2021

Gavi
The Vaccine Alliance

Table of Contents

Conclusion

Our audit procedures were designed to provide assurance to management and the Gavi Board on the design and operating effectiveness of the key controls in the processes related to Cybersecurity threats and risks.

We confirmed through our audit procedures that the key risks associated with Cybersecurity are well understood and being effectively managed. Remediation has been agreed on the issues which were identified during this audit and the resolutions are in the course of implementation by management.

Summary of Key Issues

1. Audit Objective

The objective of this audit was to assess the design and operating effectiveness of the key controls which ensure logical and physical security of critical systems, data, and infrastructure.

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 the audit area.
The audit work was performed in accordance with ISO 27001 standards - the main reference document for the Gavi IT security policy. In addition, the audit benchmarked the implemented security policies and practices against the NIST framework (National Institute of Standards and Technology).
The audit process included review of documentation, process walkthroughs, assessing the design and operating effectiveness of key controls and assessing the governance and risk management processes.

The scope of this Targeted Testing audit covered:

- Business Applications and related Infrastructure (internal or outsourced business applications and related software or programs);
- Data/information assets;
- Network Infrastructure and related Technologies; and
- People.

3. Summary of Key Issues Arising

Internal Audit has undertaken an audit to assess Gavi's cyber-risk management across its regular activities (which also provides assurance on COVAX-related activities as these leverage the same technology infrastructure, systems, and processes). This follows a prior cyber-risk audit of 2018 and builds on the issues identified then and the improvements which were implemented.

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

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 support and assistance.

Head, Internal Audit

Annex

Annex – 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 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 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.

Distribution

Title
Managing Director, Public Engagement and Information Services
Chief Technology and Knowledge Officer

For Information

Title
Chief Executive Officer
Chief Operating Officer
Managing Director, Audit & Investigations
Head, Strategy, Governance & Chief Information Security Officer
Executive Team
Director, Legal
Head, Risk