INTERNAL AUDIT REPORT

Internal Audit on Outsourced IT and Related Services Providers
December 2024

Gavi
The Vaccine Alliance

Table of Contents

Conclusion

Our audit procedures were designed to provide assurance to management and the Gavi Board on the adequacy and effectiveness of the key controls in the processes related to the oversight and management of outsourced IT and related service providers (i.e., mission-critical service providers).

Gavi has engaged various managed and cloud service providers to assist the KMTS team in providing IT and related services and solutions to Gavi. The outsourced IT and related services include software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), infrastructure and application support managed services, managed security service provider (MSSP) which includes the security operations centre (SOC), and incident management help desk support and call centre services. Other services include firewall and network at the global health campus (GHC), cloud services including Microsoft Office Suite, SAP, Salesforce, and Sage (HR). The roles, responsibilities and accountability for each service varies depending on the type and contractual agreement signed with Gavi.

To effectively manage the performance and risks related to outsourced IT and related service providers, KMTS, over the past two years, has been undertaking key initiatives including developing the third-party management standards, and standard operating procedure – service delivery and application management. We confirmed through our audit procedures that the key risks associated with outsourced IT and related services are understood and being managed. However, we have identified the following seven medium risk issues, as summarised below.

Summary of key issues

Ref	Description	Rating *
1.	**The IT Strategy**	
	Formally define and document the IT strategy that is aligned with Gavi's business strategy.	
2.	**Daily consultancy fee rates of outsourced IT and related Service Providers**	
	Standardise daily consultancy fee rates across service providers especially for those with similar framework agreements.	
3.	**Contractual agreements with outsourced IT and related Service Providers**	
	Include standard/mandatory terms and conditions in the contractual agreement of outsourced IT and related service providers.	
4.	**Risk management of outsourced IT and related services**	
	Develop and formally document processes and activities for risk management of outsourced IT and related services.	
5.	**Performance monitoring and review of outsourced IT Service Providers**	
	Establish a standardised and consistent mechanism for monitoring and review of performance of outsourced IT service providers.	
6.	**Performance Indicators of Outsourced IT Service Providers**	
	Include performance indicators for resolution of priority three (P3) and priority four (P4) incident tickets in the evaluation of the performance of the managed service provider.	
7.	**Automation of the KPI report generation/dashboard**	
	Fully automate the KPI reports generated from the ticketing system and avoid any manual intervention to maintain data integrity and reliability.	

** 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.*

1. Summary of issues

Through our audit procedures, we have identified seven medium risk issues relating to the oversight and management of outsourced IT and related service providers which are summarised here below. Three of these issues are specific to the outsourced IT context, and four, while observed in this audit, point to more generic procurement risks which were also observed in A&I's audit of procurement, for which the report was issued in October 2024. These latter four are described here for their relevance to the outsourced IT context, however the related recommendations for improvement and management action plans can be found in the report of the audit of procurement.

KMTS has already implemented the agreed actions for all three issues specific to the outsourced IT context, which is extremely positive.

Acknowledgement of prior management initiatives to improve the process.

KMTS, over the past two years, has been undertaking key enhancements to help the oversight and management of outsourced IT and related service providers, especially on performance and service delivery. Some of these include:

- Development and implementation of the third-party management standards,
- Development and implementation of the standard operating procedure – service delivery and application management, and
- Aligning the performance and service delivery monitoring reviews to SLAs and KPIs of service providers.

1. The IT Strategy

Formally define and document the IT strategy that is aligned with Gavi's business strategy.

In 2022 KMTS recognised and communicated to AFC as a guiding principle that the IT strategy should be aligned to Gavi business strategy by stating that *"…investment strategy/priorities to be incorporated into Gavi strategy, corporate priorities and TPM process. And adjustments can be made to react to corporate priorities/re-prioritisation, reduce portfolio risk and optimise portfolio benefits"*. At the time of the audit, the IT strategy was yet to be formalised as a comprehensive strategy document properly aligned to the Gavi strategy.

This could have impacted the efficient and effective realisation of Gavi's business strategy, especially on technology and related investment priorities. KMTS has subsequently defined and documented the IT strategy in alignment with Gavi's business strategy and hence the action is closed.

2. Daily consultancy fee rates of outsourced IT and related services (see procurement audit)

Standardise daily consultancy fee rates across service providers especially for those with similar framework agreements.

KMTS uses different daily consultancy fee rates (i.e., rate cards) across service providers though a similar framework agreement has been signed with them as preferred service providers. For instance, the daily fee rate of consultants with similar experience/skillsets carrying out similar scope of work and who are based in the same location is not the same.

Gavi may be paying varying amounts for the same services across service providers. In addition, paying consultants who have similar experience/skillsets different daily rates for similar scope of work is not in line with Gavi's commitment to fairness and equity.

3. Contractual agreements with outsourced IT and related service providers (see procurement audit)

Include standard/mandatory terms and conditions in the contractual agreement of outsourced IT and related service providers.

We noted that key/mandatory clauses were missing in some of the contractual agreements including:

- The clause on Prevention of Sexual Exploitation, Abuse and Harassment (PSEAH) was not included in two out of six service providers' contracts reviewed.
- The clause on the "rights to audit" service providers, and the requirement for them to share with Gavi their audit reports was not included in two out of six service providers' contracts reviewed.
- The requirement for a "cooling-off" period when hiring staff from a service provider was not included in all the six sampled contracts.

Gavi's reputation could potentially be negatively impacted in the event of SEAH-related misconduct by staff of service providers. The lack of an audit clause in the contracts implies that A&I could be unable to access records and information required to enable it to effectively carry out its assurance mandate over the activities of the service providers. In addition, without a "cooling-off" period, there could be potential conflict of interest if ex-staff of Gavi service providers are recruited and assigned tasks that could be in conflict with what they were doing before as service providers.

4. The risk management processes and activities for outsourced IT and related service providers (see procurement audit)

Develop and formally document processes and activities for risk management of outsourced IT and related services.

KMTS maintains a full list of outsourced services by service provider and by business process owner. The team also captures the business impact assessment for each service provider with ratings of high, medium, and low impact using factors like dependency, penetration, and risk exposure. However, the rationale for the rating and weight for each factor and the risk mitigation actions or controls implemented to manage the risks to the residual level are not documented.

Proper guidelines on how to develop and operationalise key risk management processes and activities need to be formalised and could include the following:

- risk identification, analysis, evaluation, and treatment processes using appropriate tools.
- continuous and proactive risk monitoring and review process, including identifying emerging risks.
- systematic approach to track the risk mitigation actions or controls implemented.

Lack of documented guidelines on the risk management processes and activities could lead to inconsistencies in the approach and/or an ineffective risk management system.

5. Performance monitoring and review of outsourced service providers (see procurement audit)

Establish a standard and consistent mechanism for monitoring and review of performance of outsourced IT service providers.

The process of monitoring and performance reviews of outsourced service providers is not consistent. For example, there are differences or inconsistencies in:

- the performance reporting format,
- the alignment of performance reviews to specific SLAs and KPI indicators and measures,
- the format of review meeting minute records, e.g., some of the review meeting minutes are in email bullet point form while others use power point presentations, and
- the tracking and follow up of action items, setting up due dates and owners for action items, indicators of the status, etc.

Lack of consistency in the approach and tools for monitoring the performance of service providers could make it difficult to evaluate whether Gavi is obtaining value for money and compare performance across service providers.

6. Performance Indicators of Outsourced IT service providers

Include performance indicators on resolution of priority three (P3) and priority four (P4) incident tickets in the evaluation of the performance of the managed service provider.

The evaluation of the performance of the managed service provider does not consider the time taken to resolve priority three (P3 - medium) and priority four (P4 – low) tickets raised by users via the IT service portal for support and yet some of the user requests in these categories are usually very critical and/or affect the majority of users. For instance, 99% of the tickets raised by users between January and September 2023 were P3 (8%) and P4 (91%) tickets. Currently, only very high and high priority tickets (P1 and P2) are considered in the evaluation of the performance of the managed service provider. This choice of metric for performance evaluation means that service providers do not respond quickly enough to P3 and P4 tickets , despite the fact that these affect the majority of users. Our analysis of open tickets at the time of the audit indicated that about 41 P3 and P4 tickets had been unresolved for a period of between 21 and 122 business days (60% of the tickets were related to users of Gavi's main systems/business applications).

Gavi may not be effectively holding the service providers to account regarding their performance due to the current approach of focusing on very high/high priority(P1/P2) tickets, which constitute only 1% of tickets raised by users. In

addition, the majority of users may not be getting timely and adequate support from the service providers thereby impacting their efficiency and experience in the use of the systems.

KMTS has now included P3 and P4 priority tickets in the metric of performance evaluation (KPIs) of vendors, and hence the action is closed.

7. Automation of the KPI report generation/dashboard

Fully automate the KPI reports generated from the ticketing system and avoid any manual intervention to maintain data integrity and reliability.

The KPI reports and performance review presentation slides are prepared by the service providers from the ticketing system. As a result, the KMTS team has to validate the reliability and integrity of the data and content of reports, which is both time consuming and inefficient. According to the SOP - service delivery and application management, section 3.4.3.1, the service providers are responsible for entering the data into the tool (ticketing system) while KMTS is responsible and accountable for the reliability and integrity of the ticketing system extract and its quality. However, at the time of the audit, it was the service providers who were preparing and providing their own KPI reports and performance review presentation slides from the system.

The reliability and integrity of the KPI reports and performance slides cannot be assured as they are not prepared by someone who is fully independent of the process.

KMTS has fully automated the SLA/KPI reporting out of Service Now system following our observation. The Automated dashboard is used in the performance review of service request tickets, and hence the action is closed.

2. Background

KMTS has engaged various cloud and managed service providers to assist the KMTS team in providing IT services and solutions to the organisation. The managed and outsourced IT services include software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), infrastructure and application support managed services, and managed security service provider (MSSP) among others. The roles, responsibilities and accountability for each service varies depending on the type and contractual agreement signed with Gavi. KMTS is currently working with service providers in the following key areas:

- Infrastructure and application support managed services (i.e., includes application support services, platform and infrastructure support services, tools implementation and support services, network connectivity and other professional services).
- Managed security services including the security operations centre (SOC) and incident management.
- Help desk support and call centre services.
- Firewall and network at the global health campus (GHC).
- Cloud services.

According to the data obtained from KMTS, the total spending on outsourced IT and related services (i.e., IT software, hardware, managed services, consultancy services, telephony, etc.) for the year 2022 amounted to ~$16.4 million.

3. Objectives and Scope

3.1 Audit Objective

This audit was focused on the assessment of the design and operating effectiveness of the key controls in the oversight and management of outsourced IT and related service providers mainly in the following areas:

- The adequacy of the design and the operating effectiveness of the key controls regarding the selection process, to ensure that the most suitable service providers are engaged in line with Gavi's policies, rules, and regulations.
- Whether the risks associated with outsourcing such as continued availability of services, security of information, acceptable levels of service, among others, are adequately and effectively mitigated through appropriate controls.
- Whether the objectives of outsourcing are being achieved and the organisation is making the best use of outsourcing.

3.2 Audit Scope and Approach

This audit covered the outsourced IT and related service providers selection process, contract management, risk management, and performance and service delivery management systems, based on a sample review of major service providers for year 2023.

The following areas have been excluded from the audit scope (i.e., either they have been covered in other audits or have a distinct risk profile):

- Individual consultants and/or contractors services.
- Non-IT and related outsourced services.

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 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
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.