INTERNAL AUDIT REPORT

Data Security, Business Continuity Plan & Disaster Recovery Audit

July 2018

Conclusion

Our audit procedures were designed to provide assurance to management and the Gavi Board on the adequacy and implementation of the controls on data security, business continuity management and disaster recovery procedures.

We have identified controls that we considered relevant and necessary for adequate management of data security, business continuity and disaster recovery. The appropriateness of measures taken by Gavi to address the risks on data security, business continuity and disaster recovery are evaluated through the effectiveness of these controls.

Through our audit procedures, we have identified certain control weaknesses related to the management of data security, business continuity and disaster recovery as detailed below.

Key Internal Audit Issue Summary (High and Medium)

Issue Description	Rating	Ref	Page
Business Continuity Management (BCM)			
The Business Continuity Management process needs to be formally designed (including development and implementation of policies and procedures)	High	1	6
Disaster Recovery Plan (DRP)			
The Disaster Recovery Plan needs to be updated and implemented	High	2	8
Network Security			
A vulnerability management programme needs to be designed and implemented and malware protection processes enhanced.	High	3	10
Intrusion Detection and Prevention and Data Loss Prevention systems need to implemented and deployed.	High	4	12
Logical Security			
The IT governance framework needs to be formalised	Medium	5	13
The process of identification and classification of information assets needs to be formalised	Medium	6	15
Segregation of duties (SoD) matrix needs to be developed (including implementation of monitoring and access review)	Medium	7	18
Security Program			
The information security awareness and sensitisation programme for end-users needs to be formalised	Medium	8	19

Contents

Summary of Findings

Through our audit procedures, we have identified four high-rated issues related to the Business Continuity Management, Disaster Recovery Plan and Security programs.

Business continuity Management (BCM)

There is limited focus on business continuity management at Gavi. The current process is not formally designed and policies and procedures have not been developed and implemented to surround practices of management in term of business continuity. In the current situation, if Gavi were to face any type of unexpected event or disaster, it is likely that the organisation would not be able to respond adequately to maintain and recover its key activities. Management as well as staff are therefore not aware of behaviours to adopt in a crisis situation and also given that most important assets and activities have not been formally identified and classified to ensure they are considered in priority in such situations.

Disaster Recovery Plan (DRP)

Following the initial design of the DRP in 2010, Gavi has not implemented processes to maintain an accurate and up to date DR plan for its business needs.

DRP is not updated on a periodic basis and it doesn't include all relevant IT layers for Gavi's critical applications supporting key activities.

Gavi has no policies to activate the DRP. In the current situation, it is difficult to align the backup strategy with the Recovery Point Objective (RPO) that should be approved as part of the BCP or the DRP. In addition, we are unable to confirm that Gavi's infrastructure (including backup sites), is consistent with the DRP. The DRP is consequently not tested on a regular basis to ensure it is robust. We also noted that training (including relevant material) is not provided to GAVI's employees.

Vulnerability management, malware protection processes and network documentation

Gavi does not have a consistent vulnerability management programme. Regular vulnerability assessments and penetration tests are not conducted.

Malware protection is solely running on end user workstations (servers and SMTP relay are not included in the malware protection scope) and this is not properly documented. Therefore the risk of malicious software finding its way to users' workstations is high when there is no antivirus solution running on mail servers.

The network of the organisation's infrastructure is not documented and kept up-to-date to facilitate risk assessment and identification of potential issues regarding ongoing IT projects.

Gavi has not implemented and deployed Intrusion Prevention and Detection Systems. In addition, the Data Loss Prevention process has not been established or implemented. We also noted that the organisation does not maintain technical IT documentation regarding the external access configuration and settings.

Information Security Awareness and Sensitisation Programme

Employees and contractors are currently not well-informed particularly on cyber-attack matters and there seems a low security maturity level. Currently employees are not sensitised on cyber-security matters through mandatory training programmes in line with industry best practices for risk management.

Other Issues identified

In addition, we identified six medium-rated issues related to third party reliance (outsourced services), logical security, and network management. A detailed analysis of all issues raised, including the two low-rated issues, is included in the appendices.

Audit Objective

Our audit assessed the adequacy and effectiveness of the internal controls over Business continuity management, disaster recovery procedures and data security.

Audit Scope and Approach

We adopted a risk-based audit approach based on our assessment of the system of internal controls.

Our audit approach included interviewing the IT team, reviewing management and committee reports, reviewing a sample of applications and related documents and sample-testing evidence of the controls in place. In the course of the audit we also considered the procedure and guidance documents as well as the IT systems supporting the processes.

This audit was designed to assess the:

- Design and operating effectiveness, where possible, of the key controls;
- Design and implementation of business continuity procedures, disaster recovery plan and data security;
- Quality of implemented governance and risk management practices; and
- Compliance with relevant policies, procedures approved by the management.

Summary of Findings

The scope of this audit covered the following key areas in relation to business continuity management, disaster recovery planning and data security:

- Logical security
- Physical security
- Log controls
- Network
- Change Management
- Data classification
- Third party reliance
- Incident management
- Business continuity plan
- Disaster recovery plan

Background

Currently, the risk of significant disruption of the Secretariat (i.e. based in Geneva and Washington DC) is rated as 'High'. A high level analysis performed during the project inception phase revealed the following:

- Business Continuity (BC) and Disaster Recovery (DR) plans currently exist for a minimum of activities and assets in Gavi.
    - Finance and Accounting have BC plans in place but they appear outdated
    - DR plans are in place for servers but also relatively outdated; moreover, the IT strategy is moving away from having its own data centre and towards a managed cloud service solution
    - None of these plans have been rehearsed in the recent past; so their effectiveness is unknown.
- Basic IT security practices are in place but the majority seem to be only reactive. Some key activities, such as data backups, are not performed in a structured and consistent manner or could even be missing.
- Gavi is developing a Crisis Management Policy and this is yet to be integrated into the organisation's ways of working. In addition, the organisation does not have a clear governance structure for managing crises as well as clearly defined incident response plans.
- Gavi does not have a clear and complete schedule of training and rehearsals of emergency responses, business continuity and disaster recovery plans.

The main conclusion from our review is that Gavi's overall organisational resilience is low and action is required in order to address the identified gaps. The Operations (Ops) and Knowledge Management and Technology Services (KMTS) teams consequently decided to initiate a Gavi-wide BC / DR Programme, under joint leadership.

Risk appetite considerations

The Alliance seeks to maintain a low level of risk related to the quality and robustness of Secretariat processes, systems and management to prevent interruption of critical information systems and business operations.

The Alliance has a low appetite for the risk that critical information systems or data become significantly compromised by a cyber-attack or technology failure.

The Operational Risk Management Framework

The Business Continuity/Disaster Recovery management process is a key component of Gavi's Operational Risk Management Framework, which pulls together crisis management, Business Continuity / Disaster Recovery planning and the on-going IT and staff security management under one coherent structure.

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
1	**High**	**Business Continuity Management System (BCMS) and Business Continuity Plan (BCP) need to be defined** Business Continuity Planning (BCP) is the creation of a strategy through the recognition of threats and risks facing a company, with an eye to ensure that personnel and assets are protected and able to function in the event of a disaster. A business continuity management system has not been developed. A BCP has also not been documented and implemented.	Threats to business operations and Gavi's exposure to such threats may not be adequately identified and appropriate response mechanisms defined to ensure that should such events occur, they are adequately managed to minimise the disruption to operations. Management may not adequately identify and allocate the resources, including systems, needed to respond to crisis.	**Within 1 year:** a) Develop and introduce a Business Continuity Management System (BCMS) consisting of: established policies and objectives; responsibilities; and management processes for implementation, performance assessment and review. b) Periodically conduct a Business Impact Analysis (BIA) differentiating critical and non-critical activities, assessing their likelihood of occurrence and potential impact on operations. c) Develop a BCP or multiple BCPs depending on the dependencies, taking into account Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Business continuity management requires the collaboration of several units in Gavi: IT, HR,	Accepted Operations and KM&TS teams launched a BCDR program end of 2017. The first phase consisted of running an RFP to select a provider to work with Gavi on developing a robust and scalable resilience capability that enables Gavi to maintain the delivery of key services and activities. The program kicked off in quarter 1. The deliverables have been identified around three workstreams and work will be done during the project to ensure that all the recommended actions for management are covered within the 3 workstreams below: Workstream 1 (W1): a) Develop a BCMS with policies and responsibilities matrix	Managing Director, Finance & Operations/ Managing Director, Public Engagement & Information Services (MD, PEIS) Steering Committee members: Chief Knowledge Officer (CKO) / Director, Operations. / Director, Legal / Director, HR	W1: end Q2 2018 W2: end Q3 2018 W3: end Q4 2018	Started

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
				facilities management, communication, etc. d) Develop a training program for key employees involved in the BCP process and create awareness of the BCP within the organisation. **Recurrent:** a) Periodically review, maintain and test the BCP in line with industry best practice to ensure it remains fit-for-purpose by testing its feasibility and operating effectiveness. b) Perform regular BIA, risk assessment and impact scenarios. c) Review and update the BCP based on new inputs and update the training program. The changes should be presented to senior management for review and approval.	b) Assess the current BCDR capabilities, conduct BIAs and identify the RTO/RPO c) Develop the strategy and the delivery plans for BCDR d) Conduct structured tests for each plan e) Develop a training plan for staff workstream 2 (W2) f) Develop a data classification and prioritisation system to enable data loss prevention g) Conduct a review of basic security provision workstream 3 (W3) h) Develop and implement a Governance and Management Framework for the future management and development of the BCDR capabilities (revisit BCMS). i) Include			

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
					recommendations for a managed DR solution for Gavi j) Define metrics and KPIs which will be used to enable Gavi to assess and develop the maturity of the Business Continuity program k) Develop a Continuous Improvement Strategy. The BCDR program was tightly linked to the Global Health Campus (GHC) move.			
2	**High**	**The Disaster Recovery Plan (DRP) needs to be updated** Following the initial design of the DRP, processes have not been implemented to ensure that the DRP remains updated and relevant to Gavi's business needs. The following was noted: a) The DRP is not updated on a periodic basis. Additionally, the DRP	Inadequate response in case of an event which may lead to: • disruption of business operations; • potential threat to employees' lives; and • loss of management control and assets.	Management should: a) Based on the business continuity planning (BCP), maintain a DR Plan which is up to date, and ensure all relevant external and internal factors and changes are taken into consideration. b) Update the DRP on a regular basis based on formal business impact analysis, risk assessments	Accepted The KMTS team currently maintains a backup of its business applications and ensures that its data and infrastructure is secured through the different security layers implemented (firewall, mobile device management, security against internet threats	MD, PEIS. CKO, Head, KM&TS	DRP Design (W3): end Q4 2018 W4: Q2 2019	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		does not include all relevant IT layers for Gavi's critical applications supporting key activities. b) There are no policies to activate the DRP, making it difficult to align the backup strategy with the RPO that should be approved as part of the BCP or the DRP. In addition, we could not verify whether the current infrastructure, including backup sites, is consistent with the DRP. c) The DRP is not tested on a regular basis to ensure its robustness. d) Training (including development of relevant material) is not provided to employees.		and the results of regular tests. c) Regularly test the DRP to ensure that it remains aligned to the business needs. Gavi's exposure to threats should be appropriately addressed so that in the event that they materialise, they have a limited and known impact on business and activities; and d) Develop training materials and ensure that staff are trained on the DRP strategy.	among others). The move of Gavi's infrastructure and applications to a hosted cloud solution has been the strategy of Gavi to enhance its security practices and limit the risk on Gavi. We do believe that tighter security and a comprehensive DRP is needed and as part of the BCRD Program, the DRP design will be delivered in W3 of the RFP. The actual development, implementation and recurrent tests will be delivered in workstream 4 (W4).			

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
3	**High**	**Vulnerability management programme needs to be designed and implemented** There is lack of a consistent vulnerability management program. In addition, regular vulnerability assessments and penetration tests are not carried out. **Malware protection processes need to be enhanced** Malware protection is solely running on end user workstations and is not properly documented. For instance servers and SMTP relay are not included in the malware protection scope. There is no antivirus solution running on mail servers to prevent any malicious software from entering deep within the foundation network and reach the users workstations. Furthermore, there is no IT documentation on the antivirus solution.	• Gavi is not efficiently protected against zero day disclosures or easily exploitable vulnerabilities; • Vulnerabilities may not be quickly identified, assigned and tracked to ensure that they are resolved; • Critical vulnerabilities may remain unpatched without regular vulnerability assessments; • Lack of malware detection on the email servers could result in malicious software	a) Define a vulnerability management program with regular and scheduled internal and external vulnerability scans, as well as regular penetration testing on new Gavi-owned software or solution deployment. b) Deploy antivirus solutions on the email proxy servers, to analyse incoming and outgoing emails, and block those that have not been scanned. c) Document Gavi's network, for instance through a global diagram, and ensure it is updated on a regular basis. . d) Include root-cause analysis in the incident management documentation.	Accepted The KM&TS team has already implemented an email protection control. Spams and phishing emails (~10,000) have been identified and blocked last year. The KM&TS team will continue to enhance its security by implementing the recommended actions. This effort will be accelerated after the Gavi move to the GHC.	MD, PEIS CKO, Head, KM&TS.	a) Q3 2018 b) Q1 2018 c) Q3 2018 d) Q2 2018	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		Network infrastructure needs to be documented The network infrastructure has not been documented to facilitate risk assessment and identification of potential issues regarding ongoing IT projects. As a result, we could not evaluate the effectiveness of any network segmentation in place. **Incident response needs to be documented** Gavi does not maintain any incident response documentation. Root cause analysis is not carried out to prevent recurrence.	intrusion on user systems. Outgoing malicious email sent by infected end user system could also impact Gavi's reputation (including blacklisting); • Without any network documentation, it is difficult to effectively assess the risks associated with ongoing IT project or determine the security level provided by any network segregation that might be in place. The organisation could therefore be vulnerable to					

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
			lateral movement of malicious software, leading to its fast and wide propagation. Ransomware are specifically eager to easy lateral movement; and • Lack of root cause analysis denies management the opportunity to effectively identify and address the causes to disruption thereby increasing the likelihood of recurrence.					
4	**High**	**Intrusion Detection and Prevention and Data Loss Prevention systems need to be implemented; and**	Increased exposure to external attacks through exploitation	a) Build remote access and VPN documentation reflecting current settings and technology used. This	Accepted	MD, PEIS CKO, Head, KM&TS.	a) Q3 2018 b) Q4 2018	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		external access configuration and settings need to be documented We noted that there is no Intrusion Detection System or Intrusion Prevention System that has been implemented. Further, there is no Data Loss Prevention process in place. There is no technical IT documentation on external access configuration and settings.	of network vulnerabilities. • There is increased risk of data exfiltration by users who can upload sensitive data on remote hosts. • Attackers having access to Gavi's internal network could also benefit from the lack of DLP as they are not restricted on the data they can send out of the internal network.	access should also be included in regular vulnerability assessments. b) Perform a global risk assessment of system and network security in order to identify critical network zones and deploy Intrusion Detection (IDS) and Intrusion Prevention System (IPS) capabilities at key points in the network. c) Perform a global risk assessment and data classification in order to identify locations where sensitive data is hosted or manipulated and deploy DLP capabilities, such as system agents running on workstations, scanning incoming and outgoing patterns, or USB/optic media blocking agents.	This activity is tightly linked to the GHC setup and will be accelerated after the Gavi move to the GHC. The data loss prevention will be linked to the output of the data classification exercise. Data classification is a deliverable of BCDR workstream 2.		c) Q1 2019	
5	**Medium**	**The IT governance framework needs to be formalised**	Lack of a formal framework to develop procedures and standards for	**Immediately:** a) Develop a formal governance framework,	Accepted The KM&TS team has drafted an update of the IT	MD, PEIS/ CKO	IT Policy: Q1 2018	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		A governance charter provides management and employees with a high level understanding of governance activities and responsibilities. This framework usually includes IT and logical security perimeter in order for management to develop policies, procedures and standards that are aligned across the organisation and be aware of data security issues. a) We noted that there is no formal IT governance framework that has been developed. b) The IT policy has not been updated since 2010 and does not reflect the current status of the organisation.	logical access management poses the following risks to the organisation: • users having access privileges beyond those necessary to perform their assigned duties; • inappropriate changes being made directly to data through means other than application transactions; • systems not being adequately configured or updated to restrict system access to properly authorised and appropriate users; and	including a governance charter. b) Update the IT policy and ensure it is reviewed and updated on a periodic basis (or when any major changes occur in the organisation). c) Develop an IT security policy. **Within 1 year:** a) Evaluate the current procedures and standards against the IT policy and the IT security policy to ensure that procedures and standards are aligned with the principles approved by management. b) Develop a training programme for all staff and contractors to ensure that they are aware of the policies and the security requirements.	User Acceptance Policy for approval by the SMT. Out of this policy, there will be a set of standard operating procedures (SOPs) and guidelines drafted and communicated to users; a training program is planned to get all users informed about the new policy and any updated procedures and guidelines		IT Security Policy: Q3 2018 SOPs: Q4 2018 Communication: Q1 2018 Review IT Policy: once per year	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
			• inappropriate changes being made to application systems or programs (this risk is particularly high with a high probability of non-detection) due to the lack of security level measurement and detection measures.	c) Develop an acceptable user policy to be signed by the users.				
6	**Medium**	**a) The process of identification and classification of information assets needs to be formalised** Management has not developed and implemented a policy regarding information assets and key information assets have not been identified and classified. While we noted that senior management has a good understanding of the key	• Systems cannot be configured in accordance with the criticality or sensitivity of the information assets to enhance data security • Increased risk of unauthorised access, modification	**Within 1 year:** a) Develop an information assets classification and protection policy to create a formal framework for data classification and protection. b) Prepare an inventory of all information assets and classify them in accordance with the policy.	Accepted This effort is linked to the BCDR workstreams and will be implemented once the design out of the BCDR is finalised.	MD, PEIS, CKO, Head, KMTS	Q4 2018 – Q1 2019	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		information assets which it tends to protect appropriately, the practices were however not formalised and documented. **b) A data classification policy is not in place and there are ineffective controls regarding data leakage** Management has not implemented controls on sensitive data classification.	and leakage of sensitive data. • Lack of strong logical and physical controls on data increases the risk of users (i.e. employees and contractors) inadvertently broadcasting or gaining unauthorised access to critical and sensitive information.	c) Implement appropriate controls to protect information assets. The level of control should be based on the criticality and sensitivity of the information assets being protected. d) Identify information assets owners to monitor on a regular basis the security of information assets. e) Implement a data leak prevention system. The system should be based on strong logical controls to restrict access to sensitive data (secured folders, restricted disk, dedicated application, etc) and should reduce the risk of inappropriate broadcast by restricting data extraction (e.g. it should only allow upload of data using the dedicated disks). f) Identify data owners and implement controls to				

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
				ensure access to the data is approved by the owners based on business needs. **Recurrent:** a) Update the information assets inventory and the list of information assets owners. b) Conduct an audit of information assets protection. c) Conduct an audit of critical data to ensure access is appropriately restricted and only allowed following approval by the data owner. d) Monitor access to restricted data and ensure that all modifications and uploads have been duly approved.				

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
7	**Medium**	**Segregation of duties (SoD) matrix needs to be developed** Management has not developed an SOD matrix for its critical applications. As a result, user roles and privileges have not been defined and assigned based on need. Given that there are no guidelines and principles on SOD, employees involved in user access provisioning and user access reviews do not have the tools and knowledge to detect SOD issues and address the correlated risk through configured preventive controls in the application of manual detective controls.	Users may have excess or conflicting privileges which may be manipulated to inappropriately access unauthorized information or perpetrate fraud resulting in financial, IT and reputational risk for Gavi. The failure to put in place an SOD matrix and monitor segregation of duties and conflicting access exposes the organisation to IT related and financial risks. In the current situation, management is not able to address the risk that users may have access privileges beyond those necessary to perform their assigned duties.Loss of data integrity	**Within 1 year:** a) Identify critical applications exposed to the SOD risk and develop an SOD matrix by identifying user roles and assigning privileges based on the roles. b) Identify privileges associated with each role in the application (identify conflicting privileges in the SOD matrix and consequently roles that should not be combined).Define an approval process for users who may need conflicting roles. c) Implement mitigating procedures and controls for the activities of users' with conflicting roles. **Recurrent:** Periodically review the user access lists (including roles and privileges in the critical	Accept The recommendations will be implemented within the proposed timeframe.	MD, PEIS, CKO, Head, KM&TS	Q2 2018	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
			resulting from unauthorised access to data and information. Users with conflicting access privileges could make inappropriate changes directly to data thereby impacting the integrity of the data. In addition, the risk of inappropriate and unauthorized access to data is high.	applications). Ensure that roles and privileges have been dully approved and that mitigating controls have been implemented as expected when reviewing the user access lists.				
8	**Medium**	**There is need to develop a formal information security awareness and sensitisation programme for end-users** There is no formal information security awareness and sensitisation programme for end users. Currently, employees are expected to rely on directives established by management to ensure their actions are appropriate. In addition,	Security breaches resulting from lack of and/or limited awareness of the Gavi information security principles by employees. Increased risk of employees installing malwares inadvertently through unauthorised devices	a) Develop information security and sensitisation awareness training materials and ensure that all staff and contractors undergo mandatory training. b) Identify a security champion from business (non-IT) who can be reached for security dilemmas.	Accepted In 2017, the KM&TS team started creating awareness within Gavi by running informative sessions and communicating via the Service Desk on how to secure users' identities and to protect against malicious attacks. A more comprehensive training is currently being developed and will be	MD, PEIS. CKO, Head, KMTS	Short term: Q1 2018 Training: Q3 2018 Periodic updates: once	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		employees are not periodically challenged to ensure they remain aware of potential threats that could arise from malicious third parties. This is corroborated by an incident on 18 October 2016 in which these vulnerabilities were exploited. This security incident was documented by service desk (SUP0028389).	or phishing campaigns due to limited and/or minimal information security awareness. Employees may also not be aware of how to respond to potential attacks, thereby compromising the information security of the organisation. Employees who are not well informed of security principles to observe to prevent data leakage increase the threat of unauthorized access to sensitive data by both internal and external sources. The risk is further increased by the lack of a clear data classification framework.	c) Implement a phishing campaign to test and educate users. **Recurrent:** a) Perform periodic updates of the training material and consider assessing employees' understanding periodically. b) Perform phishing campaigns and review the results to ensure employees remain aware and attentive to the risk. c) Implement periodic security principles reminders to maintain employees' and contractors' awareness of policies applicable at Gavi.	provided to users in the coming months.		per year	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
9	**Medium**	**The process of incident management should be enhanced** The policy and Standard Operating Procedures (SOPs) on incident risk management have not been duly approved by management. Key attributes for classification and prioritisation have been documented in the policy and the SOPs. However, these are not applied by all users. In addition, the control on incident management as designed is only partially implemented. One of the key parameters is incident classification/rating which determines resource allocation and prioritisation of resolution. In light of the foregoing, GAVI could experience a major incident and fail to investigate and resolve it in a timely manner due to inappropriate	The policies and SOPs which are still in draft may not be implemented consistently and potentially create confusion in the process of identification, classification and resolution of incidents. Failure to strictly enforce the policy may lead to delay in resolution of incidents. Furthermore, inconsistent classification of incidents may lead to inefficiencies in root-cause analysis, which may create additional costs and higher risk exposure.	**Immediately/short term:** a) KM&TS management should review and approve the policy and the SOPs and define a process for periodic review and update. b) Users should be trained on the classification of incidents to ensure that the help desk is prioritizing critical incidents appropriately. Management could consider developing a short tutorial for employees on the intranet page with an email address for creating tickets. **Within 1 year:** Implement a ticketing tool interface that allows users to create tickets directly and automatically classify incidents based on the users' answers to basic questions.	Accept The KMTS team has been working on finalising the IT processes and implementing them. There have been delays incurred due to competing priorities. The KMTS has recruited a Service Delivery and Operations Manager; one of his objectives is to finalise the IT operating procedures, ensure that the Service Desk is operating accordingly and that users are informed of the way the Service Desk and Operations teams are working. The Self Service portal has been planned in 2017 but deprioritised against other business priorities. In 2018, the design of the self-service portal will depend heavily on how the GHC will be operating.	MD, PEIS. CKO, Head, KMTS	Policies and SOPs: Q2 2018 Self-service portal: Q4 2018	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		allocation of help desk's resources.						
10	**Medium**	**There is need for periodic review of the activity logs** Due to system limitations, logging is not enabled within Gavi's critical systems. As a result, users' activities are not monitored or audited on a regular basis to detect unauthorised or inappropriate activity. Under such circumstances, management may not be able to detect SOD conflicts and users with access privileges beyond what is required to perform their assigned duties. Management may also not be able to detect systems not appropriately configured so as to restrict access to properly authorised and appropriate users. Finally, management may not be able to detect inappropriate changes made to application systems or	Management may not be able to detect and address the following on a timely basis resulting in disruption of activities and/or loss of confidential information: a) SOD conflicts and users with access privileges beyond what is required to perform their assigned duties. b) Systems that are not appropriately configured to restrict access to properly authorised and appropriate users. c) Inappropriate changes made to application systems or	**Short term:** Develop a framework for review/audit of activity logs. The framework should include, among other items: • The types of audit logs to be enabled and types of activities to be captured; • The scope i.e. applications and databases covered by the strategy; • The frequency of review; • A defined criteria for investigation and the documentation that should be maintained to evidence management actions; • Assignment of the monitoring responsibility; and • Strategy and procedures for responding to unauthorised system activity.	Accepted. The KM&TS team has recently moved the operations of its Azure data centre to a managed service provider. The objective of the first phase of this effort has been to test the viability of the solution. In the next months, the KM&TS team will work closely with the service provider to include the short term recommended solutions. As part of the GHC setup, a Security Information and Event Management (SIEM) is foreseen for the common data centre. Gavi will benefit from this setup to activate its own SIEM.	MD, PEIS. CKO, Head, KMTS	Short term: Q3 2018 Long term: Q2 2019	

Appendix 1: High and Medium Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		programs.	programs. d) Inappropriate users' activities in the system.	**Long term:** Assess the viability of the implementation of Security Information and Event Management (SIEM) tool, which provides real-time analysis of security alerts generated by network hardware, database and applications. Such a system would facilitate an efficient and effective log management process.				

Appendix 2: Low Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
11	**Low**	**Service level management** During our audit, we observed that the existing policy for service level management is not implemented as designed. For critical service providers, it's essential that Gavi maintains the right to independently monitor service performance and gain a level of assurance regarding effectiveness of the service provider's internal controls. In the current situation, Gavi is not in a position to ensure that the service level agreed is met and that a strong control environment is maintained by the service provider that meets Gavi standards. Gavi should have access to reports on service performance to be able to compare these against the agreed service level, identify performance gaps and conduct root cause analysis.	The service providers may not be fully accountable to Gavi regarding the agreed service level and maintenance of a control environment which meets minimum standards and safeguards Gavi's assets.	The current policy for Service level management (SLM_PCY_001_V1.0) already requires management to monitor service performance and perform service review. **Short term:** 1) Given that the formal framework already exists, we recommend that this is implemented in full for all new contracts with service providers. There should be an amendment to existing contracts to provide for annual review. The service providers should be requested to share with Gavi from time to time any independent assurance reports on their performance and internal control system. The IT related contract agreements should have a standard clause that grants Gavi audit rights to undertake independent	Accepted SLAs and OLAs exist with different service and platform providers. What is needed is to get an aggregated set of SLAs across the different services and platforms, update the policy as needed and define reporting mechanisms and frequency.	MD, PEIS. CKO, Head, KMTS	Q2 2018	

Appendix 2: Low Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
				reviews as and when deemed fit.				
12	**Low**	**There is need for periodic review of physical access to the data centre** The server room is a sensitive facility which should be accessed by those in charge of IT only for specific reasons. Failure to monitor access to the data centre makes it difficult for management to hold anyone accountable in the event of a security breach involving the systems and the network. Physical access to the data centre is currently not reviewed by management on a periodic basis to ensure that access is granted only to authorised and appropriate individuals. We note that access is currently restricted by a badge reader and an authorised user access list. However, KM&TS management should ensure that users on the list gain access on a need basis (e.g. security	Unauthorised access to the data centre/server room may not be detected on a timely basis and this may potentially result in unauthorised access to the IT infrastructure and/or circumvention of the logical access controls.	• Implement periodic review of access to the data centres. The periodic review should incorporate all users who have access and any exceptions noted resolved promptly.	Accepted This was tightly linked to the GHC move and the availability of the data centres.	MD, PEIS, CKO, Head, KM&TS	Q2 2018	

Appendix 2: Low Rated Detailed Findings & Recommendations

Issue No.	Issue Rating	Issue Description	Risk/Implication	Recommended Actions for Management	Management Comments	ET Member/ Action Owner	Target Completion Date	Status
		personnel should only access the data centre when there is an identified risk and this should be documented).						

Appendix 3: Summary of Performance Ratings and Distribution List

Summary Performance Ratings on Areas Reviewed

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	Address a fundamental control weakness in relation to internal controls, governance and/or risk management that should be resolved as a priority
Medium	Address a control weakness in relation to internal controls, governance and/or risk management that should be resolved within a reasonable period of time
Low	Address a potential improvement opportunity in relation to internal controls, governance and/or risk management

Distribution

Title
Managing Director, Public Engagement and Information Services, Public Engagement & Information Services
Chief Knowledge Officer, Knowledge Management & Technology Solutions
Head, Enabling Technology, Knowledge Management & Technology Solutions

For Information

Title
Chief Executive Officer
Deputy Chief Executive Officer
Managing Director, Audit & Investigations
Executive Team
Director, Legal
Head, Risk