INTERNAL AUDIT

Penetration Test & Security Audit Report

JULY 2018

Gavi
The Vaccine Alliance

Conclusion

Our audit procedures were designed to provide assurance to management and the Gavi Board on the adequacy and effectiveness of the IT controls related to the security of Gavi's network infrastructure.

The network infrastructure consists of Gavi applications hosted internally and in the cloud. Access to these applications via employee workstations or laptops is managed centrally by Active Directory where user accounts and permissions are stored. Gavi offers various types of remote access to end-users through the Internet to its internal network using a Virtual Private Network (VPN).
Following this audit, management is undertaking various remedial actions to enhance the security of Gavi's network infrastructure.

Through our audit procedures, we have identified high risk issues relating to the security of one of the systems exposed to the internet, the management of privileged accounts, the security of workstations and servers, and authentication and access controls as summarised below.

Key Internal Audit Issue Summary

Issue Description	Rating
External penetration test	
There is need to enhance the security of Gavi's systems exposed to the internet	H
There is need to enhance authentication and access controls (including enforcing multi-factor authentication for all accounts)	H
There is need to enforce the use of secure protocols to guard against the risk of interception of communication	M
Internal penetration test	
There is need to enhance the security of workstations	H
There is need to perform security updates and patches on all Windows machines and third party applications	H
There is need to enhance the security of the most privileged accounts (domain admin accounts)	H
There is need to implement full disk encryption to enhance the security of data on laptops and workstations	M

Contents Page

Summary of Findings

Audit Objective

Our audit assessed the adequacy and effectiveness of the IT controls related to the security of Gavi's network infrastructure. The exercise involved undertaking a security audit, also referred to as Penetration Test (PEN Test) with the objective of identifying vulnerabilities which could be exploited by an attacker to compromise parts of, or the entire system.

Audit Scope and Approach

In order to perform this security audit, we acted like real attackers and used several approaches to assess the global security level of Gavi's infrastructure. The penetration test was aimed at identifying weaknesses and vulnerabilities that could be exploited by external or internal attackers to compromise and gain access to the sensitive applications used by Gavi, be they hosted internally or in the Cloud.

Please note that the following areas were excluded from the audit scope:

- Social engineering;
- Denial of Service attacks (DoS); and
- Actively searching for vulnerabilities within the various Cloud services. This is up to the service providers and therefore was considered out of scope.

Background

This audit was carried out in early 2018. As serious weaknesses and security gaps were found that could have been exploited to inflict harm on the organisation, the leadership of both the organisation and the Audit and Finance Committee, at the request of the Managing Director, Audit & Investigations agreed to publish a redacted version of this internal audit report. This decision was taken in line with the Gavi Access to Information Policy. The policy states that Gavi is committed to ensuring that an open and transparent disclosure system is put in place. However, there may in some instances be legal, operational and practical considerations that are necessary to preserve the organisation's interests, as well as those of its staff and its various partners, which may prevent Gavi from achieving full disclosure including Information whose disclosure is likely to endanger the proper conduct of any Gavi operation or activity.

Summary of Key Issues Arising

Through our audit procedures, we have identified high and medium risk issues as summarised below.

External Penetration Test

There is need to enhance the security of Gavi's systems exposed to the internet

The penetration test involved assessing the vulnerability of the Gavi internal network to external attack. The test revealed a critical vulnerability in one of the systems exposed to the Internet which has been subsequently addressed by management.

There is need to enhance authentication and access controls to Gavi systems (including enforcing multi-factor authentication for all accounts)

The external penetration exercise also tested the robustness of authentication and access controls of users to Gavi systems. Some of the selected users' accounts were compromised mainly because of weak passwords and the fact that multifactor authentication had not been enforced for all accounts.

There is need to enforce the use of secure protocols to guard against the risk of interception of communication

The external penetration test revealed vulnerabilities in the information transmission channels with increased risk of man-in-the-middle attacks.

Internal Penetration Test

There is need to enhance the security of workstations

The internal penetration exercise tested the security of workstations and servers and identified vulnerabilities which could be exploited to compromise the entire network.

There is need to perform security updates and patches on all Windows machines and third party applications

The internal penetration test identified workstations and servers with missing patches, updates or with configuration errors.

There is need to enhance the security of the most privileged accounts (domain admin accounts) in the domain

The internal penetration test identified vulnerabilities related to the management of the domain admin accounts. Domain admin accounts have full rights to administer the domain including adding and removing accounts/users, groups, computers (i.e. from workstations), assigning rights to access services in the domain (i.e. through Active Directory), managing audit and security logs, modifying passwords and system shut down. These accounts also have local administrator privileges on every single machine within the domain.

There is need to implement full disk encryption to enhance the security of data on laptops and workstations.

The confidentiality and integrity of the information on laptops and workstations may be compromised due to lack of full disk encryption of the hard drives.

Other Issues identified

Other nonsignificant issues were identified during the penetration test but they have a less direct impact on the targeted applications.

Security of the wireless networks

The wireless networks function as designed and there are no major vulnerabilities that were identified during the penetration testing exercise.

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 the Knowledge Management & Technology Solutions team for their assistance during this audit.

Head Internal Audit

Appendix 1: Summary of Performance Ratings and Distribution List

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
Manager, Information 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