Memorandum

Annexure D

File Ref # 28/7/1/2

TO: **Mr. HILMI DANIELS**
CHAIRPERSON OF THE AUDIT COMMITTEE

FROM: **Mr. COLLINS LETSOALO**
CHIEF EXECUTIVE OFFICER

SUBJECT: **DEPARTMENT OF TRANSPORT: PROGRESS REPORT ON AUDIT FINDINGS RAISED BY AUDITOR GENERAL (AGSA) AS AT 30 JUNE 2023**

TYPE OF MEMORANDUM:

Information Memorandum		**Decision Memorandum**	
(Tick ✓ the applicable block. If you have selected the 'Decision Memorandum' also tick ✓ the applicable option of relevance to your submission)		1. Strategy Endorsement	
		2. Commercial Options	
		3. Recommendation for Approval	✓

1. Purpose

1.1 The purpose of this memorandum is to request the Audit Committee to recommend to the Board to approve the submission of the Progress report on Audit findings raised by AGSA as at 30 June 2023 to the Department of Transport (DOT).

2. Background

2.1 The Department of Transport (DOT) requires all entities reporting to the Minister of Transport to submit a Progress report on Audit Findings raised by the AGSA on a quarterly basis.

2.2 The report of the RAF has been completed using the DOT template and is consistent with the information contained in the Internal Audit Tracker for the period ended 30 June 2023.

3. Discussion

3.1 The progress report on Audit findings raised by AGSA as at 30 June 2023 contains findings raised during the 2019/2020 and 2020/21 financial years audit, which have not been resolved, there are **two (2)** remaining findings for the 2019/2020 financial year which are ICT security related.

3.3 In the 2020/2021 financial year a total number of forty-four (44) findings was raised of which eleven (11) findings will not be tracked as eight (8) of those were in dispute and management could not provide any further remedial actions, and on three (3) management and AGSA could not agree on action plans. This resulted to thirty-three (33) trackable findings of which twenty-seven (27) were resolved, and **six (6)** remained unresolved and will be tracked monthly.

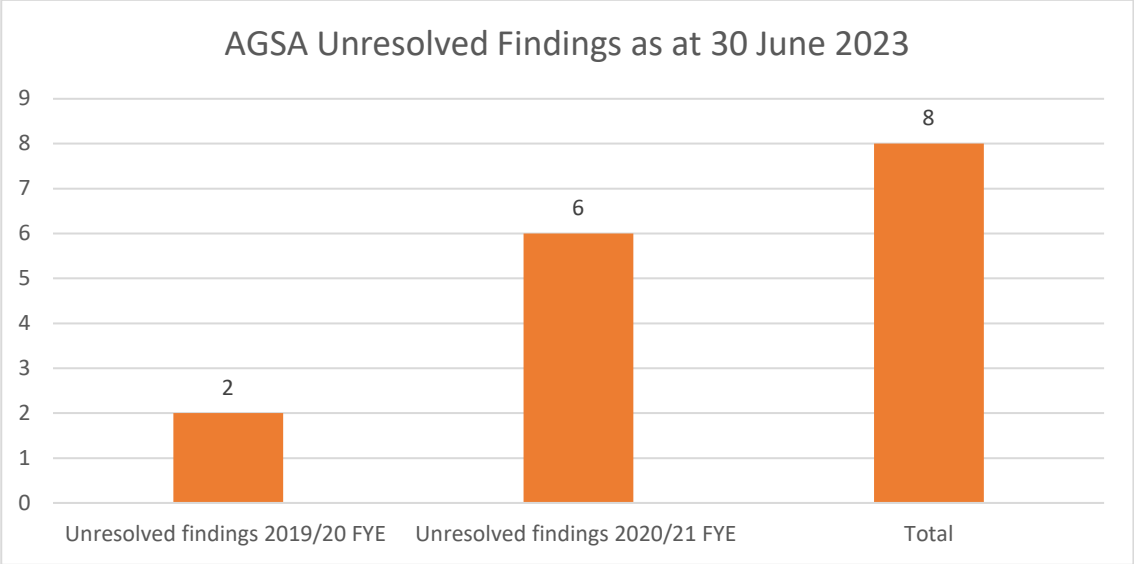
Below is the list of the total outstanding eight (8) findings:

Financial Year 2019/2020	
1.	Review of administrator activities on the firewall not performed
2.	Security Information and Event Management solution has restrictions that affect security events detection and alerting capabilities
Financial Year 2020/2021	
3.	Review of administrator activities on the firewall not performed (Repeat finding)
4.	Security Information and Event Management solution has restrictions that affect security events detection and alerting capabilities (Repeat finding)
5.	There was no process for monitoring and analysing of administrators' activities and events
6.	Anti-virus and anti-malware standards were outdated and not catering for the changes in the infrastructure
7.	Information and communication technology patch management methodology outdated
8.	Lack of critical information and communication technology resources due to positions being vacant

Table below indicates findings dashboard.

	Quarter 1 (30 June 2023)
Unresolved findings	**2** Unresolved findings raised during the 2019/20 FYE
	6 Unresolved findings raised during the 2020/21 FYE
Total Unresolved findings	**8**
Resolved findings	**0** Resolved findings raised during the 2019/20 FYE
	0 Resolved findings raised during the 2020/21 FYE

Total resolved findings	**0**



4. Consultation

4.1 Internal Audit conducts monthly follow-up process on the unresolved findings with the relevant stakeholders.

5. Legal Implications

5.1 None.

6. Communication Implications

6.1 None.

7. Financial Implications

7.1 None.

8. Recommendations

8.1 It is recommended that the Audit Committee recommends to the Board to approve the submission of the Progress report on Audit findings raised by the AGSA as at 30 June 2023 to the Department of Transport.

I hereby confirm that relevant and applicable RAF Policies, procurement processes, PFMA and its Regulations, including any other regulatory requirements, shall be complied with.

Recommendations

It is recommended that the Audit Committee recommends to the Board to approve the submission of the Progress report on Audit findings raised by the AGSA as at 30 June 2023 to the Department of Transport.

Signatures:

Prepared by:

Radikwena D Phora
Radikwena D Phora (Jul 12, 2023 08:45 GMT+2)

Mr. Radikwena Phora
Chief Internal Audit Officer
Date: Jul 12, 2023

Supported by:

Collins Letsoalo (Jul 26, 2023 00:34 GMT+2)

Mr. Collins Letsoalo
Chief Executive Officer
Date:
Comments:

None

Recommended for approval by:

Mr. Hilmi Daniels
Chairperson of the Audit Committee
Date:
Comments:

DOT AGSA TRACKING FINDINGS REPORT AS AT 30 JUNE 2023

No	Finding Description	Management Comments/ Action Plan	Internal Audit Comments
Financial Year 2019/2020			
Information Communication Technology			
1.	Review of administrator activities on the firewall not performed	**June 2023** RAF ICT is no longer using Splunk as a SIEM Solution, LogRythym is the current SIEM. Firewall logs were configured in to the SIEM as from August 2022 and ICT is currently collecting the log as from August 2022. **Responsible Person** Name: Monene Sono Position: Acting Senior Manager – Infrastructure Development and Business Continuity **Target Date:** 31 March 2021 ICT Management to review administrator activities logs as soon as they are available on Splunk. **Responsible Person** Name: Monene Sono Position: Acting Senior Manager – Infrastructure Development and Business Continuity Implementation date: 31 March 2021	**Unresolved** **June 2023** Cognisance was taken of the fact that now there is a SIEM solution in place such as LogRhythm where firewall logs are ingested, and this was confirmed during the Network Security Management Review that was concluded recently in FY2022/2023 (Q4). We then sent a request to ICT Security Team requesting evidence of the review of administrators logs. Through discussion on MS Teams with Tshepo Simbine (Specialist: Information Security) on 04 July 2023, we noted that evidence confirming that firewall administrator activities are being reviewed could not be provided to

		Auditor's conclusion Management comments are noted. However, an assessment of the corrective actions agreed upon	Internal Audit. Therefore, the finding will remain unresolved. **March 2023** This was validated as part of the SIEM solution review during the Networks Review completed in Q4 of 2022/23 and it was noted firewall logs are part of the logs that are being ingested on the SIEM. However, there was no evidence to confirm that the logs are being reviewed. Therefore, the finding remains unresolved.
2.	Security Information and Event Management solution has restrictions that affect security events detection and alerting capabilities	**June 2023** **Updated Action Plan as per Networks Security Review report 19 June 2023** **1. Review current SIEM/SOC service provider performance.** Conduct a comprehensive review of the current SIEM/SOC service provider's performance. This includes assessing their ability to detect and respond to security incidents in a timely and effective manner. This review will begin on **1st June 2023 and will be completed by 31st July 2023**. **2. Improve communication and response protocols.** Work with the SIEM/SOC service provider to improve communication and response protocols. This includes establishing clear guidelines for when and how the service provider should communicate incidents to RAF, as well as how quickly they are expected to respond to incidents. This process will start on **1st July 2023 and is expected to be completed by 31st August 2023**. **3. Implement continuous monitoring and reporting.** Implement a continuous monitoring and reporting system for the SIEM/SOC solution. This will involve regular reviews of the solution's performance, as well as regular reporting to RAF management on the solution's effectiveness.	**Unresolved** **June 2023** Cognisance is taken that the action plans were updated as part of Networks review that was issued in June 2023. Therefore, Internal Audit will follow up after the target date. **March 2023** This was validated as part of the SIEM solution review during the Networks Review completed in Q4 of 2022/23. Internal Audit noted the following during the review: • Key infrastructure components such as servers

		The implementation of this system will begin on **1st September 2023 and is expected to be completed by 30th September 2023**. **4. Enhance SIEM/SOC capabilities.** If the current service provider cannot meet the revised standards and expectations, consider enhancing the SIEM/SOC capabilities by either upgrading the current solution or transitioning to a new service provider. The procurement process for this would begin on **1st September 2023, with the implementation to be completed by 31st March 2024**. **5. Training and awareness.** Improve training and awareness for RAF ICT Security team members on the new protocols and standards, as well as how to respond to alerts and incidents. This training will begin **1st February 2024 and is expected to be completed by 31st March 2024**. **Responsible Person** Monene Sono: Monene Sono: Acting Senior Manager: Information Security, IT Risk and Governance **Revised Target Date** 1. 31 July 2023 2. 31 August 2023 3. 30 September 2023 4. 31 March 2024 5. 31 March 2024 **Original Agreed Action Plan as per 2020/21 Auditor General report** ICT management will continue with the on-premise solution, however, will not be investing in the solution. ICT Management will include the SIEM capability within the long-term Cyber Security Operations Centre (CSOC) engagement.	(Windows operating system, SQL server, UNIX etc), firewalls etc were configured to ship logs to the SIEM solutions. • Monitoring of activities and reporting of security activities logged on the SIEM was being done by the service provider and tickets logged with RAF to investigate where anomalies were noted. • Some key alerts such as detection and blocking of file uploads containing viruses. • Logging of key activities such as dropping and altering of tables on databases such as SQL server. • Alerts that notify ICT Security staff when sensitive activities such as adding users to privileged groups such as Domain admin, etc. However, Internal Audit was not satisfied with the operating effectiveness of the control due to the above control weaknesses noted.

		Internal control deficiency **Financial and performance management – IT systems** The entity has deployed an enterprise version of Splunk; however, the deployed solution has limitations that restricts feature-sets due to indexing size, which limits input sources. The current deployment has been a test case to trial the SIEM solution to see the value that Splunk could provide to the entity. **Responsible Official** Name: Monene Sono Position: Acting Senior Manager – Infrastructure Development and Business Continuity Implementation date: 31 January 2022 (Dependency on successful SCM process to acquire CSOC) **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed during the next audit.	

No	Finding Description	Management Comments/ Action Plan	Internal Audit Comments
Financial year 2020/2021			
Information Communication Technology			
3.	Review of administrator activities on the firewall not performed	**June 2023** RAF ICT is no longer using Splunk as a SIEM Solution, LogRythym is the current SIEM. Firewall logs were configured in to the SIEM as from August 2022 and ICT is currently collecting the log as from August 2022. **Management response** ICT Management notes the finding. It is confirmed that the current RAF Cisco Firewall generates huge volumes of logs daily, but it is not designed to maintain historical log data which is why a syslog server is required for this purpose. Splunk was therefore identified to perform the syslog server functions by collecting critical audit logs from the Firewall and maintain historical data for future use or reviews as stated in the Information Security Framework Policy. The logs generated include changes done by the administrators which follow a Change Control process. It must further be noted that standard or normal changes were documented and pre-approved to be excluded from the Change Control Process but are logged through Service Desk and reported back to Change Advisory Board meetings for noting. The service provider was already consulted to confirm the level of detail that the firewall in place can generate the logs and they've agreed to send confirmation in writing. **Action plan** The logs generated on the firewall will be reviewed to ensure they are aligned to the approved standard and critical logs change management document. The review will include ensuring that Splunk is collecting identified logs from the firewall and there is	**Unresolved** **June 2023** Cognisance was taken of the fact that now there is a SIEM solution in place such as LogRhythm where firewall logs are ingested, and this was confirmed during the Network Security Management Review that was concluded recently in FY2022/2023 (Q4). We then sent a request to ICT Security Team requesting evidence of the review of administrators logs. Through discussion on MS Teams with Tshepo Simbine (Specialist: Information Security) on 04 July 2023, we noted that evidence confirming that firewall administrator activities are reviewed could not be provided to Internal Audit. Therefore, the finding will remain unresolved. **March 2023** This was validated as part of the SIEM solution review during the Networks Review completed in Q4 of 2022/23 and it was noted firewall logs are part of the logs that are being ingested on the SIEM.

		compliance to the approved Firewall Baseline Standard document which talks to the firewall logs backup and retention periods. **Responsible Person** Lucky Mashilo/ Monene Sono Position: Senior Manager – Infrastructure Development and Business Continuity/ Manager – Networks and Telecommunications **Target Date** 31 March 2021 ICT Management to review administrator activities logs as soon as they are available on Splunk. Arinao Mulaudzi Position: Acting Senior Manager – Information Security, IT Risk and Governance **Target Date** 31 August 2021 **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed during the next audit.	However, there was no evidence to confirm that the logs are being reviewed. Therefore, the finding remains unresolved. **February 2023** This is being validated as part of the SIEM solution review which is being completed during the Networks Review that is underway in Q4. **December 2022** Internal Audit take note of the ICT comments indicating that ICT is no longer using Splunk as a SIEM Solution and a new solution (LogRythym) is currently used to collect the firewall logs since August 2022. Therefore, Internal Audit will follow-up after evidence of review of administrators' activities on the firewall is provided.
4.	Security Information and Event Management solution has restrictions that affect security events detection and alerting capabilities	**June 2023** **Updated Action Plan as per Networks Security Review report 19 June 2023** **1. Review current SIEM/SOC service provider performance.** Conduct a comprehensive review of the current SIEM/SOC service provider's performance. This includes assessing their ability to detect and respond to security incidents in a timely and effective manner. This review will begin on **1st June 2023 and will be completed by 31st July 2023**. **2. Improve communication and response protocols.** Work with the SIEM/SOC service provider to improve communication and response protocols. This includes establishing clear guidelines for when and how the service	**Unresolved** **June 2023** Cognisance is taken that the action plans were updated as part of Networks review that was issued in June 2023. Therefore, Internal Audit will follow up after the new target date. **March 2023** This was validated as part of the SIEM solution review during the Networks Review

		provider should communicate incidents to RAF, as well as how quickly they are expected to respond to incidents. This process will start on **1st July 2023 and is expected to be completed by 31st August 2023**. **3. Implement continuous monitoring and reporting.** Implement a continuous monitoring and reporting system for the SIEM/SOC solution. This will involve regular reviews of the solution's performance, as well as regular reporting to RAF management on the solution's effectiveness. The implementation of this system will begin on **1st September 2023 and is expected to be completed by 30th September 2023**. **4. Enhance SIEM/SOC capabilities.** If the current service provider cannot meet the revised standards and expectations, consider enhancing the SIEM/SOC capabilities by either upgrading the current solution or transitioning to a new service provider. The procurement process for this would begin on **1st September 2023, with the implementation to be completed by 31st March 2024**. **5. Training and awareness.** Improve training and awareness for RAF ICT Security team members on the new protocols and standards, as well as how to respond to alerts and incidents. This training will begin **1st February 2024 and is expected to be completed by 31st March 2024**. **Responsible Person** Monene Sono: Monene Sono: Acting Senior Manager: Information Security, IT Risk and Governance **Revised Target Date** 1. 31 July 2023 2. 31 August 2023 3. 30 September 2023 4. 31 March 2024 5. 31 March 2024	completed in Q4 of 2022/23. Internal Audit noted the following during the review: • Key infrastructure components such as servers (Windows operating system, SQL server, UNIX etc), firewalls etc were configured to ship logs to the SIEM solutions. • Monitoring of activities and reporting of security activities logged on the SIEM was being done by the service provider and tickets logged with RAF to investigate where anomalies were noted. • Some key alerts such as detection and blocking of file uploads containing viruses. • Logging of key activities such as dropping and altering of tables on databases such as SQL server. • Alerts that notify ICT Security staff when sensitive activities such as adding users to privileged groups such as Domain admin, etc. However, Internal Audit was not satisfied with the operating effectiveness of the control due to the above control weaknesses noted.

		Original Agreed Action Plan as per Auditor General of 2020/21 **Action Plan** ICT management will continue with the on-premise solution, however, will not be investing in the solution. ICT Management will include the SIEM capability within the long-term Cyber Security Operations Centre (CSOC) engagement. **Responsible Person** Arinao Mulaudzi Acting Senior Manager – Information Security, IT Risk and Governance **Target Date** 31 January 2022 (Dependency on successful SCM process to acquire CSOC) **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed during the next audit.	
5.	There was no process for monitoring and analysing of administrators' activities and events	**June 2023** **Management response** Information Communication Technology (ICT) note the finding, ICT will develop a process that will outline which logs should be ingested onto SPLUNK, and also determine logs that will be reviewed on a regular basis. ICT has identified and acknowledged the risk, and in a process of finalising the user account standard. **Action plan** ICT to define a process of what would be ingested onto SPLUNK, and which logs would be reviewed. ICT have identified and acknowledged the risk, and in a process of finalizing the User Account Standard. Once approved ICT will start creating admin accounts for administrative purpose separate to normal accounts by 30 November 2021. **Responsible Person**	**Unresolved** **June 2023** ICT has not provided evidence for the review of logs of Windows administrator activities being ingested on logged on the SIEM. Internal Audit will follow-up after evidence is provided. **March 2023** A meeting was held with ICT on 27 March 2023. During the meeting, it was indicated that the administrator activities performed on Windows environment are ingested on the SOC and are being reviewed on a regularly basis. However, evidence of the

		Andile Stulo Position: ICT Security Specialist **Target Date** 31 January 2022 **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed during the next audit.	logged activities and review thereof was not provided. Moreover, ICT could not confirm whether the activities that are performed by UNIX administrators were logged and ingested on the SOC, thus monitoring and analysis of activities performed by administrators on the UNIX environment was not provided. **Prior to March 2023** Reviewed the evidence and we noted that 103 hosts were enabled to ingest logs into QRADAR SIEM solution. Finding remains unresolved. Internal Audit will verify once the following evidence is obtained • A process showing which logs will be reviewed, responsible officials, and frequency of reviews. • Evidence showing that separate admin accounts for administrative purposes are created.
6.	Anti-virus and anti-malware standards were outdated and not catering for the changes in the infrastructure	**June 2023** The antivirus and anti-malware configuration standard documents are in review and circulation for sign-off and implementation. The review and signed off will be completed by 31 July 2023. **Management response** ICT note the finding and will update the antivirus standards. **Action Plan** ICT will update the antivirus standard.	**Unresolved** **June 2023** Internal Audit will follow-up after the revised target date of 31 July 2023. **March 2023** Internal Audit engaged with ICT Security regarding the status of this finding during the Networks Review in Q4 of 2022/23. ICT indicated that a resolution was passed to enforce 100% antivirus deployment compliance policy and non-compliant endpoints will be removed from the network

		Responsible Person Andile Stulo Position: ICT Security Specialist **Target Date:** 30 September 2021 Nokuthula Brown Position: ICT Security Administrator **Target Date** 30 September 2021 **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed during the next audit.	until such a time they are compliant. ICT indicated that they are still cleaning up the non-compliant endpoints and will share evidence for IA validation once this exercise is completed. IA also requested ICT Security to provide an indication of how antivirus is being managed on UNIX and Linux platforms and IA is awaiting feedback in this regard. Internal Audit will follow-up after evidence is provided.
7.	Information and communication technology patch management methodology outdated	**June 2023** Based on comments received, the security specialist had to re-define the document and has been redistributed for signature. Action Item 1: Please note that ICT will require an extension on this item, as have underestimated the amount of work required to complete this item as it touches all the departments within ICT. This process was impacted by the unavailability of resources Item 2& 3: The review has been completed, evidence was sent to IA. **Management response** ICT note the findings, however management is negotiating the move of problem management to operations, once the outcome is concluded the finding will be transferred to the appropriate control owners. ICT note the finding for problem management and will review accordingly. Patch management methodology and the process that informs the patching cycle and recurring operations will be revisited and updated to cover applications to be part of the patching cycle.	**Unresolved** **June 2023** The revised Patch Management Methodology was provided to Internal Audit for inputs. Inputs were provided to ICT on 13 March 2023. IA will validate after the approved Patch Management Methodology is submitted by ICT. Evidence of the revised and approved Change Management and Problem Management standards was provided to Internal Audit and validated.

		Action Plans ICT Security will coordinate the review plan with all relevant system/application custodians. The plan will define/update the new patch management cycle which must include all applications running on the RAF network. **Responsible Person** Andile Stulo Position: ICT Security Specialist **Target Date** 30 November 2021 **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed on the next audit.	
8.	Lack of critical information and communication technology resources due to positions being vacant	**June 2023** The process is ongoing, critical posts have been advertised. **Management response** ICT notes the finding; however, it must be noted that RAF has currently imposed a moratorium because of the re-structuring that is currently taking place. ICT have compiled Memos to deviate from the moratorium on recruitment process. Some of the submissions were approved to allow vacant positions to be filled. ICT will request approval to fill the remaining vacant positions to ensure that ICT is well capacitated to perform its functions. **Action Plans** ICT management will seek approval to advertise vacant positions. **Responsible Person** Arinao Mulaudzi/ Ntuli Letoaba/ Lucky Mashilo/ Keitihetse Teisho/ Miemie Thanjekwayo Position: Acting Chief Information Officer/ Senior Manager – Application Development and Business Intelligence/ Acting	**Unresolved** Internal Audit will follow-up after evidence is provided.

		General Manager – ICT Operations/ Senior Manager – ICT Operations and Business Support/ Senior Manager – ICT BA, EA, and PM, ICT- Architecture & Programme Management **Target Date** 30 June 2022 **Auditor's conclusion** Management comments are noted. However, an assessment of the corrective actions agreed upon by management will be performed on the next audit.	