Notes:

- *This report has been translated into Chinese. If there is any inconsistency between the English version and the Chinese version, the English version shall prevail.*
- *Consider the importance of information security, those not appropriate to be disclosed including the internal details of the system, are redacted.*

Security Risk Assessment & Audit Services for Multi-functional Smart Lampposts and Associated Devices of the Office of the Government Chief Information Officer

VERIFICATION REPORT

Version 1.1

17 JULY 2023

Version History

Version	Date	Description	Author
1.0	18/03/2023	Completed version	[redacted]
1.1	17/07/2023	Minor updates and editing	

Distribution

Copy No.	Holder
1	Office of the Government Chief Information Officer ("OGCIO")
2	[redacted]

Table of Contents

1. Executive Summary

1.1 Risk Items for Rectification

There was total 23 identified related security low risk items and 1 Area Of Improvement (AOI) in the security risk assessment of the IT Support System of the Multi-functional Smart Lampposts Pilot Scheme of the OGCIO. They were reported under Section 12 of the Security Risk Assessment and Audit Report. Their verification status in the verification stage was:

Table 1. Verification status

	Total	High Risk	Medium Risk	Low Risk	AOI
Number of completed rectification	**6**	0	0	6	0
Number of in-progress rectification	**18**	0	0	17	1
Number of acknowledged rectifications	**0**	0	0	0	0
Total number of rectifications	**24**	**0**	**0**	**23**	**1**

There were no findings in the security audit. They were reported under Section 12 of the Security Audit Report. Their verification status in the verification stage was:

Table 2. Verification status

	Total	High Risk	Medium Risk	Low Risk	AOI
Number of completed rectification	0	0	0	0	0
Number of in-progress rectification	0	0	0	0	0
Number of acknowledged rectifications	0	0	0	0	0
Total number of rectifications	0	0	0	0	0

1.2 Verification Status

In the Security Risk Assessment and Security Audit Report, the contractor provided corresponding recommendation for each risk finding, which OGCIO would evaluate the recommendations and consider applying relevant safeguards or other remedial actions. In the verification process, the contractor reviewed the security status of the IT Support System after such safeguard implementation and discussed with OGCIO the individual verification status, which is described as follows:

- **Completed:** the status review found that the recommended safeguard was properly implemented, or compensating controls were taken such that the risk was properly rectified;
- **In-Progress:** OGCIO was still implementing recommendations to rectify the risk. Possible reasons were procurement, extended construction work or testing work, as well as involvement of other government departments.
- **Acknowledged:** OGCIO had considered different options of recommended safeguard and concluded that accepting the security risk was the best choice. Typical reasons for this status were relating to rectification cost/resource justification, or integration to environment(s) that could not be controlled by OGCIO, or risk accepted.

All findings have been verified.

2. Background

An independent qualified consultancy firm (the contractor), [redacted] is invited to conduct the Security Risk Assessment and Audit (SRAA) exercise to assess the IT Support System of the Multi-functional Smart Lampposts Pilot Scheme of the OGCIO:

(a) To evaluate the security risks of the IT Support System of the Multi-functional Smart Lampposts Pilot Scheme, the Contractor has identified and recommended safeguards with the aim of strengthening the security protection of the system and the related data to an acceptable level.

(b) A security audit has been carried out to determine the state of the existing protection and to verify whether the existing protection has been implemented effectively.

(c) A verification process has been carried out to review the security status of the system(s) and data to ensure that all risks identified in the security risk assessment and security audit have been mitigated or reduced to an acceptable level.

The scope of the services covers the security areas and controls specified in Baseline IT Security Policy (S17), in particular the 14 areas listed in section 2.1 of S17.

The purpose of this document is to formally present the rectification status after the verification check of the security assessment and audit to OGCIO.

2.1 Verification ProcessObjective

The objective of this verification process is to review the security status of the IT Support System of the Multi-functional Smart Lampposts Pilot Scheme of the OGCIO to ensure that all vulnerabilities discovered in the security risk assessment and security audit have been handled and current security measures comply with Security Regulations, policies, and requirements, including the relevant government and departmental IT security policies and regulations.

3. Verification Activities

The following activities were performed during verification stage:

3.1 Planning

The Detailed Project Plan was prepared to outline the planning for the systems verification.

3.2 Information Gathering

The major tasks of information gathering included site visits, vulnerability scan, System configuration reviews and discussions.

3.3 Control Review

The contractor discussed the follow-up actions with OGCIO on the suggested security controls per the recommendations in the Security Risk Assessment and Audit Report.

3.4 Verification Tests

The Project Team reviewed the modified technical security controls, according to the recommendations in the Security Risk Assessment and Audit Report.

3.5 Reporting

Each identified risk item in the Security Risk Assessment and Audit Report was provided with corresponding recommendations. In the verification stage, the contractor reviewed the security status of the IT Support System after the implementation of relevant safeguards by OGCIO. After the verification, each risk item was marked with a verification status, which is described as follows:

- **Completed**: the status review found that the recommended safeguard was properly implemented, or compensating controls were taken such that the risk was properly rectified.
- **In-Progress**: OGCIO was still implementing recommendations to rectify the risk. Possible reasons were procurement, extended construction work or testing work, as well as involvement of other government departments.
- **Acknowledged:** OGCIO considered different options of recommended safeguard and concluded that accepting the security risk was the best choice. Typical reasons for this status were relating to rectification cost/resource justification, or integration to environment(s) that could not be controlled by the OGCIO, or risk accepted.

The contractor then prepared this verification report to document the findings and analysis results during the verification activities.

4. Security Risk Assessment Verification Results

4.1 Vulnerability Assessment & Penetration Test Findings

There was total 23 identified related security low risk items and 1 AOI in vulnerability assessment. They were reported under Section 12 of the Security Risk Assessment Report. Their verification status in the verification stage was:

Table 3. Verification status

	Total	High Risk	Medium Risk	Low Risk	AOI
Number of completed rectification	**6**	0	0	6	0
Number of in-progress rectification	**18**	0	0	17	1
Number of acknowledged rectifications	**0**	0	0	0	0
Total number of rectifications	**24**	**0**	**0**	**23**	**1**

ID	Host/IP	Name	Risk Rating [Impact x Likelihood]	Action taken	Verified status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

ID	Host/IP	Name	Risk Rating [Impact x Likelihood]	Action taken	Verified status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

ID	Host/IP	Name	Risk Rating [Impact x Likelihood]	Action taken	Verified status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

5. Security Audit Verification Results

There was no finding in the security audit. They were reported under Section 12 of the Audit Report. Their verification status in the verification stage was:

Table 4. Verification status

	Total	High Risk	Medium Risk	Low Risk	AOI
Number of completed rectification	0	0	0	0	0
Number of in-progress rectification	0	0	0	0	0
Number of acknowledged rectifications	0	0	0	0	0
Total number of rectifications	0	0	0	0	0

6. Conclusion and Follow-Up Actions

OGCIO had rectified some of the risk findings and implemented the recommendations in the Security Risk Assessment and Audit Report and took necessary actions to apply relevant safeguards before Q3 of 2023.

From this point onward, OGCIO should constantly monitor its IT Support System of the Multi-functional Smart Lampposts Pilot Scheme or future potential security vulnerabilities and take appropriate actions to rectify the risks, such as applying vendor security patches when new loopholes emerge and updating relevant control documents when there is practice change. The management and administration processes should also be regularly reviewed for any deficiency or ineffectiveness so that they could be improved during environmental change.

Finally, [redacted] recommended that OGCIO should conduct a security risk assessment and audit on a regular basis (at least once every two years) to ensure that the IT Support System complies with the latest IT security policy and standards, and security protection and safeguards are appropriately implemented.