.備註：

- *本報告中文版為英文版本的譯本。如中、英版本有任何差異，應以英文版本為準。*
- *基於資訊保安，報告中一些不適宜公開的內容會被遮蓋，包括有關系統的內部細節。*

政府資訊科技總監辦公室
多功能智慧燈柱及相關裝置的
保安風險評估及審計服務

驗證報告

版本1.1

2023年7月17日

版本歷史

版本	日期	說明	作者
1.0	2023年3月18日	最終版本	[redacted]
1.1	2023年7月17日	小幅更新與編輯	

分發

副本編號	持有者
1	政府資訊科技總監辦公室（「資科辦」）
2	[redacted]

目錄

1. 報告摘要

1.1 需要修正的風險項目

資科辦多功能智慧燈柱試驗計劃的資訊科技支援系統在保安風險評估中，共識別23項相關的低保安風險項目及1項有待改善的地方。保安風險評估及審計報告第12節已就此作出報告。有關項目在驗證階段的驗證狀況為：

表1. 驗證狀況

	總計	高風險	中風險	低風險	有待改善的地方
已完成修正的項目數量	**6**	0	0	6	0
修正進行中的項目數量	**18**	0	0	17	1
已確認修正的項目數量	**0**	0	0	0	0
修正項目總數	**24**	**0**	**0**	**23**	**1**

保安審計並無任何發現。保安審計報告第12節已就此作出報告。有關項目在驗證階段的驗證狀況為：

表2. 驗證狀況

	總計	高風險	中風險	低風險	有待改善的地方
已完成修正的項目數量	0	0	0	0	0
修正進行中的項目數量	0	0	0	0	0
已確認修正的項目數量	0	0	0	0	0
修正項目總數	0	0	0	0	0

1.2 驗證狀況

在保安風險評估及保安審計報告中，承辦商就發現的每項風險提供相應建議，資科辦會評估有關建議，並考慮採取相關的保障措施或其他補救行動。在驗證程序中，承辦商對實施上述保障措施後資訊科技支援系統的保安狀況進行覆檢，並與資科辦討論個別項目的驗證狀況，詳情如下：

- 已完成：狀況覆檢發現建議的保安保障措施已妥為實施或已採取輔助控制措施，有關風險因而已妥為修正。
- 進行中：資料辦仍在實施修正風險的建議，原因可能是由於採購、延長建築工程或測試工作，以及涉及其他政府部門。
- 已確認：資科辦已考慮建議的不同保安保障措施選項，斷定接受保安風險是最佳選擇。出現此狀況的原因一般與修正成本／資源的理據，或須與非資科辦可控制的環境整合，或風險已獲接受有關。

所有結果均已獲驗證。

2. 背景

獨立合資格顧問公司（承辦商）[redacted]獲邀進行保安風險評估及審計工作，以評估資科辦多功能智慧燈柱試驗計劃的資訊科技支援系統：

(a) 為評估多功能智慧燈柱試驗計劃的資訊科技支援系統的保安風險，承辦商已識別並建議保安保障措施，旨在加強該系統和相關數據的安全保護至可接受的水平。
(b) 已進行保安審計，以確定現有保護的狀況，並驗證現有保護是否得以有效實施。
(c) 已進行驗證程序，覆檢該系統和數據的保安狀況，以確保在保安風險評估和保安審計中識別的所有風險已予緩解或減低至可接受水平。

服務範圍涵蓋《基準資訊科技保安政策》(S17) 所訂明的保安範疇和控制措施，尤其是S17第2.1節列載的14個範疇。

本文件的目的是向資科辦正式交代經驗證檢查保安評估及審計後的修正狀況。

2.1 驗證程序目的

是次驗證程序的目的是覆檢資科辦多功能智慧燈柱試驗計劃的資訊科技支援系統的保安狀況，以確保在保安風險評估及保安審計中發現的所有安全漏洞均已獲處理，現時的保安措施符合保安規例、政策及規定，包括政府及部門的相關資訊科技保安政策及規例。

3. 驗證活動

在驗證階段進行了下列活動：

3.1 規劃

擬備詳細項目計劃，勾劃系統驗證的規劃。

3.2 資料收集

資料收集的主要工作包括實地視察、保安漏洞掃描、系統配置覆檢和討論。

3.3 管控覆檢

承辦商根據保安風險評估及審計報告的建議就建議的保安控制措施與資科辦討論跟進工作。

3.4 驗證測試

項目團隊根據保安風險評估及審計報告的建議覆檢已修改的技術保安控制措施。

3.5 報告

在保安風險評估及審計報告中識別的每項風險項目均有相應的建議。在驗證階段，承辦商對資科辦實施相關保障措施後資訊科技支援系統的保安狀況進行覆檢。經驗證後，每項風險項目均會標示驗證狀況，詳情如下：

- 已完成：狀況覆檢發現建議的保安保障措施已妥為實施或已採取輔助控制措施，有關風險因而已妥為修正。
- 進行中：資科辦仍在實施修正風險的建議，原因可能是由於採購、延長建築工程或測試工作，以及涉及其他政府部門。
- 已確認：資科辦已考慮建議的不同保安措施選項，判定接受保安風險是最佳選擇。出現此狀況的原因一般與修正成本／資源的理據，或須與非資科辦可控制的環境整合，或風險已獲接受有關。

承辦商繼而編製本驗證報告，以記錄在驗證活動中的發現和分析結果。

4. 保安風險評估驗證結果

4.1 保安漏洞評估及滲透測試結果

在保安漏洞評估中，共識別23項相關的低保安風險項目和1項有待改善的地方。保安風險評估報告第12節已就此作出報告。有關項目在驗證階段的驗證狀況為：

表3. 驗證狀況

	總計	高風險	中風險	低風險	有待改善的地方
已完成修正的項目數量	**6**	0	0	6	0
修正進行中的項目數量	**18**	0	0	17	1
已確認修正的項目數量	**0**	0	0	0	0
修正項目總數	**24**	**0**	**0**	**23**	**1**

ID	主機/IP	名稱	風險評級 [影響 x 可能性]	已採取的行動	驗證狀況
[redacted]					

ID	主機/IP	名稱	風險評級 [影響 x 可能性]	已採取的行動	驗證狀況
[redacted]					

ID	主機/IP	名稱	風險評級 [影響 x 可能性]	已採取的行動	驗證狀況
[redacted]					

5. 保安審計驗證結果

保安審計並無任何發現。保安審計報告第12節已就此作出報告。有關項目在驗證階段的驗證狀況為：

表4. 驗證狀況

	總計	高風險	中風險	低風險	有待改善的地方
已完成修正的項目數量	0	0	0	0	0
修正進行中的項目數量	0	0	0	0	0
已確認修正的項目數量	0	0	0	0	0
修正項目總數	0	0	0	0	0

6. 結論及跟進措施

資科辦已於2023年第三季前修正部分發現的風險，實施保安風險評估及審計報告中的建議，並採取必要行動實施相關保障措施。

資科辦今後應持續監察其多功能智慧燈柱試驗計劃的資訊科技支援系統或日後可能出現的保安漏洞，並採取適當措施修正風險，例如在出現新漏洞時應用供應商的保安修補程式，在作業模式改變時更新相關的控制文件等。此外，亦應定期覆檢管理和行政程序中的任何不足或無效之處，以便在環境轉變時可予改善。

最後，[redacted]建議資科辦定期（至少每兩年一次）進行保安風險評估及審計，以確保資訊科技支援系統符合最新的資訊科技保安政策及標準，安全保護及保障措施得以妥善實施。