備註：

- *此報告中文版為英文版本譯本，如中、英文兩個版本有任何不一致之處，應以英文版本為準。*
- *考慮到資訊安全的重要，報告中一些不適宜公開的內容包括有關系統的內部細節會被遮蓋。*

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驗證報告

版本 1.0
2020 年 11 月 12 日

保安風險評估及審計服務

文件資料

計劃名稱：	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		
文件版本日期：	2020年11月12日	**文件版本編號：**	1.0
質量評核方法：	獨立質量評核		

分發名單

至	**行動***	**日期**	**電話／傳真**
政府資訊科技總監辦公室	審查	2020年11月12日	

**行動類型：核准、審查、通知、歸檔、需要行動、出席會議、其他（請列明）*

版本歷史

版本編號	**版本日期**	**說明**	**檔案名稱**
1.0	2020年11月12日	最終版本	OGCIO SRAA Verification Report v1.0.docx

目錄

簡稱

經常在本文件使用的簡稱如下：

「香港特區政府」或「政府」	香港特別行政區政府
資科辦	政府資訊科技總監辦公室
該系統	多功能智慧燈柱及相關裝置
項目團隊	獨立的第三方評估員／審計師
S17	《基準資訊科技保安政策》

1. 項目背景

為香港特別行政區政府（「香港特區政府」或「政府」）轄下政府資訊科技總監辦公室（「資科辦」）所提供的服務如下：

(a) 評估多功能智慧燈柱及相關裝置（「該系統」）的保安風險，識別和建議保安保障措施，旨在加強該系統和相關數據的保安保護至可接受的水平。

(b) 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。

服務範圍須涵蓋《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。

本文件的目的是正式交代該系統保安風險評估及審計工作所提出建議的實施狀況。

1.1 保安審計狀況釋義

在保安風險評估階段，就每項風險評估結果均會提出相應的建議。在保安審計階段，項目團隊檢查有關建議的實施狀況，並與資科辦討論目前的進度。個別修正狀況可以是：

- **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**：資科辦已考慮所有保安保障措施建議的選項，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。

1.2 保安審計目標和範圍

是項工作的保安審計目標是就實施保安保障措施後的保安狀況進行驗證檢查，以確保在上一次保安風險評估所識別的所有保安漏洞已根據保安風險評估報告提出的建議修正和解決，並建議其他保安保障措施以作改善（如適用）。

2. 驗證方法

2.1 規劃

擬備詳細項目計劃，勾劃保安審計工作的規劃。

2.2 資料收集

資料收集的主要工作包括文件覆檢、實地視察、保安漏洞掃描、系統配置覆檢和討論。

2.3 控制覆檢

項目團隊根據保安風險評估的建議就建議的保安控制措施與資科辦討論跟進工作。

2.4 測試

項目團隊根據保安風險評估的建議覆檢已修改的技術保安控制措施。

2.5 報告

在保安風險評估及審計報告中就每項評估結果均會提出相應的建議。在保安審計階段，項目團隊覆檢有關建議的修正狀況，並與資科辦討論目前的進度。個別修正狀況可以是：

- **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**：資科辦已考慮所有保安保障措施建議的選項，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。

項目團隊繼而編製本保安審計報告，以記錄在保安審計過程中的發現和分析結果。

2.6 清理和跟進

在保安審計報告獲接納後，敏感資料會交還資科辦或銷毀。

3. 驗證摘要

在保安風險評估及審計中，根據保安風險評估及審計報告所述該系統發現有 4 項中度風險、11 項低風險和 5 個有待改善的地方。

表 1. 主機和網絡掃描的修正狀況

	總數	高風險	中度風險	低風險	有待改善的地方
已完成修正的數量	**4**	0	4	0	0
修正在進行中的數量	**10**	0	0	8	2
已確認修正的數量	**0**	0	0	0	0
修正總數	**14**	**0**	**4**	**8**	**2**

表 2. 一般控制覆檢的修正狀況

	總數	高風險	中度風險	低風險	有待改善的地方
已完成修正的數量	**2**	0	0	1	1
修正在進行中的數量	**4**	0	0	2	2
已確認修正的數量	**0**	0	0	0	0
修正總數	**6**	**0**	**0**	**3**	**3**

3.1 主機和網絡掃描結果：

報告標題	報告風險	S17 範疇	描述	驗證狀況
[redacted]	低	接達控制	[redacted]	進行中 目標於 2021 年 1 月前完成。
	低	系統購置、發展及維護		進行中 目標於 2021 年 1 月前完成。

[redacted]	低	加密方法	[redacted]	進行中 目標於 2021 年 1 月前完成。
	低	加密方法		進行中 目標於 2021 年 1 月前完成。
	有待改善的地方	通訊保安		進行中 目標於 2021 年 1 月前完成。
	中	系統購置、發展及維護		已完成

[redacted]	中	通訊保安	[redacted]	已完成
	中	接達控制		已完成
	中	系統購置、發展及維護		已完成
	低	操作保安		進行中 目標於 2021 年 1 月前完成。

[redacted]	低	操作保安	[redacted]	進行中 目標於 2021 年 1 月前完成。
	低	操作保安		進行中 目標於 2021 年 1 月前完成。
	低	系統購置、發展及維護		進行中 目標於 2021 年 1 月前完成。
	有待改善的地方	通訊保安		進行中 目標於 2021 年 1 月前完成。

3.2 一般控制結果

報告標題	報告風險	S17 範疇	描述	驗證狀況
[redacted]	低	實體及環境保安	[redacted]	進行中 目標於 2021 年 1 月前完成。
	低	接達控制		已完成
	有待改善的地方	資產管理		已完成
	有待改善的地方	系統購置、發展及維護		進行中 目標於 2021 年 1 月前完成。
	低	接達控制		進行中 目標於 2021 年 1 月前完成。
	有待改善的地方	加密方法		進行中 目標於 2021 年 1 月前完成。

4. 報告摘要

總括而言，資科辦已採取必要的行動，以評估和／或實施保安風險評估及審計報告就該系統提出的所有建議。是次保安風險評估及審計並無觀察到高風險項目。資科辦已覆檢所有已識別的風險評估結果，並已計劃於 2021 年 1 月前完成保安保障措施。總括而言，該系統的保安水平為**滿意**。

附錄 I. 參考資料

本附錄開列是次評估工作所使用的參考材料，以及資科辦在實施保安保障措施及／或理解本報告時可參考的材料。

資訊保安標準

- *香港特區政府《保安規例》*
- *《基準資訊科技保安政策》[S17]*
- *香港特區政府互用架構*
- *《資訊科技保安指引》[G3]*

一般保安資訊

- 電腦緊急事故應變小組統籌中心：互聯網保安問題的主要報告中心。http://www.cert.org/
- 常見漏洞與風險(Common Vulnerabilities and Exposures)項目：常見漏洞與風險旨在將公眾已知的所有漏洞及保安風險的名稱標準化。 https://cve.mitre.org
- Security Focus：Security Focus 是互聯網上最全面及受到信賴的保安資訊來源。該網站不偏不倚，為終端用戶、保安愛好者及網絡管理員以至保安顧問、資訊科技管理人員、資訊科技總監及保安總監等保安社群的所有成員，提供客觀、及時、全面的保安資訊。http://www.securityfocus.com/
- 開放網路應用程式安全計劃(OWASP)：OWASP 建立一個開源社區，旨在協助增進有關網上應用程式及網頁服務保安事宜的知識。參與者既可貢獻自己的知識以教育他人，亦可通過該項目編寫的文件及軟件學習有關內容。http://www.owasp.org/

~~ 保安風險評估及審計驗證報告完~~