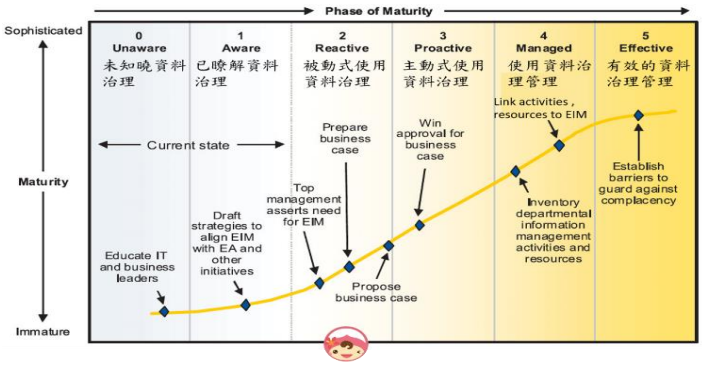
審計機關創新提案表

提案範圍	■審計 □非審計
提案單位	■單位提案（桃園市審計處）□個人提案
提案人員	主要提案人姓名：稽察　林文棟　貢獻度：50% 參與提案人姓名：審計員　古勤燕　貢獻度：30% 參與提案人姓名：審計兼科長　邱麗英　貢獻度：20%
提案名稱	**創新運用Python、SEO網頁診斷分析工具查核桃園市資通安全及數位資財服務，促請強化整體資安防護與管理效能**
提案創新性	1.**創新目的：** (1)**因應我國資安防護策略計畫推動與資通安全管理法及相關子法公佈施行，加強查核桃園市政府依法整備情形：**我國自 90 年起推動資通安全(下稱資安)基礎建設工作，行政院為逐步提升我國資通安全防禦能量，於 98 年核定「國家資通安全發展方案」，作為中央、地方政府建構資安縱深防禦架構之依據，迄今歷經 5 個推動階段，完成政府機關資安責任等級分級機制、成立國家級資安監控中心、建立資安事件通報應變及政府資安聯防監控與資安情報分享機制等階段性里程碑，目前第六期(110 至 113 年)方案持續推動中，並規劃 113 年底前政府機關所有 A 級與 80%之 B 級機關成熟度需達成第 3 級以上，以提升整體資安防護韌性；另於108 年度正式施行資通安全管理法(下稱資安法)及 6 項配套子法，督促各級政府機關需加強整備資通安全環境。桃園市政府暨所屬機關配合資安法之規定，每 2 年函送該府暨所屬機關資通安全責任等級調查結果至行政院核定，依資安治理成熟度分布，截至 111 年 11 月止桃園市政府暨所屬各機關成熟度達第 3 級(制度化型)者，僅警察局 1 個機關(占 12.5%)，尚與行政院規劃 113 年達成目標（80%）差距甚大，有待加速提升資安治理完備度，以如期達成政府整體資安防禦目標。 (2)**聚焦媒體及立監兩院關注焦點，加強考核桃園市政府及所屬機關資安業務辦理成效，促請落實安全防護及完備管理機制：**近來國內公、私部門接連發生重大個資外洩事件，舉如：戶政資料保管不當外洩、健保署醫療個資遭員工竊取盜賣、iRent 資料庫防護機制不足等，致屢遭各界質疑公私部門對於個人資料(下稱個資)保護及外洩事件處置等應變措施不足；又全球資訊科技進步及物聯網普及應用暨網路攻擊威脅驟增，各界對於個資保護議題極為重視，如歐盟為提升個人資料保護規範密度，並建立歐盟境內一體適用之管理規範，於 2016 年 4 月 14 日通過「一般資料保護規則」(General Data Protection Regulation, 簡稱 GDPR)，自 2018 年 5 月 25 日起全面施行，該法旨在提升及確保當事人資料權利保護，要求強化個資專責機關權限及課予資料外洩時之通報義務與提高處罰額度等，對於經營活動影響甚巨。行政院於 107 年 5 月 24 日第 3601 次院會責成國家發展委員會成立「個人資料保護專案辦公室」加強跨部會因應 GDPR 之協調整合，俾與時俱進及

因應 GDPR 適足性認定所需。經查 111 年度桃園市政府資料治理與管制情形，依美國數據管理協會(Data Management Association，簡稱 DAMA) 資料治理框架評估結果，成熟度偏低（得分 2.6，屬被動式管制，圖 1)，主要係資料分散在各局處及不同系統，單位間對資料治理理解與熟悉度不足，亦未針對機關間交換運用個資之保護管制及處理，暨訂定一致標準規範，凸顯該府資料治理環境尚處於準備階段，有待提升整體資安保護，強化相關管控機制並落實執行，以降低及防範資安風險帶來之衝擊。

圖 1　Gartner’s Data Governance Maturity Model 資料治理成熟度模型



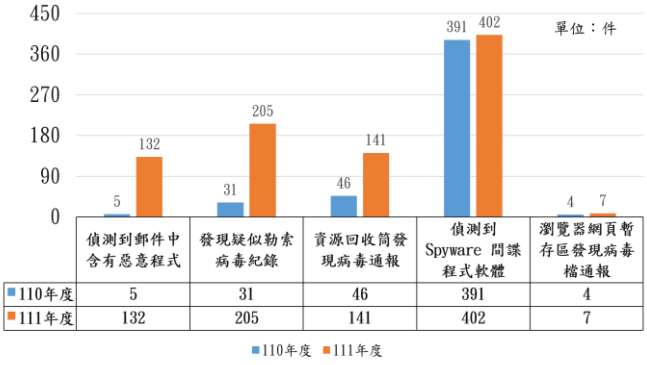
評估成熟度偏低，得分2.6分，屬被動式管制。

資料來源：整理自資訊科技局提供資料。

2.創新程度：

(1)首創採用美國數據管理協會(DAMA)資料治理框架評估市政資料治理成熟度，輔以 Python 程式語言及 Excel 軟體進行文字探勘發掘機關資安異常情事，促請強化資安治理，有效提升審計工作效率：為評核桃園市政府整體資料治理與管制情形，經採用美國數據管理協會(DAMA)資料治理框架使用 Gartner’s Data Governance Maturity Model(資料治理成熟度模型，附件 1)分作 6 等級評估治理成熟度，復運用 Python 程式設計軟體導入 pandas 及 os 分析模組，以 for 循環結合 join paragraphs 批量彙總市府及所屬機關(單位)資安管理共 423 份、計 3,384 頁稽核報告 (.word.pdf)，並導入 Excel 進行文字探勘，據以篩選機關未落實資通安全責任等級分級辦法，其中應辦事項(計有 21 項不符合及 125 項部分符合，附件 2)及資通安全維護計畫實施情形(計有 17 項不符合及 213 項部分符合)等缺失，促使市府督促缺失機關加強資安稽核，並加速籌組桃園市資料治理推動會及研擬《桃園市數據自治條例》強化個資保護與資安政策指引，俾保障安全之數位治理環境。

(2)率先運用 Screaming Frog SEO Spider 等網頁連結診斷工具爬梳市政開放平臺及提供之數位資財服務，促請通盤檢討網頁弱點、錯誤及易造成民眾誤解等資訊，與檢討免費無線上網用量逐年減少之使用熱點，以有效改善並節省經費，提升審計查核成果：市府經打造「桃園網路 e 指通」、「福利智慧雲」、「桃園市政府資料開放平臺」及「iTaoyuan 無線上網」等數位資財服務供民眾使用，共開放資料集 4,845 項、提供線上福利申辦查詢 256 項次及免費上網服務計 325 個熱點。本案運用 Screeming Frog SEO Spider 及 Online Broken Link Checker 等 SEO(搜尋引擎優化 Search Engine Optimization，簡稱 SEO)網頁連結診斷工具爬梳平臺，發

	現共有 537 個連結資源不存在或錯誤，或造成民眾誤解等資訊，及部分免費無線上網熱點使用量已逐年減少等情(附件 3、4)，經促請通盤檢討改善，截至 112 年 6 月底止已修正平臺全數錯誤並再清查改善服務項目計 104 項，且除保留部分地區民眾免費無線上網需求熱點外，已移除 170 個熱點，節省經費約 1,293 萬餘元。
實施方法及過程	**1.導入創新方法之必要性(現況或現行制度規章之缺點)** 近年來隨著資訊科技的蓬勃發展，各級政府莫不投入大量資源與人力，積極推動業務數位化，並引進人工智慧（Artificial Intelligence，AI）、大數據、區塊鏈及 5G 行動通訊等技術，建構數位政府及智慧城市，以改善服務品質及提升價值。 桃園市為落實智慧城市建設，透過跨局處協調推動各項智慧城市科技治理，其中資訊科技局經爭取國家發展委員會「亞洲．矽谷 5G 創新應用計畫」補助經費 4,600 萬元，刻正執行包括市政資料治理暨大數據分析平台等資料串接服務與驗證，以打造資料驅動決策之智慧政府。資訊科技局 111 年度共編列 4,568 萬餘元辦理市政資料治理暨大數據分析平台建置及資安管理制度維護與防護監控等計畫，提供市政府及網域所屬機關資安應辦事項管理與部署防護監控。桃園市政府投入巨額經費規劃市政智慧治理，以服務市民所需，惟現行資料治理成熟度偏低，尚未訂定機關間交換運用個資之保護管制及處理，且部分機關資安認知管理欠佳，與近年資安監控通報病毒及惡意程式攻擊事件遽增(圖2)，亟待督促加速推動整體資料治理機制，及完備制度規範與異地備援，避免機敏資料遭竊取或外洩風險。本案爰秉持創新及專業之核心價值，積極運用 Python 程式語言等各種審計技術方法辦理查核，並擴展運用 SEO 網頁連結診斷電腦稽核軟體新知發展數位審計能力，強化各項數位發展計畫之考核，落實審計創新。 **圖 2　近 2 年度桃園市資安防護監控情形**  資料來源：整理自資訊科技局提供資料。 **2.推動過程遭遇困難點，以及突破或解決的具體策略或方案** **<遭遇困境>** **(1)人工處理大量文字數據資料缺乏效率：**本案查核之採購案，依契約規定，廠商須提供書面報告書及電子檔作為履約成果，尚無資訊系統化或結構化資料可供存取或篩選。其中資安管理制度維護案，依資訊科技局提供 111 年度市政府及所屬共 65 個機關(單位)辦理資安管理維護資料共 1,095 筆，其中資安管理稽核報告計有 423 筆電子檔案（.word.pdf），如進行逐筆檔案瀏覽以找出問題缺失實屬不易，並且採取每份稽核報告共計 3,384 頁逐一搜尋之

方式亦相當費時，又面對大量文字數據等資訊，以人工肉眼方式判斷各單位資安稽核結果是否存有異常並加以彙整統計，常因受限於人眼視力、精神及注意力偏差而有遺漏或誤植，且不具效率。

(2)**取得網頁技術專業用語資料解讀不易**：資安防護監控案，廠商提供桃園市數位行政資源與公開資訊平臺，如「福利智慧雲」、「桃園網路ｅ指通」、「桃園市政府資料開放平臺」等網站弱點掃描服務，針對網址(Uniform Resource Locator，簡稱 URL)以專業軟體(Qualys、nessus)檢測是否存在弱點，以找出可能入侵管道。惟取得該檢測結果計 105 筆掃描資料，內容包含 Active Server Pages (ASP)等網頁技術用語，除非具有資訊專門背景，否則一般外界解讀不易，且以風險等級(高中低)數量表達，未能直接呈現網站具體問題，需另尋其他替代方案驗證網站及數位服務資訊。

<解決方案>

本案資訊科技局辦理資安管理維護及防護監控等採購案均屬 111 年度，分別由承攬廠商交付資安管理稽核及網站弱點掃描等成果資料合計 1,200 筆。謹就上述本案查核遭遇困難點，施以突破或解決的具體策略或方法，分述如次：

(1)**撰寫 Python 程式有效進行文字探勘**：本案採取撰寫 Python 程式進行文字探勘工作，以降低使用不明來源軟體潛藏之資安風險，對於後續程式之維護及擴展等較具有彈性，惟過程產生程式錯誤屬無法避免之缺點，須經多方校核及驗證，以減少錯誤發生。該程式核心執行程序係運用 Python 程式設計軟體導入 OS 分析模組讀取目標文件夾內所有稽核報告電子檔(.pdf) 並生成文件清單，再導入 PDF plumber 分析模組，以 for 循環提取清單內之所有內容並予合併保存為單一文字檔(.txt)後，利用 pandas 分析模組讀取檔案，及使用 dataframe、split 函數進行文字處理並導入 Excel 剖析稽核對象、日期與缺失，據以綜整機關未落實資通安全責任等級分級辦法應辦事項及資通安全維護計畫等缺失。

(2)**運用 SEO 網頁連結診斷工具爬梳網站平臺**：依「福利智慧雲」、「桃園網路ｅ指通」、「桃園市政府資料開放平臺」等數位行政資源與公開資訊平臺網址 URL，運用來自英國 Screaming Frog 公司開發之 SEO 暨網站分析軟體 Screeming Frog SEO Spider，與國立成功大學計算機與網路中心專文推薦之網站連結檢測工具(Online Broken Link Checker)進行網站連結診斷，配合提供之網站弱點分析結果，並透過上開工具爬梳市政開放平臺及提供之數位資財服務，找出網站平臺弱點或待改善網頁診斷等資訊。

3.建立制度規章或興革精進作為

本案桃園市因應資通科技（Information Communications Technologies, ICTs）發展智慧城市，已規劃資料城市治理提供創新數位服務回應市民所需，惟查核發現市政資料治理成熟度偏低，部分機關資安認知與管理情形欠佳，形成個資安全漏洞或系統遭勒索病毒事件，又網域部署資安監控通報發現病毒及惡意程

	式攻擊事件遽增，衍生資料安全與保護疑慮，經函請加速推動整體資料治理機制及完備制度規範與異地備援，達成資訊服務不停頓及避免駭客攻擊造成資訊癱瘓風險，並參酌 GDPR 研訂適當管理措施以確保各部門對於民眾資料之保障，避免機敏資料遭竊取或外洩風險情事，提升數位治理效能。該府刻正籌組桃園市資料治理推動會，及研擬《桃園市數據自治條例》強化個人資料保護與資安政策指引，與盤點重要核心與業務關鍵系統，規劃異地租用雲端運算資源或 IDC(Interner Data Center)機房備援方式，俾保障資料治理安全之數位環境。 **4.是否屬涉及全國之共同性議題、涉及兩個以上政府間之跨域議題或執行過程須跨單位協力合作** 本案涉及地方政府配合中央資通安全發展方案執行與公務機關之關鍵基礎設施（CI）資安防護辦理情形等，均攸關政府資通訊安全與民眾隱私權保護之良窳，進而影響國家安全。經考評桃園市政府資安管理之落實程度，促請機關重視資安防護，減少資安事件發生；另因應政府數位資訊業務再造，促請加速推動整體資料治理機制與完備制度規範，又為再加強考核市府資訊安全威脅與防護，經提案核定併入本部第六廳 113 年度聯合數位審計施政工作重點，俾厚植政府整體資安防護及提升數位治理效能。
實際成果	**1.本提案在效果、效率、品質及其他方面已產生之質性與量化績效** **(1)質性績效：** **促請市府加速推動整體資料治理機制，及完備制度規範與異地備援，避免機敏資料遭竊取或外洩風險：**桃園市政府及所屬辦理資安維護及數位建設，核有機關資安認知與安全管理情形欠佳，及通報發現病毒及惡意程式攻擊事件較 110 年度增加逾 2 倍，衍生資料安全與保護疑慮，經建請研謀改善，該府參採本處建議，已督促 15 個資安缺失機關加強管理及納入 112 年度稽核重點，並借鏡國內已設置資料治理委員會之城市經驗，刻正籌組桃園市資料治理推動會及研訂《桃園市數據自治條例》強化個人資料保護與資安政策指引，暨盤點重要核心與業務關鍵系統租用雲端運算資源或機房備援方式，保障資料治理安全之數位環境。 **(2)量化績效：** **A.促請修正 641 個網站平臺錯誤資訊，並裁罰廠商違約金 35 萬餘元：**經運用 SEO 網頁診斷工具爬梳數位行政資源與公開資訊平臺網站，共發現並促請修正 537 個連結資源不存在或錯誤，或容易造成民眾誤解等 104 項數位行政資訊服務項目，並針對平臺系統維運廠商裁處績效及逾期違約金 35 萬餘元。 **B.促請檢討免費無線上網使用熱點，有效節省經費 1,293 萬餘元：**市府提供免費無線上網用量逐年減少，經函請檢討使用率偏低熱點，該府經參採本處建議，除考量弱勢族群、服務偏鄉及部落地區民眾等需求保留免費無線上網服務熱點外，已依序移除使用人次較少之點位，截至 112 年 6 月底止已移除 170 個熱點，

節省經費約1,293萬餘元，有效提升數位建設資源使用效益。

2.本提案對組織內部產生之正面影響力

本案由同仁間採團隊協力合作方式，尤其新進審計同仁透過「數位圖資與資料平臺」等多元管道學習運用Python程式語言，以有效批量彙總單位之資安管理稽核報告資料並導入Excel進行文字剖析及統計分析，進而發掘機關資安管理漏洞或遭勒索病毒事件等管理欠佳情事，復運用SEO網頁連結診斷工具爬梳桃園市政開放平臺及提供之數位資財服務，以找出數位服務項目易造成民眾誤解或待改善網頁診斷資訊。藉由自主學習、分享、創新，精進審計工作品質及技術方法，獲致具體成效。

3.本提案影響外部利害關係人之規模及層面

隨著資訊科技發展，積極運用資訊科技輔助審計查核，能有效提升審計功能及審計效率。本案運用創新技術方法查核成果，已分別於109及111年度桃園市政府總決算審核報告資訊科技局與市政府主管重要審核意見揭露，**獲媒體112年8月29日報導「勒索病毒案1年飆升至205件 桃園草擬數據自治條例護資安」**(附件5)，可踐行國際最高審計機關組織(INTOSAI)於2019年9月第23屆會員代表大會(INCOSAI)發布「莫斯科宣言(Moscow Declaration)」，建議最高審計機關應有效回應科技進步所帶來之機會，強化對公共課責及透明之影響力，除運用數據分析及人工智慧等工具，以強化創新，並扮演策略參與者、知識交換者及前瞻產出者之角色。

4.本提案可延續或擴大運用程度，及供其他單位學習或複製延伸應用價值

行政院為實現蔡總統「數位國家、智慧島嶼」政策綱領，自2016年起啟動「數位國家·創新經濟發展方案(2017-2025年)」，投入大量經費促進國家社會之數位轉型。審計機關職司監督各級政府預算之執行，審核財務收支，考核其績效，並持續充實新知及善用各種技術方法，發展數位審計。本案經運用Python程式套件及Excel資料剖析功能，完成文字探勘、擷取及分析工作，大幅減少文件以人工肉眼方式逐筆瀏覽判讀等作業時間，且有效綜整具體缺失；另運用開放之網頁連結診斷工具，發掘桃園市數位行政資源與公開資訊平臺網頁連結資源不存在或錯誤資訊，彌補網頁技術輸出結果解讀不易，及弱點掃描工具結果未能直接呈現網站具體問題，可供審計單位借鏡複製並延伸應用。