



資通安全弱點通報系統(VANS) 推廣教材

檢測防禦中心
112年5月9日

課程簡介



- 本單元課程時間總計3小時
- 目標：協助機關具備執行資訊資產弱點管理與安全性更新管理之能力
- 課程重點
 - 資訊資產弱點管理說明與實作
 - 安全性更新管理說明與實作
- 實作產出
 - 資訊資產弱點管理實作結果
 - 安全性更新管理實作結果

課程行政事項



- 上課時間安排

上午	下午	課程內容
9:00 ~ 9:15	14:00 ~ 14:15	資通安全弱點通報系統說明
9:15 ~ 11:30	14:15 ~ 16:30	資通安全弱點通報系統實作
11:30~12:00	16:30 ~ 17:00	問題討論

- 課程進行中，為確保學習效果請勿使用3C產品
- 本課程含公務人員終身學習時數3小時，請記得簽到
- 上課中有任何需求，請告知行政人員或講師

課程大綱



- 前言與法規政策說明
- 資通安全弱點通報系統說明
- 資通安全弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習1
 - 弱點通知與修補作業
 - 實作練習2
 - 資訊資產與已安裝KBID更新作業
 - 實作練習3



- 前言與法規政策說明
- 資通安全弱點通報系統說明
- 資通安全弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習1
 - 弱點通知與修補作業
 - 實作練習2
 - 資訊資產與已安裝KBID更新作業
 - 實作練習3



- 不定期爆發之重大弱點，若未能即時反應與修補，將**嚴重影響機關業務正常運作**，亦可能造成**機關形象受損**
- 當弱點爆發時，如能確實**掌握機關資通系統與使用者電腦情況**，即可**快速因應**，將損害降至最低

快速反應

- 如何在弱點發布後，**快速反應**所面臨的威脅與**掌握受影響版本**

確認範圍

- 如何在確認受影響版本後，可確實**掌握受影響範圍**

應變處理

- 如何在確認受影響範圍後，**快速因應處理**

事後追蹤

- 如何在應變處理後，持續**追蹤弱點修補情形**

資通安全管理法應辦事項規定(1/2)



- 依「資通安全責任等級分級辦法」，資安責任等級A級、B級、C級之公務機關及關鍵基礎設施提供者應導入資通安全弱點通報機制

制度面向	辦理項目	資安責任等級	辦理內容
技術面	資通安全弱點通報機制	A、B級 公務機關	一、初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料
		A、B級 特定非公務機關	一、關鍵基礎設施提供者初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式完成提交資訊資產盤點資料 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料

資通安全管理法應辦事項規定(2/2)



制度面向	辦理項目	資安責任等級	辦理內容
技術面	資通安全弱點通報機制	C級 公務機關	<p>一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p> <p>二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p>
		C級 特定非公務機關	<p>一、關鍵基礎設施提供者初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p> <p>二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p>



- 前言與法規政策說明
- 資通安全弱點通報系統說明
- 資通安全弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習1
 - 弱點通知與修補作業
 - 實作練習2
 - 資訊資產與已安裝KBID更新作業
 - 實作練習3

資通安全弱點通報機制



- 資通安全弱點通報機制(Vulnerability Alert and Notification System, VANS)結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項
 - 定期蒐集資通系統與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標
 - 將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊





- 確認資訊資產弱點

- 蒐集機關使用之軟體資訊，並與國際權威弱點資料庫進行比對，當使用軟體存在重大弱點時，即時得知與應變處理

- 降低重大弱點管控與追蹤之成本

- 利用弱點資料庫搭配自動比對方式，提供機關相關弱點資訊與自我檢查機制

- 追蹤資訊資產弱點修補情形

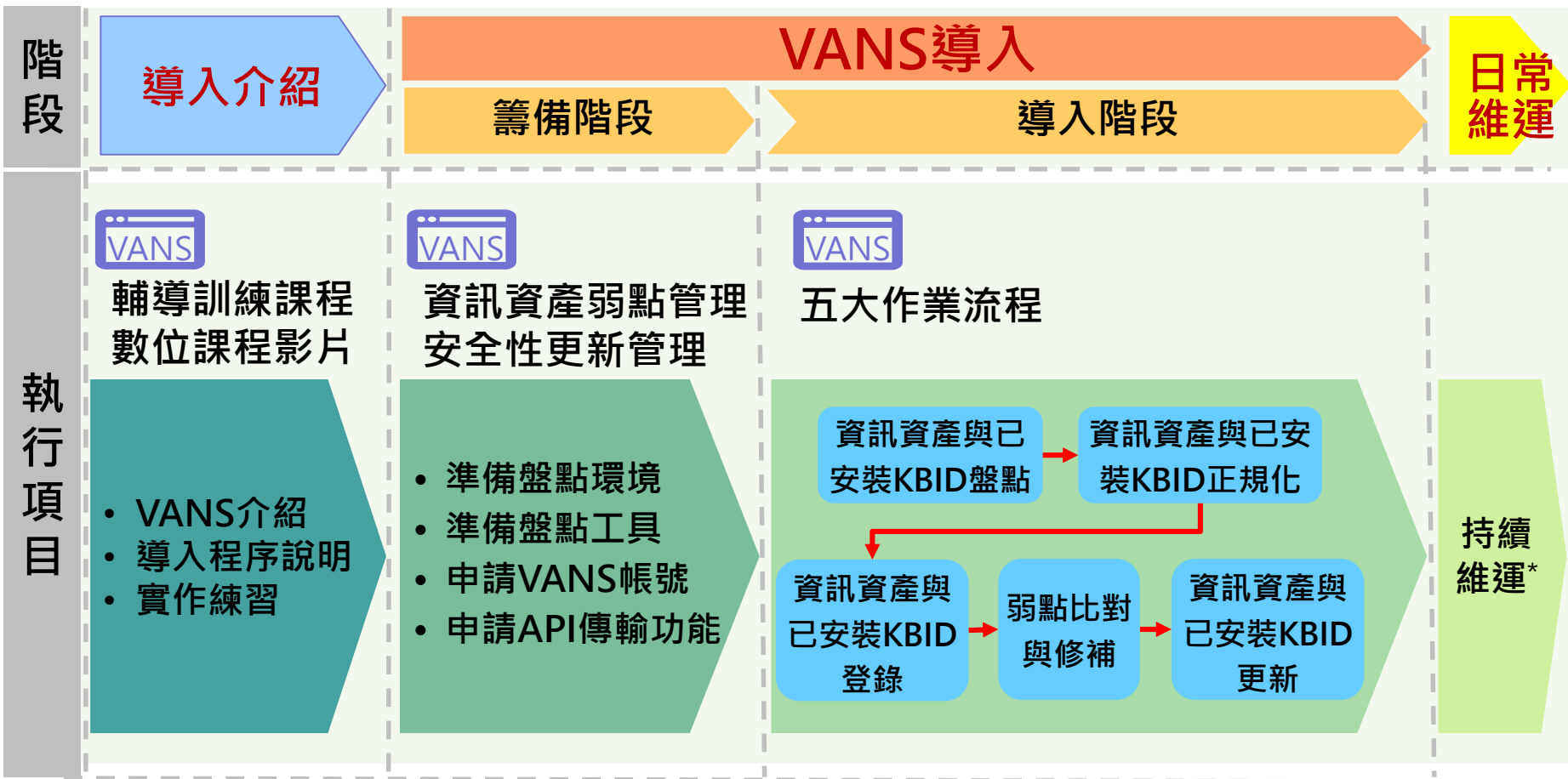
- 依照機關訂定之風險值門檻，及時提醒資訊資產風險情形，並進行弱點評估與修補作業

- 強化安全性更新落實情形

- 搭配上傳微軟系列軟體已安裝安全性更新，以協助機關確認微軟資產之安全性更新缺漏項目，更精準呈現微軟弱點修補情形



VANS機制導入作業流程

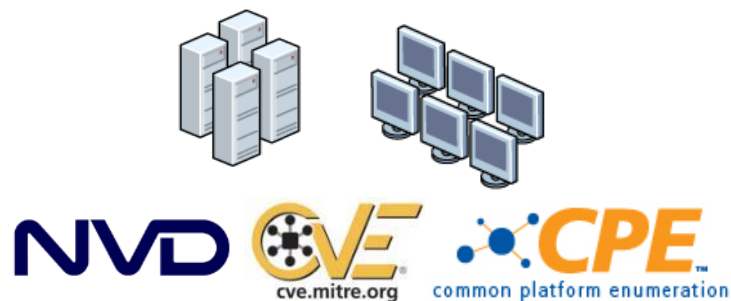


*持續維運：包含定期執行及不定期執行(例如資產異動時)

系統介紹



- VANS系統提供機關**登錄資訊資產**，藉由系統**自動與NVD弱點資料庫比對**，羅列出**資訊資產之弱點**，俾利機關**掌握可能面臨之資安風險**，以強化**資訊資產之資安管理**



資通安全弱點通報系統 (VANS)

一般帳號登入

機關管理者帳號登入

公告

1. 為提升安全性，本系統已將HTTPS加密等級提升至TLS 1.1以上，再請留意瀏覽器需支援TLS 1.1以上方可瀏覽本系統，謝謝。
2. 因應網域名稱調整事宜，「資通安全弱點通報系統」已完成憑證更換，並將網址由「<https://vans.ncst.nat.gov.tw/>」調整為「<https://vans.nat.gov.tw/>」，API網址亦同步進行調整，後續請使用新網址進行連線與傳輸。

聯絡資訊如下：

系統登入與操作系統異常相關問題：

國家資通安全研究院
服務電話：(02)6631-6423
服務信箱：VansService@nics.nat.gov.tw

機關管理者帳號審核與業務相關問題：

數位發展部資通安全署 吳忠家先生
服務電話：(02)3356-8067
服務信箱：zhonggia@acs.gov.tw

機關管理者帳號	<input type="text"/>	
iAuth個人帳號	<input type="text"/>	
密碼	<input type="password"/>	
<input type="button" value="登入"/>	<input type="button" value="申請個人帳號"/>	<input type="button" value="忘記密碼"/>

資訊資產盤點標的



- 蒐集範圍：資通系統與使用者電腦之軟體資產



應用程式

應用程式或網站伺服器

程式語言執行環境

網站採用第三方元件

開發框架

資料庫

- Adobe
- Apache

- Microsoft Office
- ...



作業系統



ubuntu®



- 軟體名稱
- 開發廠商名稱

- 版本資訊
- 軟體安裝數量

資訊資產呈現方式(1/3)



- 資通系統與使用者電腦組成多變，所安裝之軟體套件多樣，難有資產管理系統能提供一體適用之軟體套件蒐集方式
- 不同廠商針對同一軟體資產，可能有不同描述方式



資訊資產呈現方式(2/3)



- **Common Platform Enumeration(簡稱CPE)**，為美國國家標準技術研究所(NIST)所提出標準化方式，用以描述與識別企業內的應用程式、作業系統及硬體設備等資訊資產，最新版本為2.3
- **CPE條目格式**
 - 主要分為三大類：**作業系統(o)**、**應用程式(a)**及**硬體(h)**
 - 主要資訊：**廠商名稱(vendor)**、**產品名稱(product)**、**產品版本(version)**、**產品更新(update)**、**產品版次(edition)**、**語系(language)**

弱點呈現方式



- Common Vulnerabilities and Exposures(簡稱 CVE)羅列各種資安弱點，並給予編號以便查閱
- CVE目標為將所有已知弱點與相關風險資訊標準化，俾利於各個弱點資料庫與安全工具之間統一弱點相關資料
- 現由美國非營利組織MITRE所屬之National Cybersecurity FFRDC負責營運維護
- 每一個資安弱點皆賦予一個CVE專屬編號，格式如下：

-CVE-YYYY-NNNN

西元紀年 流水號





- **National Vulnerability Database(簡稱NVD)**為NIST所建置，專門用來蒐集各種弱點資訊之資料庫網站
 - 自MITRE取得CVE列表，並增加修補建議連結、嚴重性評分(CVSS分數)及影響等級等資訊
 - 建立CPE與CVE對應關係，以解決弱點與資訊資產之對應關係
 - VANS系統每天更新1次資產與弱點資訊

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



微軟安全性更新(1/2)



- 微軟系列軟體之弱點多數透過安裝安全性更新進行修補，而不會改變軟體版本資訊
 - CPE條目僅包含軟體版本等資訊，無法有效判斷是否完成弱點修補
- 藉由盤點已安裝安全性更新(KBID)，以了解資通系統與使用者電腦安全性更新實際情況
 - 協助管理者**確認微軟系列產品安全性更新缺漏項目**，以強化**安全性更新落實情形**
 - 重大弱點爆發時，可**確認未安裝安全性更新之資通系統與使用者電腦數量與範圍**，並進行應變處理



微軟安全性更新(2/2)



- 以Microsoft **Windows 10**作業系統而言，因CPE僅會列出大版本(如22h2)，**透過Windows Update進行安全性更新作業不會異動大版本資訊(22h2)**，導致難以透過CPE判斷Windows Update更新情形
- VANS系統可透過機關上傳之已安裝KBID，判斷弱點修補狀態

cpe:2.3:o:microsoft:windows_10_22h2:-:*:*:*:*:*:x64:*

Microsoft Windows 10 22h2

🏠 檢視更新記錄 **安裝KBID後不會變更大版本**

✓ 品質更新 (50)

2023-02 Cumulative Update for Windows 10 Version **22H2** for x64-based Systems (KB5022834)

已順利在 2023/2/16 安裝

2023-01 適用於 x64 系統 Windows 10 Version **22H2** 的累積更新 (KB5019275)

已順利在 2023/2/2 安裝

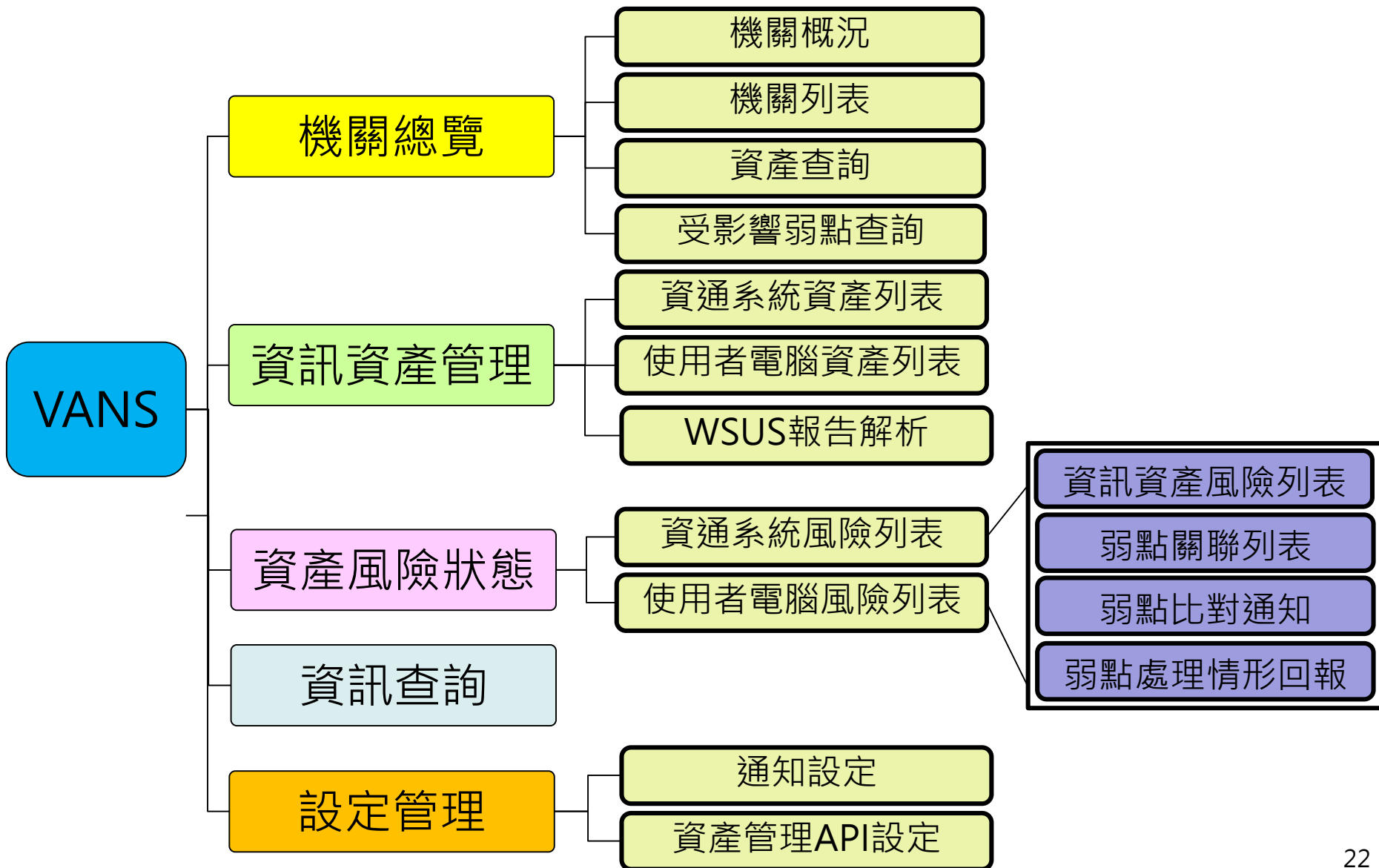
2023-01 適用於 x64 系統 Windows 10 Version **22H2** 的累積更新 (KB5022282)

已順利在 2023/1/12 安裝

2022-12 適用於 x64 系統 Windows 10 Version **22H2** 的累積更新 (KB5021233)

已順利在 2022/12/14 安裝

系統功能總覽



系統介面說明



系統名稱

全螢幕 登出

資通安全弱點通報系統



登入人員

顯示/隱藏
功能選單列

- 首頁
- 機關總覽
- 機關概況
- 機關列表
- 資產查詢
- 受影響弱點查詢
- 資訊資產管理
- 資產風險狀態
- 資訊查詢
- 設定管理

功能選單列

機關總覽 > 機關概況

功能路徑

檢視方式

資通系統 使用者電腦

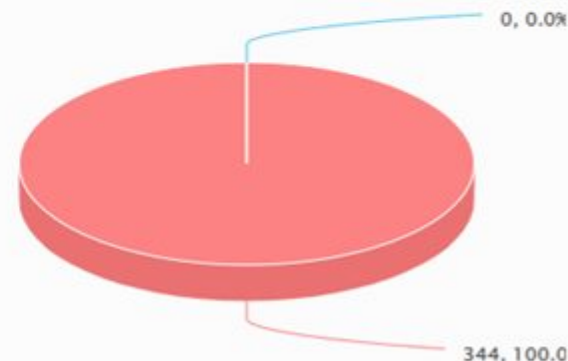
功能頁面

資通系統資產類別統計



資訊資產總數 微軟系列軟體總數

資通系統弱點處理情形(CVE)



已修補弱點數 未修補弱點數

服務申請流程



聯絡資訊
服務電話：(02)6631-6423
服務信箱：VansService@nics.nat.gov.tw



申請個人帳號

- 於iAuth平台申請個人帳號

資安人員身分驗證系統(iAuth平台)
<https://www.ncert.nat.gov.tw/iAuth2/>



機關提出申請

- 於iAuth平台提出**VANS**帳號申請
- 於VANS專區下載並填寫**機關管理者帳號申請(異動)單**，完成後Email予資安署



參閱操作手冊

- 操作諮詢
- 服務說明

資安院VANS專區
<https://www.nics.nat.gov.tw/Vans?lang=zh>



開始使用服務

- 資料建立
- 弱點比對

VANS系統
<https://vans.nat.gov.tw/>

VANS帳號管理(1/2)



● 管理者帳號權限異動

- 單一機關至多**2個**機關管理者帳號
- 有異動需求時，請填寫**機關管理者帳號申請(異動)單**，完成後Email予資安署，審核通過後，資安院將協助進行後續處理

● 閒置帳號鎖定

- 若iAuth帳號長達**180天**未有登入行為，則將進入**鎖定狀態**，無法登入系統進行操作
- 可透過iAuth平台重新啟用帳號

VANS帳號管理(2/2)



- 機關登入VANS系統分為下列兩種帳號

機關管理者帳號

機關管理者帳號

iAuth個人帳號

密碼

登入 申請個人帳號 忘記密碼

- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視機關各帳號資產異動紀錄
- ✓ **申請API介接IP並重新產生API Key**

一般權限帳號

一般權限帳號

iAuth個人帳號

密碼

登入 申請個人帳號 忘記密碼

- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視機關各帳號資產異動紀錄
- ✓ **檢視API Key**



- 前言與法規政策說明
- 資通安全弱點通報系統說明
- 資通安全弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習1
 - 弱點通知與修補作業
 - 實作練習2
 - 資訊資產與已安裝KBID更新作業
 - 實作練習3

執行規劃

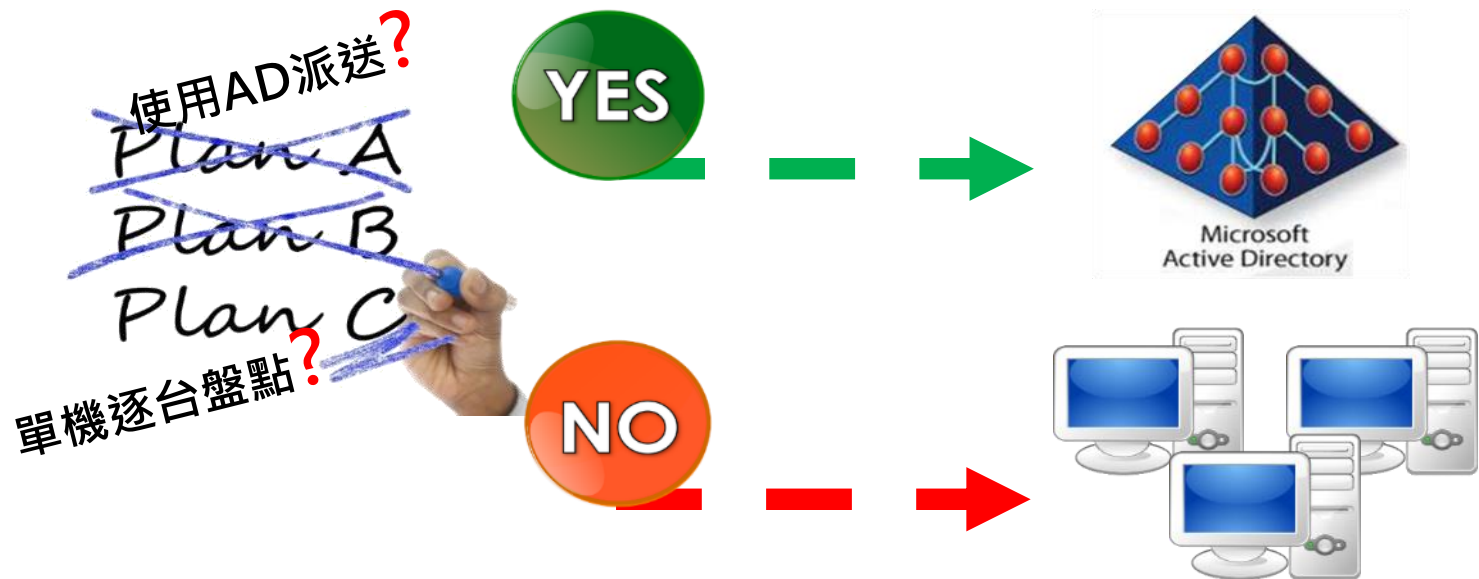


- 依據機關環境擬定導入執行規劃

- 執行範圍：本部/本部與所屬、資通系統/使用者電腦

- 執行時程：人力評估、導入測試起訖時間、正式導入起訖時間

- 執行方式：單機/AD派送GPO執行、第三方工具執行

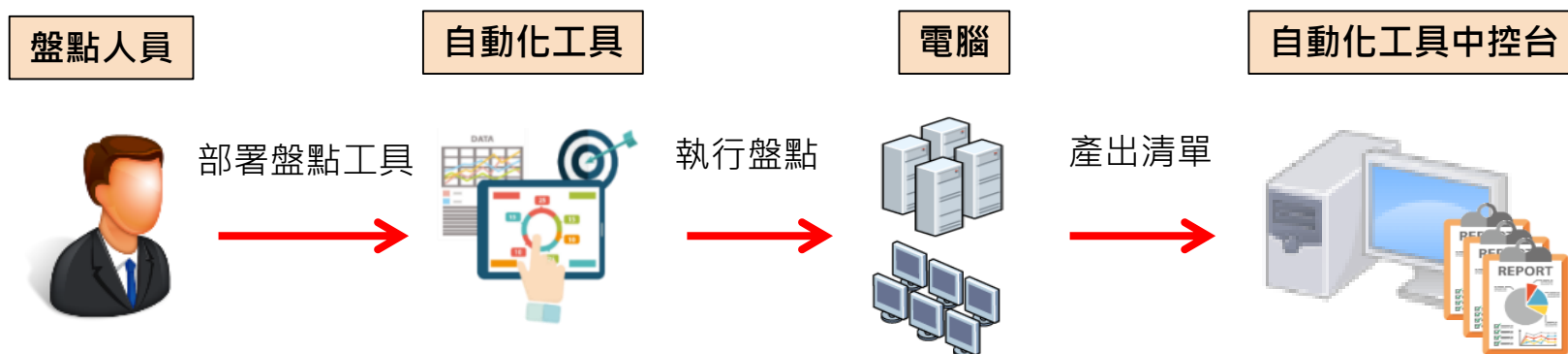


情境說明(1/3)



- 定期透過**自動化工具**或**系統指令**進行資訊資產與已安裝KBID之盤點與正規化，以利後續可登錄至VANS系統
- 可依機關資訊環境自由選擇合適之**資料蒐集方式**

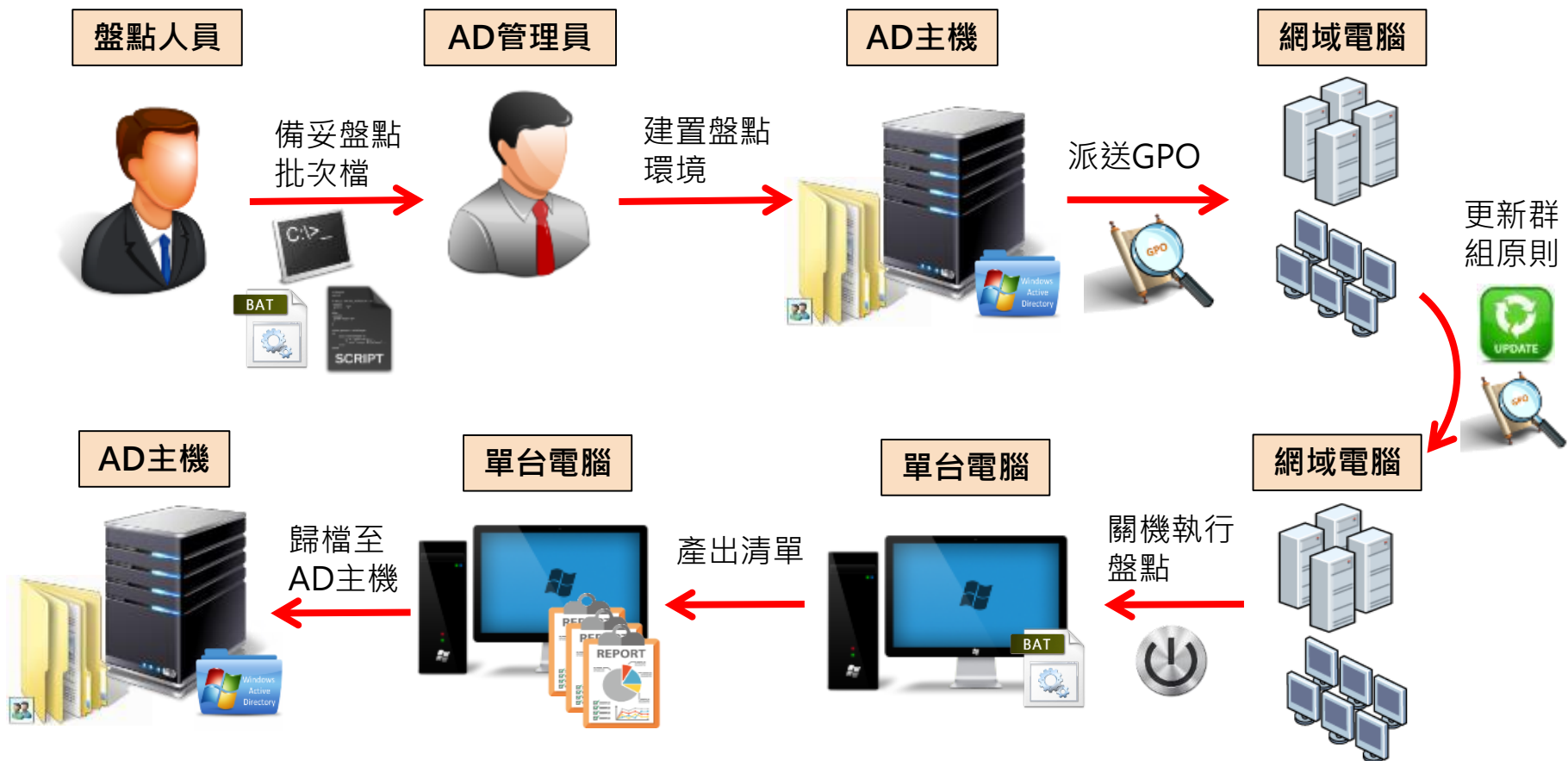
1 透過**自動化工具**盤點



情境說明(2/3)



2 透過系統指令批次盤點



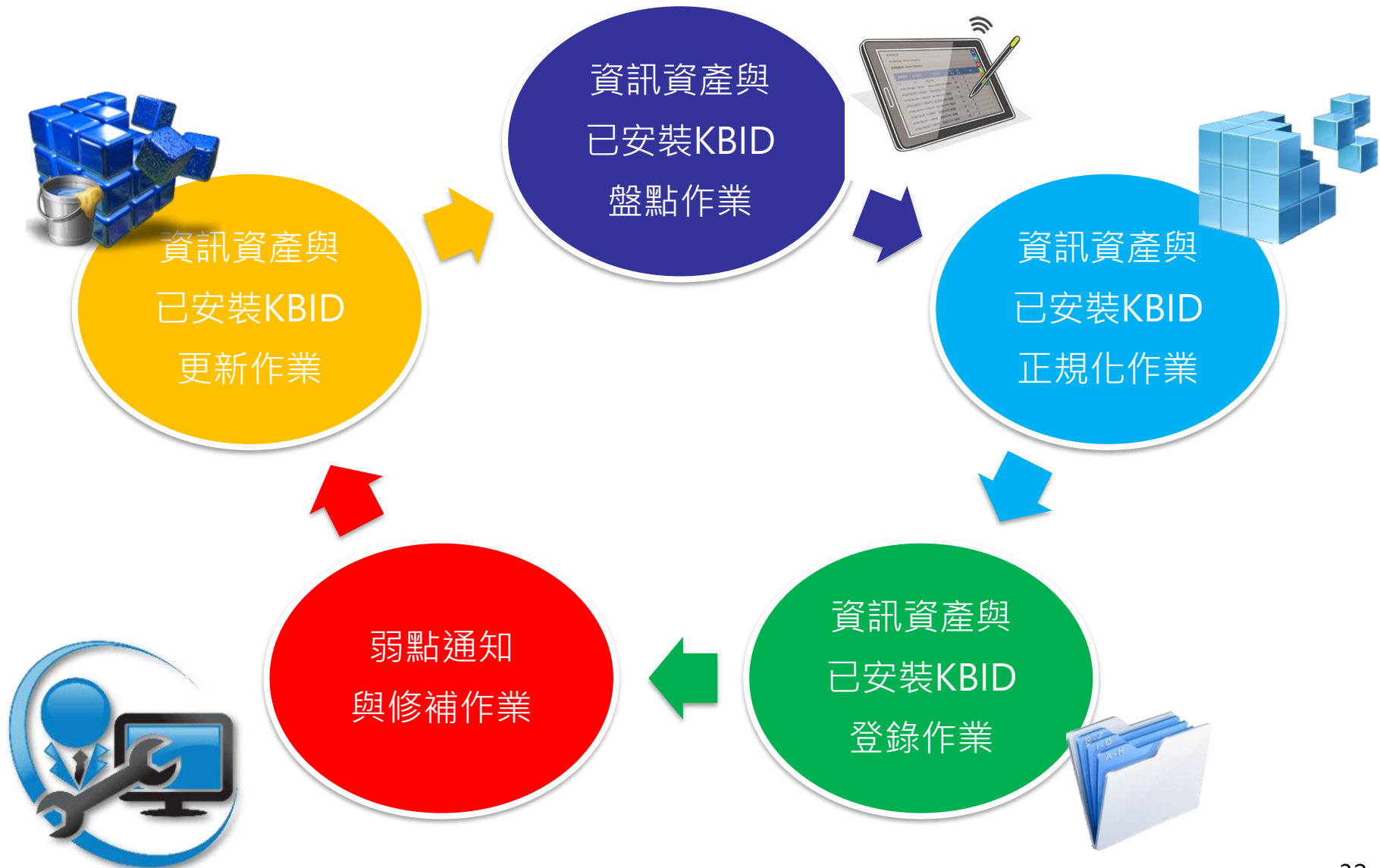
情境說明(3/3)



3 透過系統指令單機盤點



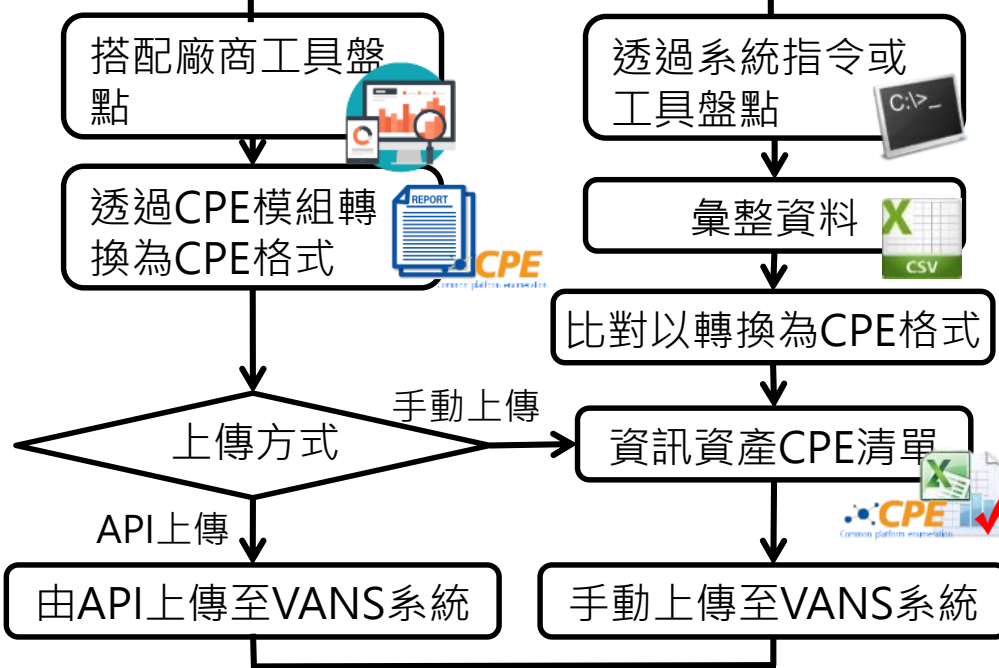
導入作業流程



資訊資產弱點管理總覽



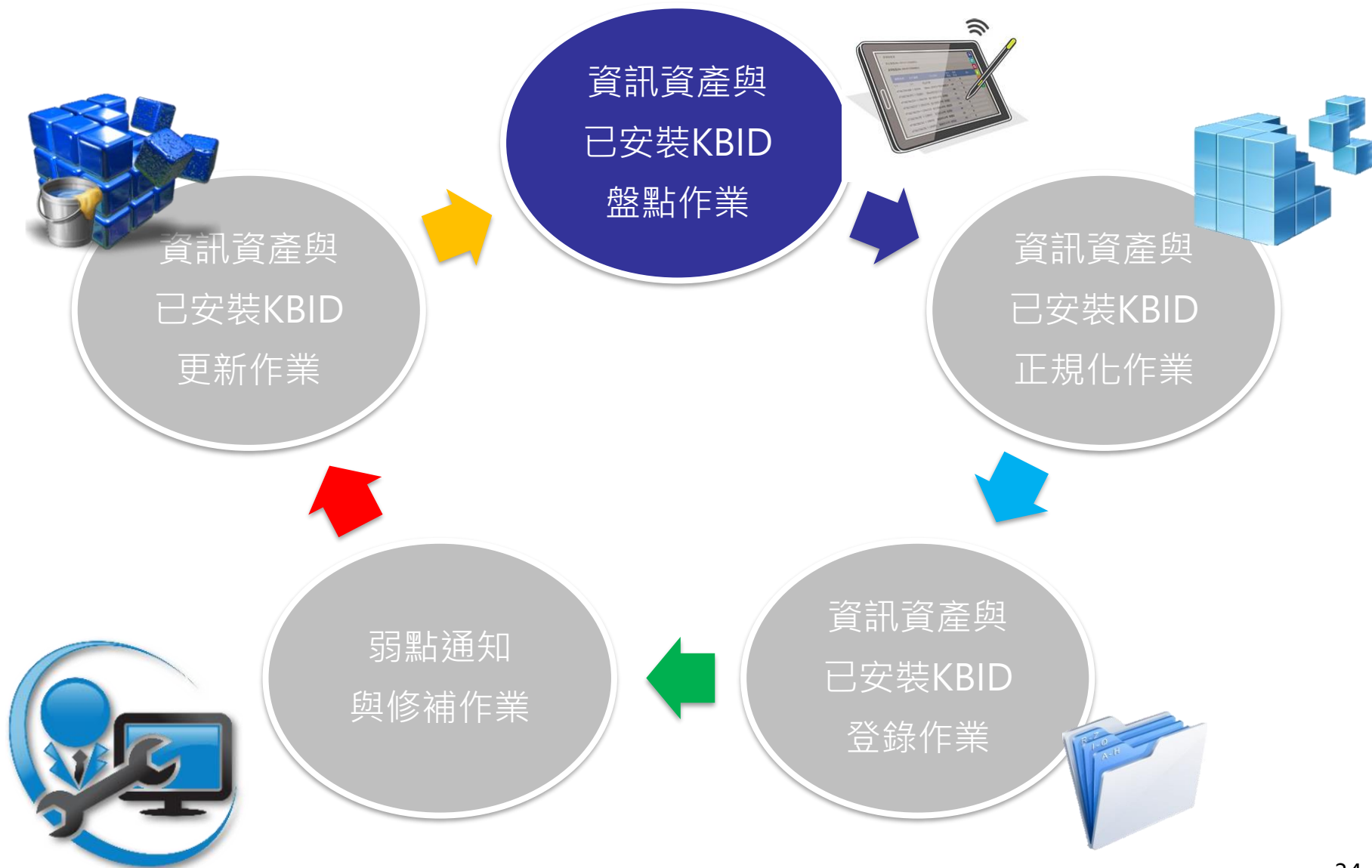
透過廠商工具產出CPE格式報表，並可透過API上傳至VANS系統



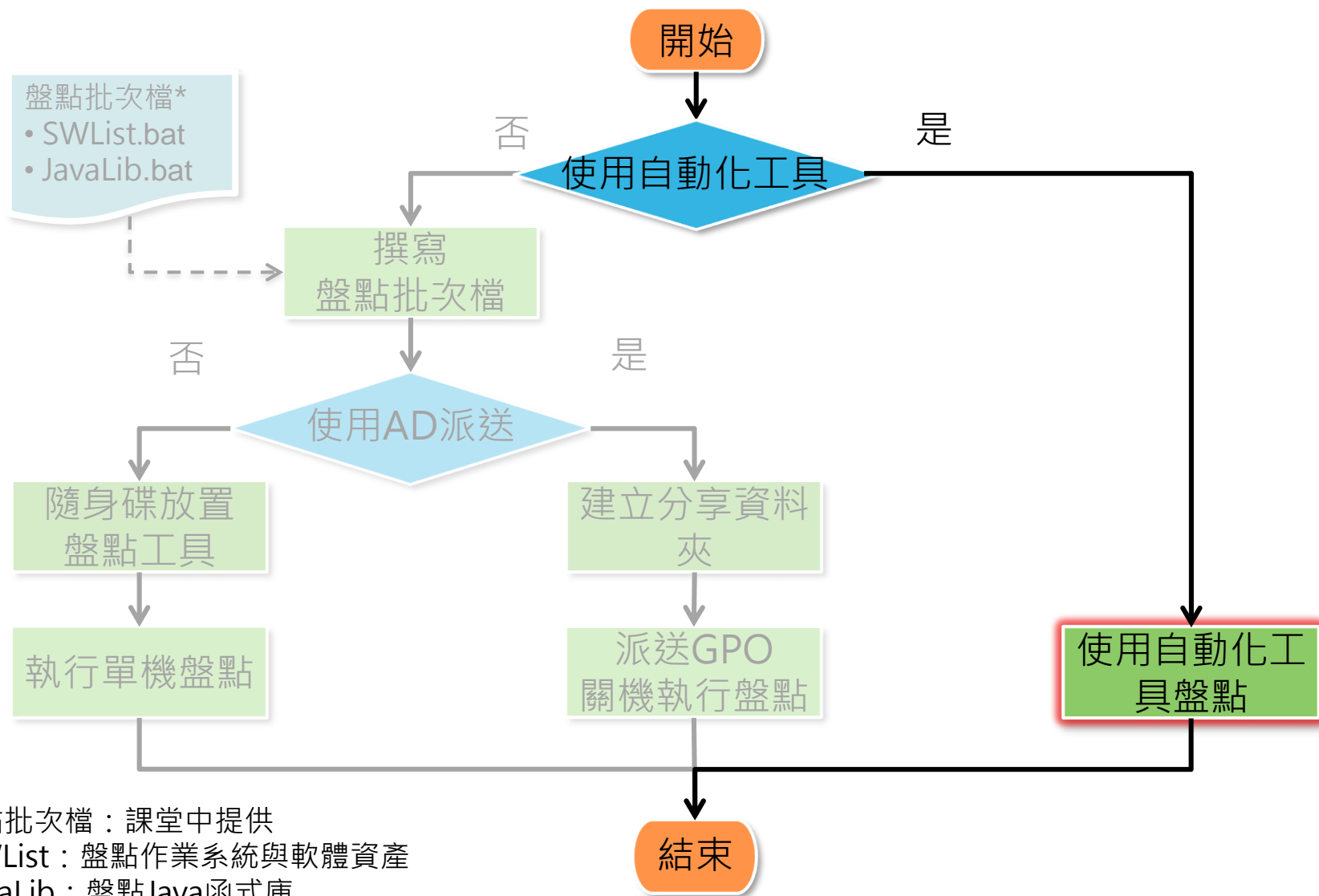
透過AD派送批次檔方式盤點軟體資產資訊，再以PowerQuery擴充套件彙整



導入作業流程



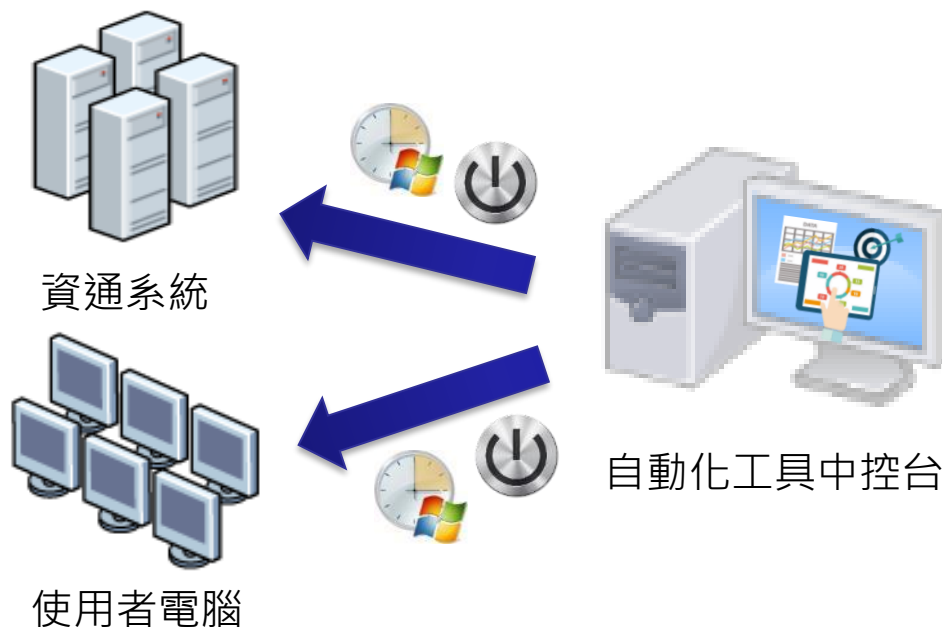
盤點作業流程



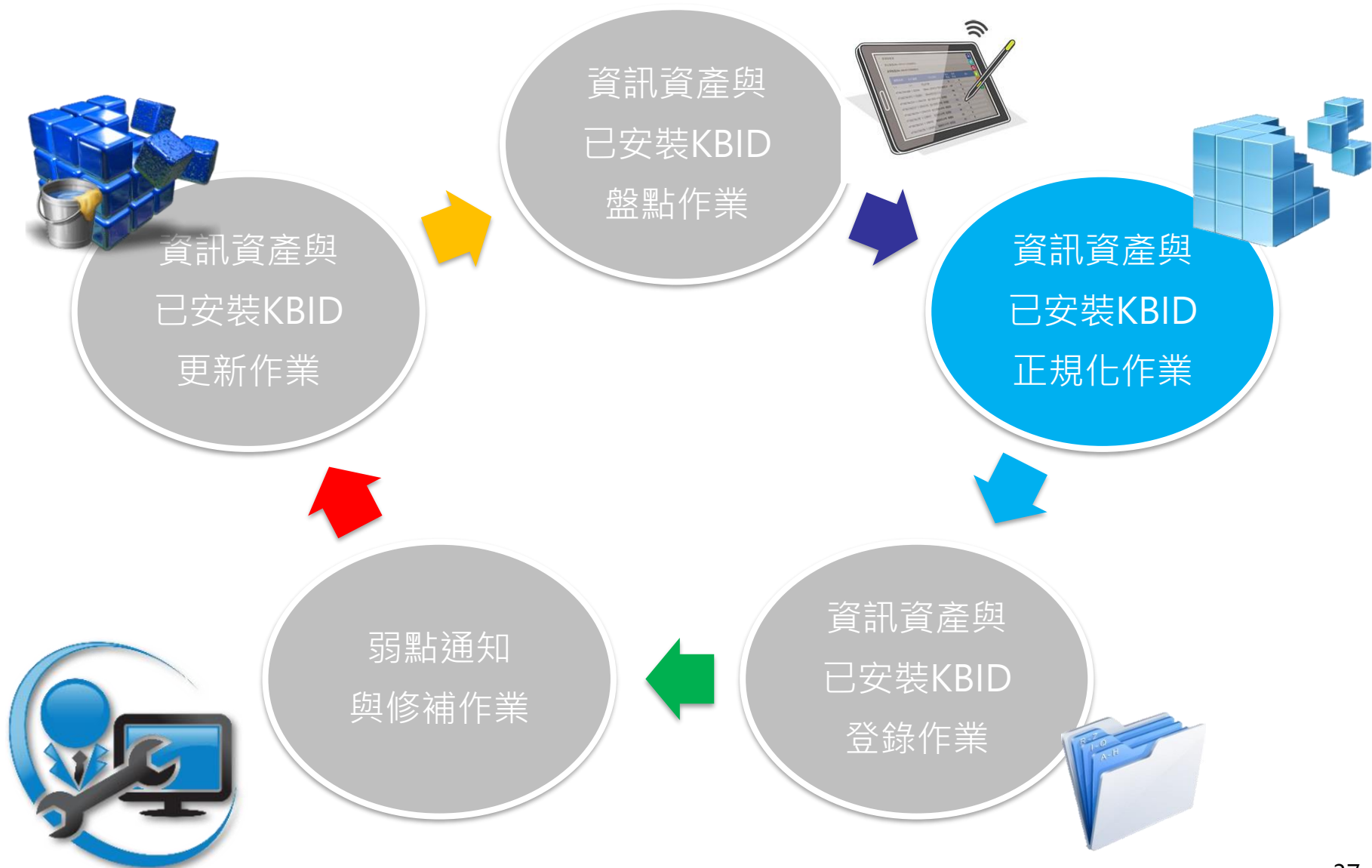
運用自動化工具盤點



- 於資通系統與使用者電腦部署**自動化工具**
- 透過設定排程或指定條件觸發時，進行**資訊資產**
與已安裝KBID盤點



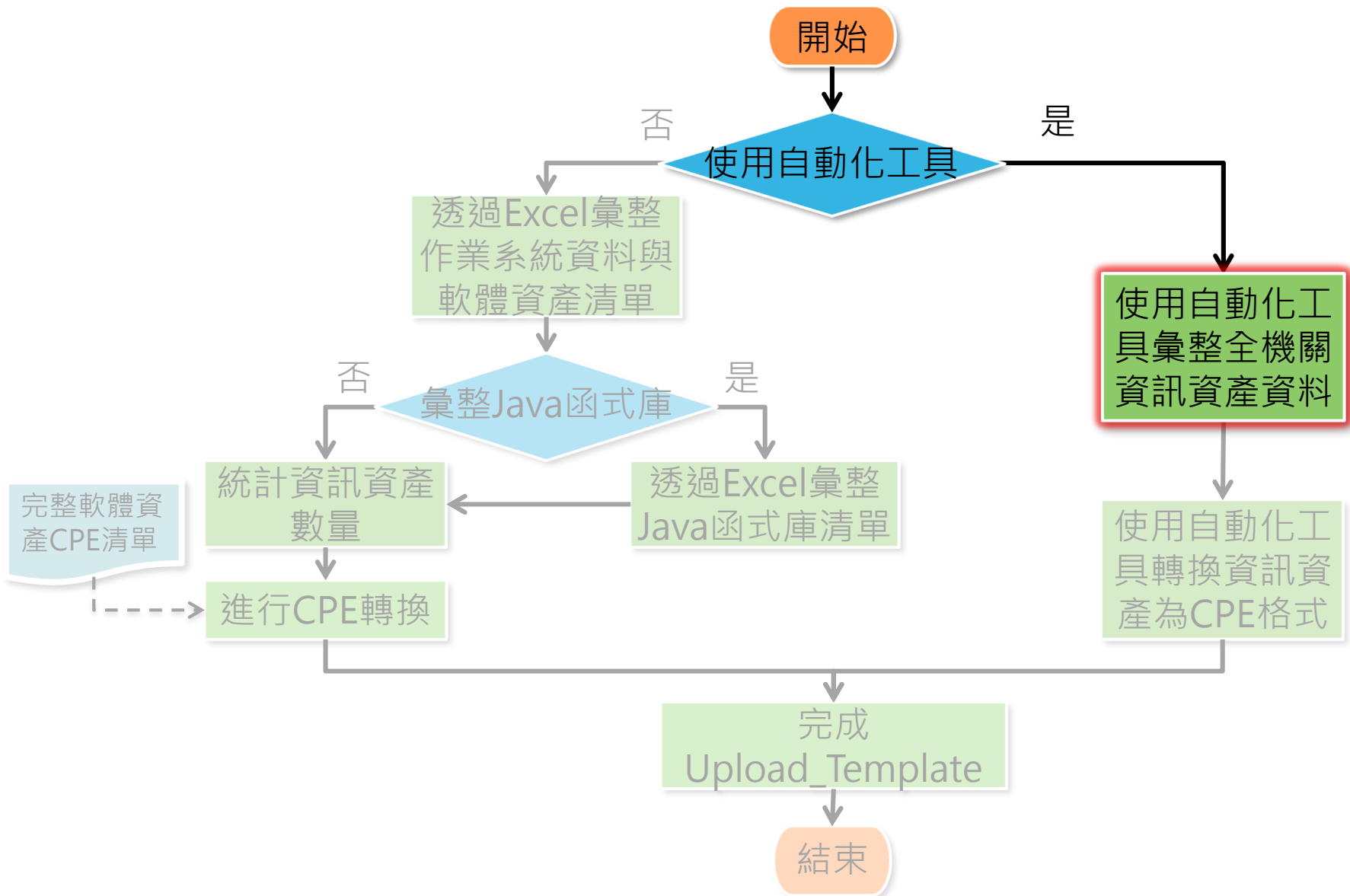
導入作業流程





資訊資產正規化作業流程

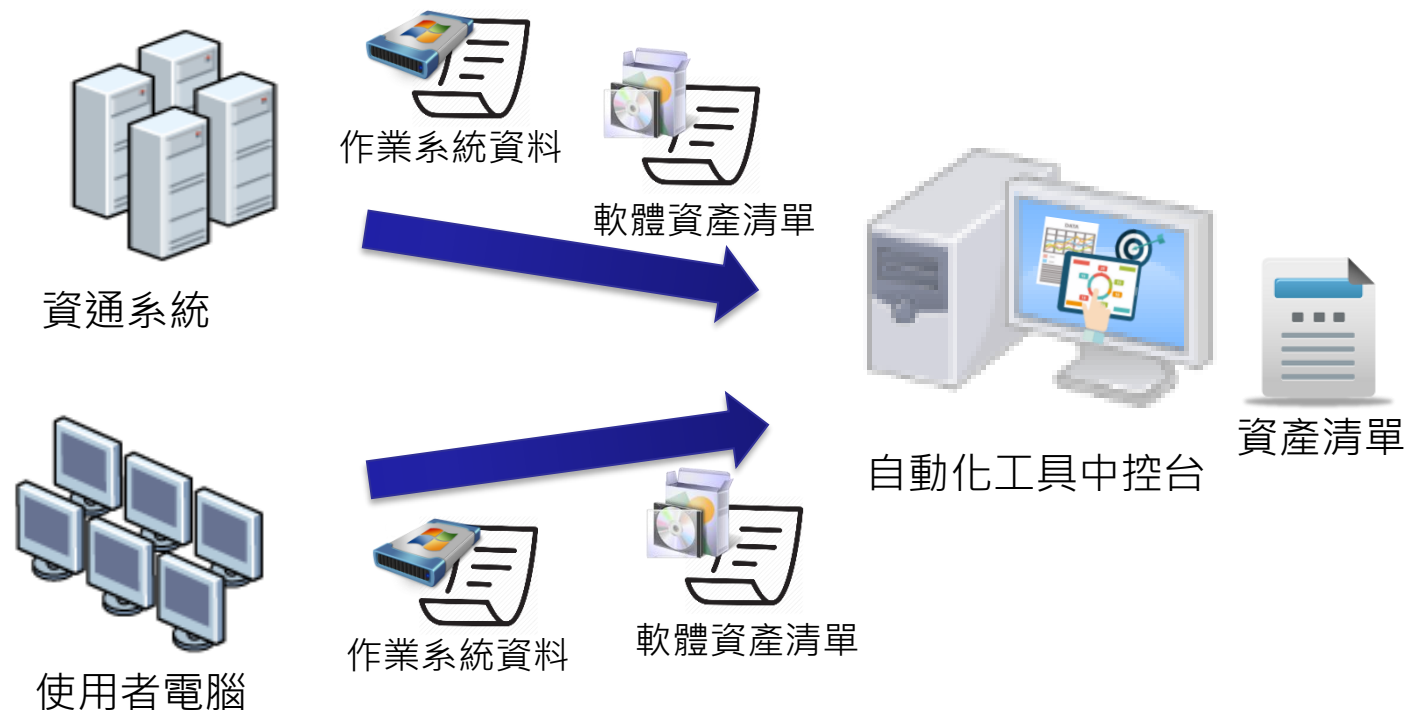
資訊資產正規化作業流程



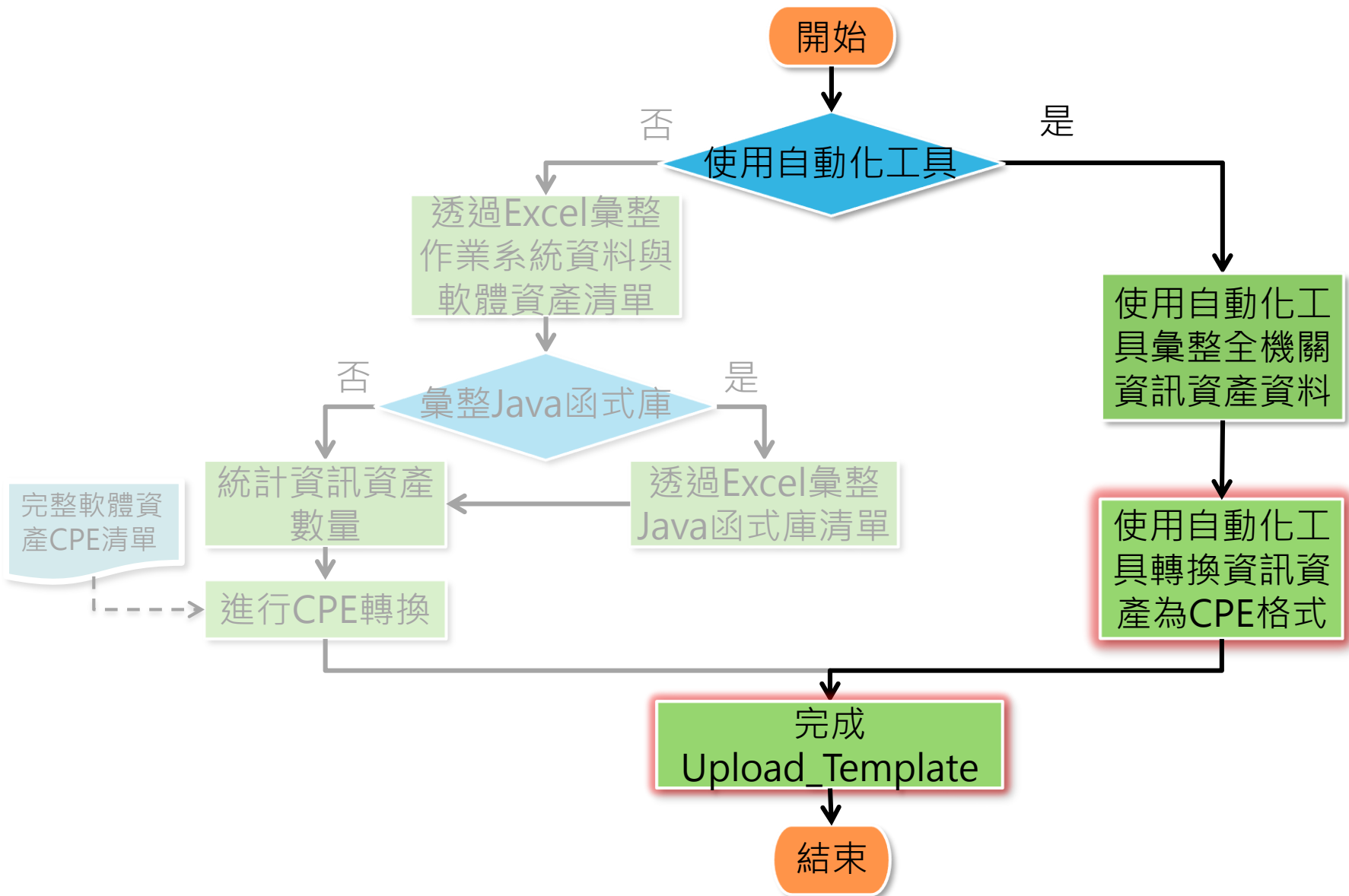
使用自動化工具彙整資訊資產



- 自動蒐集資通系統與使用者電腦作業系統、軟體資產及已安裝KBID等內容
- 自動去識別化整併為全機關資產清單，並提供反查對照功能，便於機關管理資產清單
- 透過排程定時回傳盤點結果予自動化工具中控台



資訊資產正規化作業流程





使用自動化工具轉換資訊資產格式

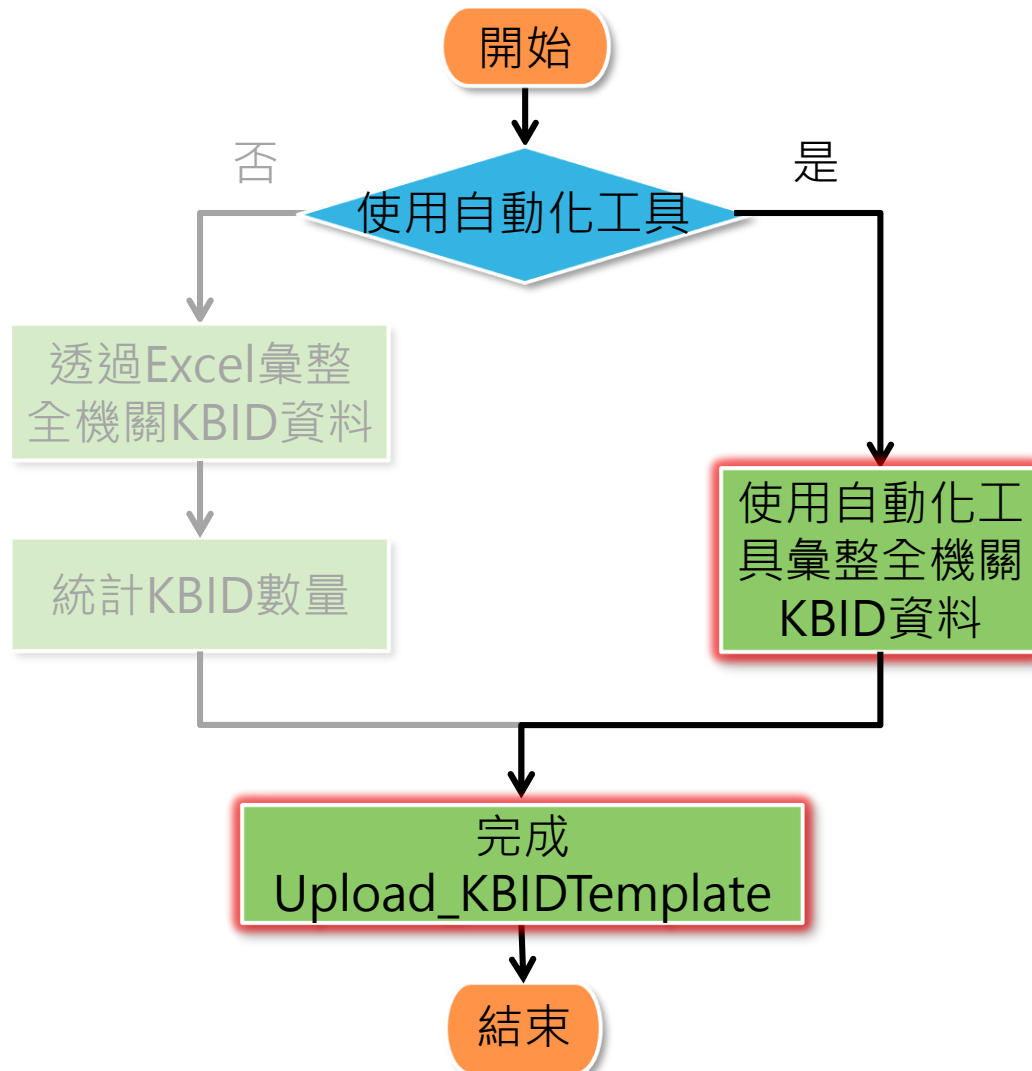
- 自動更新NVD最新CPE條目，並將常見資產格式轉換為CPE格式
- 自動依據VANS系統所需上傳之欄位格式完成 Upload_Template





已安裝KBID正規化作業

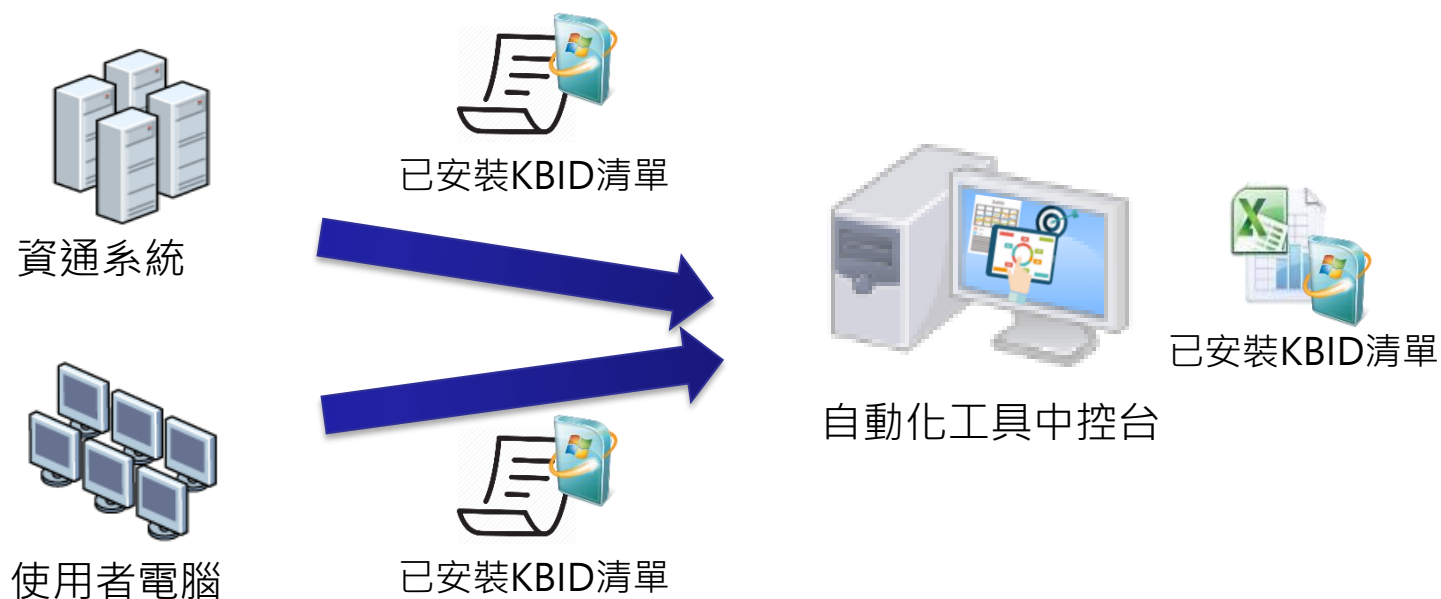
已安裝KBID正規化作業流程



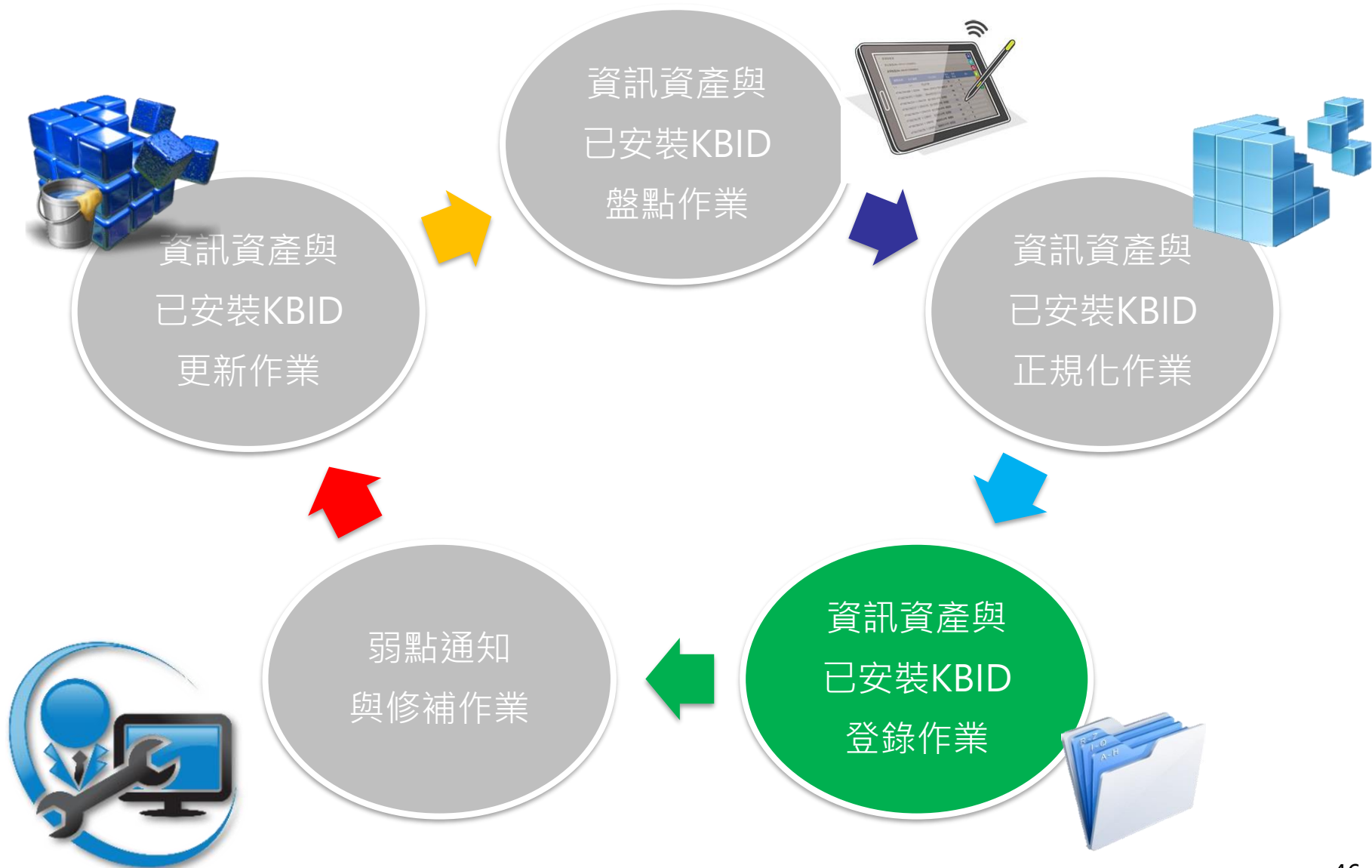
使用自動化工具彙整已安裝KBID



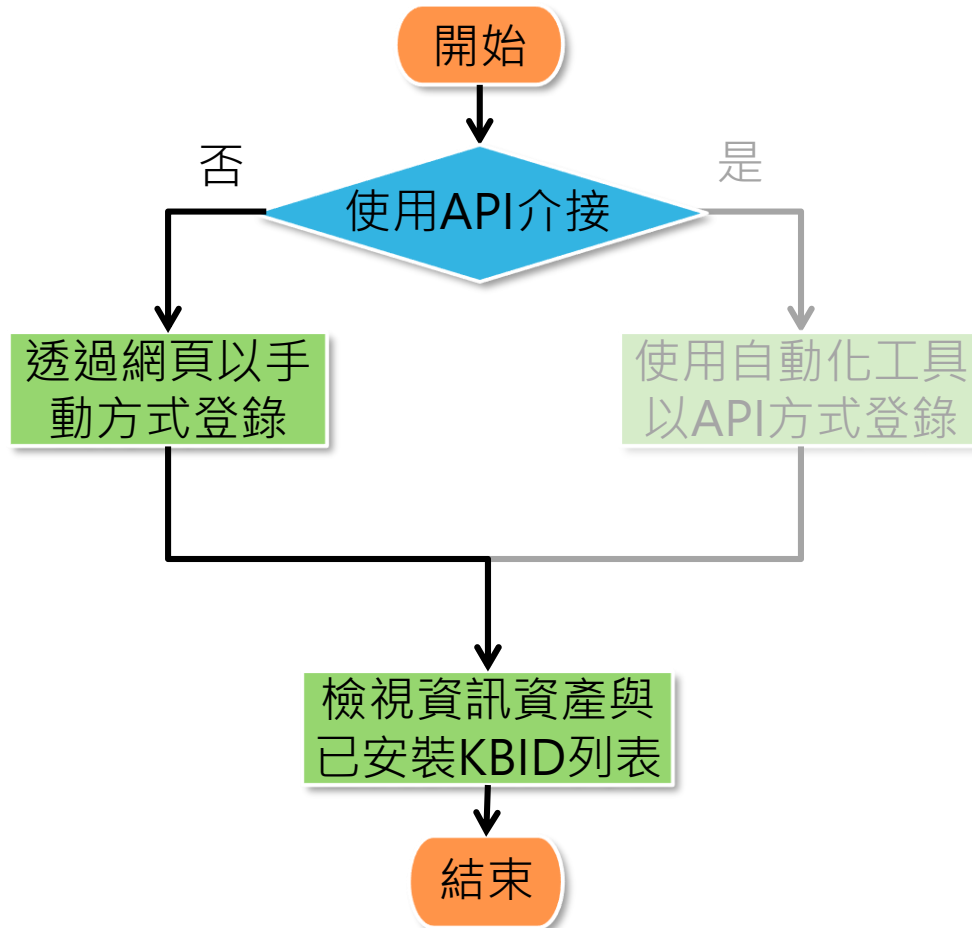
- 自動化蒐集與彙整資通系統與使用者電腦之已安裝KBID
- 透過排程定時回傳盤點結果予自動化工具中控台
- 自動去識別化整併為全機關已安裝KBID清單，並提供反查對照功能，便於機關管理已安裝KBID清單
- 完成已安裝KBID清單



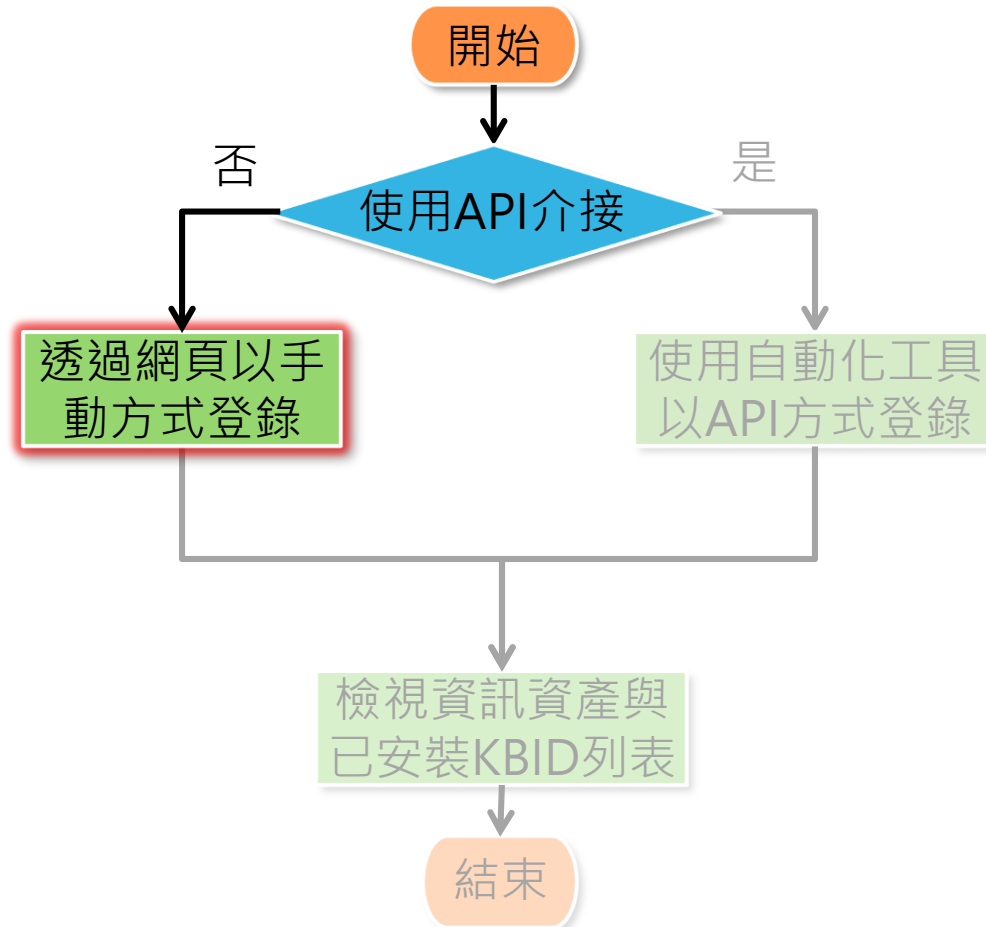
導入作業流程



登錄作業流程



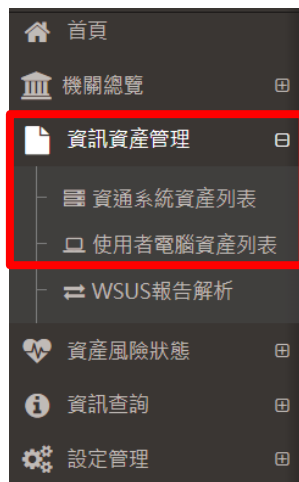
登錄作業流程



網頁登錄-資訊資產(1/2)



- STEP1：於VANS系統點選資產清單上傳
– 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- STEP2：選取已完成之**上傳清單**



網頁登錄-資訊資產(2/2)



- STEP3：點選「上傳」，等待系統解析清單
- STEP4：待收到解析完成通知信，即完成登錄

資訊資產管理 > 資通系統資產列表 > 資產清單上傳

☑ 資產CPE清單上傳

選擇檔案 Upload_Template.xlsx

※使用Excel編輯ods檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。

上傳

上傳清單成功，系統正在解析清單中，解析完成後將會寄發郵件通知

返回列表頁



敬啟者 您好

此為「資通安全弱點通報系統」之通知郵件。

【REDACTED】於 VANS 系統之弱點比對完成，請至 VANS 系統檢視資訊資產風險列表結果。

謝謝。

網頁登錄-已安裝KBID(1/2)



- STEP1：於VANS系統進行已安裝KBID清單上傳
– 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- STEP2：瀏覽並上傳已完成之**上傳清單**

The screenshot illustrates the process of uploading KBID lists in the VANS system. It is divided into two main sections connected by a blue downward arrow.

Top Section: The breadcrumb navigation is "資訊資產管理 > 資通系統資產列表". The main heading is "上傳資通系統已安裝KBID清單". There are three blue buttons: "CPE清單 / 範本下載", "資產 / 已安裝KBID上傳", and "資產清單匯出". Below these, a dropdown menu is open, showing "資訊資產列表" and "已安裝KBID清單上傳" (highlighted with a red box).

Bottom Section: The breadcrumb navigation is "資訊資產管理 > 資通系統資產列表 > 已安裝KBID清單上傳". The main heading is "已安裝KBID清單上傳". There is a red box around the "選擇檔案" (Choose File) button, which has "Upload_KBIDTemplate.xlsx" selected. Below the button, there is a warning message: "※使用Excel編輯ods檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。". An "上傳" (Upload) button is visible at the bottom right.

網頁登錄-已安裝KBID(2/2)



- STEP3：點選「上傳」，等待系統解析請單
- STEP4：待收到解析完成通知信，即完成登錄

資訊資產管理 > 資通系統資產列表 > 已安裝KBID清單上傳

已安裝KBID清單上傳

選擇檔案 Upload_KBIDTemplate.xlsx

※使用Excel編輯ods檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。

上傳

上傳清單成功，系統正在解析清單中，解析完成後將會寄發郵件通知

回列表頁

2023/3/8 (週三) 上午 12:23

V VANS <vans@nics.nat.gov.tw>

測試帳號1使用者電腦已安裝KBID清單解析完成

收件者 [REDACTED]

簽名者 簽章發生錯誤，請按一下簽章按鈕，以取得詳細資訊。

敬啟者 您好

此為「資通安全弱點通報系統」之通知郵件。

[REDACTED] 於 VANS 系統上傳之已安裝 KBID 清單已解析完成，請至 VANS 系統檢視已安裝 KBID 清單登錄結果。

謝謝。

WSUS解析-已安裝KBID(1/3)



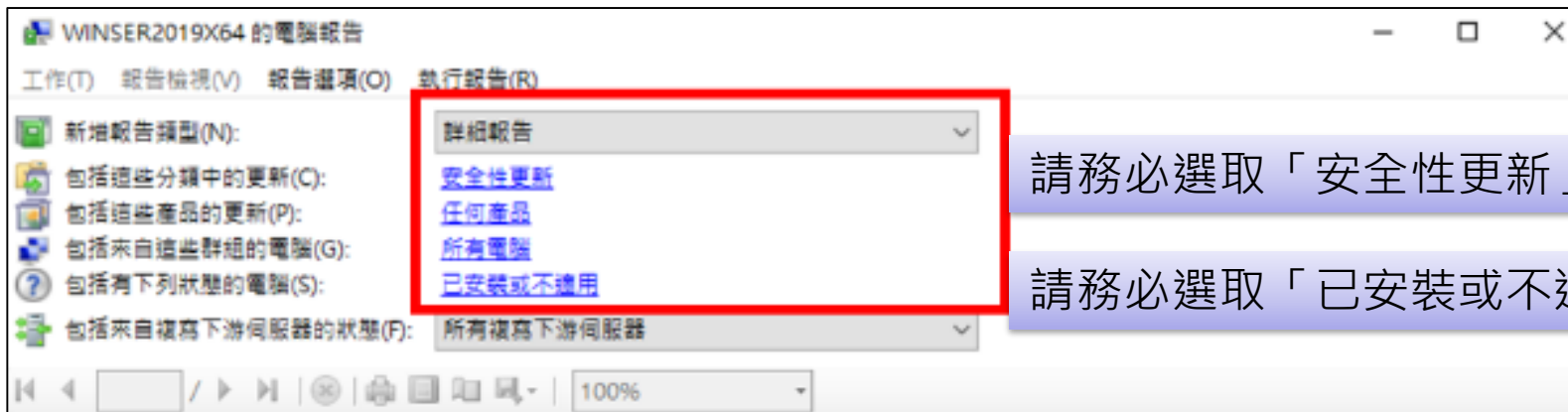
- 透過解析從WSUS匯出之電腦報告，產出已安裝KBID清單，供使用者逕行上傳至資通系統/使用者電腦資產列表
- STEP1：請點選「報告」→選擇「電腦詳細狀態」



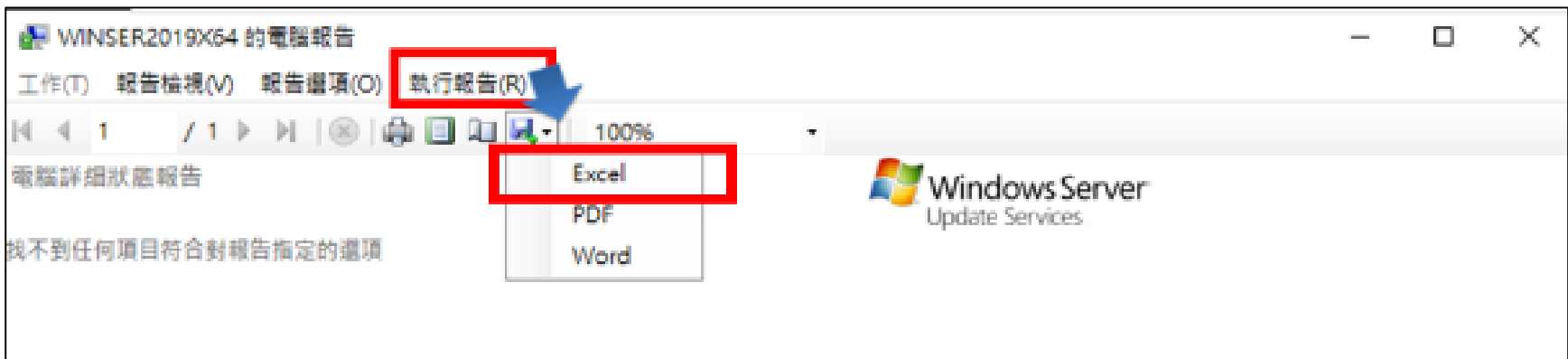
WSUS解析-已安裝KBID(2/3)



- STEP2：WSUS報告-選擇「報告選項」→「詳細報告」，選擇欲上傳解析的產品種類與已安裝的KBID



- STEP3：WSUS報告-選擇「執行報告」→選擇「Excel」



WSUS解析-已安裝KBID(3/3)



- STEP4：於VANS系統中上傳報告進行解析
 - 「資訊資產管理>WSUS報告解析」→「填入機關OID與名稱」→「選擇檔案」→「開始解析」

資訊資產管理 > WSUS報告解析程式

WSUS報告解析程式

機關OID與名稱

請輸入機關OID 請輸入機關名稱

請輸入機關OID 請輸入機關名稱

請選擇WSUS電腦詳細報告檔案(可選擇多份報告)

報告上傳與解析

選擇檔案 未選擇任何檔案

新增上傳欄位

開始解析

報告解析結果與下載

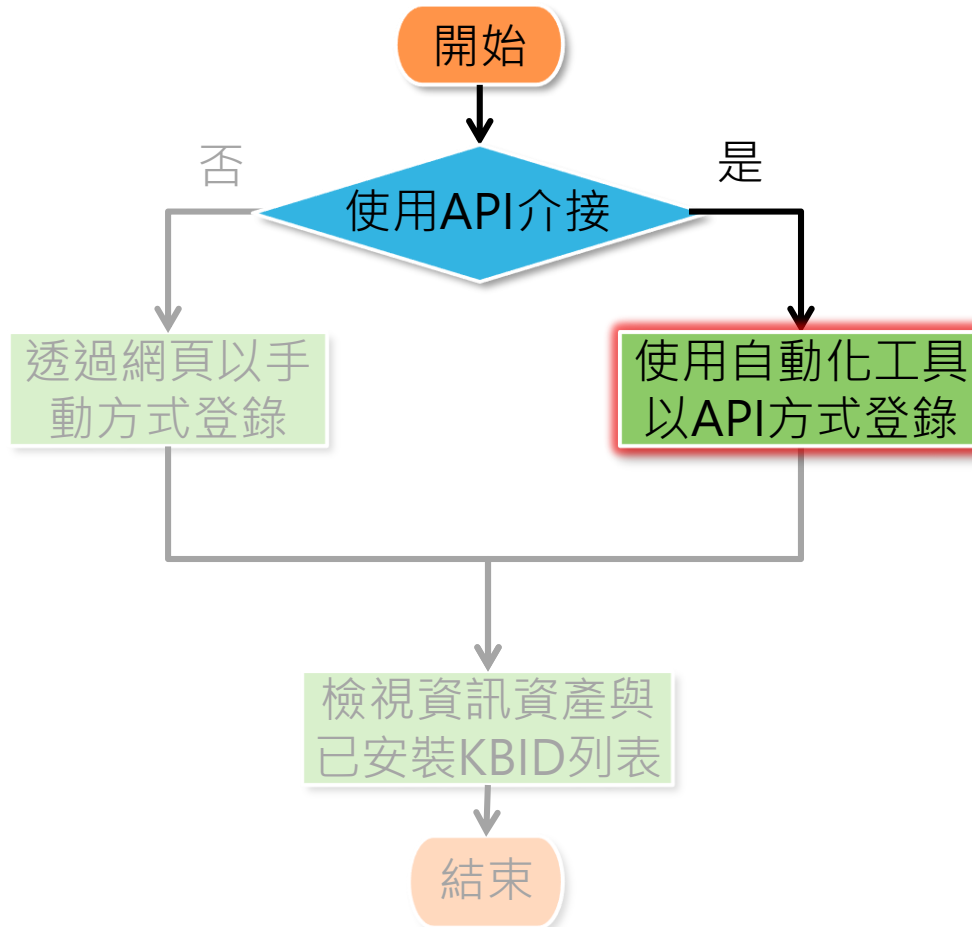
檔案名稱	更新時間	狀態	錯誤訊息
WINSER2019X64 的電腦報告_05076416_名稱修正_test_1669712612460.xlsx	2022-11-29 17:11:35	提供下載	

Showing 1 to 1 of 1 entries

Previous 1 Next

- 透過WSUS派送安全性更新之機關，可運用「WSUS報告解析」功能產出已安裝KBID清單，以降低人工作業時間成本

登錄作業流程



使用自動化工具以API方式登錄(1/3)



- 前置作業申請-於VANS系統申請API Key
 - STEP1：以系統管理者帳號登入VANS系統
 - STEP2：設定管理>資產管理API設定
 - STEP3：點選「重新產生API Key」



使用自動化工具以API方式登錄(2/3)



● 前置作業申請-填寫API介接IP申請單

- STEP1：以系統管理者帳號登入VANS系統
- STEP2：設定管理>資產管理API設定
- STEP3：輸入欲申請之IP，並送出
- STEP4：於VANS專區下載API介接申請表單填寫並核章，完成後提供資安署審核(<https://www.nics.nat.gov.tw/Vans?lang=zh>)

設定管理 > 資產管理API設定

機關資產管理API key

使用以下API key存取系統

🔍 📄

IP設定

請輸入欲申請之IP

📍 ****

送出

已申請IP地址	狀態	刪除
---------	----	----

資通安全弱點通報機制(VANS)

資通安全弱點通報系統(Vulnerability Analysis and Notice System, 簡稱VANS)結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

有任何VANS相關問題，歡迎來信至VansService@nics.nat.gov.tw詢問!

申請作業表單 | 教育訓練教材 | 數位教材影片 | FAQ

帳號申請說明文件
資通安全弱點通報系統(VANS系統)帳號申請說明文件_v1.3_1111222.pdf
【檔案完整性驗證碼SHA256】92b9702986f7d0733233b5bb5fef774afea6b373cc054dcf0a18064fc4ed4625

帳號申請表單
附表-資通安全弱點通報系統(VANS系統)機關管理者帳號申請(異動)單v1.10_1120131.xlsx
【檔案完整性驗證碼SHA256】6e810f2d0953e85b41c41e32b3af7ea37591685ce7ab895f8683e71a6297ba25

API介接申請表單
資通安全弱點通報系統(VANS系統)API介接申請(異動)單v1.9_1111220.xlsx
【檔案完整性驗證碼SHA256】0b46b11b8dfbe72515c19b4d8307143225abfe5aed4f15bd7296ded3bc92e77

使用自動化工具以API方式登錄(3/3)



- 待收到審核結果通知信，說明IP完成開通時，即可使用自動化工具以API方式登錄資訊資產與已安裝KBID

 API Key

 機關資訊

 API傳輸網址



您好:

1.貴單位的 VANS API 介接 IP 已完成開通，可透過 API 方式傳輸資訊資產至 VANS 系統。

2.VANS 系統對外 IP : [REDACTED]

VANS API 傳輸使用 port : [REDACTED]

VANS API 傳輸網址如下：

a. 資訊資產

資源系統(System) :

<https://vans.nat.gov.tw> [REDACTED]

使用者電腦(Computer) :

<https://vans.nat.gov.tw> [REDACTED]

b. 已安裝 KBID

資源系統(System) :

<https://vans.nat.gov.tw> [REDACTED]

使用者電腦(Computer) :

<https://vans.nat.gov.tw> [REDACTED]

3.VANS API 操作說明與 JSON 範例提供如附檔。

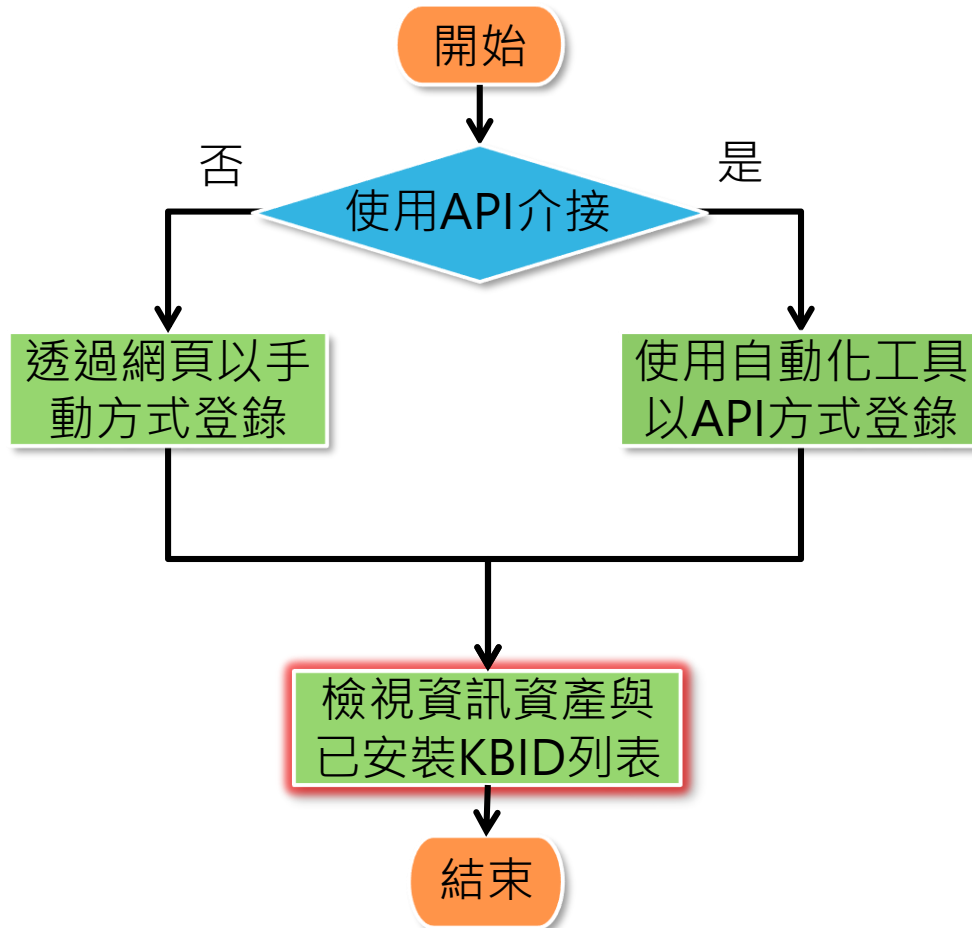
以上說明，謝謝。



VANS系統



登錄作業流程



檢視資訊資產與已安裝KBID列表(1/3)

- 可於**資訊資產管理**查看已登錄之資產項目
 - 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- 點選右邊「**切換至已安裝KBID列表**」可檢視已安裝KBID項目

資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 | 資產 / 已安裝KBID上傳 | 資產清單匯出 | **切換至已安裝KBID列表**

資訊資產列表

資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 | 資產 / 已安裝KBID上傳 | 資產清單匯出 | 切換至資訊資產列表

已安裝KBID列表

新增已安裝KBID

搜尋

KBID	數量	受影響產品名稱	刪除
KB2868626	1	詳細清單	刪除
KB2883200	1	詳細清單	刪除
KB2887595	1	詳細清單	刪除

檢視資訊資產與已安裝KBID列表(2/3)

- 資訊資產與已安裝KBID尚未解析或弱點尚未比對完成，暫不提供上傳功能



進行資訊資產解析與弱點比對時，暫不提供資產上傳功能



進行已安裝KBID解析與KBID串聯時，暫不提供已安裝KBID上傳功能



檢視資訊資產與已安裝KBID列表(3/3)

- 上傳資訊資產或已安裝KBID後，若資產列表或已安裝KBID列表仍無資料或尚未更新，且未出現解析中之狀態列，請確認接收通知之電子信箱是否設定正確，並檢視郵件內文之解析失敗原因

敬啟者 您好

此為「資通安全弱點通報系統」之通知郵件。

【】於 VANS 系統所上傳之資訊資產清單解析失敗，失敗原因如下：

=====

清單含錯誤 cpe 資料，軟體資產清單分頁中的第 1142 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 1470 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 1527 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 1758 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 2047 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 3500 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 3513 行
清單含錯誤 cpe 資料，軟體資產清單分頁中的第 4182 行

=====

請修正後再次上傳，謝謝。

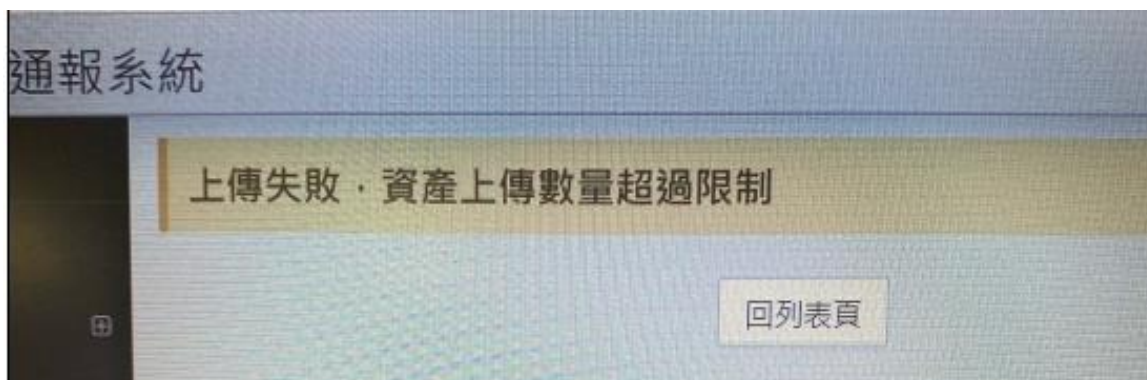
上傳失敗案例與解決方式(1/4)

- 若遭遇VANS系統使用上之問題，建議以下列格式來信 (VansService@nics.nat.gov.tw)信箱詢問，以加快處理速度
- 格式如下
 - 1.機關名稱：
 - 2.上傳方式：
 - 3.上傳使用檔案：
 - 4.上傳時間：
 - 5.錯誤訊息截圖：
 - 6.補充說明：

上傳失敗案例與解決方式(2/4)

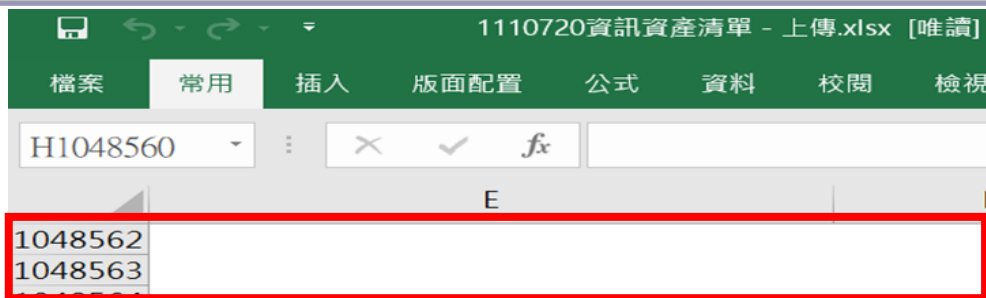


案例1.透過網頁登錄資訊資產時，出現「上傳失敗，資產上傳數量超過限制」錯誤訊息，該如何處理？



Suggestions

- 錯誤原因：上傳Excel檔案格式內含多行空白，導致超出系統10萬筆上限限制
- 建議作法：上傳前檢查並刪除空白列



上傳失敗案例與解決方式(3/4)



案例2. 透過網頁上傳已安裝KBID後，收到解析失敗通知信時，該如何處理？

敬啟者 您好

此為「資通安全弱點通報系統」之通知郵件。

[REDACTED] 於 VANS 系統所上傳之已安裝 KBID 清單解析失敗，失敗原因如下：

=====
清單含錯誤 KBID 資料，已安裝 KBID 清單-1 分頁中的第 564 行
=====

請修正後再次上傳，謝謝。



Suggestions

- 上傳前請檢查KBID清單是否符合下列格式要求：
 - 已安裝KBID數量：純數字
 - 已安裝KBID：KB+純數字

	C	D
1	已安裝KBID數量	已安裝KBID
564	2	2007 MICROSOFT OFFICE SUITE SERVICE PACK 3 (SP3)

上傳失敗案例與解決方式(4/4)



案例3. 使用相同資料來源轉換成不同格式，可成功透過網頁以Excel方式上傳，但透過API方式上傳出現「0406」錯誤訊息，該如何解決？

```
1 {
2   "Message": "A-PC-0406",
3   "Describe": "發生非預期錯誤"
4 }
```



Suggestions

- 上傳前可檢查有無跳脫字元，若有，請於跳脫字元前額外增加一個反斜線，以利系統識別與解析

錯誤寫法：" product_vendor": "Software AG Products: C:\SoftwareAG

正確寫法："product_vendor": "Software AG Products: C:\\SoftwareAG

```
2842 {
2843   "oid": "2.16.886. [REDACTED]",
2844   "unit_name": [REDACTED],
2845   "asset_number": "1",
2846   "product_name": "Google\Chrome",
2847   "product_vendor": "Chrome 雲端桌面",
2848   "product_version": "1.0",
2849   "category": "Software",
2850   "cpe23": "N/A",
2851   "product_cpename": "N/A"
2852 },
```



實作練習1

實作練習1(環境說明)



● VANS系統_實作站

– 登入資訊

- 網址：已儲存於瀏覽器
「我的最愛列」
- 帳號：student01~45
- 密碼：1111

– 機關資訊

- 機關OID：student01~45
- 機關名稱：student01~45

資通安全弱點通報系統 (VANS)

公告

- 為提升安全性，本系統已將HTTPS加密等級提升至TLS 1.1以上，再請留意瀏覽器需支援TLS 1.1以上方可瀏覽本系統，謝謝。
- 因應網域名稱調整事宜，「資通安全弱點通報系統」已完成憑證更換，並將網址由「https://vans.nccst.nat.gov.tw/」調整為「https://vans.nat.gov.tw/」，API網址亦同步進行調整，後續請使用新網址進行連線與傳輸。

聯絡資訊如下：
系統登入與操作系統異常相關問題：
國家資通安全研究院
服務電話：(02)6631-6423
服務信箱：VansService@nics.nat.gov.tw

機關管理者帳號審核與業務相關問題：
數位發展部資通安全署 吳忠家先生
服務電話：(02)3356-8067
服務信箱：zhonggia@acs.gov.tw

實作練習1(1/2)



- 請以「實作練習1」提供之Upload_Template與Upload_KBIDTemplate執行登錄作業
- 本項練習時間**10分鐘**

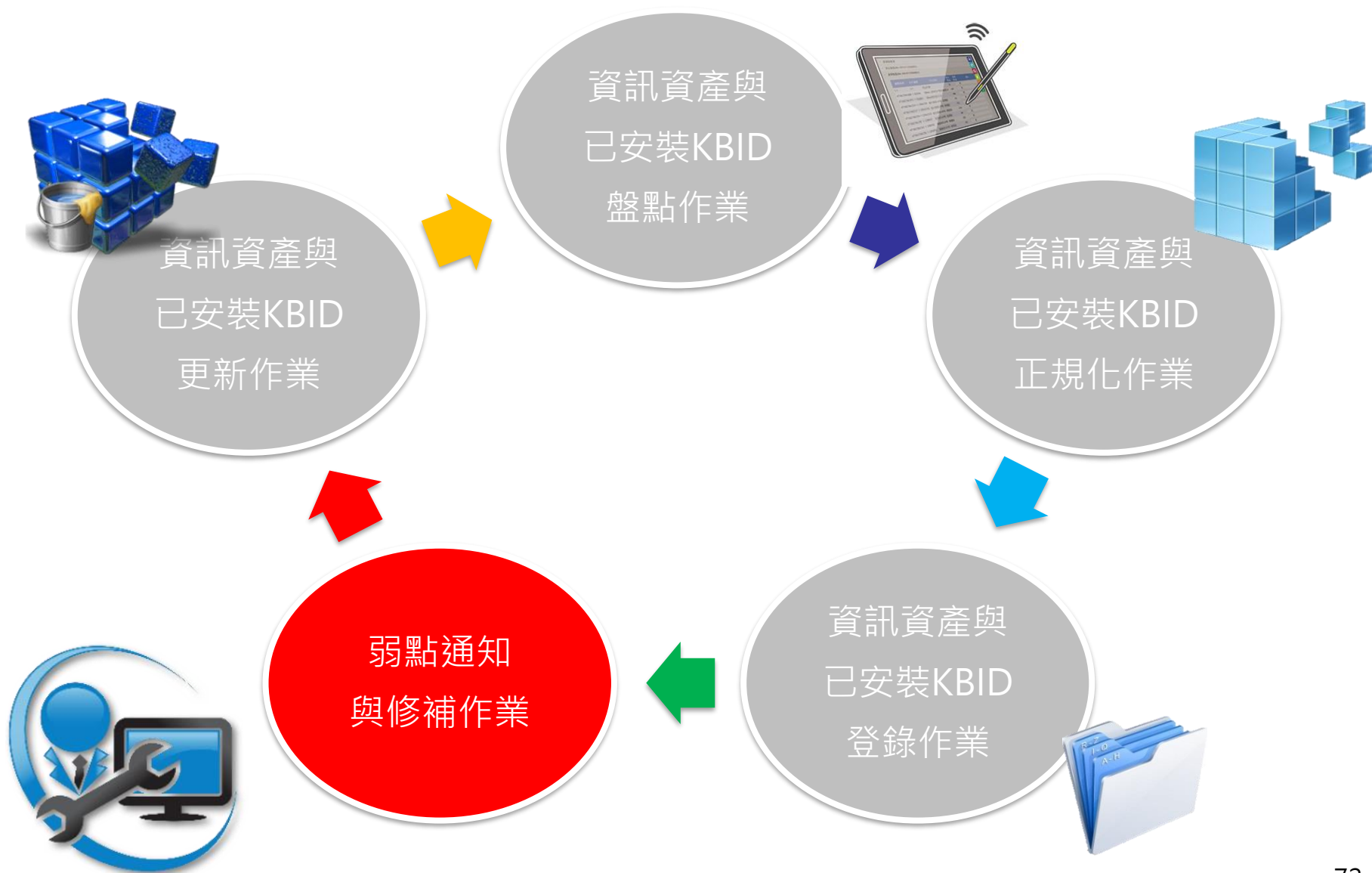
項次	執行項目	產出項目/執行結果												
1	<p>進行通知設定</p> <ul style="list-style-type: none">● 通知設定：ON● 分數設定：4.0● 電子郵件設定：欲接收通知之電子郵件	<p>檢視設定接收通知之信箱</p> <p>資通安全弱點通報系統</p> <table border="1"><caption>CVSS v3.0 Ratings</caption><thead><tr><th>Severity</th><th>Base Score Range</th></tr></thead><tbody><tr><td>None</td><td>0.0</td></tr><tr><td>Low</td><td>0.1-3.9</td></tr><tr><td>Medium</td><td>4.0-6.9</td></tr><tr><td>High</td><td>7.0-8.9</td></tr><tr><td>Critical</td><td>9.0-10.0</td></tr></tbody></table>	Severity	Base Score Range	None	0.0	Low	0.1-3.9	Medium	4.0-6.9	High	7.0-8.9	Critical	9.0-10.0
Severity	Base Score Range													
None	0.0													
Low	0.1-3.9													
Medium	4.0-6.9													
High	7.0-8.9													
Critical	9.0-10.0													

實作練習1(2/2)

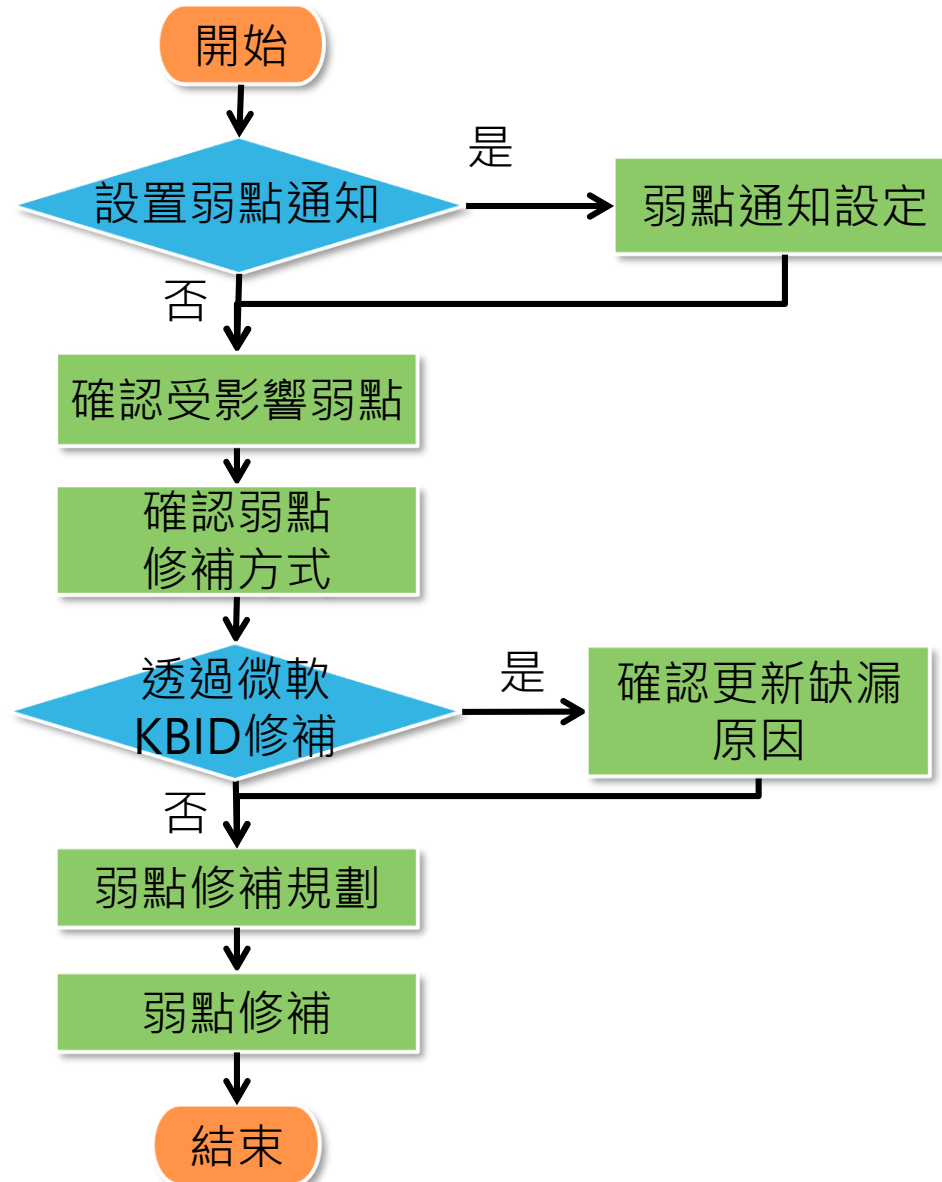


項次	執行項目	產出項目/執行結果
2	開啟Upload_Template (路徑：學員資料夾\01.實作練習\實作練習1\Upload_Template.xlsx) <ul style="list-style-type: none">填寫機關OID與機關名稱完成Upload_Template	Upload_Template.xlsx
3	開啟KBID上傳清單 (路徑：學員資料夾\01.實作練習\實作練習1\Upload_KBIDTemplate.xlsx) <ul style="list-style-type: none">填寫機關OID與機關名稱完成KBID上傳清單	Upload_KBIDTemplate.xlsx
4	上傳Upload_Template至VANS系統	於資產列表檢視登錄結果
5	上傳Upload_KBIDTemplate至VANS系統	於已安裝KBID列表檢視登錄結果

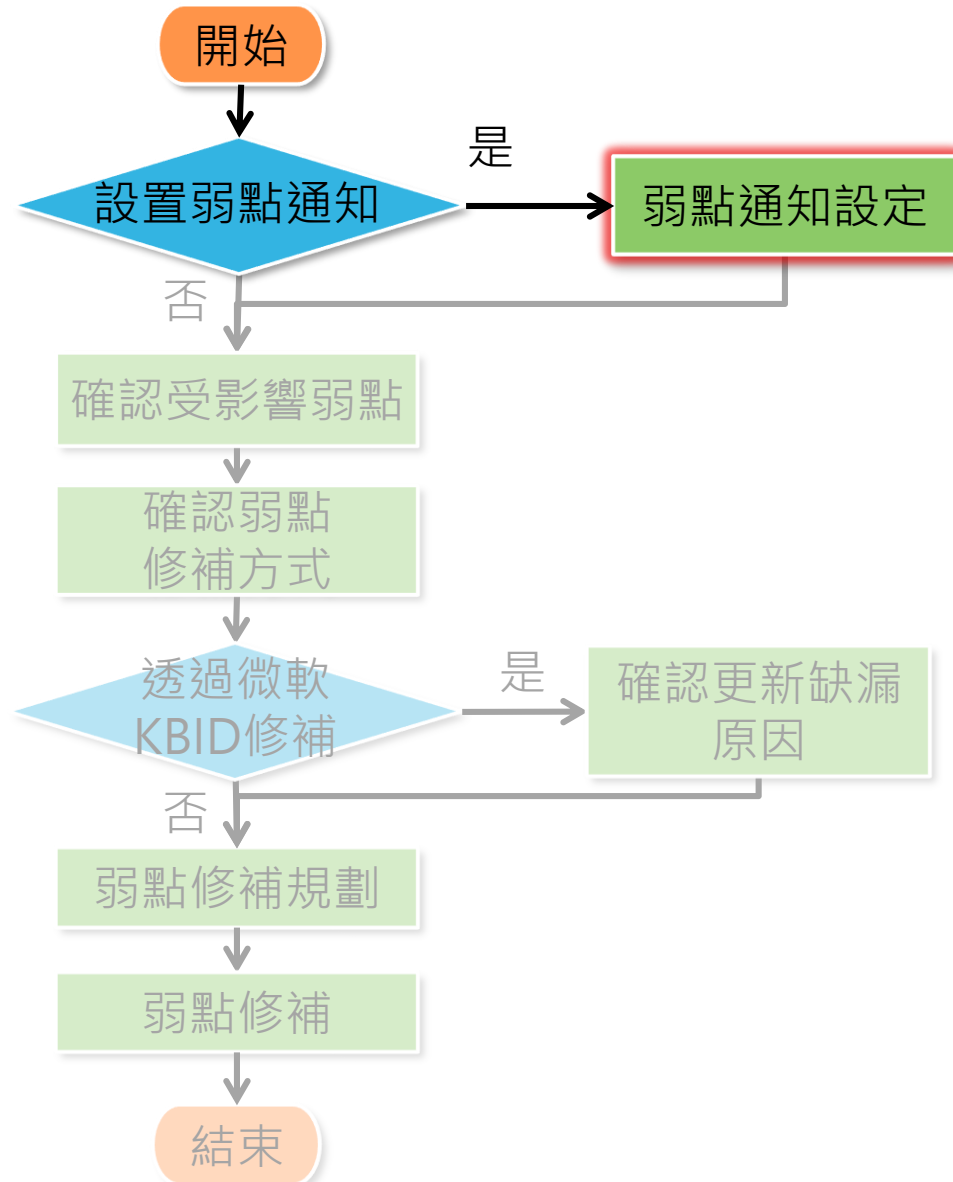
導入作業流程



弱點通知與修補規劃作業流程



弱點通知與修補規劃作業流程



弱點通知設定(1/3)



- 首次登入VANS系統，需先進行弱點通知設定
 - 弱點通知設定包含通知開關、CVSS分數門檻及接收通知Email

弱點通知設定(2/3)



- 後續變更弱點通知設定，可於通知設定調整
 - 設定管理 > 通知設定

設定管理 > 通知設定

弱點通知之分數設定

請輸入欲接收弱點通知之分數

調整設定CVSS分數門檻

設為預設值 設定

弱點通知之電子郵件設定

請輸入欲接收弱點通知之電子郵件

設定接收通知Email

新增電子郵件欄位 設定

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

可參考ISMS弱點修復基準
設置CVSS分數門檻

通知設定

請選擇是否接收弱點通知

ON

通知開關

設定

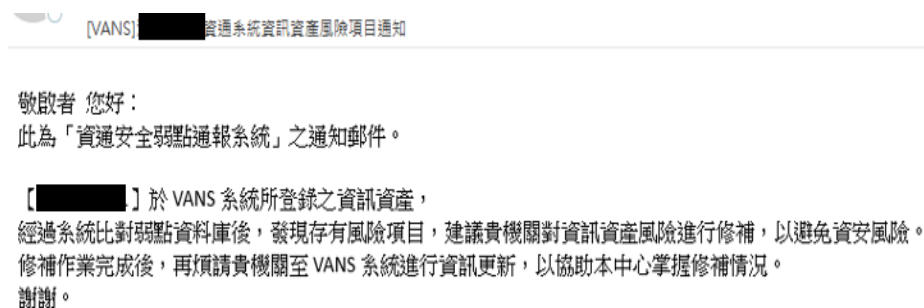
弱點通知設定(3/3)



- 資訊資產與NVD弱點資料庫自動比對後，若有開啟弱點通知功能，VANS系統將於比對出高於CVSS分數門檻之弱點時寄送通知信

– 寄送通知信予**接收通知Email**

– 於VANS系統上顯示**弱點比對通知**



- 同一項資產的同一個弱點只會於**首次比對到時進行1次通知**，之後**不會再出現相同之弱點通知**

資產風險狀態 > 資通系統資產風險狀態 > 弱點比對通知

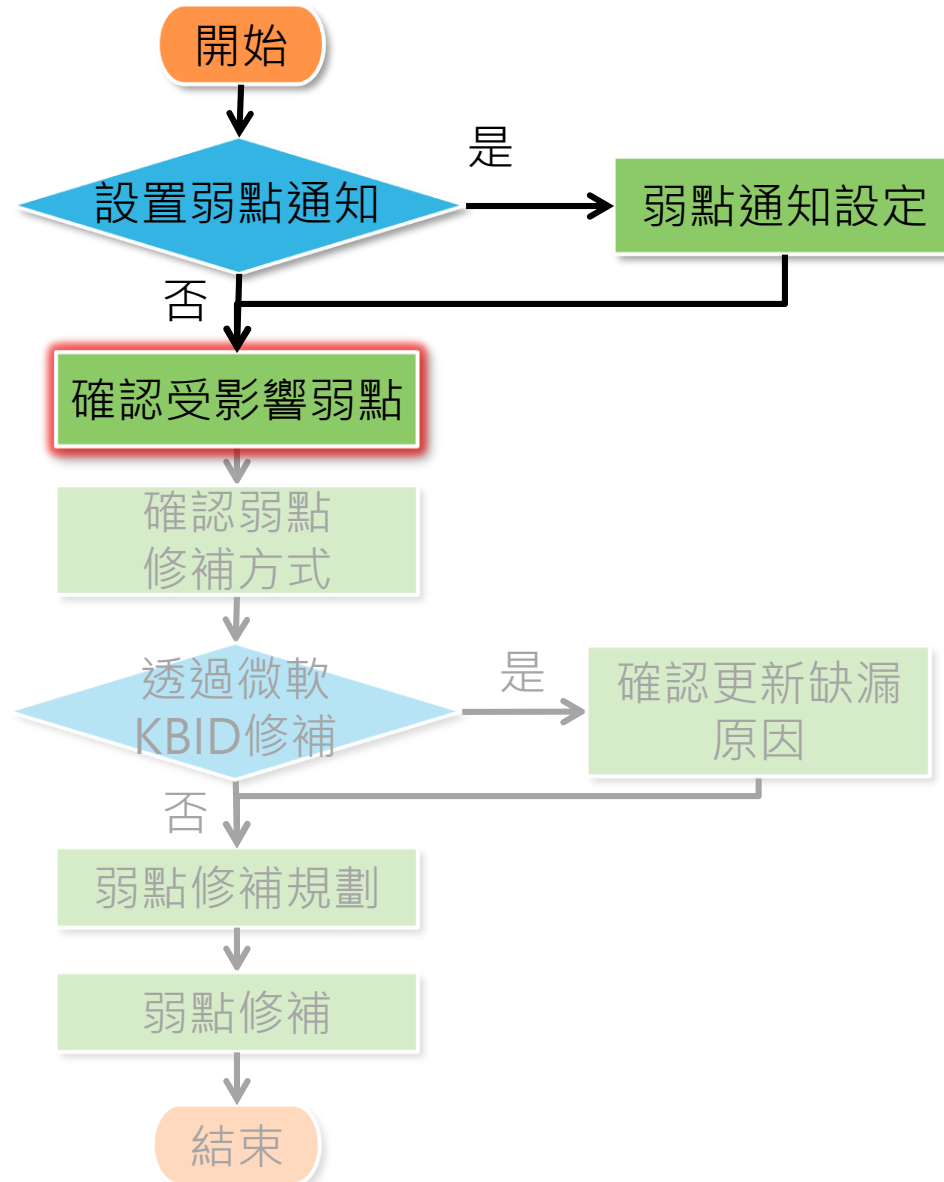
弱點通知列表

通知時間	資產數量	弱點數量	詳細資訊	通知顯示	匯出勾選弱點通知
2019-11-17 00:37:17	1	171	開啟	ON	<input type="checkbox"/>
2019-11-08 16:39:21	28	456	開啟	ON	<input type="checkbox"/>

Showing 1 to 2 of 2 entries

Previous 1 Next

弱點通知與修補規劃作業流程



確認受影響弱點-資訊資產風險列表



● 於資訊資產風險列表，檢視各資訊資產存在之弱點

– 資產風險狀態 > 資通系統風險狀態/使用者電腦風險狀態 > 資訊資產風險列表

Home 首頁
Institution Overview 機關總覽
Information Asset Management 資訊資產管理
Asset Risk Status 資產風險狀態
Communication System Risk Status 資通系統風險狀態
Information Asset Risk List 資訊資產風險列表
Weakness Correlation List 弱點關聯列表
Weakness Comparison Notification 弱點比對通知
Weakness Handling Status Report 弱點處理情形回報
User Computer Risk Status 使用者電腦風險狀態
Information Query 資訊查詢
Setting Management 設定管理

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

Download Weakness List 下載弱點清單 | Upload Weakness Improvement Measures 上傳弱點改善措施

全部 | 資安院

資訊

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*****	1	7.50	2	2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*****	1	7.50	1	1	詳細資訊

Apache

詳細資訊

填寫勾選改善措施 | 全部勾選 | 全部取消

	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input type="checkbox"/>	CVE-2014-0114	7.5	2014-04-30 18:49:00	2021-01-27 02:15:00	填寫改善措施

顯示第 1 到第 2 項記錄，共 2 項記錄

關閉

確認受影響弱點-弱點關聯列表

- 若欲查詢特定弱點，透過弱點關聯列表搜尋CVE編號或查詢弱點爆發時間區間，以確認受影響之資訊資產與範圍
 - 資產風險狀態 > 資通系統風險狀態/使用者電腦風險狀態 > 弱點關聯列表



The screenshot displays the 'Weakness Correlation List' (弱點關聯列表) interface within the ISI Asset Risk Management System. The breadcrumb path is 'Asset Risk Status > Information System Risk Status > Weakness Correlation List'. The system is identified as '資安院' (National Cyber Security Agency).

The search criteria are set to 'Please enter CVE number' (請輸入CVE編號) with a search button. The start time (起始時間) is 2021-07-01 and the end time (結束時間) is 2021-09-01, both with search buttons.

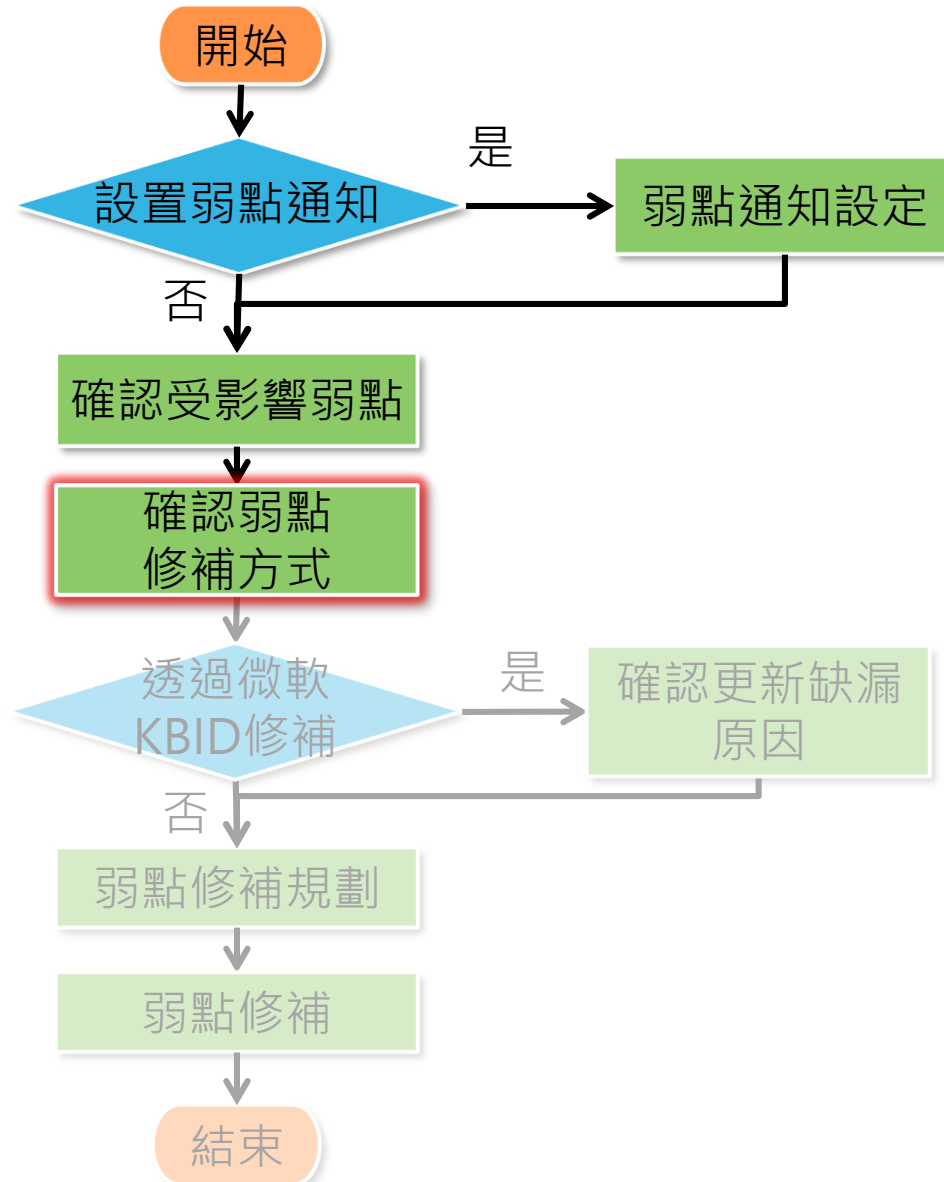
The main content area shows a list of vulnerabilities. The first entry is CVE-2021-34510, with a CVSS Score of 4.6, published on 2021-07-15 02:15:00, and updated on 2021-08-19 01:08:00. A search bar and a menu icon are located above the table.

影響資產名稱	影響資產廠商	影響資產版本	影響CPE2.3	比對時間
Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:datacenter:*x64:*	2021-08-18 05:03:28

顯示第 1 到第 1 項記錄，總共 1 項記錄

The second entry is CVE-2021-30640, with a CVSS Score of 6.4, published on 2021-07-12 11:15:00, and updated on 2021-08-10 11:08:00.

弱點通知與修補規劃作業流程



確認弱點修補方式(1/4)



- 可至NVD官網確認弱點修補方式
- 以資訊資產風險列表為例，點選「詳細資訊」檢視JDK 1.8.0 Update 202之弱點資訊

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

下載弱點清單 上傳弱點改善措施 全部 資安院

資訊

搜尋

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:****:*	1	7.50	2	2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:****:*	1	7.50	1	1	詳細資訊
Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8	cpe:2.3:a:oracle:jdk:1.8.0:update202:****:*	1	7.00	34	34	詳細資訊
Microsoft Office 專業增強版 2019 - zh-tw	Microsoft Corporation	16.0.14228.20250	cpe:2.3:a:microsoft:office:2019:****:~:*	1	7.10	184	184	詳細資訊

確認弱點修補方式(2/4)



- 點選弱點編號，可查看弱點描述與相關連結

詳細資訊

CVE編號	CVSS	發布時間	更新時間	改善措施	填寫勾選改善措施	全選
CVE-2014-0429	10	2014-04-16 08:55:00	2018-01-05 10:29:00	填寫改善措施	<input type="checkbox"/>	
CVE-2014-0432						
CVE-2014-0446						



CVE資訊

[查看弱點描述](#) 關閉

CVE-2014-0429 NVD-CWE-noinfo

Summary Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.

[NVD官網弱點說明連結](#) <https://nvd.nist.gov/vuln/detail/CVE-2014-0429> [查看NVD官網說明](#)

CVSS Score: 10

Access Vector

AccessComplexity: LOW

AccessVector: NETWORK

Authentication: NONE

確認弱點修補方式(3/4)



- 參閱NVD官網建議弱點修補方式

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698	
http://marc.info/?l=bugtraq&m=140852974709252&w=2	
http://rhn.redhat.com/errata/RHSA-2014-0675.html	
http://rhn.redhat.com/errata/RHSA-2014-0685.html	
http://security.gentoo.org/glsa/glsa-201406-32.xml	
http://security.gentoo.org/glsa/glsa-201502-12.xml	
http://www.debian.org/security/2014/dsa-2912	原廠說明連結
http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html	Vendor Advisory
http://www.securityfocus.com/bid/66856	

確認弱點修補方式(4/4)



- 透過弱點詳細資訊中的連結，查閱原廠或相關廠商建議弱點修補方式

Security vulnerabilities are scored using CVSS version 2.0 (see [Oracle CVSS Scoring](#) for an explanation of how Oracle applies CVSS 2.0). Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update (CPU). Oracle does not disclose information about the security analysis, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see [Oracle vulnerability disclosure policies](#).

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply CPU fixes as soon as possible. Until you apply the CPU fixes, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

Oracle strongly recommends that customers apply security fixes as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security fixes announced in this CPU, please review [previous Critical Patch Update advisories](#) to determine appropriate actions.

Product Dependencies

Oracle products may have dependencies on other Oracle products. Hence security vulnerability fixes announced in this Critical Patch Update may affect one or more dependent Oracle products. For details regarding these dependencies and how to apply patches to dependent products, please refer to Patch Set Update and Critical Patch Update April 2014 Availability Document, [My Oracle Support Note 1618213.1](#).

確認弱點修補方式-微軟類



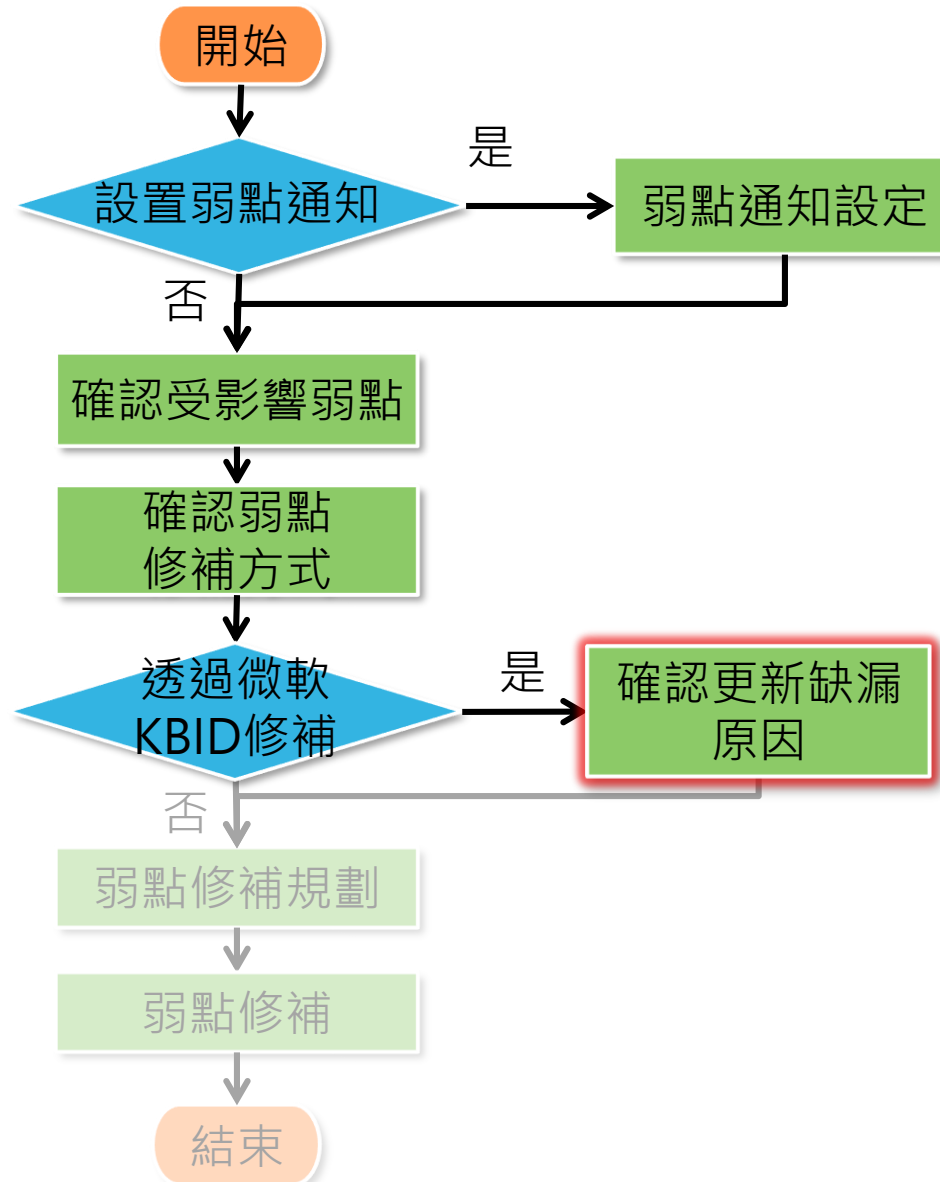
- 微軟類之CVE，可透過詳細資訊中的「查看修補KBID」欄位
 - 呈現已安裝KBID(分子)與應安裝KBID數量(分母)
 - 紅色為尚有缺漏KBID，綠色為已安裝足量之KBID
 - 點選可檢視修補該弱點之KBID

The screenshot displays a web interface for CVE management. The top section, titled '詳細資訊' (Detailed Information), shows a table with columns for CVE ID, CVSS, release time, update time, mitigation status, and '查看修補KBID' (View KBID). The row for CVE-2020-0646 shows a mitigation status of '填寫改善措施' (Fill in improvement measures) and a '查看修補KBID' of '0/30', where '0' is highlighted in red. Below this, a 'KBID資訊' (KBID Information) section shows a table with columns for KBID, quantity, and affected product name. The row for KB4532935 shows a quantity of 0 and a '詳細清單' (Detailed List) button, which is highlighted in red. A tooltip for KB4532935 lists affected products: 'Microsoft .NET Framework 4.8 on Windows Server 2016' and 'Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)'. Blue arrows indicate the flow from the '查看修補KBID' field to the 'KBID資訊' section and then to the '詳細清單' button.

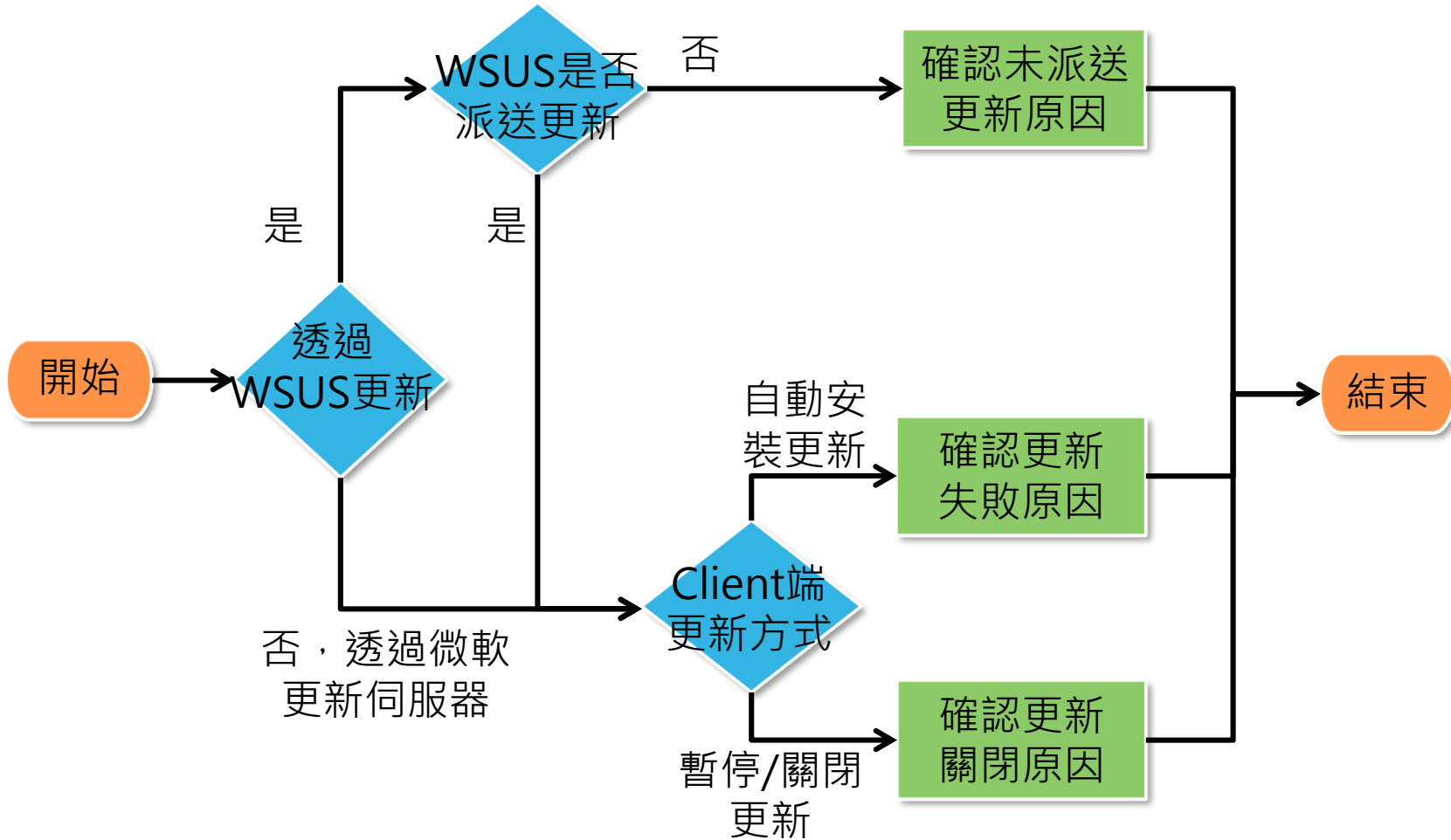
CVE編號	CVSS	發佈時間	更新時間	改善措施	查看修補KBID
CVE-2020-0646	10	2020-01-15 07:15:00	2020-03-27 01:15:00	填寫改善措施	0/30

KBID	數量	受影響產品名稱
KB4532933	0	詳細清單
KB4532935	0	Microsoft .NET Framework 4.8 on Windows Server 2016 Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)
KB4532936	0	詳細清單
KB4532938	0	詳細清單
KB4534976	0	詳細清單

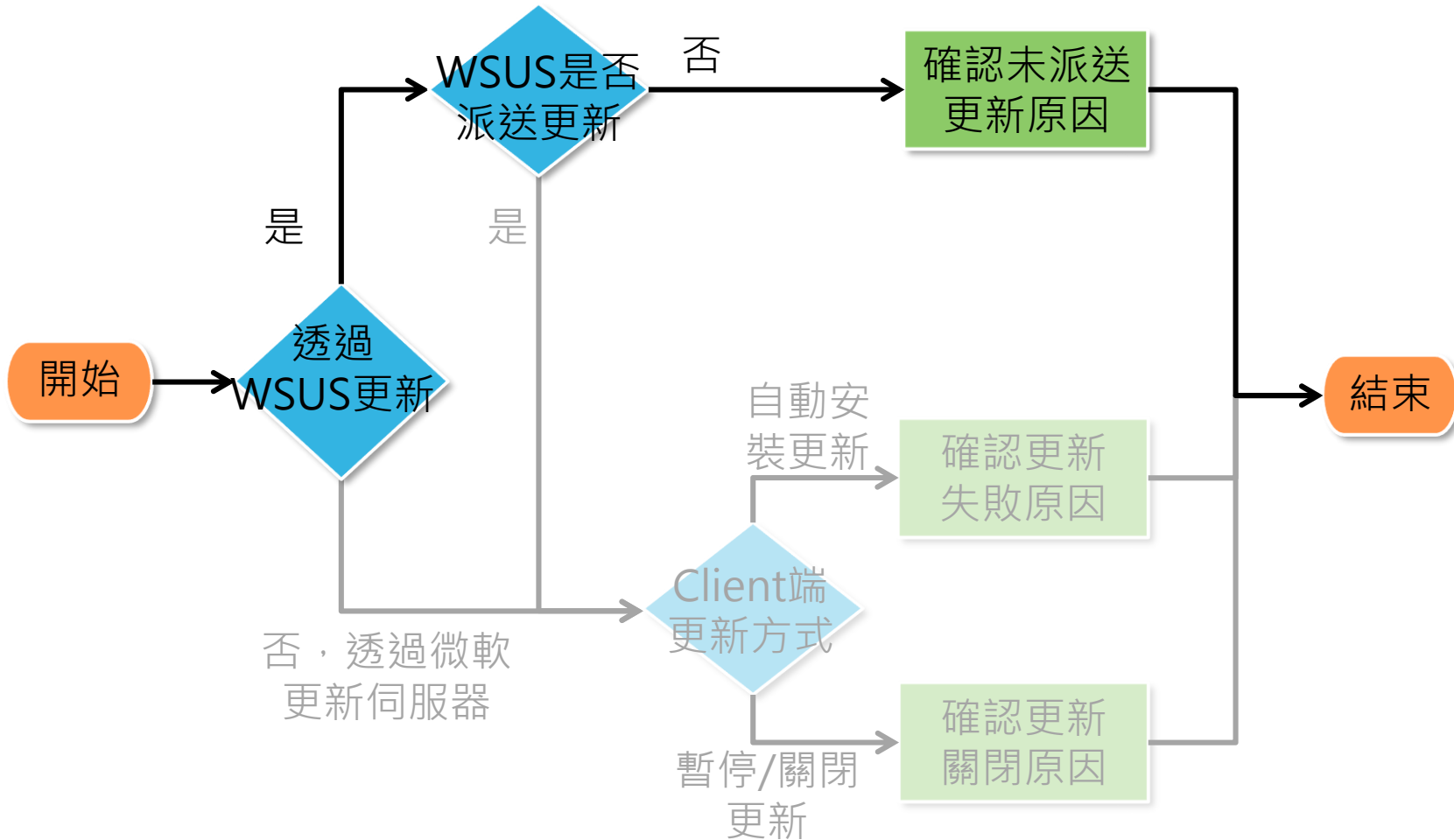
弱點通知與修補規劃作業流程



確認更新缺漏原因



確認更新缺漏原因



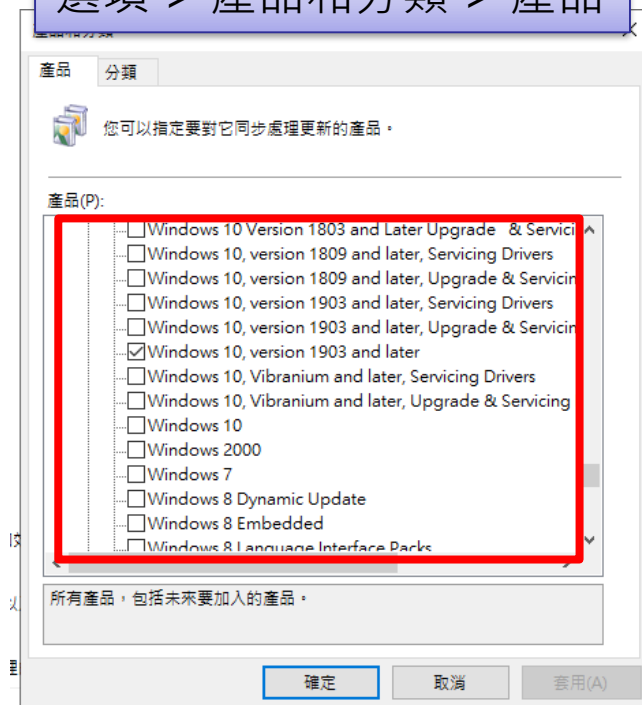
確認WSUS更新派送狀態(1/2)



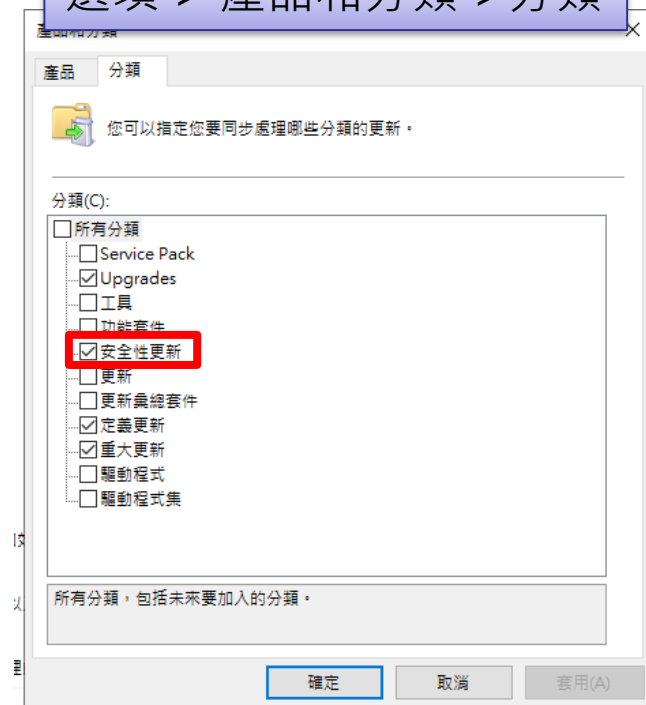
● 若透過WSUS派送更新，需至WSUS伺服器確認下列設定

- 可搭配資訊資產清單或資產管理系統，確認機關內**所有微軟系列品項**，確保**完整勾選所需之產品**
- 確認有勾選「**安全性更新**」類別

選項 > 產品和分類 > 產品



選項 > 產品和分類 > 分類



確認WSUS更新派送狀態(2/2)



- 確認缺漏更新是否已於WSUS核准派送

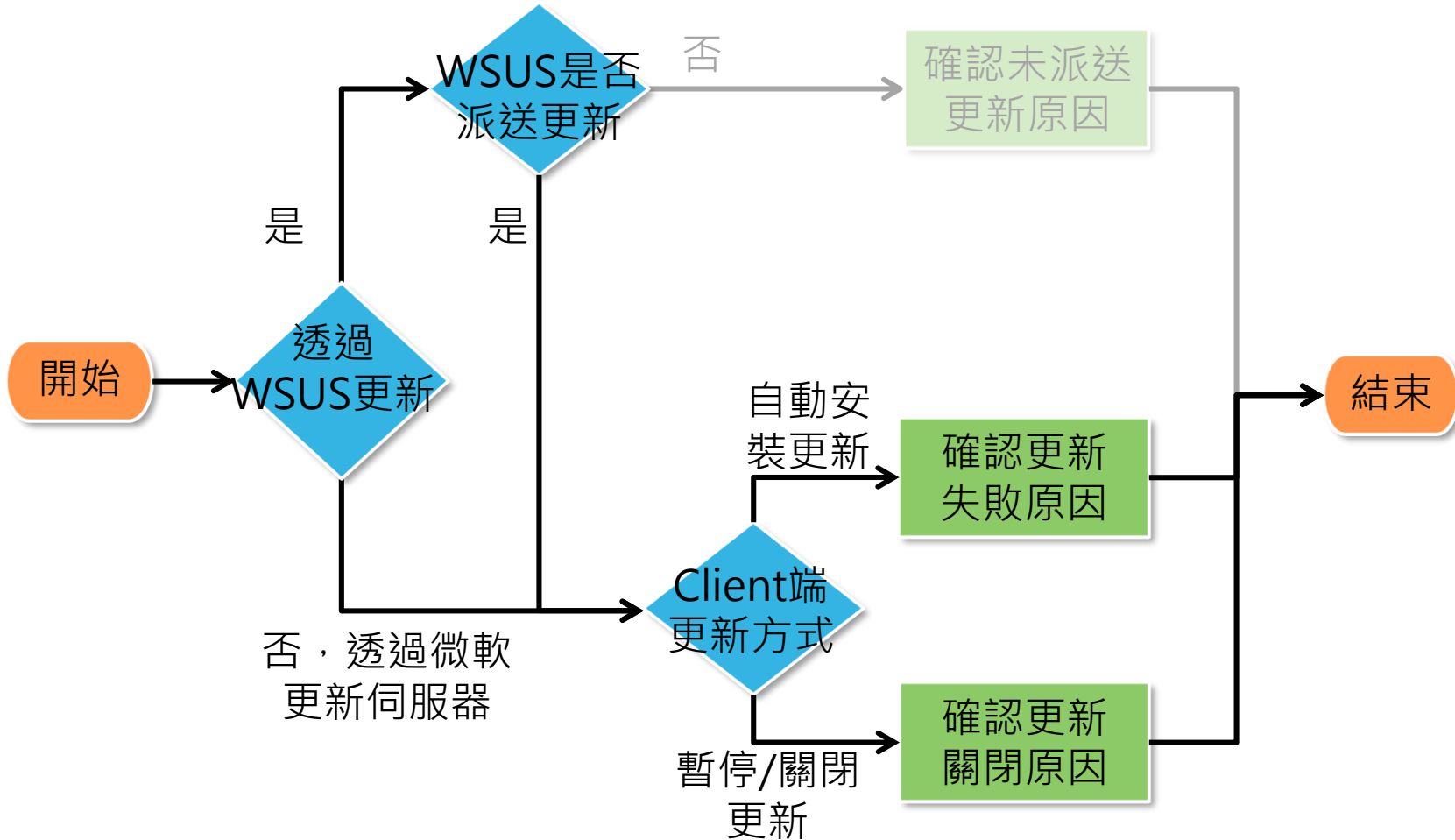
The screenshot illustrates the process of approving updates in the WSUS console. The main window shows a list of updates, with the '核准(A)...' option highlighted. A context menu is open over the selected update. A yellow arrow points from the context menu to the '核准更新' dialog box. In the dialog box, '已核准安裝(I)' is highlighted. Another yellow arrow points from the dialog box to the '核准進度' window, which shows a green progress bar and a log of actions.

電腦群組	核准	期限
所有電腦	未核准	不適用
尚未指派的管理	未核准 (繼承)	不適用 (繼承)
已核准安裝(I)	Ctrl+I	
已核准移除(R)	Ctrl+R	
未核准(N)	Ctrl+N	
期限(D)	>	
與父代相同(P)	Ctrl+P	
套用到所有子系(C)	Ctrl+C	

動作	結果
正在從 所有電腦 移除 2020-05 適用於 x64 系統 Windows 10 Version 1903 的 .NET F...	成功
正在核准 2020-05 適用於 x64 系統 Windows 10 Version 1903 的 .NET Framework 3...	成功

- 若上述確認完畢後，仍有缺漏更新，則需確認是否為Client端問題

確認更新缺漏原因



確認Client端更新狀態



- Client更新失敗時，建議臨機於「Windows Update」頁面查看更新失敗之更新項目與錯誤代碼，並至微軟官方頁面查詢錯誤代碼涵義，並尋找解決方案
 - <https://docs.microsoft.com/zh-tw/windows/deployment/update/windows-update-error-reference>
- 另需確認Client端更新是否遭關閉或暫停，而導致未正常更新

Microsoft | Docs 文件 Learn Q&A 程式碼範例 節目 事件

Microsoft 365 解決方案與架構 應用程式和服務 訓練 資源

登入 免費帳戶

依標題篩選

部署及更新 Windows 用戶端

- > 開始使用
- > 規劃
- > 準備
- > 部署
 - > 部署 Windows 用戶端
 - > 部署 Windows 用戶端更新
 - > 使用商務用 Windows Update
 - > 監視 Windows 用戶端更新
- > 疑難排解
 - > 解決升級錯誤
 - > 疑難排解 Windows Update
 - 如何疑難排解 Windows Update
 - 退出保護保留
 - 判斷 Windows Update 的來源

文件 / Windows / 部署 /

依元件排列的 Windows Update 錯誤碼

發行項 • 2022/06/17 • 1 位參與者

適用於

- Windows 10
- Windows 11

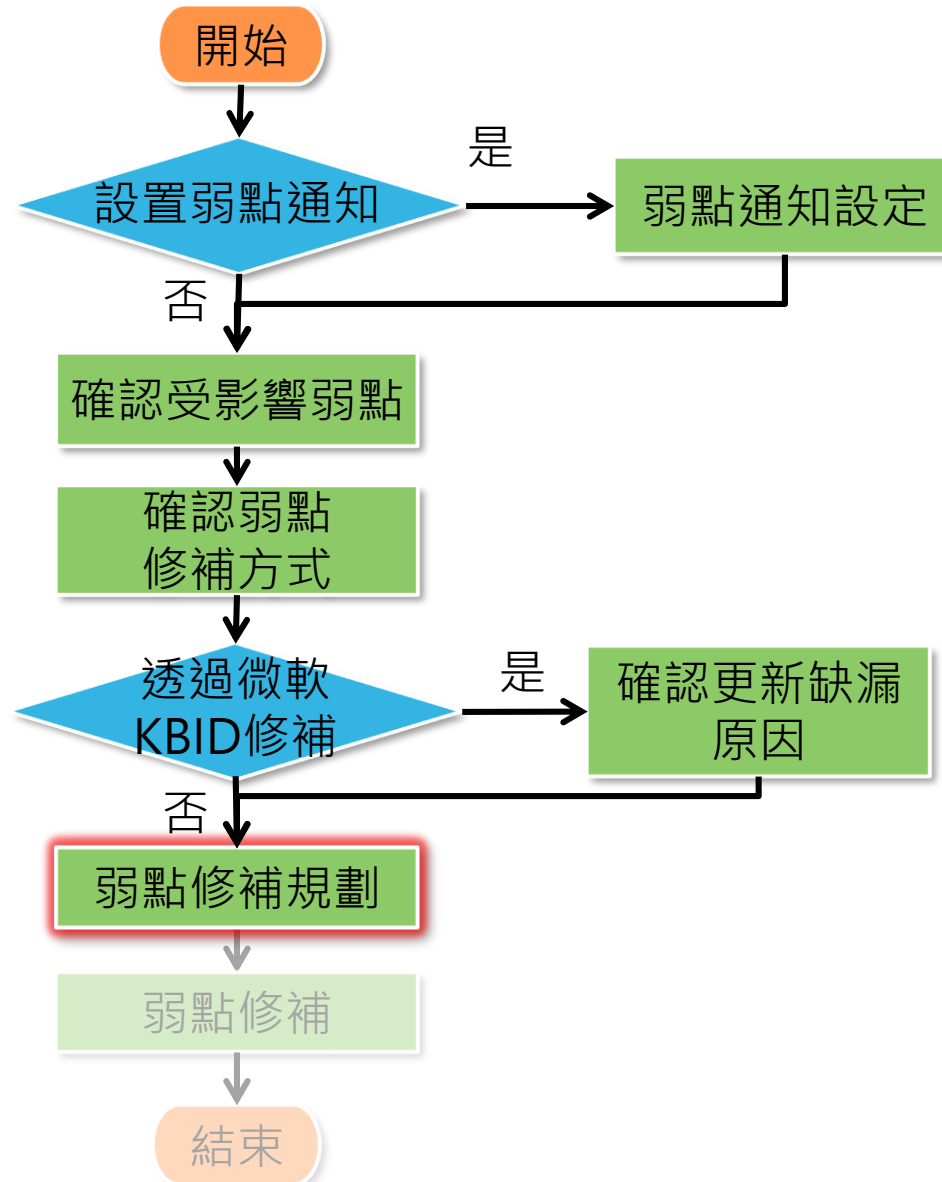
本章節列出 Microsoft Windows Update 的錯誤碼。

透過Ctrl+F搜尋錯誤代碼

自動更新錯誤

錯誤碼	訊息	說明
0x80243FFF	WU_E_AUCLIENT_UNEXPECTED	有另一個 WU_E_AUCLIENT_* 錯誤碼未涵蓋的使用者介面錯誤。
0x8024A000	WU_E_AU_NOSERVICE	自動更新無法服務傳入的要求。

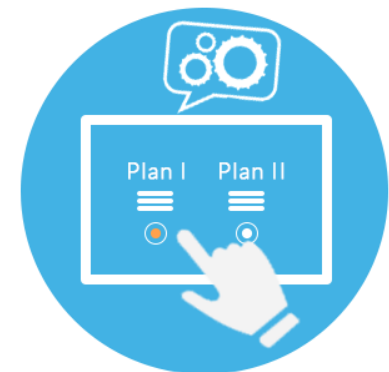
弱點通知與修補規劃作業流程



弱點修補規劃(1/6)



- 依據機關ISMS政策訂定弱點修復基準與修復時程，若無法立即修補、安裝安全性更新或須接受風險之弱點，可針對該風險填寫改善措施
- 針對達到弱點修復基準之弱點進行修補規劃
 - 確認是否可透過更新方式修補弱點？
 - 是否有其他替代修補措施？
 - 預計修補時程



弱點修補規劃(2/6)



- 改善措施填寫方式分為單筆填寫、批次填寫及上傳更新

– 資產風險狀態 > 資通系統風險狀態/使用者電腦風險狀態 > 資訊資產風險列表

The screenshot displays the '資訊資產風險列表' (Information Asset Risk List) interface. The sidebar on the left contains navigation options: 首頁, 機關總覽, 資訊資產管理, 資產風險狀態, 資通系統風險狀態, 資訊資產風險列表 (highlighted with a red box and a blue arrow), 弱點關聯列表, 弱點比對通知, 弱點處理情形回報, 使用者電腦風險狀態, 資訊查詢, and 設定管理.

The main content area shows a table of assets with columns: 資產名稱, 資產廠商, 資產版本, CPE2.3, 資產數量, 風險指數, 弱點數量, 未填寫改善措施數量, and 弱點資訊. A blue arrow points to the '詳細資訊' (Detailed Information) button for the first asset.

The detailed view shows a table of vulnerabilities with columns: 填寫勾選改善措施 (highlighted with a red box), CVE編號, CVSS, 發佈時間, 更新時間, and 改善措施 (highlighted with a red box). The table contains two entries:

填寫勾選改善措施	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input type="checkbox"/>	CVE-2014-0114	7.5	2014-04-30 18:49:00	2021-01-27 02:15:00	填寫改善措施

At the bottom of the detailed view, there is a '關閉' (Close) button.

弱點修補規劃(3/6)



- 單筆填寫：可針對各弱點進行弱點修補規劃
 - STEP1：確認弱點後，點選「填寫改善措施」，針對該弱點進行修補規劃
 - STEP2：點選「送出」即完成填寫改善措施
 - 填寫改善措施請避免使用 >、<、&、"或'等特殊字元

詳細資訊

填寫勾選改善措施 全部勾選 全部取消

搜尋

<input type="checkbox"/>	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	<input type="button" value="填寫改善措施"/>
<input type="checkbox"/>	CVE-2014-0114	7.5			<input type="button" value="填寫改善措施"/>

顯示第 1 到第 2 項記錄，總共 2 項記錄

填寫改善措施

請勿使用 >、<、&、"或' 字元填寫改善措施

關閉

弱點修補規劃(4/6)



- 批次填寫：可針對同樣修補方式之弱點進行批次弱點修補規劃
 - STEP1：確認弱點後，勾選左方的方格並點選填寫勾選改善措施，以進行多筆CVE之弱點修補規劃
 - STEP2：點選「送出」即完成填寫改善措施
 - 填寫改善措施請避免使用 >、<、&、"或'等特殊字元)

詳細資訊

填寫勾選改善措施 全部勾選 全部取消

搜尋

	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input checked="" type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input checked="" type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input checked="" type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-01-27 02:15:00	填寫改善措施

顯示第 1 到第 2 項記錄，總共 2 項記錄

填寫改善措施

請勿使用 >、<、&、\" or ' 字元填寫改善措施

送出 關閉

弱點修補規劃(5/6)



● 上傳更新：將弱點比對結果匯出並填寫改善措施後，上傳弱點清單登錄弱點修補規劃

- 點擊「產製弱點清單」等待清單產製完成，進入系統執行「下載弱點清單」功能可匯出弱點比對結果，並通知相關長官、資通系統/使用者電腦負責人或廠商
- 可於CVSS分數欄位篩選，針對達弱點修復基準之弱點進行修補
- 若改善措施為「尚未填寫」則表示尚未對該弱點進行修補規劃

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

產製弱點清單 下載弱點清單 上傳弱點改善措施 全部

資訊

弱點比對完成時間：2023-05-02 11:56 產製弱點清單時間：2023-05-03 10:05

資產名稱	資產廠商	G	H	I	J	K	L	M	N	O
Microsoft Windows Server 2019 Standard 7 64-bit	Microsoft Corporation	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
Microsoft Windows Server 2012 Standard 7 64 位元	Microsoft Corporation	microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	ms and Office LPAC Page	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
Microsoft Windows Server 2016 Datacenter	Microsoft Corporation	microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
Microsoft Windows Server 2016 Datacenter	Microsoft Corporation	microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補

G	H	I	J	K	L	M	N	O
CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	ms and Office LPAC Page	gov/view/vuln/detail?v	N/A	尚未填寫
microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	尚未填寫
microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	尚未填寫

弱點修補規劃(6/6)



- 從「資訊資產風險列表」之「處理情形」檢視各軟體資產尚未填寫改善措施之弱點數量

– 資產風險狀態 > 資通系統風險狀態/使用者電腦風險狀態 > 資訊資產風險列表

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

產製弱點清單 下載弱點清單 上傳弱點改善措施

全部

國家資通安全研究院

資訊

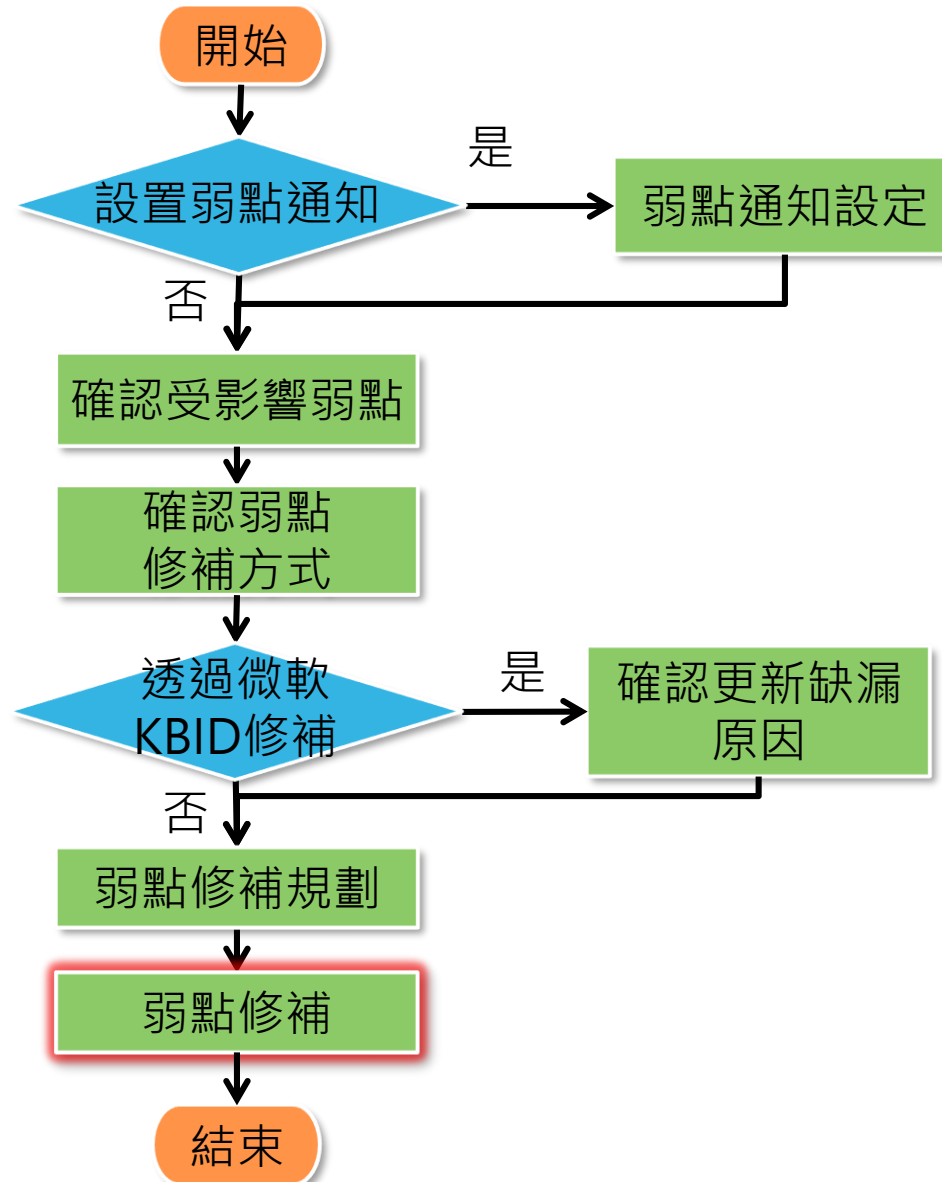
弱點比對完成時間：2023-05-02 11:56 產製弱點清單時間：2023-05-03 10:05

搜尋



資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
Microsoft Windows Server 2019 Standard 7 64-bit	Microsoft Corporation	10.0.17763	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:standard:*:x64:*	4	5.77	2043	0	詳細資訊
Microsoft Windows Server 2012 Standard 7 64 位元	Microsoft Corporation	6.2.9200	cpe:2.3:o:microsoft:windows_server_2012:-:*:*:standard:*:x64:*	6	5.80	1784	1077	詳細資訊
Microsoft Windows Server 2016 Datacenter 8 64 位元	Microsoft Corporation	10.0.14393	cpe:2.3:o:microsoft:windows_server_2016:-:*:*:datacenter:*:x64:*	29	5.64	1326	18	詳細資訊
Adobe Flash Player 11 ActiveX	Adobe Systems Incorporated	11.3.300.257	cpe:2.3:a:adobe:flash_player:11.3.300.257:*:*:*:*:*	1	9.31	783	783	詳細資訊
Adobe Flash Player 11.3 r300	Adobe	11.3.300.257	cpe:2.3:a:adobe:flash_player:11.3.300.257:*:*:*:*:*	1	9.31	783	783	詳細資訊

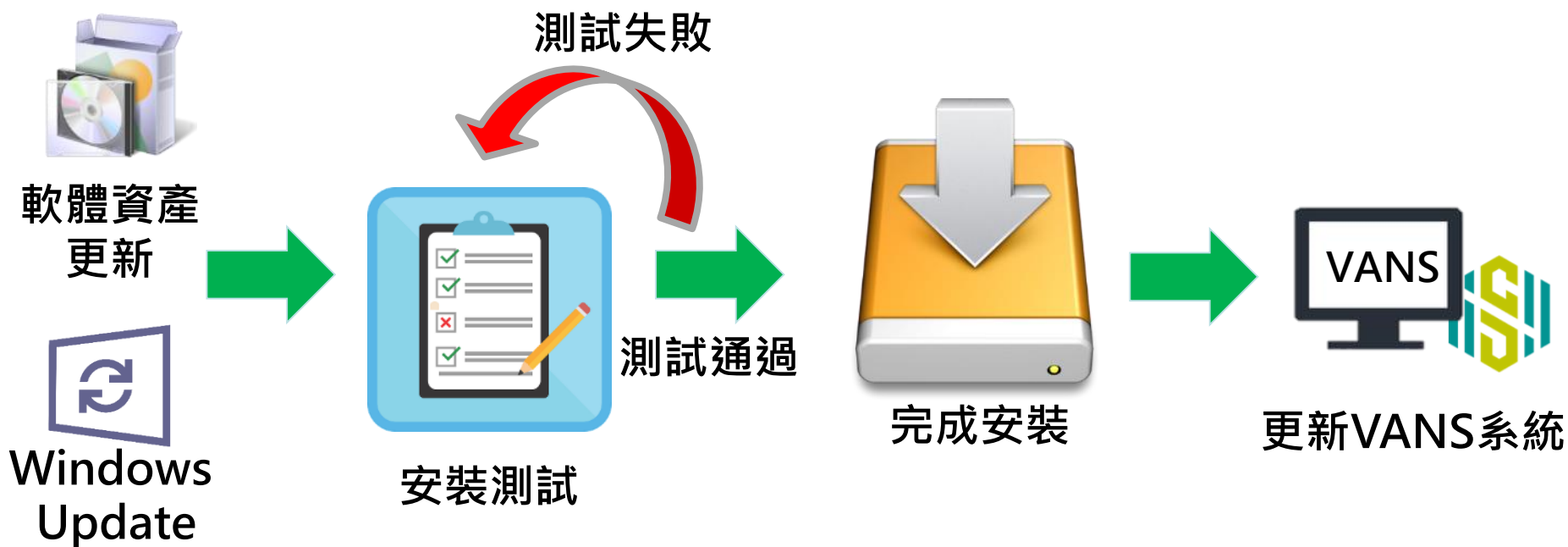
弱點通知與修補規劃作業流程



弱點修補



- 異動軟體版本與派送安全性更新前，建議進行測試以確認安裝更新後，日常作業與服務仍可正常運作
- 修補完成後，更新VANS系統之資訊資產與已安裝KBID，以檢視弱點修補情形





實作練習2

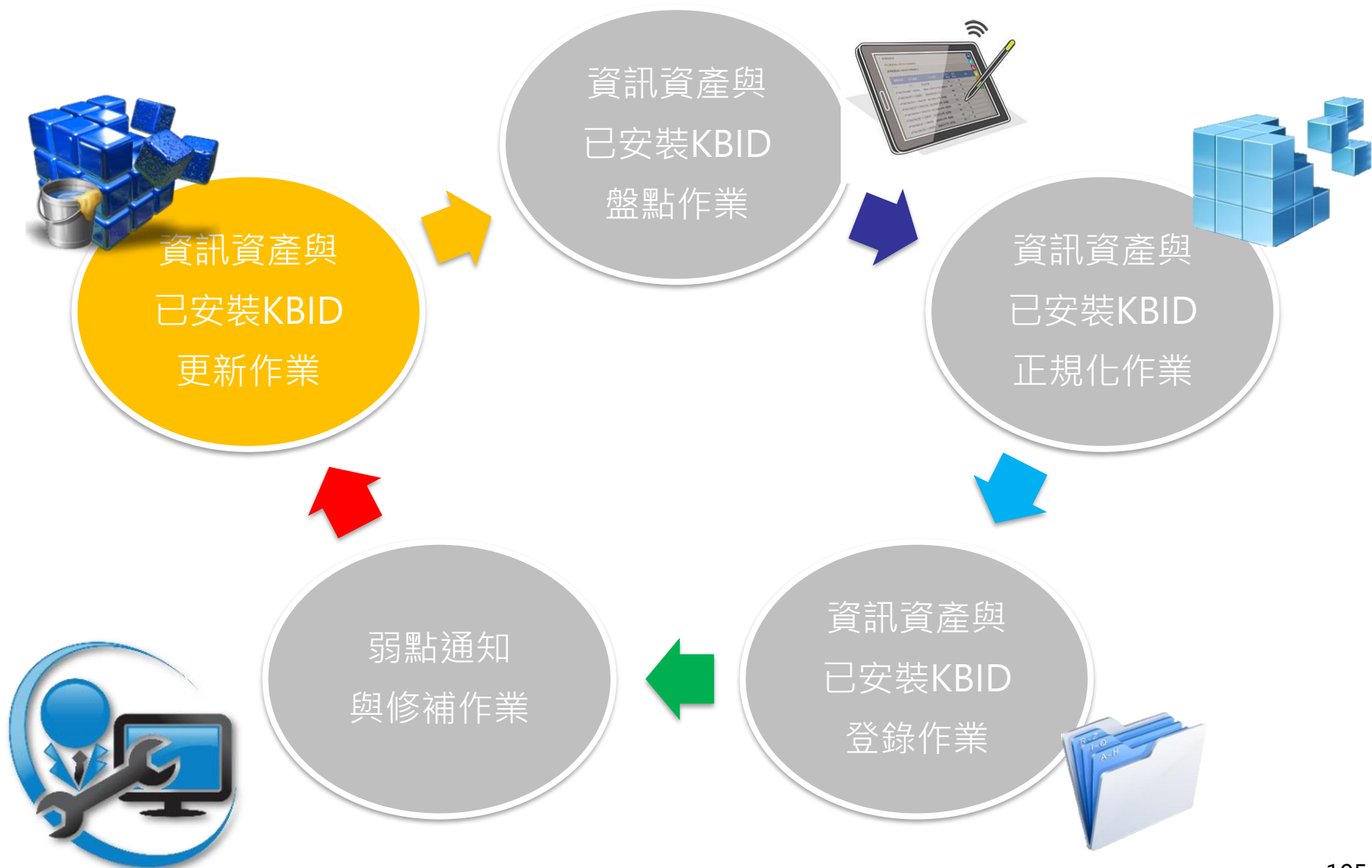
實作練習2



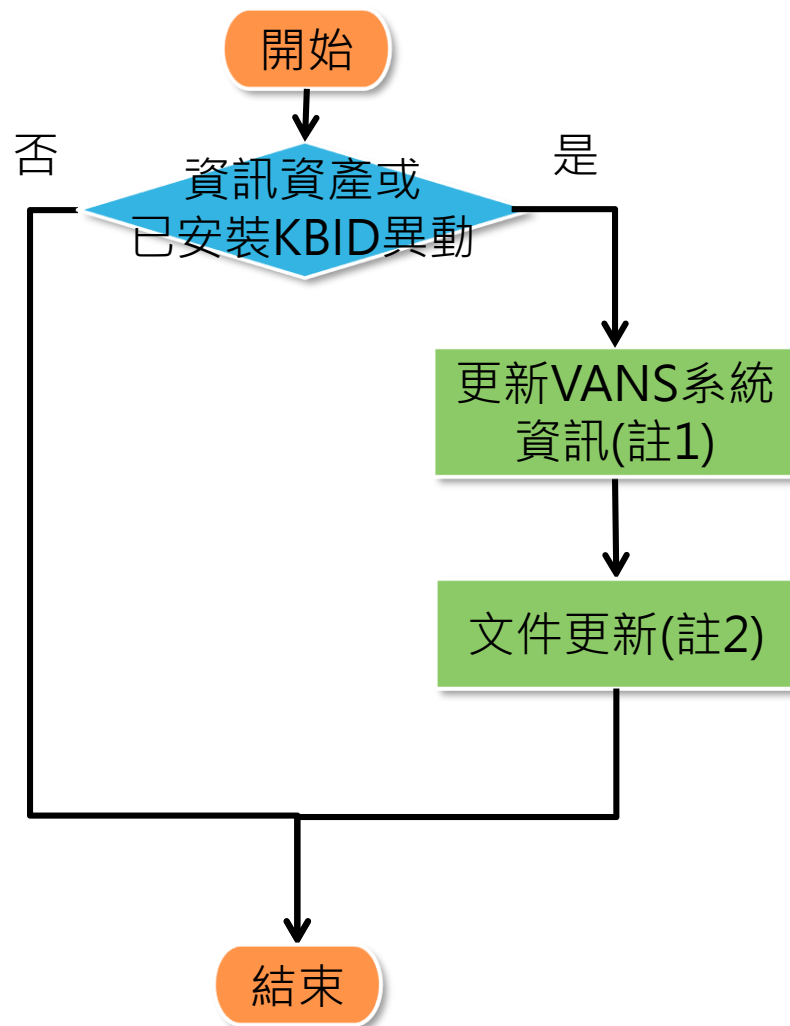
- 檢視弱點通知，並進行弱點修補規劃
- 本項練習時間**20分鐘**

項次	執行項目	產出項目/執行結果
1	於 資訊資產風險列表 檢視Apache Tomcat 9.0之弱點，透過查詢建議修補方式填寫改善措施	<ul style="list-style-type: none">● 填寫弱點清單中的改善措施● 改善措施範例： 因系統服務使用，故須請系統維護負責人評估後再進行版更作業
2	於 資訊資產風險列表 檢視Windows Server 2012 R2之弱點，查詢CVE-2021-34448，透過查詢建議修補方式填寫改善措施	<ul style="list-style-type: none">● 填寫弱點清單中的改善措施● 改善措施範例： 安全性更新預計測試7天後進行全機關派送

導入作業流程



資訊資產與已安裝KBID更新作業流程

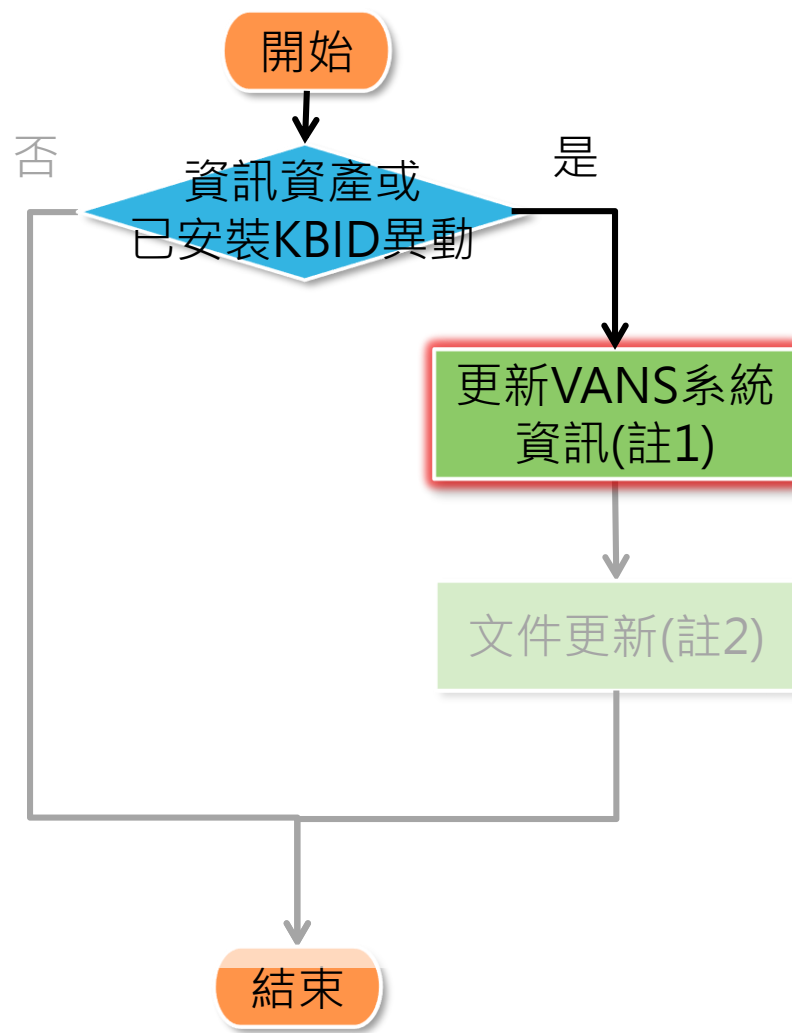


註1更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

註2文件更新：

- 1.更新資訊資產清冊
- 2.更新已安裝KBID清單
- 3.重新匯出資訊資產清單
- 4.重新匯出弱點清單

資訊資產與已安裝KBID更新作業流程



註1更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

註2文件更新：

- 1.更新資訊資產清冊
- 2.更新已安裝KBID清單
- 3.重新匯出資訊資產清單
- 4.重新匯出弱點清單

更新VANS系統資訊-批次更新



- 弱點修補後，若資訊資產或版本有異動，請至VANS系統**更新資訊資產內容**，以維持資料有效性
- 可下載已登錄至VANS系統之資訊資產接續處理，節省資訊資產更新耗費之時間

資訊資產管理 > 資通系統資產列表

下載已登錄之資訊資產清單，以利進行後續編輯

CPE清單 / 範本下載 資產 / 已安裝KBID上傳 資產清單匯出

資通系統資產清單匯出(Excel)

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱					
2	NICS	國家資通安全研究院	1	Java 8 Upd	Oracle Cor	8.0.3210.7	cpe:2.3:a:Oracle	Oracle Java SE Runtime Environment (JRE) 1.8.0 Update 321					
3	NICS	國家資通安全研究院	3	7-Zip 15.1	Igor Pavlov	15.14	cpe:2.3:a:7-Zip	7-Zip 15.14 for Windows					
4	NICS	國家資通安全研究院	3	7-Zip 16.0	Igor Pavlov	16.04	cpe:2.3:a:7-Zip	7-Zip 16.04 for Windows					
5	NICS	國家資通安全研究院	3	7-Zip 18.0	Igor Pavlov	18.06	cpe:2.3:a:7-Zip	7-Zip 18.06					

更新VANS系統資訊-單筆更新(1/2)



● 編輯資訊資產

- 透過網頁頁面進行單筆資訊資產編輯與刪除
- 更新資產時，僅可變更資產之版本、版次及數量

The screenshot displays the '資訊資產管理' (Information Asset Management) interface. A modal window titled '更新資產' (Update Asset) is open, allowing for the modification of an asset's details. The main interface shows a table of assets with columns for '資產名稱' (Asset Name), '資產廠商' (Asset Vendor), and '資產版本' (Asset Version).

資產名稱	資產廠商	資產版本
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16
commons-beanutils	N/A	1.8.0

The '更新資產' dialog box contains the following fields:

- 廠商 (Vendor): apache
- 產品 (Product): commons-beanutils
- 版本 (Version): 1.8.0
- 更新 (Update): *
- 版次 (Edition): *
- 資產數量 (Asset Quantity): 1

Buttons in the dialog include '更新資產' (Update Asset) and '取消' (Cancel). A blue arrow points from the '更新資產' button to the '編輯' (Edit) button in the table's action column. A red box highlights the '編輯' and '刪除' (Delete) buttons in the table.

更新VANS系統資訊-單筆更新(2/2)



● 編輯已安裝KBID

- 透過網頁頁面進行單筆已安裝KBID新增與刪除
- 更改KBID數量可先點選刪除，再點選新增已安裝KBID輸入KBID與已安裝數量

資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 資產 / 已安裝KBID上傳 資產清單匯出 切換至資訊資產列表

已安裝KBID列表

KBID	數量
KB2868626	1
KB2883200	1

新增已安裝KBID

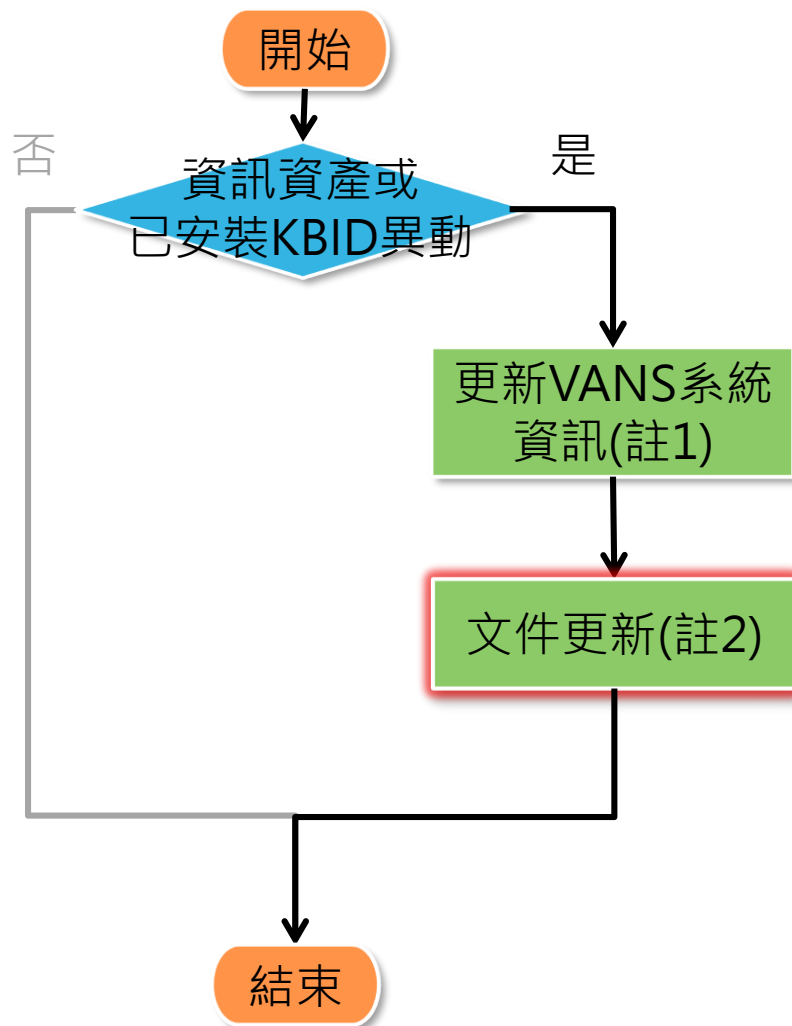
KBID: KB2868626

已安裝KBID數量: 3

新增已安裝KBID 取消

刪除 刪除 刪除

資訊資產與已安裝KBID更新作業流程



註1更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

註2文件更新：

- 1.更新資訊資產清冊
- 2.更新已安裝KBID清單
- 3.重新匯出資訊資產清單
- 4.重新匯出弱點清單

文件更新-資訊資產清單匯出



● 資訊資產清單匯出(PDF)

- 有資料留存與備查需求時，可以PDF格式匯出已登錄VANS系統之資訊資產

資訊資產管理 > 資通系統資產列表

下載已登錄之資訊資產清單，以利進行後續編輯

CPE清單 / 範本下載 資產 / 已安裝KBID上傳 資產清單匯出

資訊資產列表

資通系統資產清單匯出(Excel)
資通系統資產清單匯出(PDF)

機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱	廠商	產品	版本	更新	版
NICS	國家資通安全研究院	1	Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*:*:*:*:*:*	Apache Software Foundation Tomcat 9.0.16	apache	tomcat	9.0.16	*	*
NICS	國家資通安全研究院	1	commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons-beanutils:1.8.0:*:*:*:*:*	Apache Software Foundation Commons BeanUtils 1.8.0	apache	commons-beanutils	1.8.0	*	*
NICS	國家資通安全研究院	1	commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons-fileupload:1.3.2:*:*:*:*	Apache Software Foundation Commons FileUpload	apache	commons-fileupload	1.3.2	*	*

文件更新



- 依據弱點修補規劃執行資訊更新或下架後，進行下列文件更新作業
 - 更新資訊資產清冊與已安裝KBID清單
 - 於VANS系統匯出更新後之弱點清單，並進行弱點修補規劃

資訊資產清冊

	A	B	C	D	E	F
1	資產數量	資產名稱	資產廠商	資產版本	TEMP	資產數量
2	1	Windows Server 2012 R2 Standard x64	Microsoft Corporation	N/A	Windows Server 2012 R2 Standard	1
3	1	Windows Server 2019 Datacenter x64	Microsoft Corporation	1809	Windows Server 2019 Datacenter	1
4	1	Microsoft Visual C++ 2008 Redistributable	Microsoft Corporation	9.0.30729.6161	Microsoft Visual C++ 2008 Redistributable	1
5	2	Microsoft Silverlight	Microsoft Corporation	5.1.50918.0	Microsoft Silverlight	2
6	1	VMware Tools	VMware, Inc.	11.0.0.14549434	VMware Tools VMware, Inc. 11.0.0.14549434	1

弱點清單

	G	H	I	J	K	L	M	N	O
1	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
2	microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	... and Office LPAC P...	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
3	microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
4	microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補

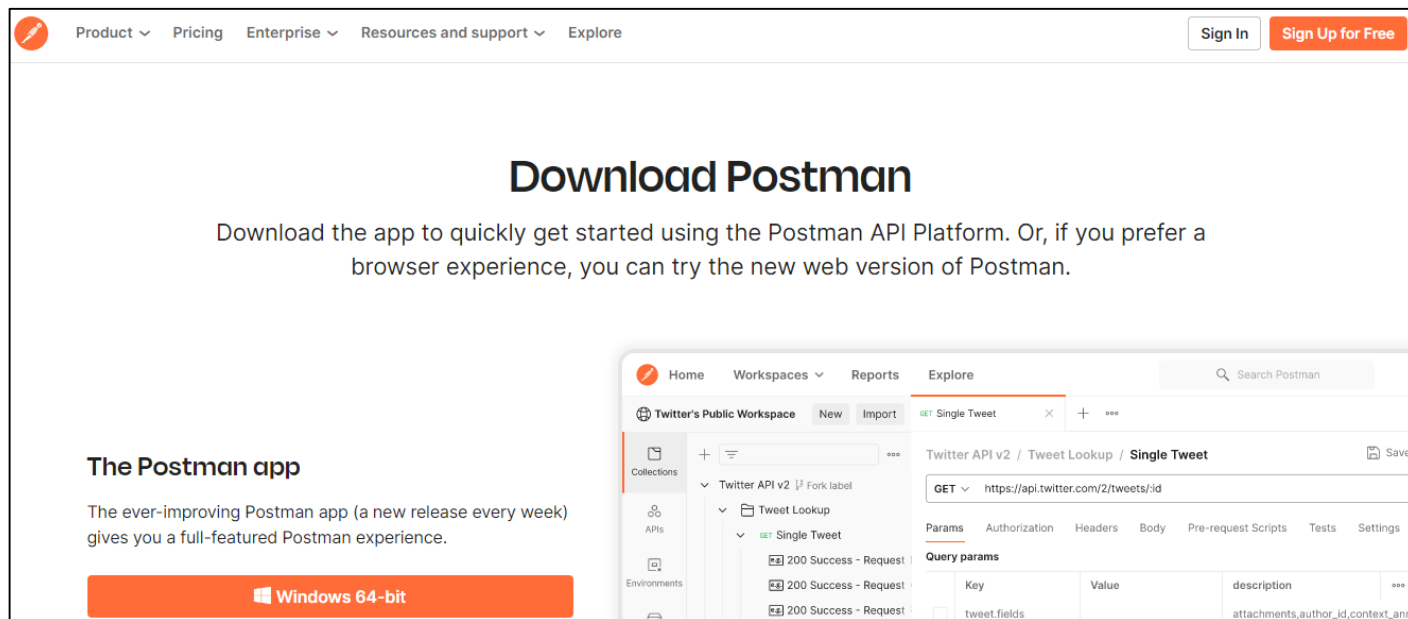


實作練習3

實作練習3(工具說明)(1/5)



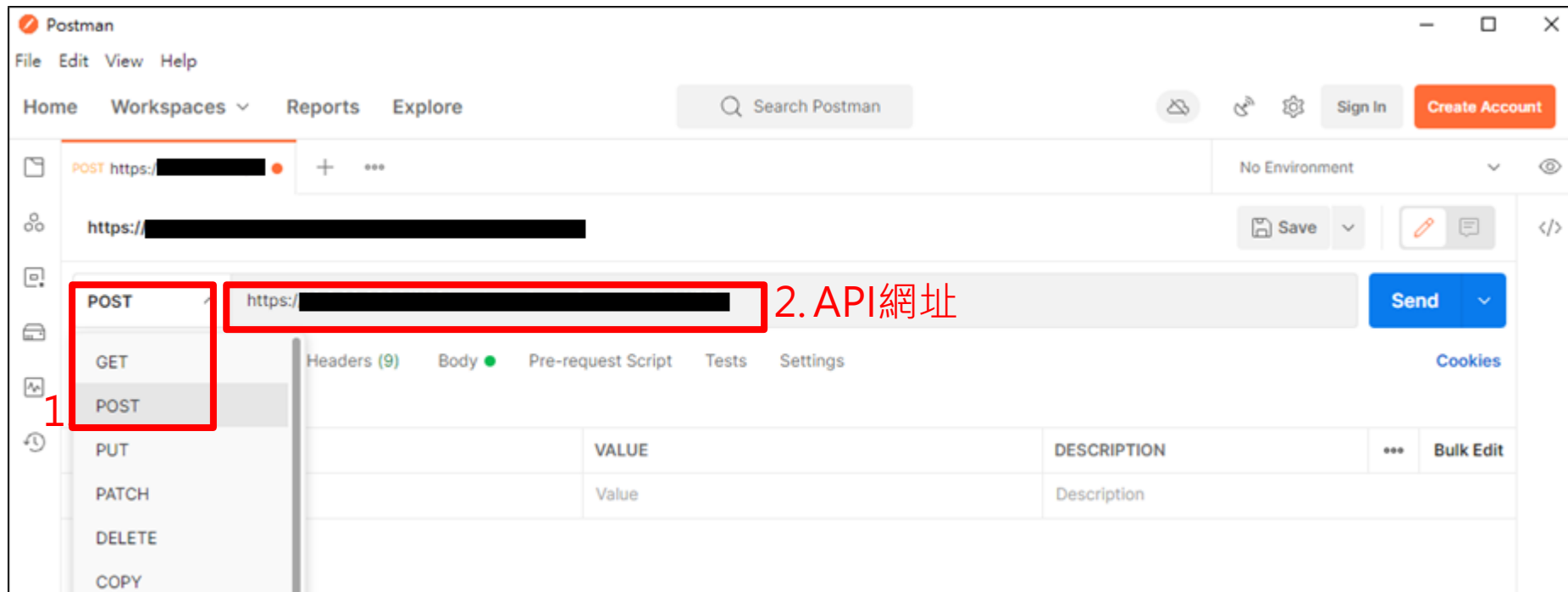
- Postman為API平台，可用來測試HTTP各種請求之工具，藉由回傳之訊息代碼即可得知測試結果
– 下載網址：<https://www.postman.com/downloads/>
- API是可把不同服務進行串接，如VANS系統可透過API接收資產管理工具傳送之資訊資產



實作練習3(工具說明)(2/5)



- API傳輸方式為POST
- 設定API網址
 - API IP申請完成通知信中將提供API網址

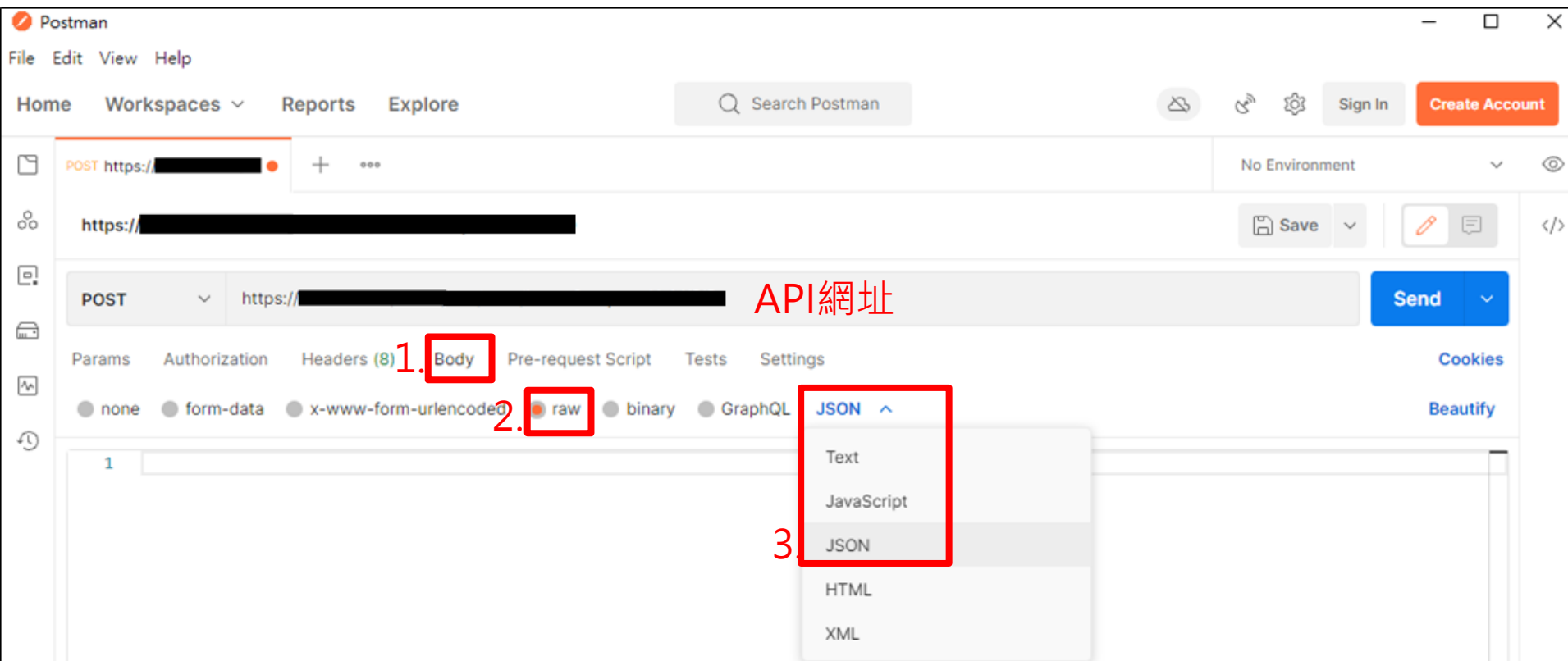


實作練習3(工具說明)(3/5)



- API傳輸格式為JSON

–Postman調整格式之步驟如下圖



實作練習3(工具說明)(4/5)



- 設定API KEY、OID及機關名稱(unit_name)

The screenshot shows the Postman interface for a POST request. The URL is `https://[redacted]`, labeled "API網址". The request body is in JSON format, with the following fields:

- `"api_key": "OVu7GP3[redacted]y&dFC8ZeQ"`, labeled "API KEY"
- `"data": [`
- `{`
- `"oid": "studentXX",` labeled "機關OID"
- `"unit_name": "studentXX",` labeled "機關名稱"
- `"kbid_number": "1",`
- `"kbid": "K62868626"`
- `},`
- `{`
- `"oid": "studentXX",`
- `"unit_name": "studentXX",`
- `"kbid_number": "1"`
- `}`
- `]`

實作練習3(工具說明)(5/5)



- 按下Send，即可於下方看到測試結果

The screenshot displays the Postman interface for a POST request. The request URL is partially redacted. The request body is a JSON object with the following structure:

```
1 { ...
2   "api_key": "OVu7GP380s[redacted]8dFC8ZeQ",
3   "data":
4   [
5     {
6       "oid": "studentXX",
7       "unit_name": "studentXX",
8       "kbid_number": "1",
9       "kbid": "KB2868626"
10    }
11  ],
12 }
```

The response status is 200 OK, with a time of 580 ms and a size of 393 B. The response body is shown in the 'Body' tab, displaying the following JSON:

```
1 {
2   "Message": "KB-PC-0101",
3   "Describe": "資料正確，系統解析清單中，完成後將會寄發郵件通知"
4 }
```

Annotations in the image include a red box around the 'Send' button and a green box around the response body.

API傳輸後回傳之訊息代碼

實作練習3



- 登錄已安裝KBID，並確認弱點修補情形
- 本項練習時間**15分鐘**

項次	執行項目	產出項目/執行結果
1	<p>透過API方式，上傳已安裝KBID</p> <ul style="list-style-type: none">開啟Postman (路徑：學員資料夾\01.實作練習\實作練習3\postman-portable.exe)設定API Key、機關OID、機關名稱送出	API回傳訊息代碼為KB-S-0101
2	<ul style="list-style-type: none">於資訊資產風險列表匯出弱點清單，搜尋並檢視 CVE-2021-34448是否完成修補安全性更新請參考KBID修補情形欄位	弱點清單



	G	H	I	J	K	L	M	N	O
1	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	D弱點說明連	KBID修補情形	改善措施
204	windows_server_2012:r2:*	CVE-2021-34448	9.3	2021/07/17 05:15:00	2021/07/23 01:06:00	Memory Corrup	view/vuln/detail?	1/1	尚未填寫
205	windows_server_2012:r2:*	CVE-2021-31956	9.3	2021/06/09 07:15:00	2021/06/14 22:43:00	Elevation of Priv	view/vuln/detail?	1/1	尚未填寫
206	windows_server_2012:r2:*	CVE-2021-1668	9.3	2021/01/13 04:15:00	2021/01/21 05:34:00	Decoder Remote	view/vuln/detail?	1/1	尚未填寫

1. 應辦事項列表中資通安全弱點通報機制(VANS)應導入範圍為何?是否有建議之上傳頻率?

- 公務機關VANS導入範圍以全機關之資訊資產為原則，有關支持核心業務持續運作相關之資通系統主機與電腦應於規定時限內完成導入；關鍵基礎設施提供者VANS之導入範圍至少應涵蓋關鍵資訊基礎設施及營運持續運作必要相關資通系統
- 有關資訊資產上傳頻率，除重大弱點通報或大量資產異動外，建議每個月至少定期上傳1次，機關如採系統化介接方式，可增加上傳頻率；並應針對發現弱點設定修補期限，未修補前應加強防護及異常偵測，以確保弱點管理之即時性及有效性

2. 限於經費無法導入伺服器該如何處理?可否例外?

- VANS導入範圍以全機關之資訊資產為原則，機關如囿於經費，可考量與核心業務之關聯性、資安風險程度及資訊資產重要性等，優先導入支持核心業務持續運作相關之資通系統主機與電腦

3. 針對高風險以上弱點，是否訂定相關修補時間?

- 目前尚未訂定修補時間，惟建議發現高風險以上之弱點時，如無法及時完成修補，應於一週內決定弱點處置方式並於VANS系統填寫改善措施

4. 填寫弱點改善內容後，資安署是否會管考後續改善結果?

- VANS機制主要協助機關進行自我弱點管理，惟若爆發重大弱點時，將參考填復內容以了解機關處理方式與進度



1.

系統所比對出之弱點，如何得知弱點存在於哪些主機呢？

- 執行資訊資產盤點作業後所產出之資訊資產清冊中，內容包含各軟體資產對應之主機資訊，可藉由弱點對應軟體資產，再由軟體資產對應主機資訊之方式，找出含有該弱點之主機

2.

VANS系統弱點比對結果中，有許多微軟產品弱點，若平時已有定期安裝安全性更新(KBID)，該如何判斷哪些弱點尚待修補？

- 若機關已完整安裝安全性更新(KBID)，大多數弱點可視為已完成修補，少數非透過安全性更新修復之弱點，建議參考微軟官方所提供之緩解措施進行處理
- 可透過VANS系統安全性更新(KBID)與弱點(CVE)關聯分析功能，查看尚待修補之弱點

3.

弱點若無法修補時，該如何處理？

- 若遇到已停止更新支援或無法修補之弱點時，機關可依據自身ISMS政策評估該弱點對機關可能產生之影響，並採取因應之配套措施，並將實際情況填寫至VANS系統改善措施中

4.

主管機關是否可替所屬機關上傳資訊資產與已安裝KBID？

- 可以。主管機關上傳資料時，可於上傳清單中填寫所屬機關OID、機關名稱欄位，即可替所屬機關上傳資訊資產或已安裝KBID

VANS常見問答(3/10)



5. 若主管機關替所屬機關上傳資訊資產，所屬機關是否需申請API介接IP？

- 因進行API傳輸者為主管機關，故僅需由主管機關申請API介接IP即可

6. 為何登入VANS系統時顯示個人帳號已被停用，遇到此狀況時該如何解決？

- 基於資安考量，超過180天未登入iAuth系統之帳號將被鎖定，於登入VANS系統時將顯示該帳號已被停用。
- 遇此狀況時，請寄信至VANS服務信箱(VansService@nics.nat.gov.tw)，確認使用者身分後將協助恢復帳號權限。

7. 如何刪除VANS系統機關管理者帳號？

- 請填寫「資通安全弱點通報系統(VANS系統)機關管理者帳號申請(異動)單」並核章後，提交資安處審查，審核過後由技服中心協助進行後續處理。

8. 未比對到CPE之資產，是否仍需上傳至VANS系統？

- 公務機關VANS導入範圍以全機關之資訊資產為原則，關鍵基礎設施提供者VANS之導入範圍至少應涵蓋關鍵資訊基礎設施及營運持續運作必要相關資通系統，因此未比對到CPE條目之資產仍需上傳至VANS系統。



1. 「資通系統資產列表」與「使用者電腦資產列表」差異為何？
- 兩者功能相同，主要依據盤點對象分為「資通系統」與「使用者電腦」，以方便機關區分與管理

2. 為什麼上傳資產清單或已安裝KBID清單後，「資產清單上傳」或「已安裝KBID清單上傳」按鈕會消失？
- 為避免重複進行上傳動作，故VANS系統之弱點比對完成前，會暫時停用「資產清單上傳」或「已安裝KBID清單上傳」功能，待收到「弱點比對完成」通知信後方可執行下一次上傳

3. 如何知道資產是否上傳成功與弱點比對完成？
- VANS系統於資產上傳成功後，會收到「資訊資產清單解析完成」通知信件
 - VANS系統於資產弱點比對完成後，會收到「資產風險項目比對完成」通知信件，依據上傳資產與弱點數量多寡及排程隊列而定，約莫1週時間比對弱點

VANS常見問答(5/10)



系統操作

4.

為什麼我收不到VANS系統的通知信?

- 請確認「設定管理」→「弱點通知之電子郵件設定」是否已經正確設定電子郵件
- 請確認「設定管理」→「通知設定」是否開啟(紅框處必須為「ON」狀態)

The screenshot displays the VANS system settings interface. On the left is a navigation menu with options like '首頁', '機關總覽', '資訊資產管理', '資產風險狀態', '資訊查詢', '設定管理', '帳號管理', '通知設定', and '資產管理API設定'. The '通知設定' (Notification Settings) option is highlighted with a red box. The main content area is divided into three sections:

- 請輸入欲接收弱點通知之分數**: A form with a text input field containing '5.0' and a '設定' (Set) button.
- 弱點通知之電子郵件設定**: A section for configuring email recipients. It includes a text input field for the email address, three rows of email icons with '刪除欄位' (Remove Field) buttons, and a '新增電子郵件欄位' (Add Email Field) button at the bottom.
- 通知設定**: A section for enabling notifications. It features a toggle switch labeled '請選擇是否接收弱點通知' (Please select whether to receive vulnerability notifications), which is currently set to 'ON' and highlighted with a red box. A '設定' (Set) button is located below.

At the top right of the main content area, there is a table showing severity levels and their corresponding base score ranges:

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

VANS常見問答(6/10)



資產上傳出現錯誤該如何排除？

1.自VANS系統下載最新版本「完整軟體資產CPE清單」



5.

2.依據錯誤訊息找到對應之CPE條目，確認是否可於「完整軟體資產CPE清單」找到完全相同之「**CPE2.3**」與「**CPE完整名稱**」

- 有找到相同「**CPE2.3**」與「**CPE完整名稱**」時，應為**正確**之CPE條目。若仍無法上傳請透過VANS服務信箱(VansService@nics.nat.gov.tw)反映
- 未找到相同「**CPE2.3**」與「**CPE完整名稱**」時，應為**錯誤**之CPE條目，無法上傳至VANS系統。請依循步驟3~6至NVD官網進行確認該CPE條目是否已遭取代

VANS常見問答(7/10)



5.

3.至NVD官網(<https://nvd.nist.gov/products/cpe/search>)查詢該CPE條目，並確認勾選「Include deprecated CPEs」

Search Common Platform Enumerations (CPE)

This search engine can perform a keyword search, or a CPE Name search. The keyword search will perform the user specified search text. The CPE Name search will perform searching for an exact match, as well specified in the user-specified CPE Name.

CPE Naming Format: 2.3 2.2

CPE Name or Keyword:

Include deprecated CPEs

4.搜尋後，點選欲查找之CPE條目

Search Results (Refine Search)

Search Parameters:

There are **1** matching records.

- Keyword:
cpe:2.3:a:oracle:jre:1.8.0:update_191:*:*:*:*
- CPE Status: FINAL,DEPRECATED
- CPE Naming Format: 2.3

Vendor	Product	Version	Update	Edition	Language
oracle	jre	1.8.0	update_191		

cpe:2.3:a:oracle:jre:1.8.0:update_191:*:*:*:* (Deprecated) [View CVEs](#)

VANS常見問答(8/10)



系統操作

5.

5. 依據頁面資訊確認該CPE條目是否已遭取代

CPE Summary

[Return to Search Listing](#)

! This CPE has been deprecated to:

- `cpe:2.3:a:oracle:jre:1.8.0:update191:*:*:*:*`

新的CPE條目

QUICK INFO

Created On: 01/14/2020

Last Modified On: 05/13/2022

遭取代的時間

CPE Names

Version 2.3: `cpe:2.3:a:oracle:jre:1.8.0:update_191:*:*:*:*` 遭取代之CPE條目

Version 2.2: `cpe:/a:oracle:jre:1.8.0:update_191`

[Read information about CPE Name encoding](#)

6. 請點選「新的CPE條目」以查看「新的CPE2.3」與「新的CPE完整名稱」，並更新至上傳清單，即可重新上傳至VANS系統

CPE Summary

[Return to Search Listing](#)

CPE Names

新的CPE2.3

Version 2.3: `cpe:2.3:a:oracle:jre:1.8.0:update191:*:*:*:*`

Version 2.2: `cpe:/a:oracle:jre:1.8.0:update191`

[Read information about CPE Name encoding](#)

This CPE has deprecated the following CPE(s):

`cpe:2.3:a:oracle:jre:1.8.0:update_191:*:*:*:*`

[CPE NAME COMPONENTS](#)

QUICK INFO

Created On: 05/13/2022

Last Modified On: 05/13/2022

Titles:

Text

新的CPE完整名稱

Locale

Oracle Java Runtime Environment (JRE) 1.8.0 Update 191

en_US



有關VANS系統上傳功能釋疑：

- (1)曾上傳資產至VANS系統，再次上傳時系統會如何處理？
- (2)透過API上傳時，系統也是以覆蓋方式處理嗎？
- (3)若是透過覆蓋方式上傳，已填寫之改善措施是否也會被覆蓋呢？

6. • (1)系統會透過覆蓋方式處理，僅留存最後一次上傳之資產。
(2)透過API上傳之資產同樣以覆蓋方式處理，僅留存最後一次上傳之資產。
(3)重新上傳後，系統會依據新上傳之資產進行弱點比對。若已填寫改善措施之弱點項目未變動，則改善措施仍會存在

VANS系統之「查看修補KBID」功能是否已有考量KB取代關係呢？

7. • VANS系統已有考量KB取代關係，請點擊CVE弱點之「查看修補KBID」欄位，彈出清單內容即顯示可修補此弱點之所有KB編號

上傳已安裝KBID至VANS系統後，要如何查看哪些弱點尚未修補？

8. • 可至資訊資產風險列表中，查看各資產「詳細資訊」之「修補KBID」欄位，該數字代表該CVE弱點之「已安裝KBID數量/應安裝KBID數量」，若已安裝KBID數量小於應安裝KBID數量，則表示該弱點尚未修補

VANS常見問答(10/10)



綜合問答

1.

VANS與弱點掃描之差異？

項目	VANS	弱點掃描
資訊蒐集方式	透過作業系統內建工具或第三方軟體，產出已安裝資訊資產清單	透過網路遠端執行掃描
弱點查詢方式	將登錄至VANS之資訊資產項目與版本進行弱點比對	透過弱掃軟體plugin進行弱點偵測
比對範圍	登錄至VANS之所有資訊資產	目標主機對外服務使用套件
時間性	下列情境會觸發1次弱點比對，最低觸發間隔為2小時 <ul style="list-style-type: none">每日與NVD更新後機關資產異動後	定期執行掃描

結論(1/2)

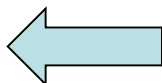


● 導入應特別注意事項

- **上傳資訊資產前**：機關應檢視欲上傳資產內容之合理性，如利用CPE條目或資產名稱檢視上傳作業系統數與實際導入電腦數量之差異，以評估資產盤點之合理性

步驟2. 將欲上傳資產之作業系統加總

步驟1. 利用關鍵字「:o:」進行篩選



部分作業系統可能有未比對到CPE條目之情形，則可用資產名稱進行搜尋

產品類別為「o」表示為作業系統

步驟3. 比較實際導入電腦數量與欲上傳作業系統數之差異，以評估資產盤點之合理性

機關OID	資產名稱	資產數量	資產名稱	CPE 2.3	資產格式
2.16.886.		7	Nero Info	N/A	custom
2.16.886.		1	OCR	N/A	custom
2.16.886.		2	VMware Player	N/A	custom
2.16.886.		21	Visual C++ 2015-2019 Redistributable (x86)	N/A	custom
2.16.886.		1	ATSignServerUser	N/A	custom
2.16.886.		1	Microsoft Office Standard 2013	o:microsoftoffice:2013:*:*:*	cpe
2.16.886.		1	Nmap 7.80	3:nmap:nmap:7.80:*:*:*	cpe
2.16.886.		1	Microsoft .NET Framework 4.8 SDK	o:microsoft:.net_framework:4.8:*:*	cpe
2.16.886.		18	Microsoft Office LTSC 標準版 2021 - zh-tw	o:microsoftoffice:2021:*:*:*:tsch	cpe
2.16.886.		1	Notepad++ (64-bit x64)	N/A	custom
2.16.886.		1	ATSignServerUser	N/A	custom
2.16.886.		1	LINE	o:corp:line:6.3.0.2329:*:*:*	cpe
2.16.886.		1	Java 8 Update 311 (64-bit)	o:oracle:jre:1.8.0:update311:*:*	cpe
2.16.886.		1	會議 Microsoft Teams	N/A	custom
2.16.886.		1	System CLR Types for SQL Server 2012	o:microsoft:sql_server:2012:*:*	cpe
2.16.886.		3	Visual C++ 2008 Redistributable - x86 9.0.30729	N/A	custom
2.16.886.		1	WinMerge 2.16.4.0	o:winmerge:winmerge:2.16.4:*	cpe

結論(2/2)



- 導入應特別注意事項

- 上傳資訊資產後：

- 於上傳資產隔天，應注意資產解析之電郵結果，如解析失敗，可能原因及相關解決方式可參考教材第61-63、126頁
- 每日：機關應注意VANS弱點電郵通知(通知分數門檻不應高於7分)，當發現高風險(CVSS 7分)以上之弱點，應儘速決定弱點處置方式並於1週內於VANS系統填寫改善措施
- 每月：機關應每月更新資訊資產，如接獲重大弱點通報或大量資產異動，亦應即時進行資訊資產更新作業





參考資料

參考資料(1/2)



- Windows Management Instrumentation
 - <https://docs.microsoft.com/zh-tw/windows/desktop/wmisdk/wmi-start-page>
- How to find the Windows version using Registry?
 - <https://mivilisnet.wordpress.com/2020/02/04/how-to-find-the-windows-version-using-registry/>
- Microsoft Docs - Dir
 - <https://docs.microsoft.com/zh-tw/windows-server/administration/windows-commands/dir>
- NVD官方網站
 - <https://nvd.nist.gov/>
- Excel從右向左查找
 - <http://www.gocalf.com/blog/excel-find-from-right.html>

參考資料(2/2)



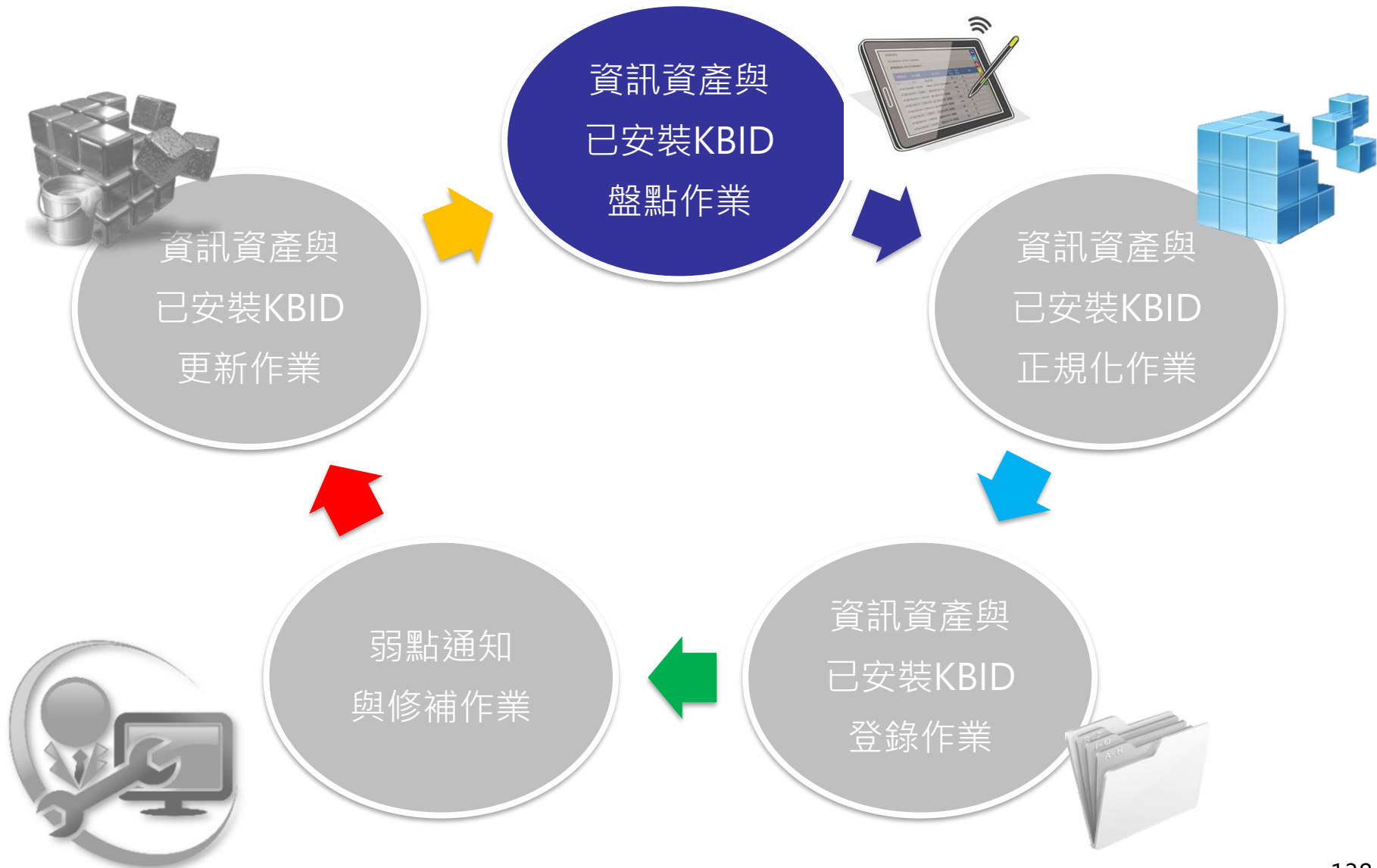
- 用來描述 Microsoft 軟體更新標準術語的說明
 - <https://support.microsoft.com/zh-tw/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro>
- Microsoft Power Query for Excel
 - <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>
- 關於 Excel 中的 Power Query
 - <https://support.office.com/zh-tw/article/Power-Query-%E5%BF%AB%E9%80%9F%E5%85%A5%E9%96%80-7104fbee-9e62-4cb9-a02e-5bfb1a6c536a>
- 瞭解如何在 Power Query (合併多個)
 - <https://support.office.com/zh-hk/article/%E5%90%88%E4%BD%B5%E5%A4%9A%E5%80%8B%E8%B3%87%E6%96%99%E4%BE%86%E6%BA%90%E7%9A%84%E8%B3%87%E6%96%99-Power-Query-70cfe661-5a2a-4d9d-a4fe-586cc7878c7d>



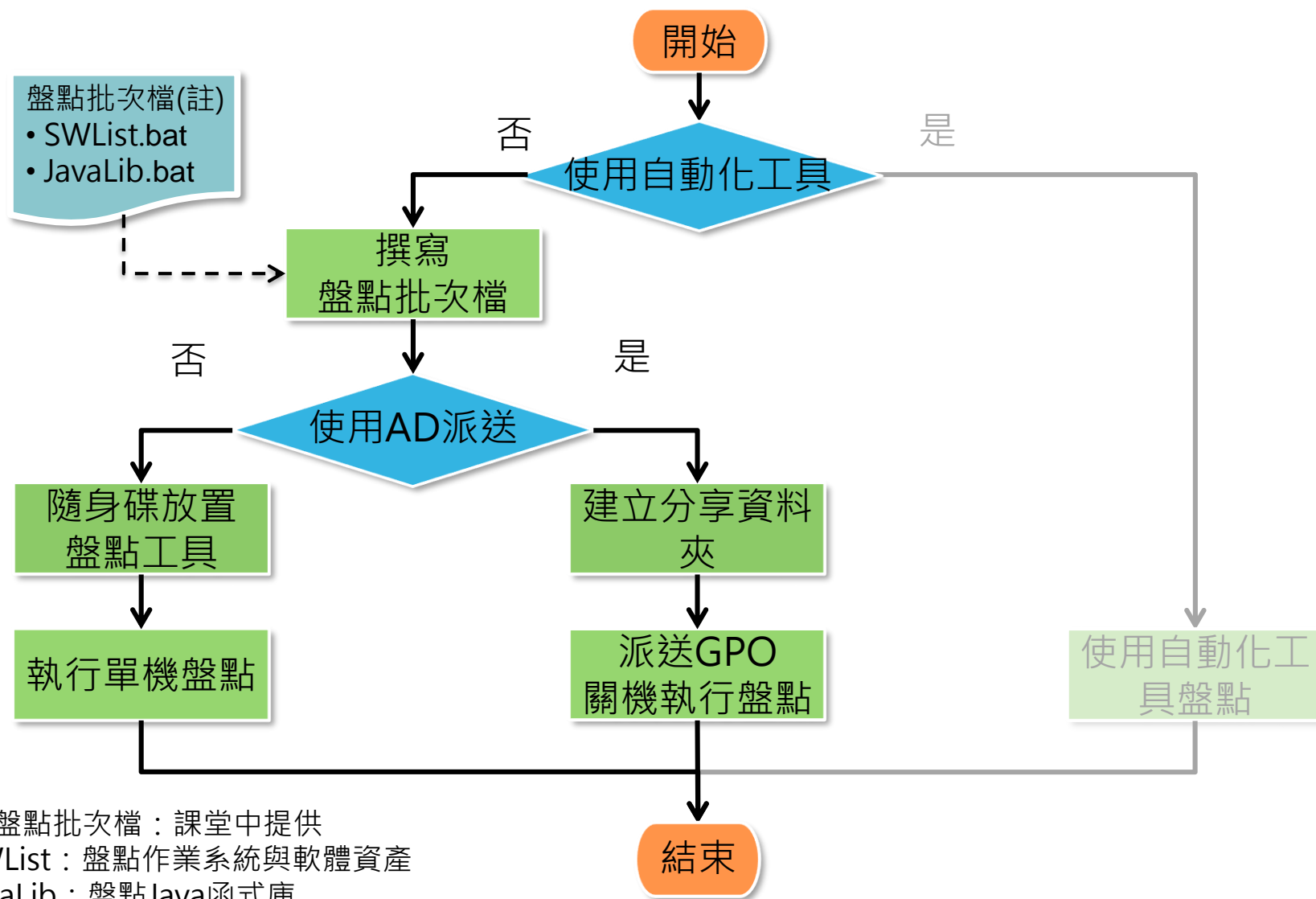
附件1

手動盤點與正規化作業流程

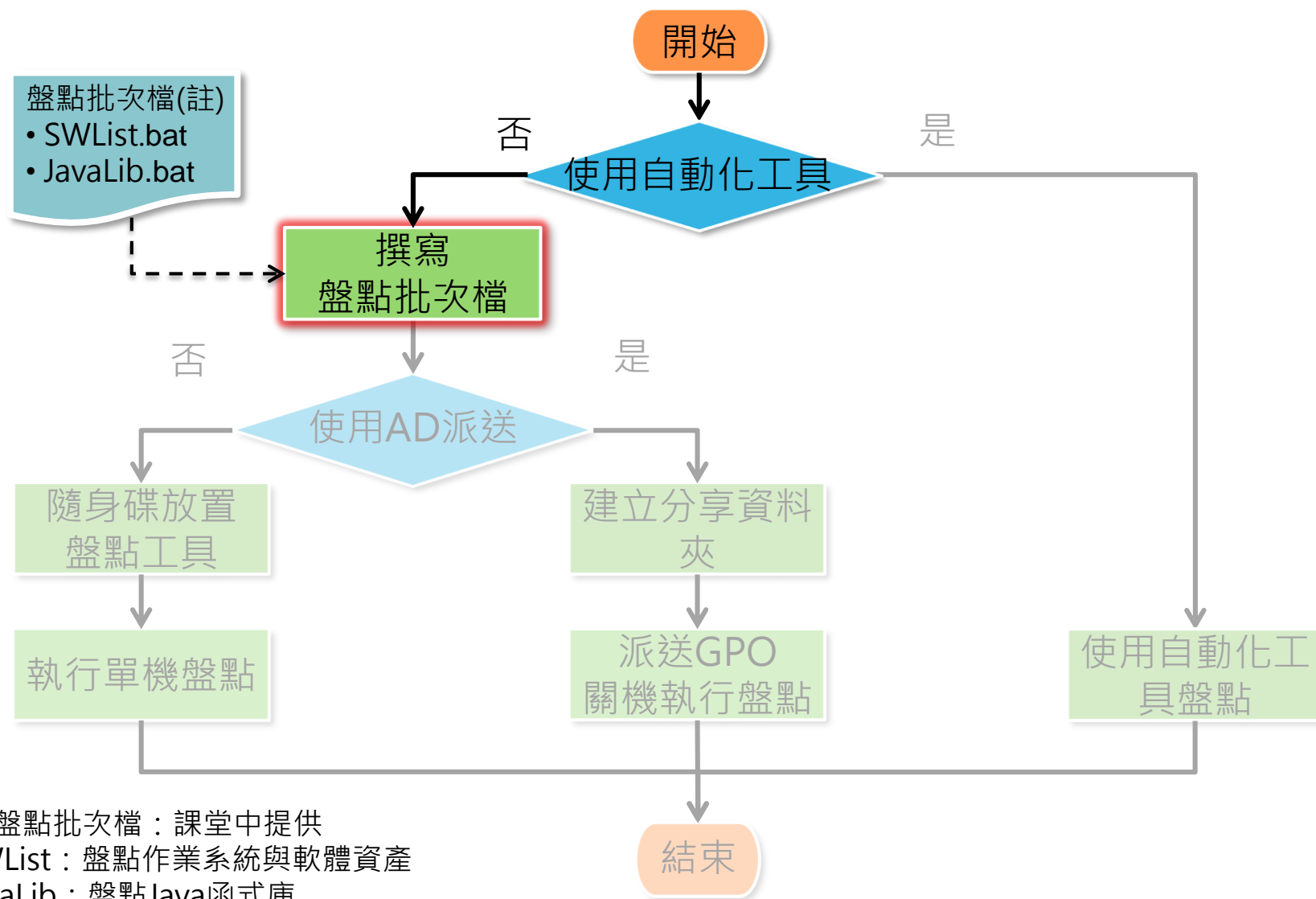
導入作業流程



盤點作業流程



盤點作業流程



註：盤點批次檔：課堂中提供

1.SWList：盤點作業系統與軟體資產

2.JavaLib：盤點Java函式庫

撰寫盤點批次檔(1/2)

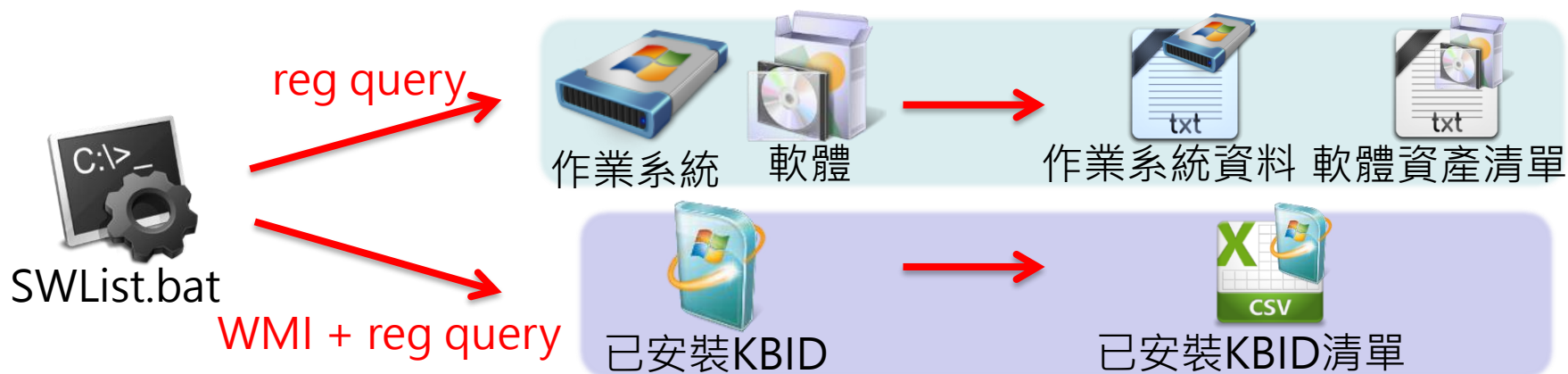


- 登錄機碼值(reg query)

- 藉由查詢登錄機碼值，可列出作業系統資訊、已安裝軟體清單及 Office 相關產品之已安裝 KBID

- Windows 管理工具(簡稱 WMI)

- 運用 Windows 平台作業系統進行檔案管理與操作之技術，讓使用者可透過 WMI 管理本機與遠端電腦，可用以盤點已安裝 KBID



撰寫盤點批次檔(2/2)



● 命令提示字元指令

- 若機關環境有使用Java函式庫時，可透過此批次檔執行盤點
- Tomcat Java函式庫路徑預設位置如下圖
 - cd C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\

```
JavaLib_v1.0.bat
1 FOR /F "tokens=2 delims=[]" %%a in ('ping -4 -n 1 %computername% ^|
  findstr [') do set NetworkIP=%%a
2
3 rem ===切換至Java函式庫位置，準備執行盤點作業===
4 cd C:\Program Files\Apache Software Foundation\Tomcat
  9.0\webapps\docs\WEB-INF\lib\
5
6 rem ===列出Java函式庫，並產出csv格式檔案至公用文件資料夾===
7 dir *.* /S /B /ON > %~dp0\3.Javalib\3.javaoutput_%computername%_
  %DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.csv
```



命令提示
字元指令



Java函式庫

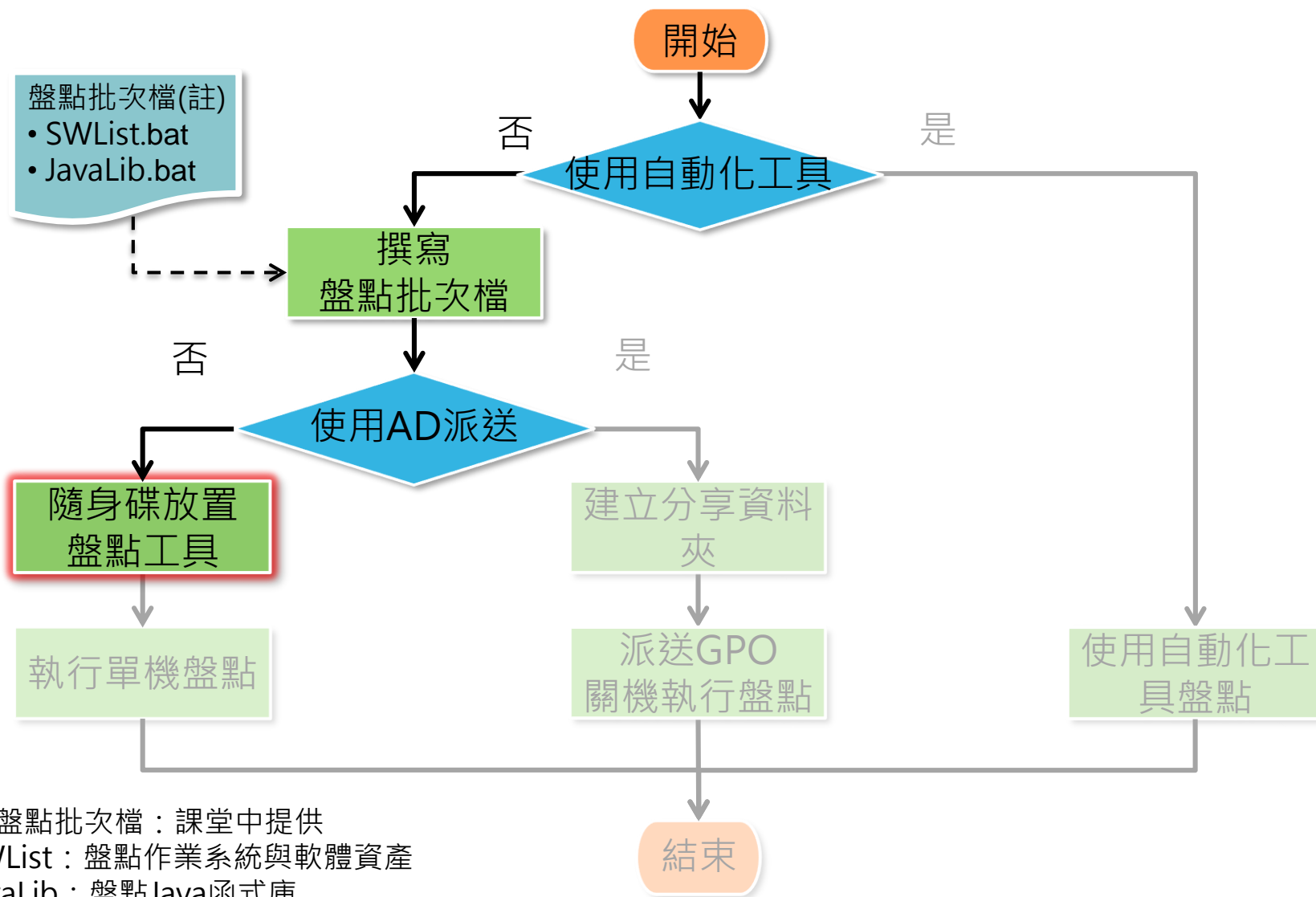


Java函式庫清單



透過系統指令單機盤點

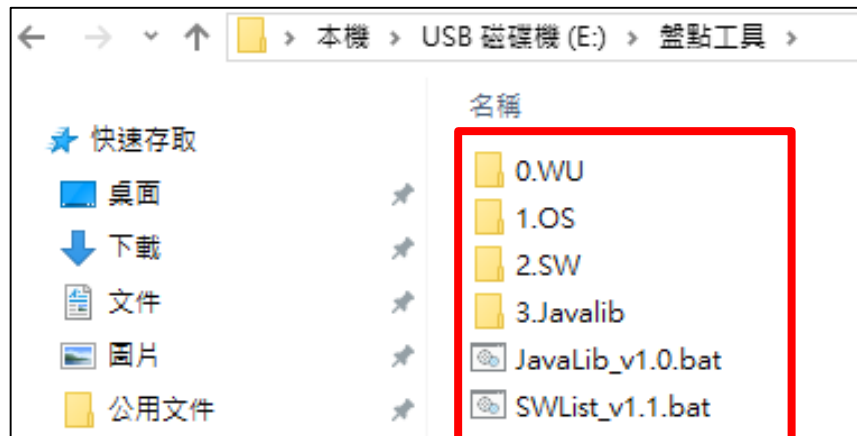
盤點作業流程



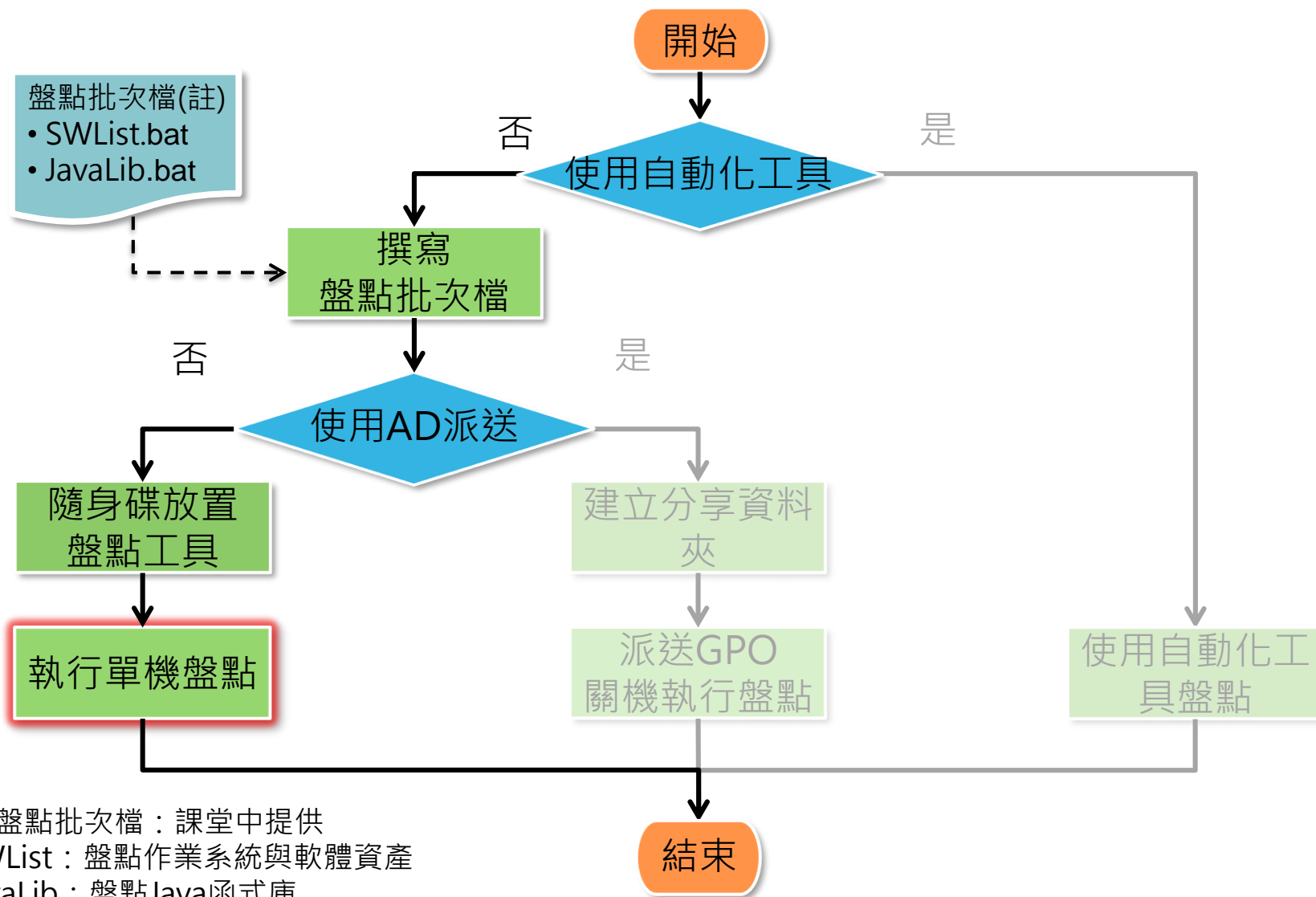
隨身碟放置盤點工具



- 於隨身碟建立資料夾放置盤點批次檔與存取結果資料夾，依欲盤點之資訊資產執行盤點批次檔
 - SWList.bat：盤點作業系統、軟體及已安裝KBID
 - JavaLib.bat：盤點Java函式庫
 - 0.WU資料夾：存取已安裝安全性更新盤點清單之資料夾
 - 1.OS資料夾：存取作業系統盤點清單之資料夾
 - 2.SW資料夾：存取軟體資產盤點清單之資料夾
 - 3.JavaLib資料夾：存取Java函式庫盤點清單之資料夾



盤點作業流程



執行單機盤點(1/2)



- STEP1：以系統管理員身分執行SWList批次檔
- STEP2：檢視盤點結果資料夾，分別為已安裝KBID清單、作業系統資訊及軟體盤點清單

USB 磁碟機 (E:) > 盤點工具

名稱

- 0.WU
- 1.OS
- 2.SW
- 3.Javalib
- JavaLibv1.0.bat
- SWListv1.3_USB.bat

開啟(O)
編輯(E)
列印(P)
以系統管理員身分執行(A)

USB 磁碟機 (E:) > 盤點工具

名稱

- 0.WU
- 1.OS
- 2.SW
- 3.Javalib
- JavaLibv1.0.bat
- SWListv1.3_USB.bat

USB 磁碟機 (E:) > 盤點工具 > 0.WU

名稱

- 0.WU_WINSER2019X64_20210808.csv

USB 磁碟機 (E:) > 盤點工具 > 1.OS

名稱

- 1.OS_WINSER2019X64_20210808.txt

USB 磁碟機 (E:) > 盤點工具 > 2.SW

名稱

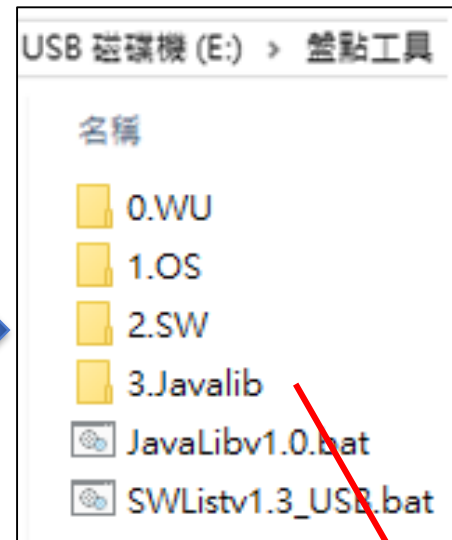
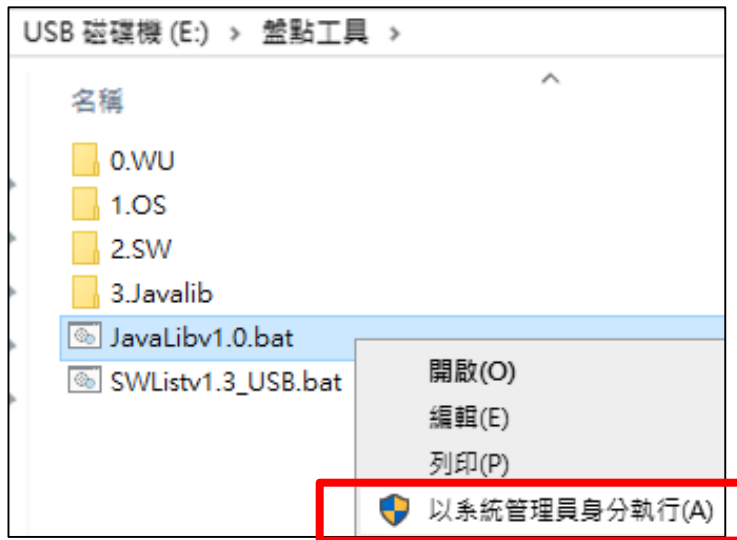
- 2.SW_WINSER2019X64_20210808.txt

盤點完成視窗自動關閉

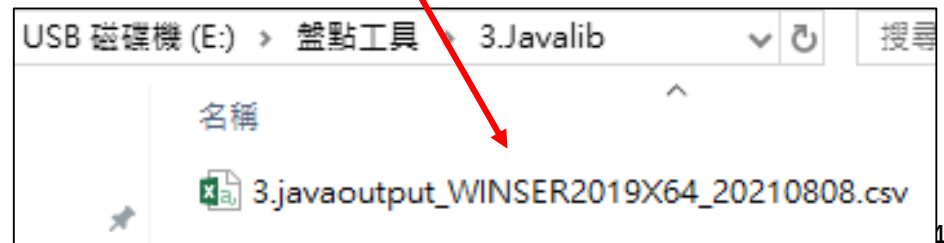
執行單機盤點(2/2)



- STEP3 : 以系統管理員身分執行JavaLib批次檔
- STEP4 : 檢視盤點結果資料夾內含Java函式庫清單



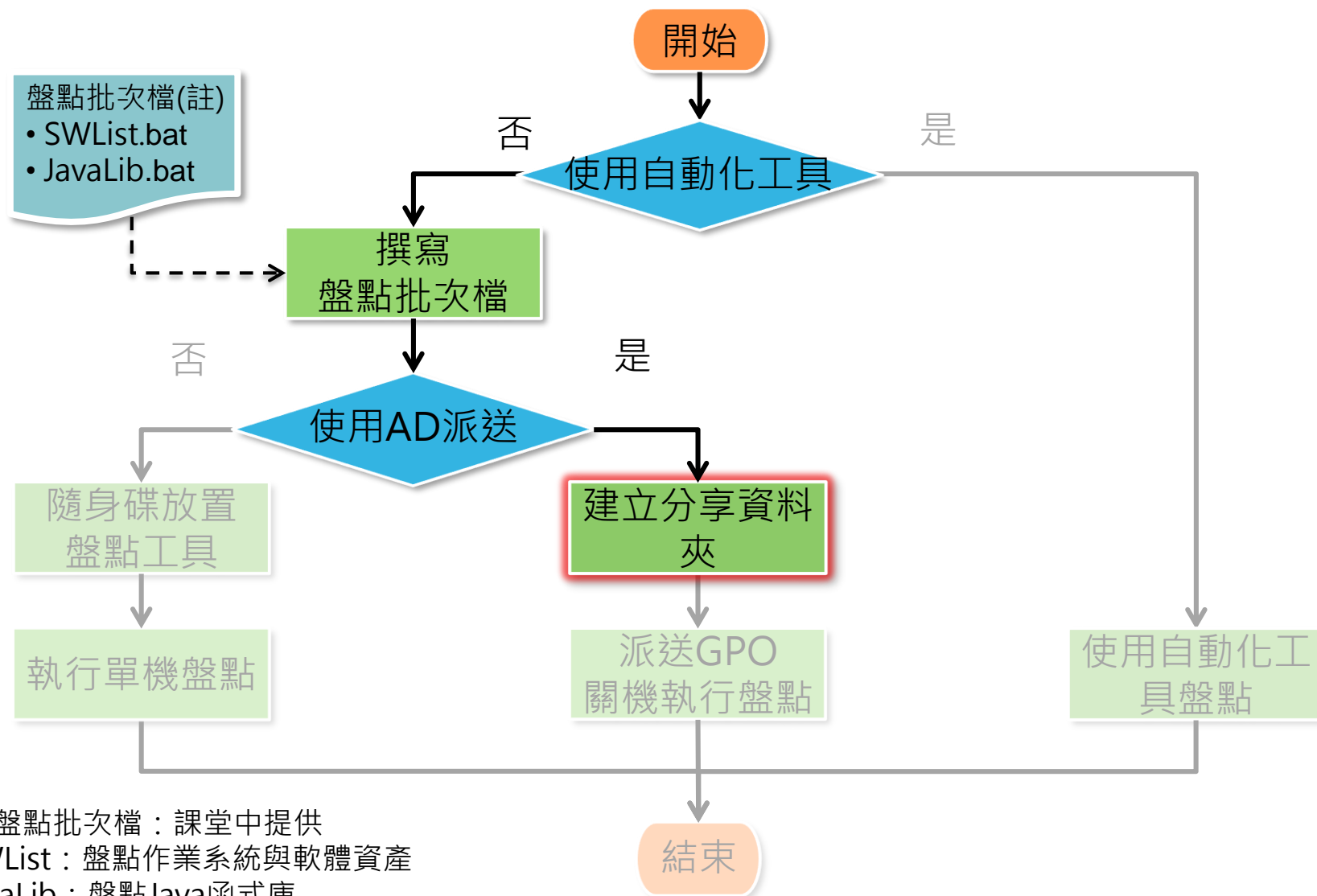
盤點完成視窗自動關閉





透過系統指令批次盤點

盤點作業流程



AD主機建立分享資料夾(1/3)



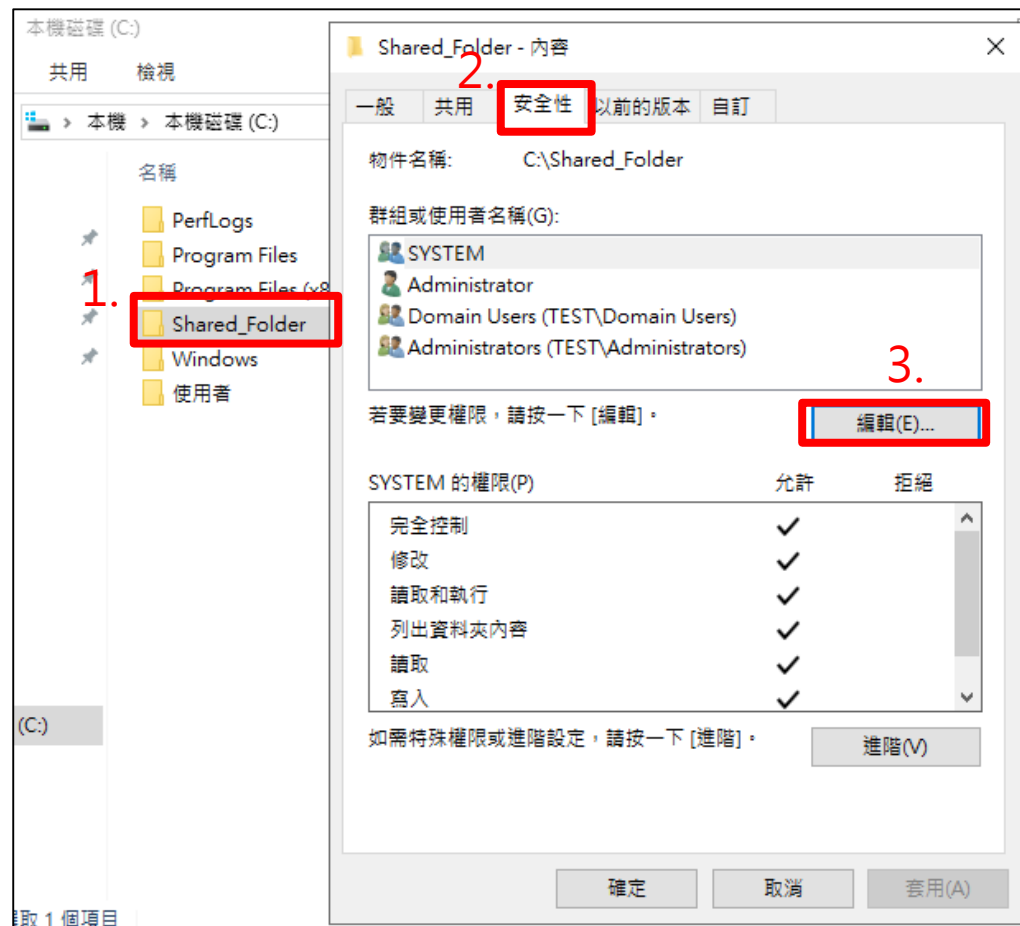
- STEP1：於AD主機建立分享資料夾 (Shared_Folder)
- STEP2：點選右鍵內容，接著點選共用頁籤，設定Domain Users可「讀取/寫入」此資料夾



AD主機建立分享資料夾(2/3)



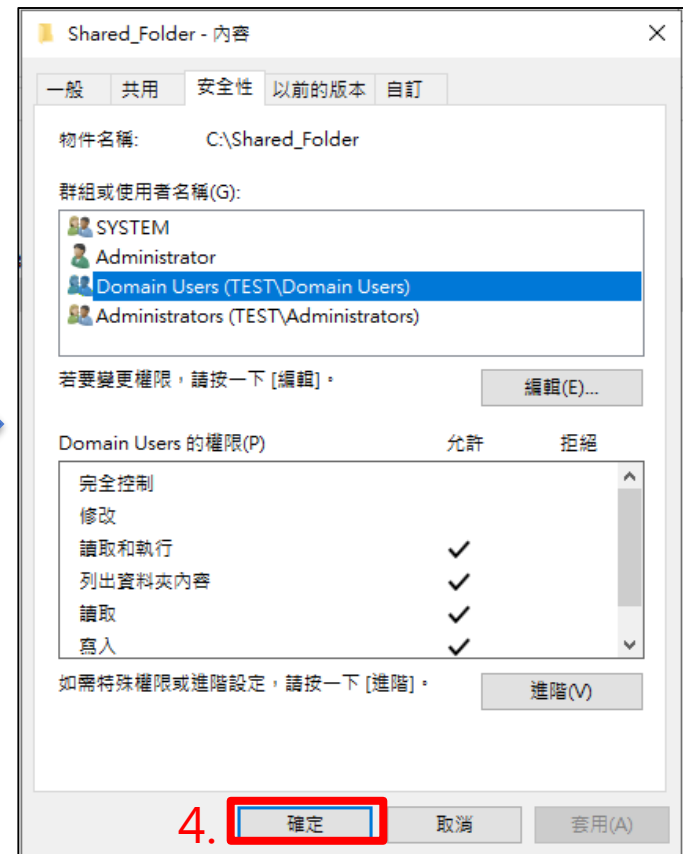
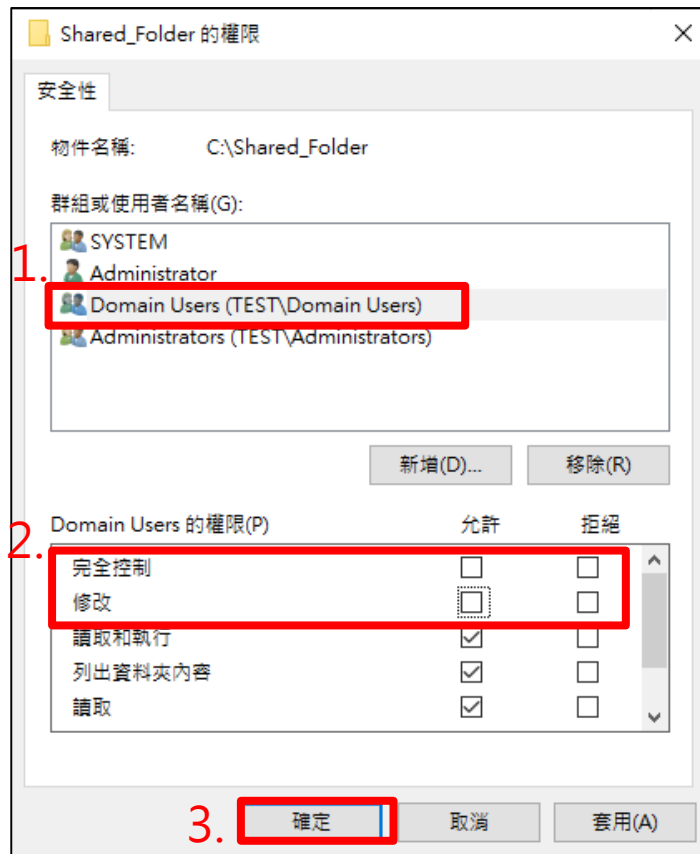
- STEP3：避免網域使用者誤刪檔案，需限縮其存取權限，切換至**安全性**頁籤，並點選編輯



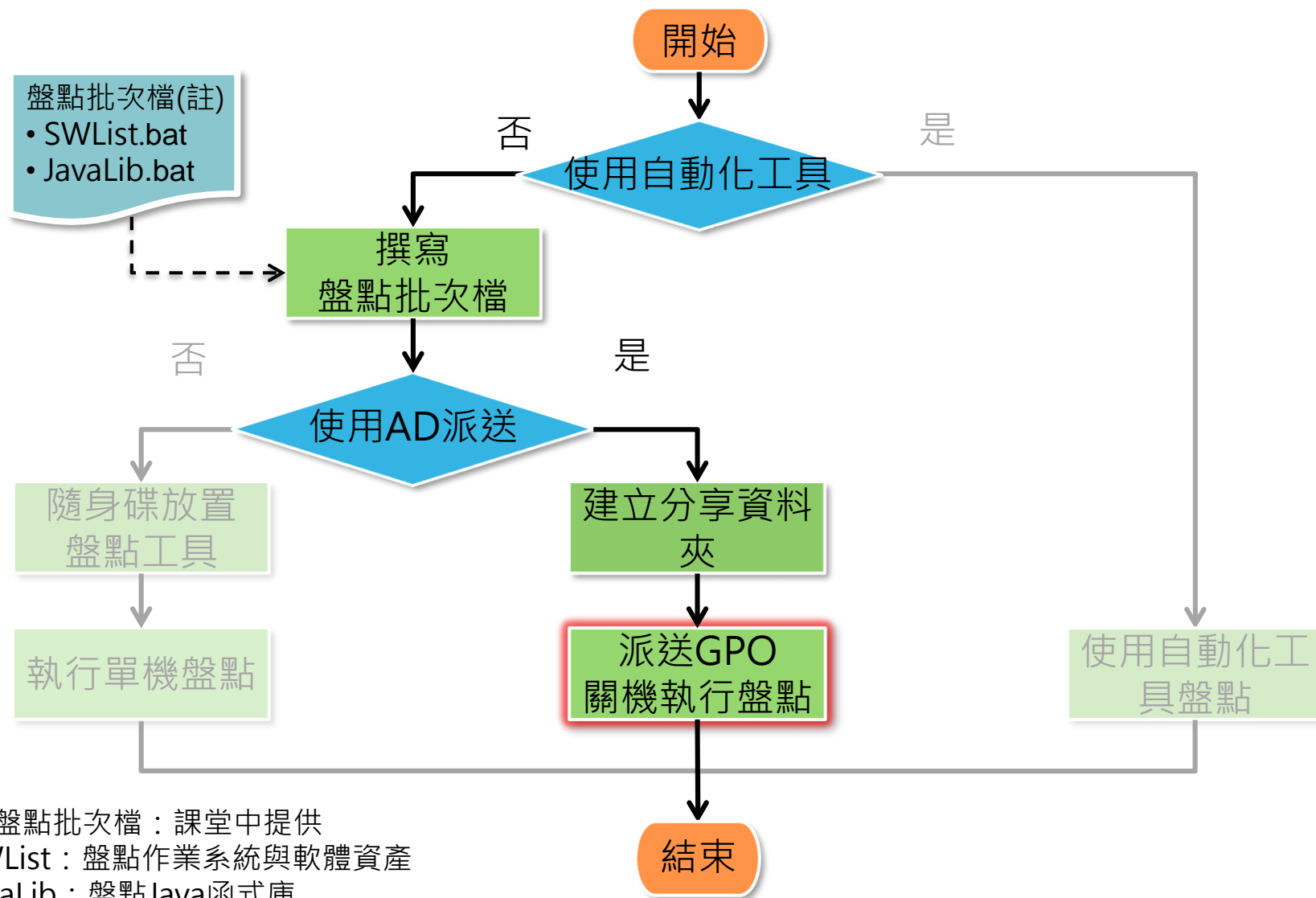
AD主機建立分享資料夾(3/3)



- STEP4：選取Domain Users並移除「完全控制」與「修改」權限，使Domain Users僅能讀取或寫入資料，但不可修改與刪除



盤點作業流程



派送GPO-關機執行(1/5)



- 在目標OU點選右鍵並建立GPO
 - 新增「關機執行」GPO

The screenshot shows the Group Policy Management console for the test.com domain. The left pane displays the tree structure with 'test.com' selected. The right pane shows the 'test.com 中的 群組原則物件' (Group Policy Objects in test.com) list. A context menu is open over the 'test.com' folder, and the option '在這個網域中建立 GPO 並將它連結到這裡(C)...' (Create a GPO in this domain and link it to here) is highlighted. A blue arrow points from this option to the '新增 GPO' (New GPO) dialog box. In the dialog box, the '名稱(N):' (Name) field contains '關機執行' (Shutdown Execution). The '來源入門 GPO(S):' (Source Starter GPO(S)) dropdown is set to '(無)' (None). The '確定' (OK) button is highlighted.

1. 在這個網域中建立 GPO 並將它連結到這裡(C)...

2. 關機執行

3. 確定

派送GPO-關機執行(2/5)



- 編輯GPO，於電腦關機時執行檢測批次檔
 - 點選剛建立的「關機執行」GPO，按右鍵選擇編輯
 - 路徑為：電腦設定\原則\Windows設定\指令碼 - (啟動/關機)\關機
 - 點擊「關機」並編輯「關機-內容」

The screenshot illustrates the process of editing a Group Policy Object (GPO) in the Group Policy Management console. The console shows the hierarchy: 群組原則管理 > 樹系: test.com > 網域 > test.com > Practice > 關機執行. A right-click context menu is open over the '關機執行' GPO, with '編輯(E)...' selected. The console then shows the path: 群組原則管理編輯器 > 檔案(F) 動作(A) 檢視(V) 說明(H) > 電腦設定 > 原則 > Windows 設定 > 指令碼 - (啟動/關機). The '關機' option is selected in the '指令碼 - (啟動/關機)' pane. The '關機 - 內容' pane is open, showing the 'PowerShell 指令碼' tab with the command '關機' and the '關機' button highlighted.

派送GPO-關機執行(3/5)



- 點選「顯示檔案」，準備放入檢測批次檔
- 因作業系統預設不允許複製檔案至網路位置，須將資料夾路徑改為本機路徑，放入盤點批次檔後即可關閉
 - 由「**\\[網域名稱]\SysVol\[網域名稱]\Policies\{關機執行GPO_GUID}\Machine\Scripts\Shutdown**」
 - 改成「**C:\Windows\SYSVOL\domain\Policies\{關機執行GPO_GUID}\Machine\Scripts\ Shutdown**」

The screenshot illustrates the process of changing the path for a shutdown script in a Group Policy Object (GPO). It is divided into three main sections:

- Left Panel (GPO Content):** Shows the '關機 - 內容' (Shutdown - Content) window. The '顯示檔案(S)...' (Show files...) button is highlighted with a red box, indicating the next step in the process.
- Top Panel (Current Path):** Shows the current path in the file explorer: `\\test.com\SysVol\test.com\Policies\A65ADF9A-D69A`. This path is highlighted with a red box.
- Bottom Panel (New Path):** Shows the new path: `C:\Windows\SYSVOL\domain\Policies\A65ADF9A-D69A`. This path is also highlighted with a red box. A yellow callout box with the text '放入盤點批次檔' (Put in the inventory batch file) points to this path. Below the path, a file named 'SWListv1.3_AD.bat' is selected and highlighted with a red box, with a '2.' next to it.

Blue arrows indicate the flow of the process: from the '顯示檔案(S)...' button to the current path, and then to the new path and the selected file.

派送GPO-關機執行(4/5)



- 選擇關機執行的檔案

- 選擇「新增」後，點選「瀏覽」並選取前一步驟放入的盤點批次檔

The image shows a sequence of four screenshots illustrating the steps to add a shutdown command to a GPO:

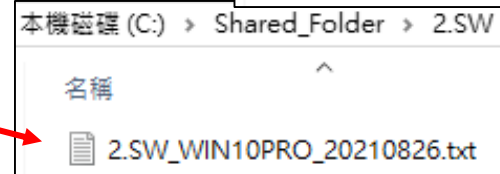
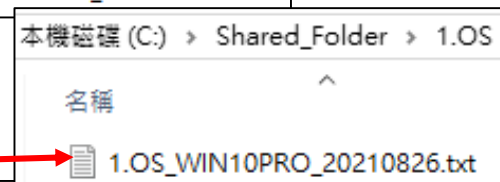
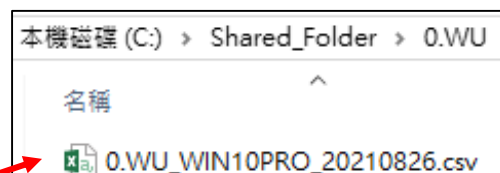
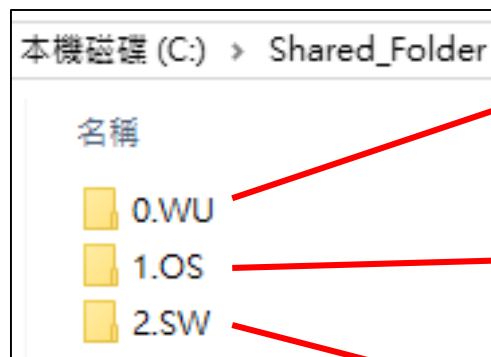
- 1.** In the '關機 - 內容' dialog box, the '新增(D)...' button is highlighted.
- 2.** In the '新增指令碼' dialog box, the '瀏覽(B)...' button is highlighted.
- 3.** In the File Explorer window, the file 'SWListv1.3_AD.bat' is selected in the 'Shutdown' folder.
- 4.** In the File Explorer window, the '開啟(O)' button is highlighted.
- 5.** In the '新增指令碼' dialog box, the '確定' button is highlighted.

派送GPO-關機執行(5/5)



- 電腦關機時，將自動執行盤點
- 盤點結果將產出至本機之「共用文件」中，並自動回存至AD主機「Shared_Folder」資料夾

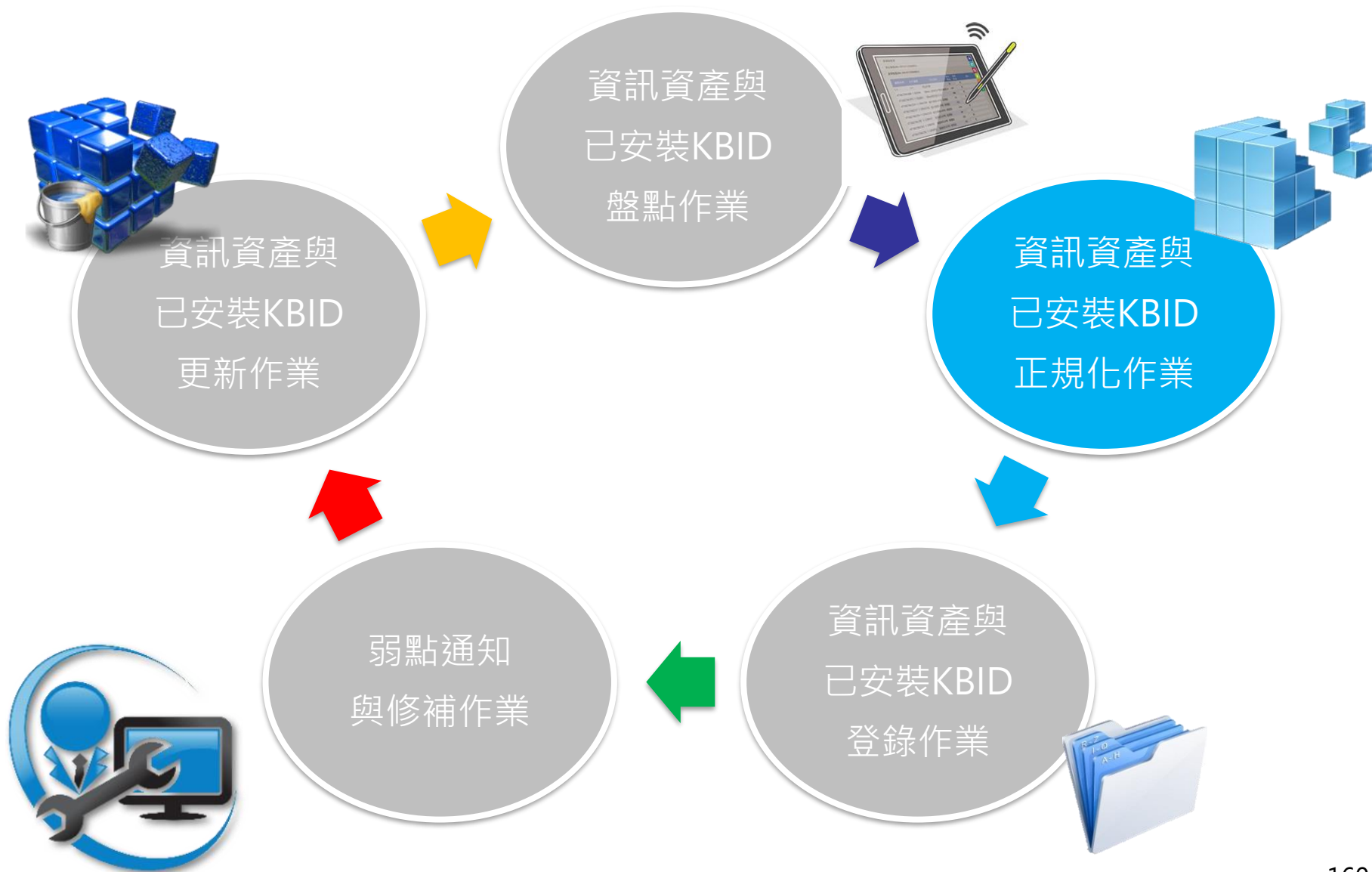
AD主機



執行盤點電腦



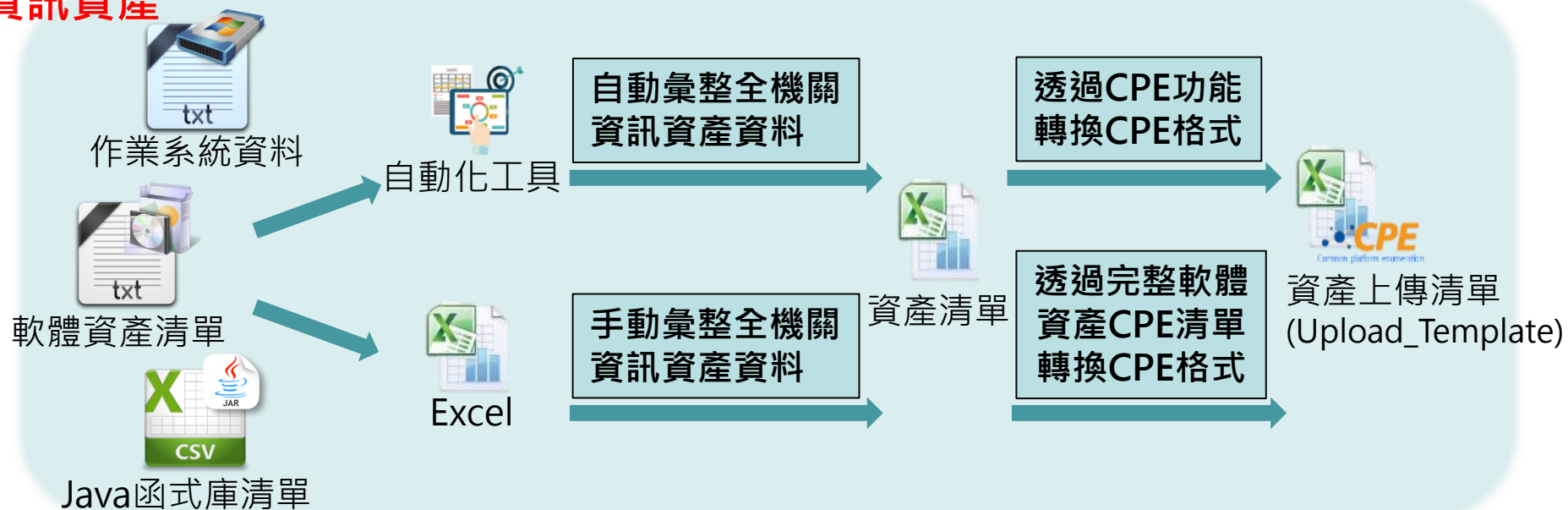
導入作業流程



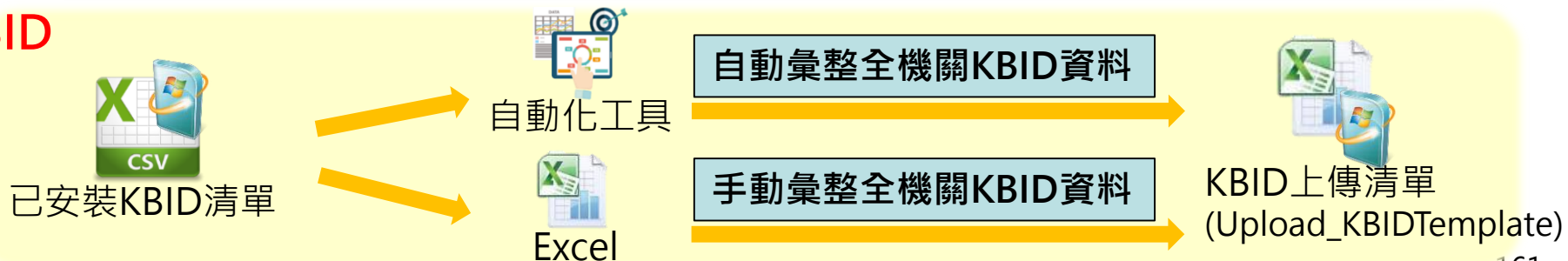
資訊資產與已安裝KBID正規化

- 透過自動化工具或Excel彙整為全機關資料，並將資訊資產轉換為CPE格式

資訊資產



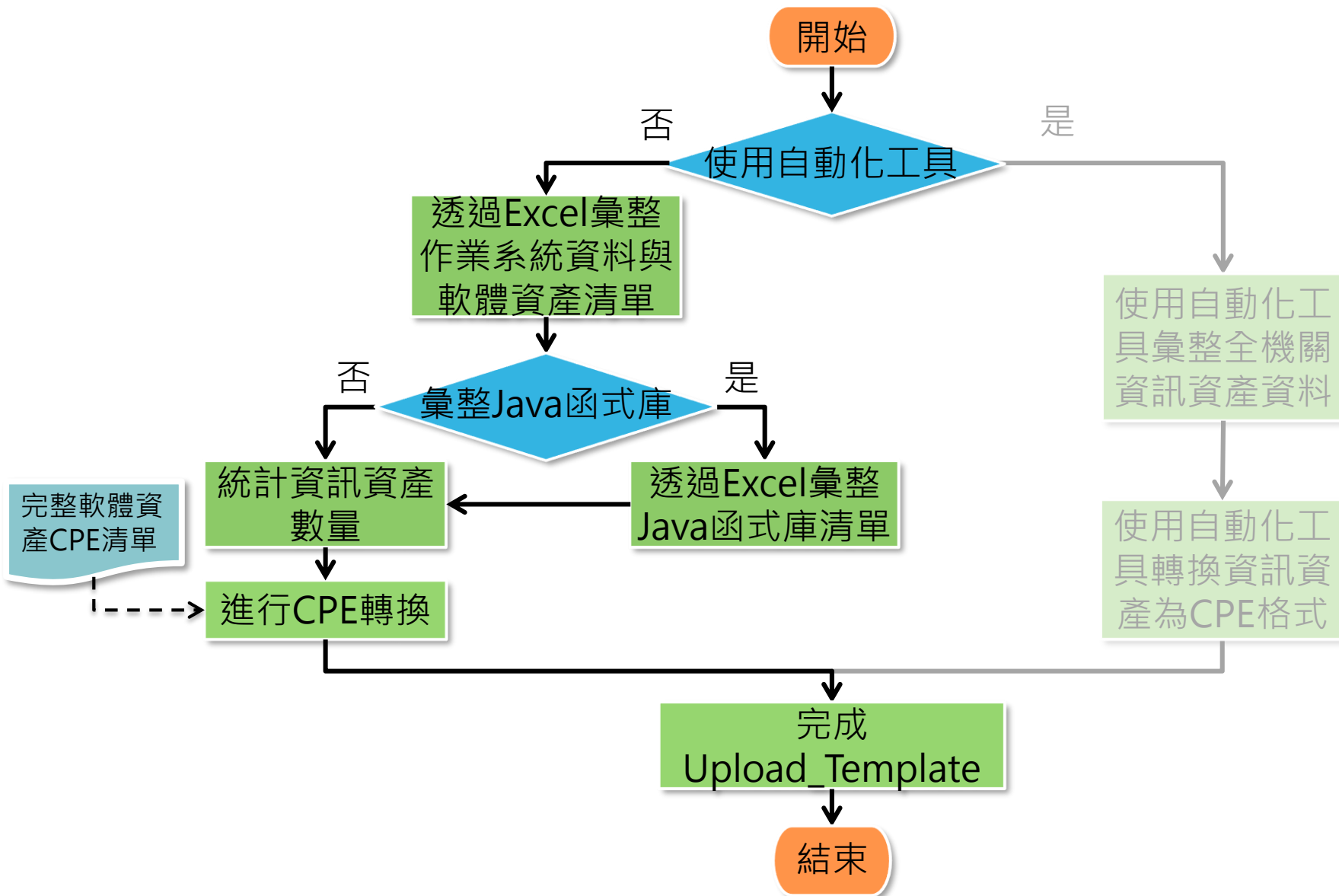
KBID



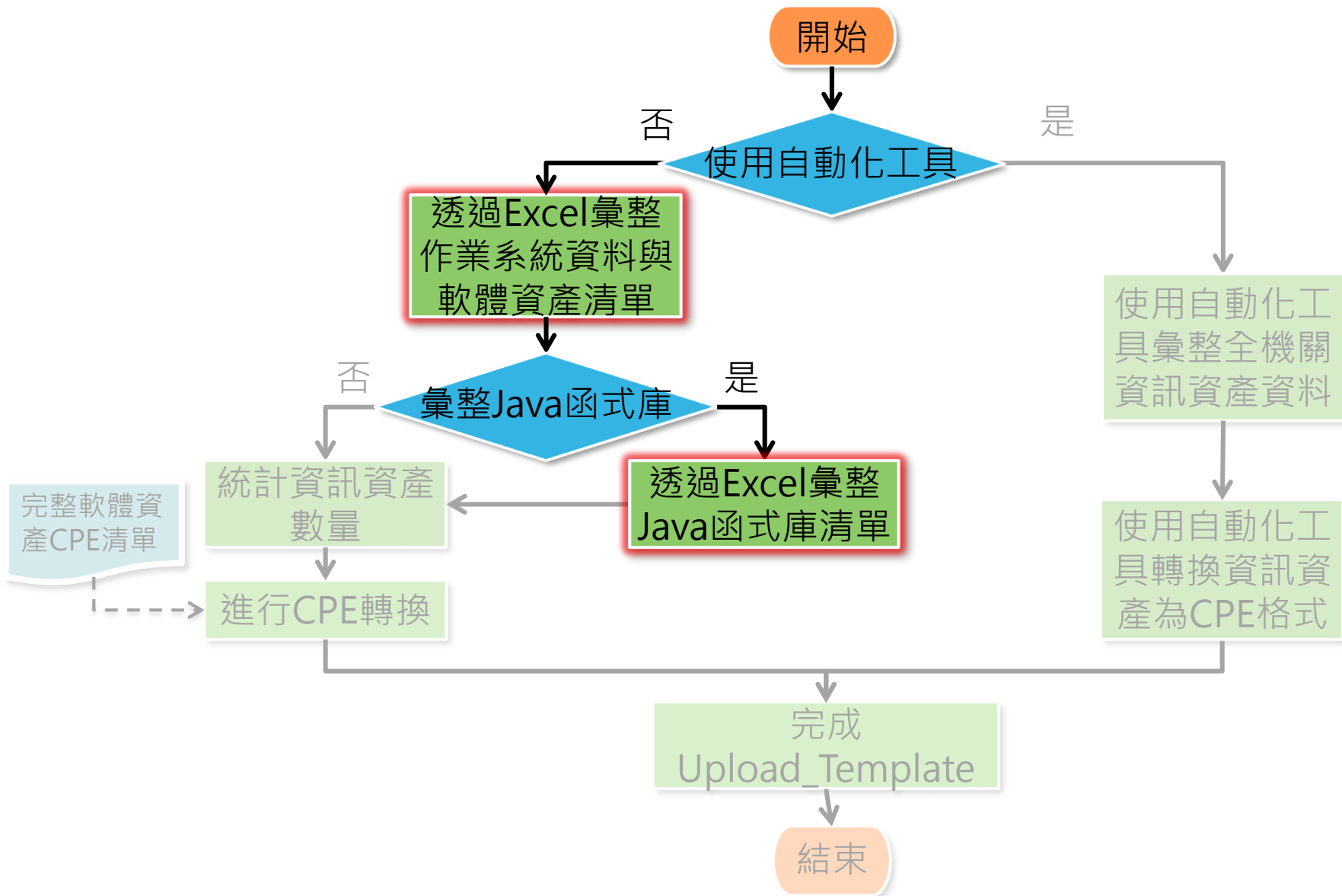


資訊資產正規化作業

資訊資產正規化作業流程



資訊資產正規化作業流程



Excel彙整功能介紹



- Microsoft Power Query for Excel可在各種不同的資料來源中合併或精簡資料



- 適用於32位元與64位元平台
- 支援作業系統版本
 - Windows 7/8/8.1/10
 - Windows Server 2008 R2/2012
- 支援Office版本
 - Microsoft Office 2010 Professional Plus(需另行安裝套件)
 - Microsoft Office 2013 (需另行安裝套件)
 - Power Query內建於Excel 2016、2019中，功能名稱為「取得及轉換」
- 須Internet Explorer 9以上之版本

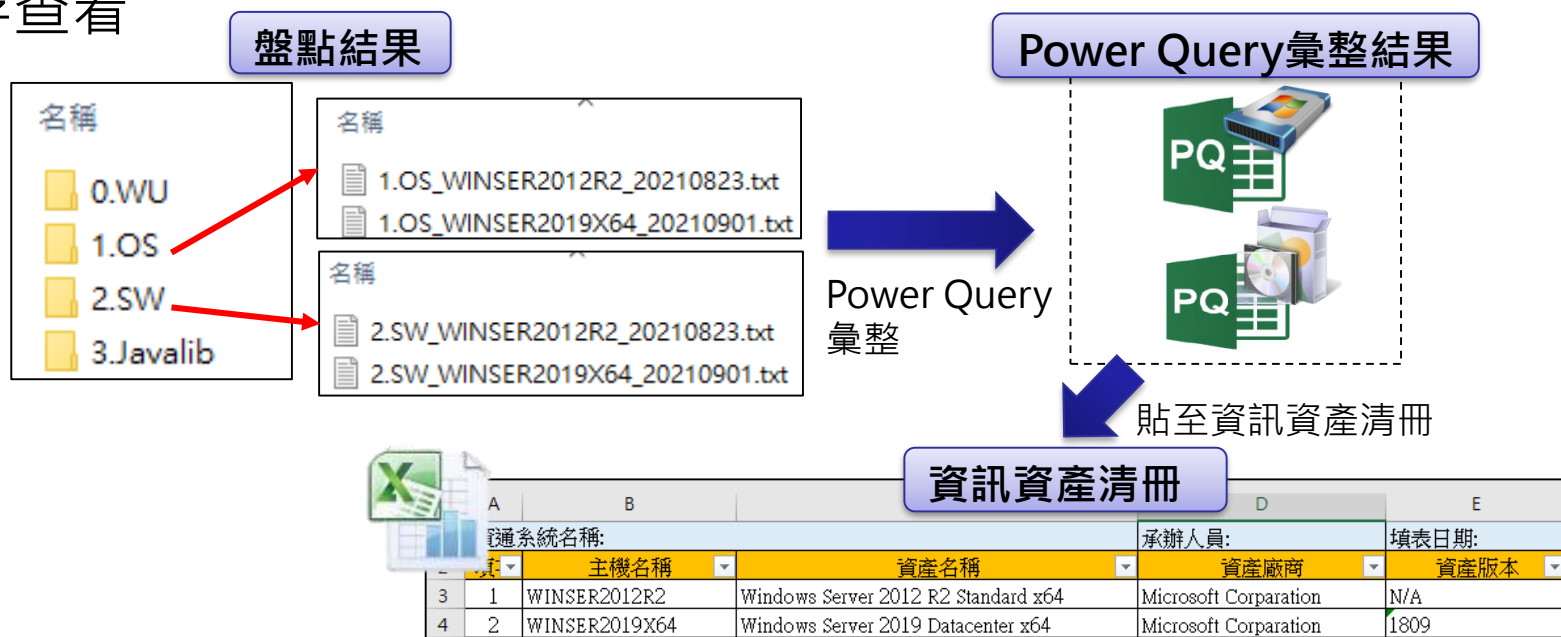
- 下載網址：

- <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>

彙整資訊資產清單



- 透過Power Query分別彙整歸類後作業系統與軟體資產之盤點結果
 - 若欲了解彙整步驟，請參閱「資通安全弱點通報系統操作手冊*」v1.8或更新版本
- 將**作業系統**與**軟體資產**彙整結果，整合至**資訊資產清冊***，以留存查看



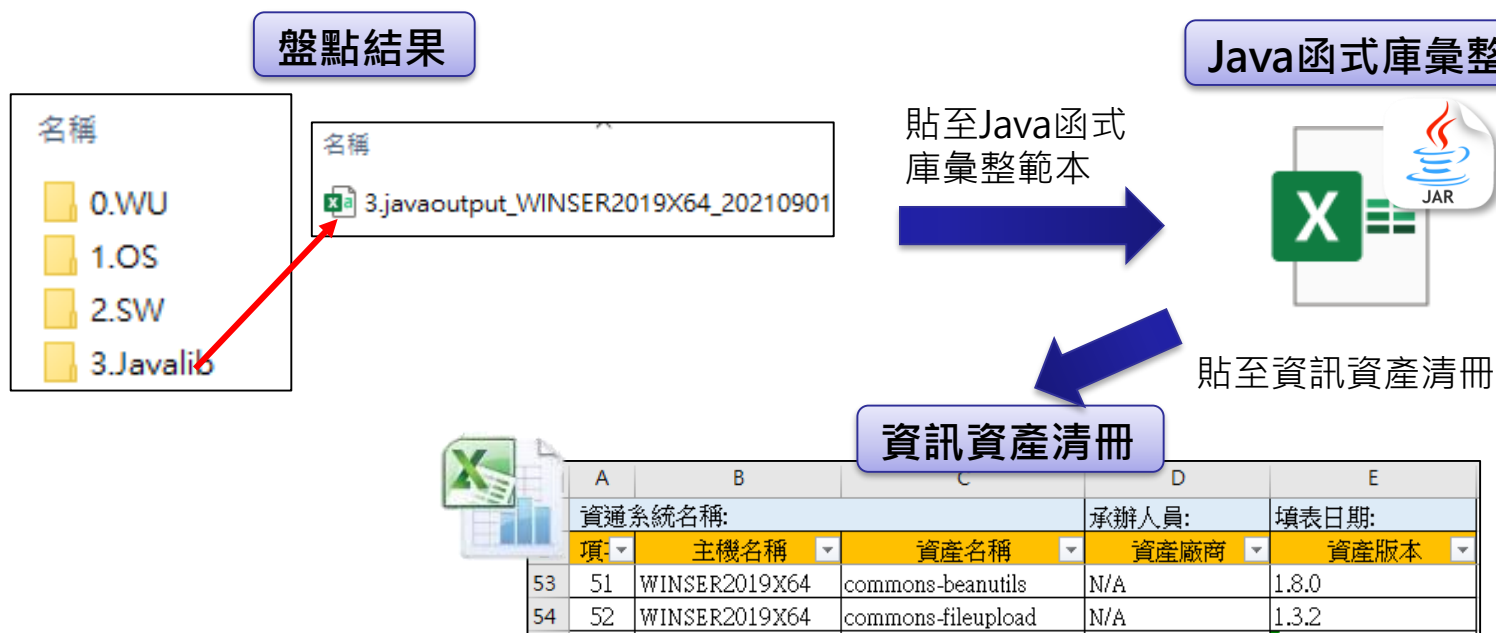
註1：操作手冊：機關管理者帳號開通之通知信提供或透過VansService服務信箱索取

註2：資訊資產清冊：課堂中提供

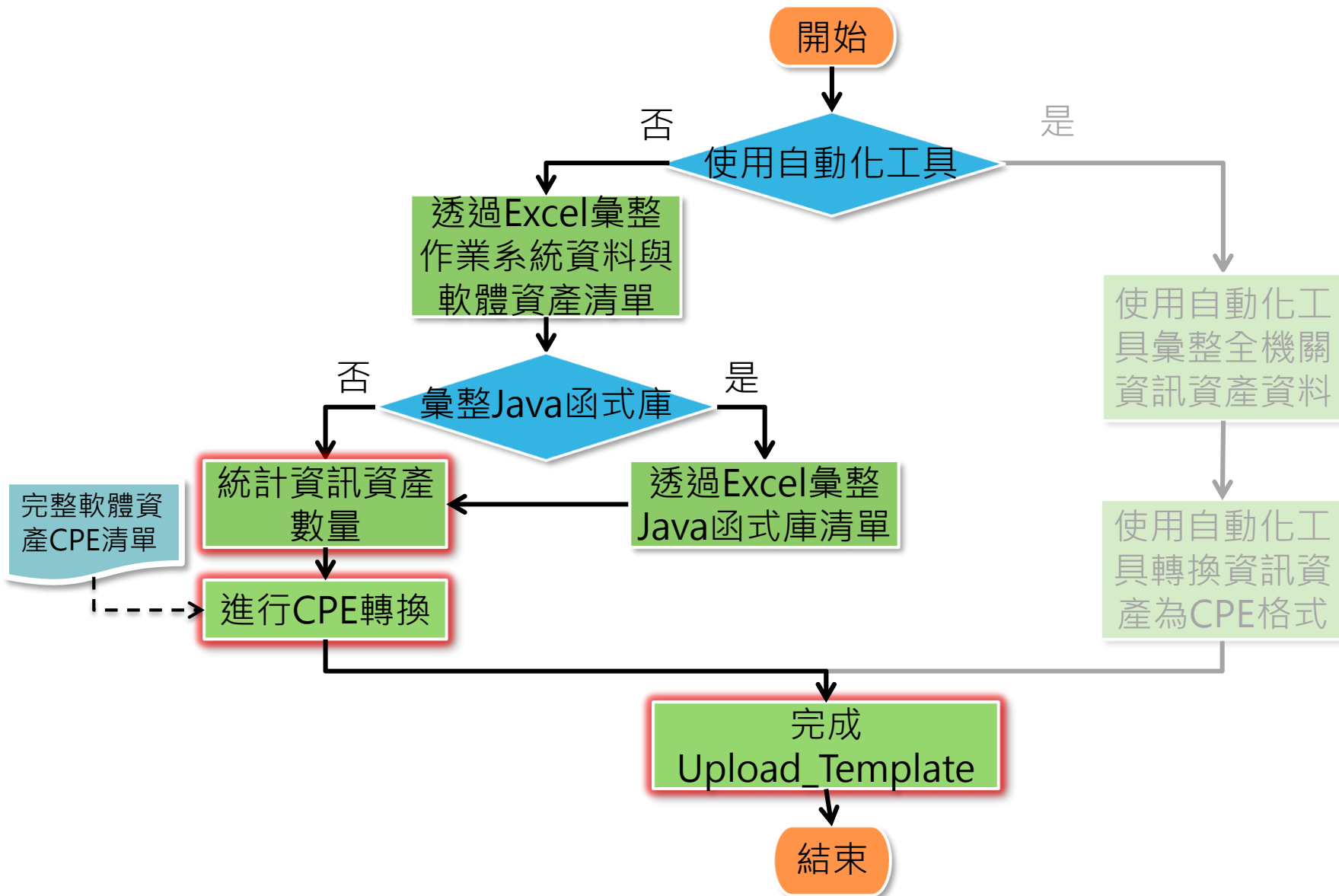
彙整資訊資產清單_Java函式庫



- Java函式庫盤點清單彙整至Java函式庫彙整範本*，以取得Java函式庫名稱與Java函式庫版本
- 將Java函式庫彙整結果，整合至資訊資產清冊，並補充主機名稱與資產廠商資訊



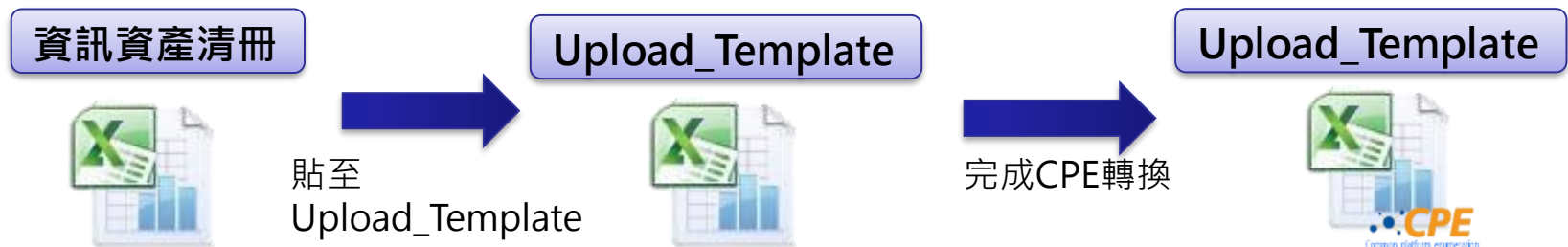
資訊資產正規化作業流程



完成Upload_Template



- 統計資訊資產數量
 - 資訊資產清冊自動計算資產數量
 - 利用移除重複項功能，以避免上傳相同之資訊資產
- 進行CPE轉換
 - 將資訊資產清冊彙整至Upload_Template(註)
 - 於完整軟體資產CPE清單*搜尋，並於Upload_Template填入資訊資產對應之CPE格式，若無則填入N/A
- 完成Upload_Template
 - 填寫機關OID與機關名稱

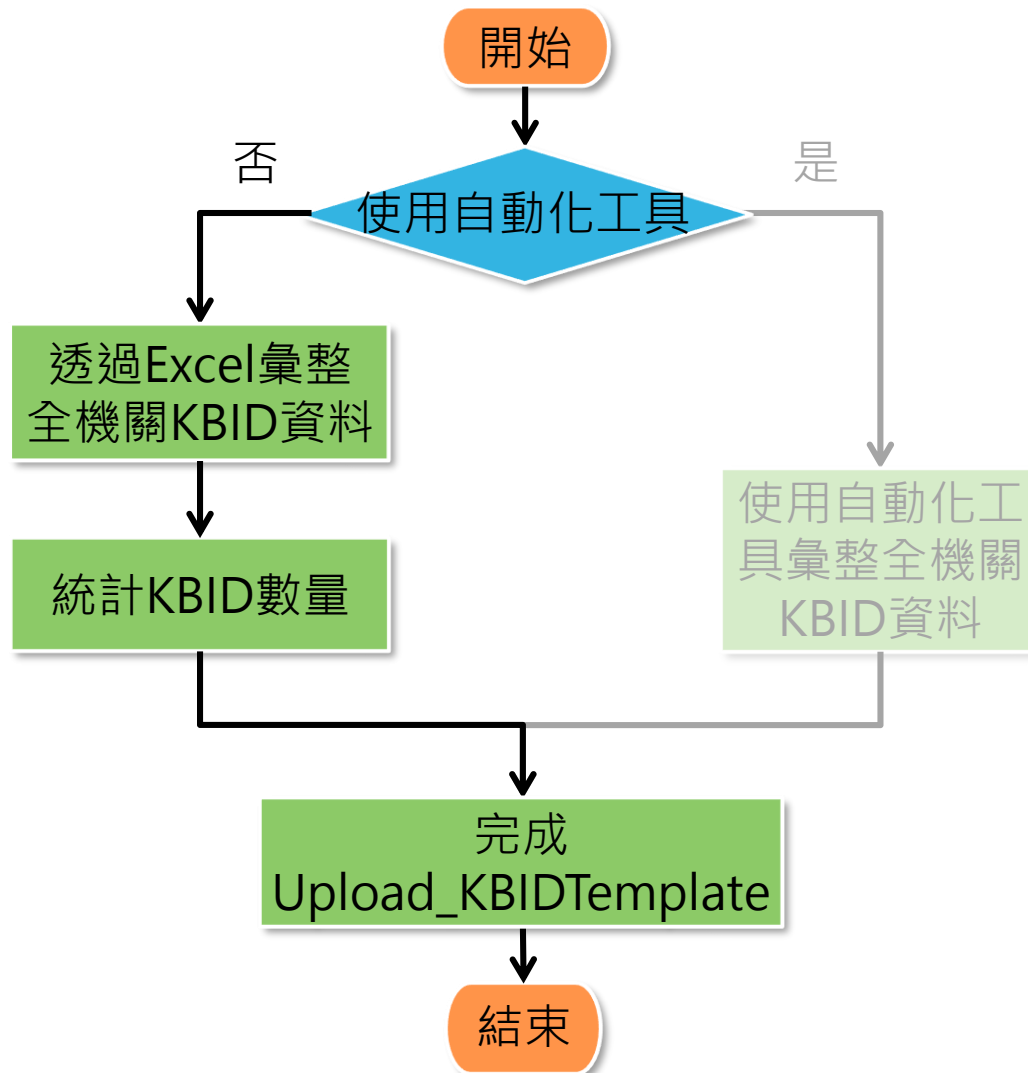


註：於VANS系統下載

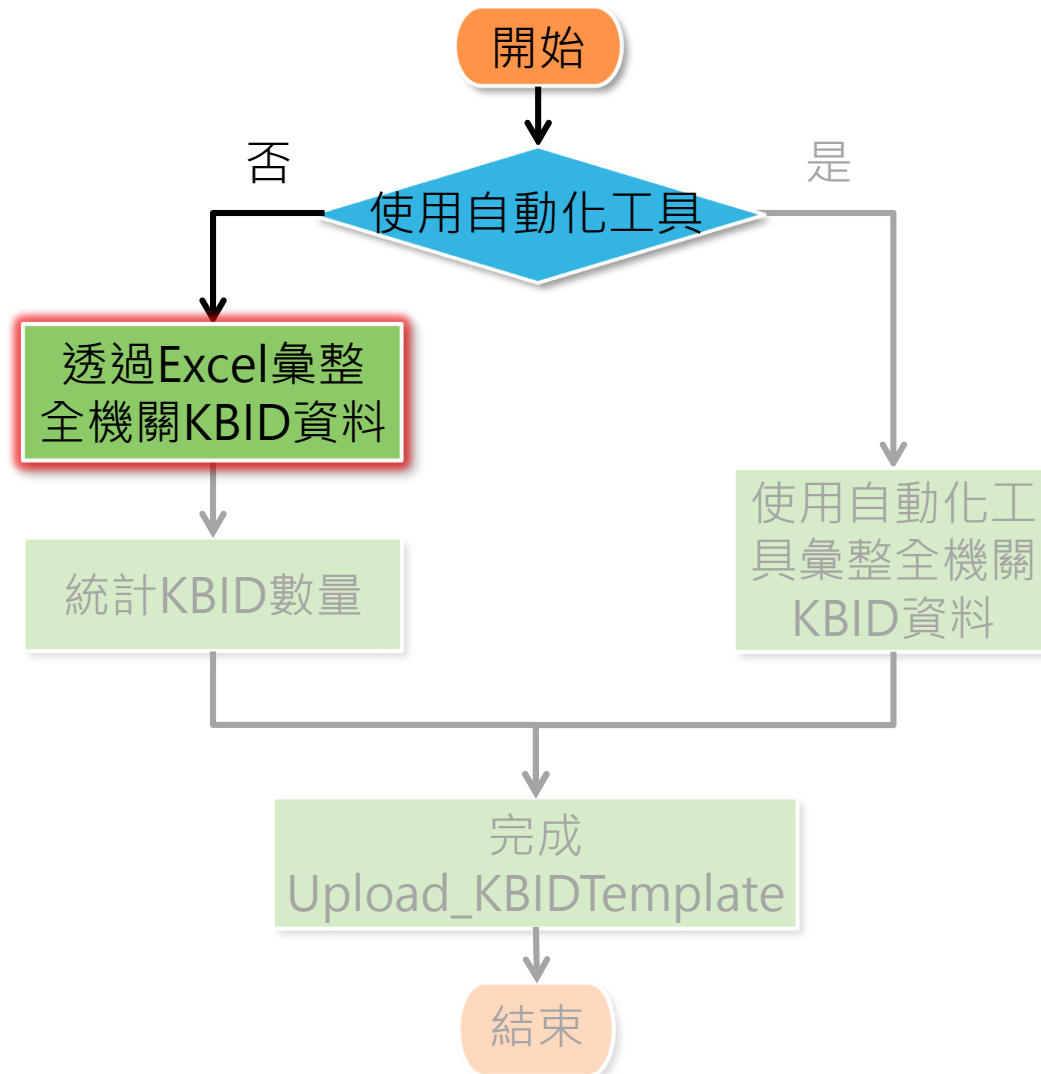


已安裝KBID正規化作業

已安裝KBID正規化作業流程



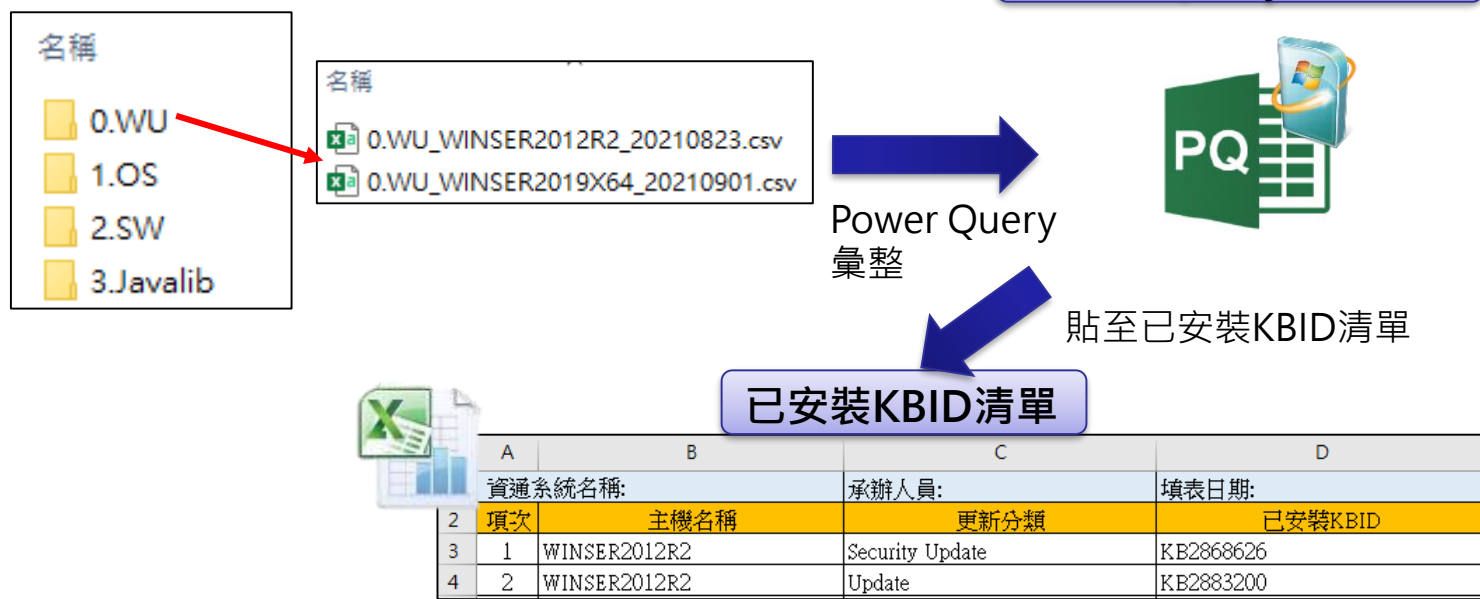
已安裝KBID正規化作業流程



彙整KBID清單



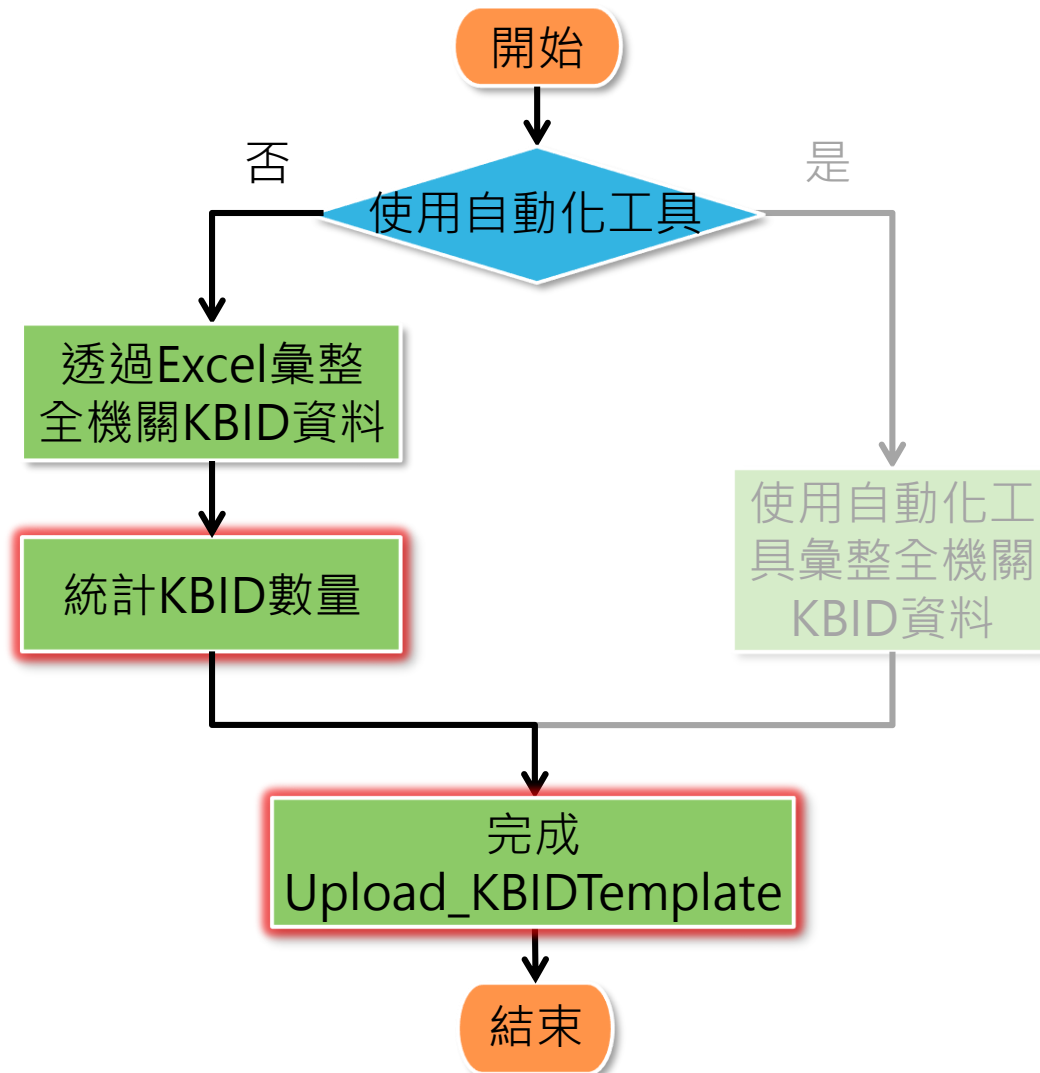
- 透過Power Query彙整歸類後已安裝KBID之盤點結果
 - 若欲了解彙整步驟，請參閱「資通安全弱點通報系統操作手冊(註1)」v1.9或更新版本
- 將已安裝KBID彙整結果，整合至已安裝KBID清單(註2)，以留存查看



註1：操作手冊：機關管理者帳號開通之通知信提供或透過VansService服務信箱索取

註2：已安裝KBID清單：課堂中提供

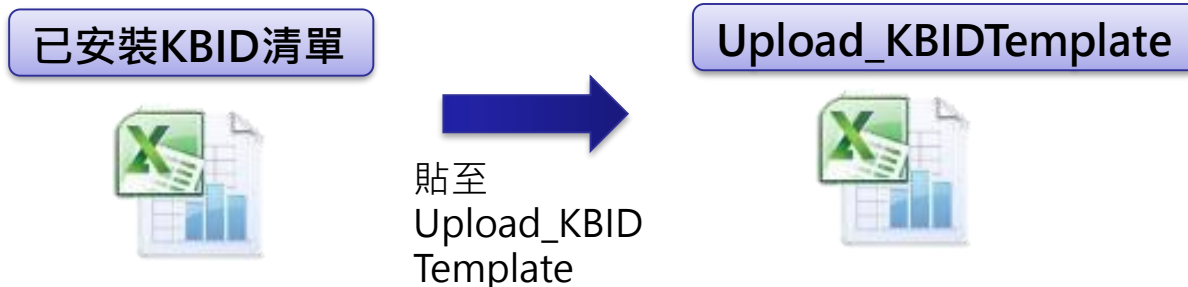
已安裝KBID正規化作業流程



完成Upload_KBIDTemplate



- 統計KBID數量
 - 已安裝KBID清單自動計算KBID數量
 - 利用移除重複項功能，以避免上傳相同之KBID
- 完成Upload_KBIDTemplate
 - 將已安裝KBID清單彙整至Upload_KBIDTemplate(註)
 - 填寫機關OID與機關名稱





附件2

WMI Windows Installer提供者 安裝步驟

安裝WMI Windows Installer(1/7)



- 若作業系統為Windows Server 2003，須安裝「WMI Windows Installer提供者」，否則指令無法運作

```
C:\> 命令提示字元 - wmic
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>wmic
wmic:root\cli>/output:"C:\Documents and Settings\install-apps.txt" product list full
節點 - III-020370ED6AA
錯誤:
代碼 = 0x80041010
描述 = 無效的類別
設備 = WMI
wmic:root\cli>
```

安裝WMI Windows Installer(2/7)



- 安裝WMI Windows Installer提供者的步驟如下：
- 步驟一：進入控制台的「新增或移除程式」



安裝WMI Windows Installer(3/7)



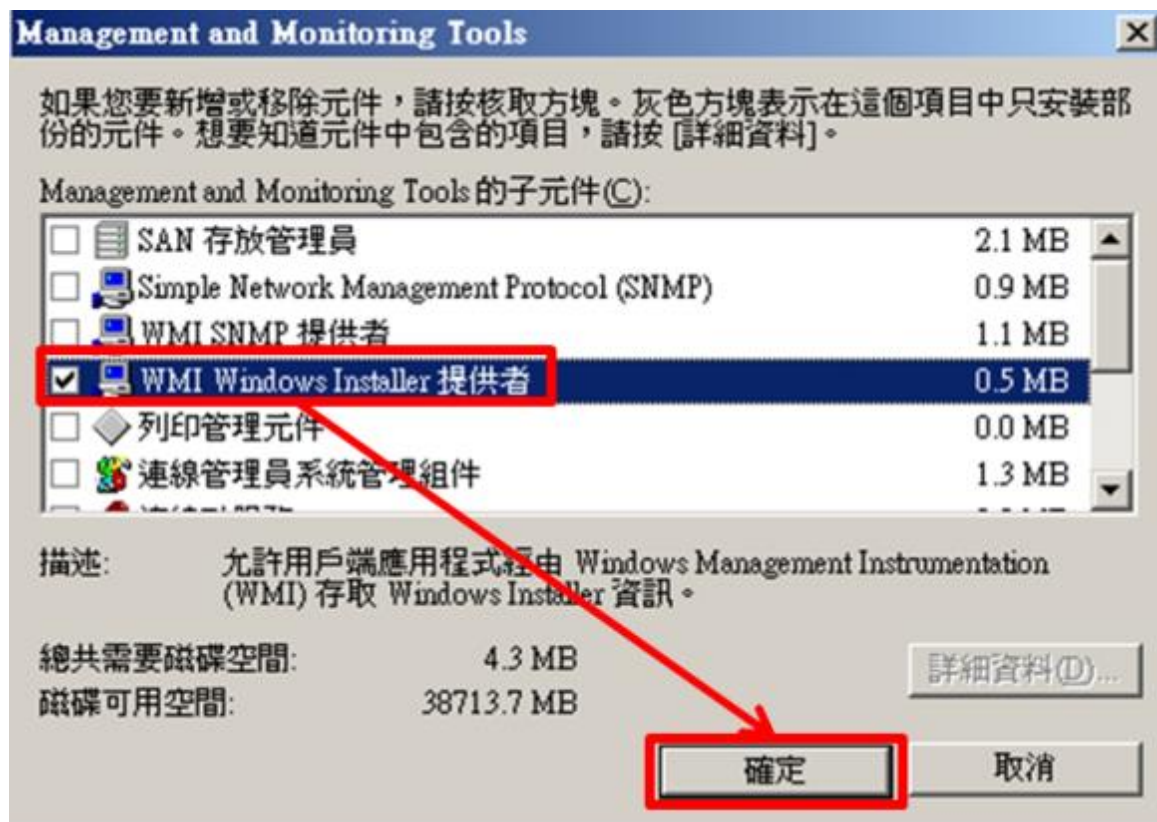
- 步驟二：點選「新增/移除Windows元件」。於Windows 元件精靈視窗中，選擇「Management and Monitoring Tools」，並點選「詳細資料」按鈕



安裝WMI Windows Installer(4/7)



- 步驟三：於「Management and Monitoring Tools」對話方塊中，勾選「WMI Windows Installer提供者」，並點選「確定」



安裝WMI Windows Installer(5/7)



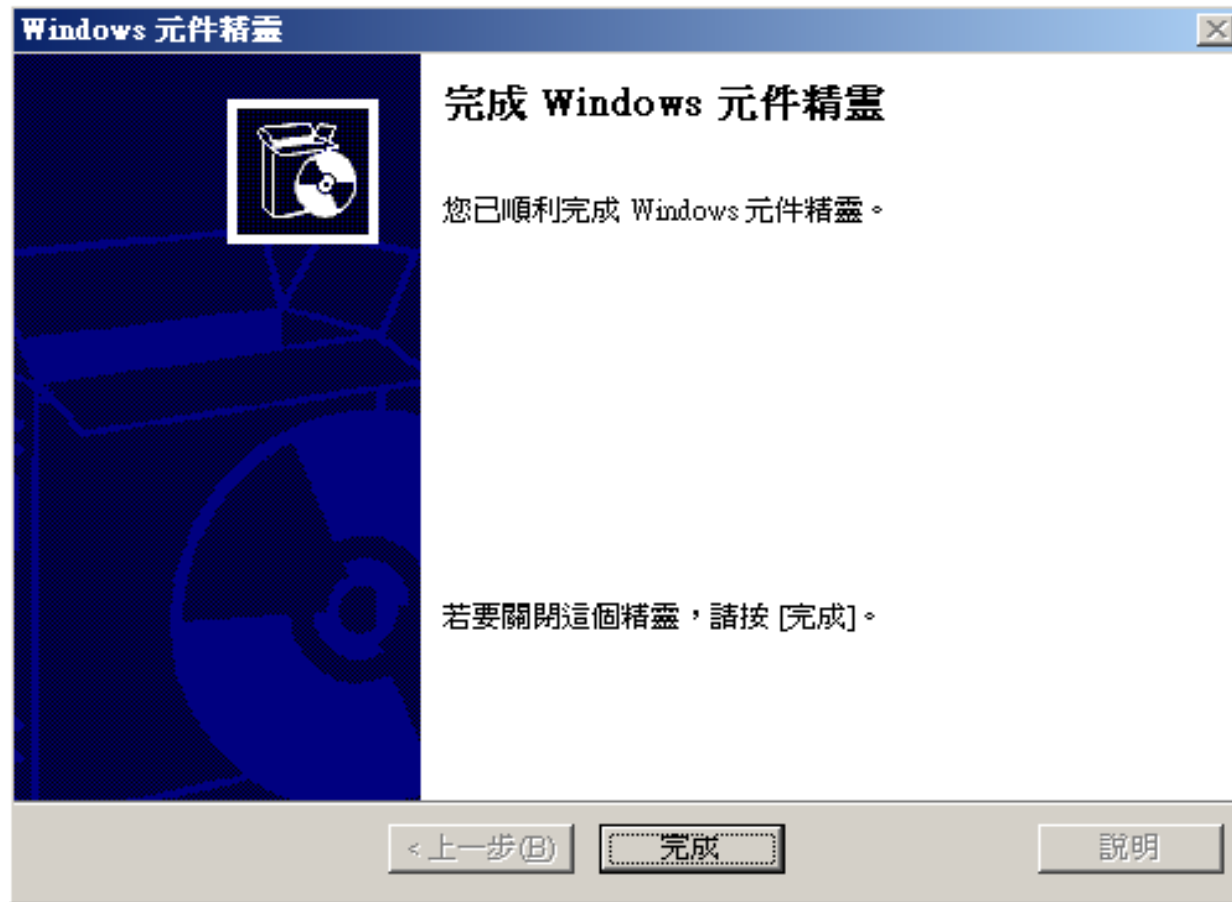
- 步驟四：點選「下一步」後，即會開始安裝「WMI Windows Installer提供者」
 - 備註：安裝時需要Windows Server 2003之安裝映像檔



安裝WMI Windows Installer(6/7)



- 步驟五：完成安裝



安裝WMI Windows Installer(7/7)



- 步驟六：安裝完成後，即可執行WMIC

2.

名稱	大小	類型	修改日期	屬性
My Music		檔案資料夾	2017/8/14 上午 10:15	
install-apps.txt	1 KB	文字文件	2017/9/25 下午 08:59	A

1.

```
C:\Documents and Settings\Administrator>wmic
wmic:root\cli>/output: "C:\Documents and Settings\All Users\Documents\install-ap
wmic:root\cli>
```



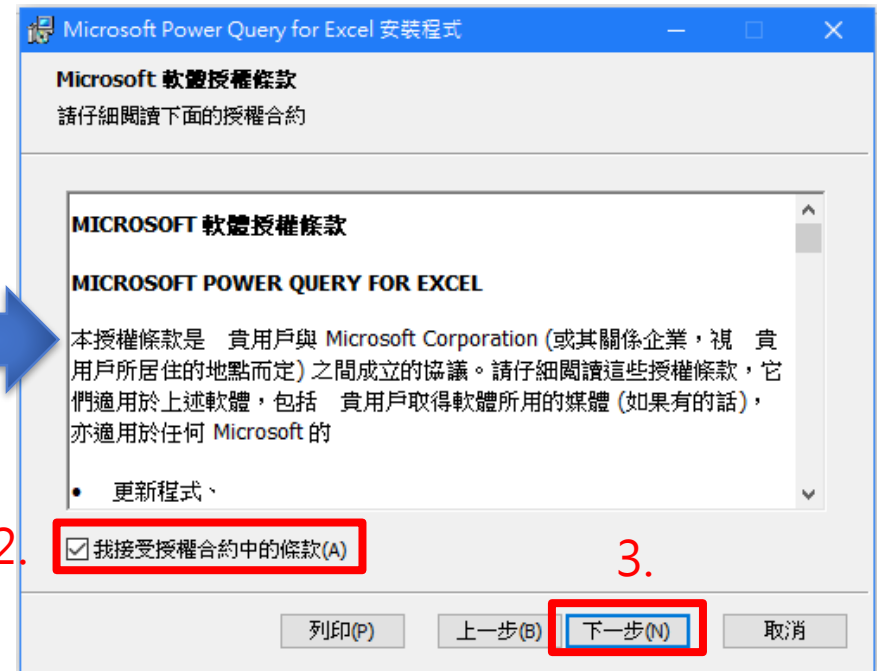
附件3

Microsoft Power Query for Excel 安裝步驟



安裝Microsoft Power Query for Excel(1/3)

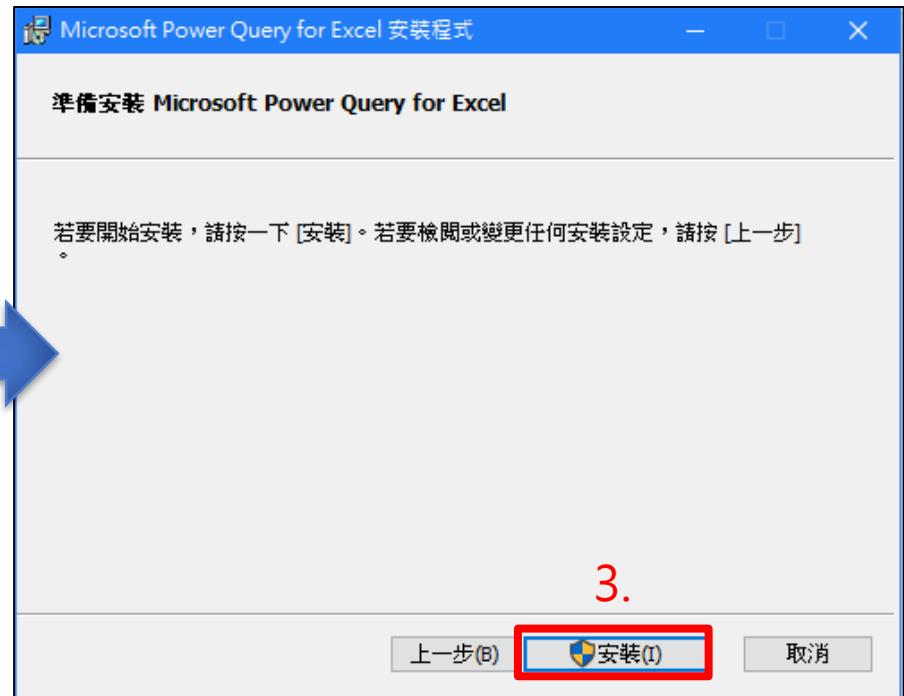
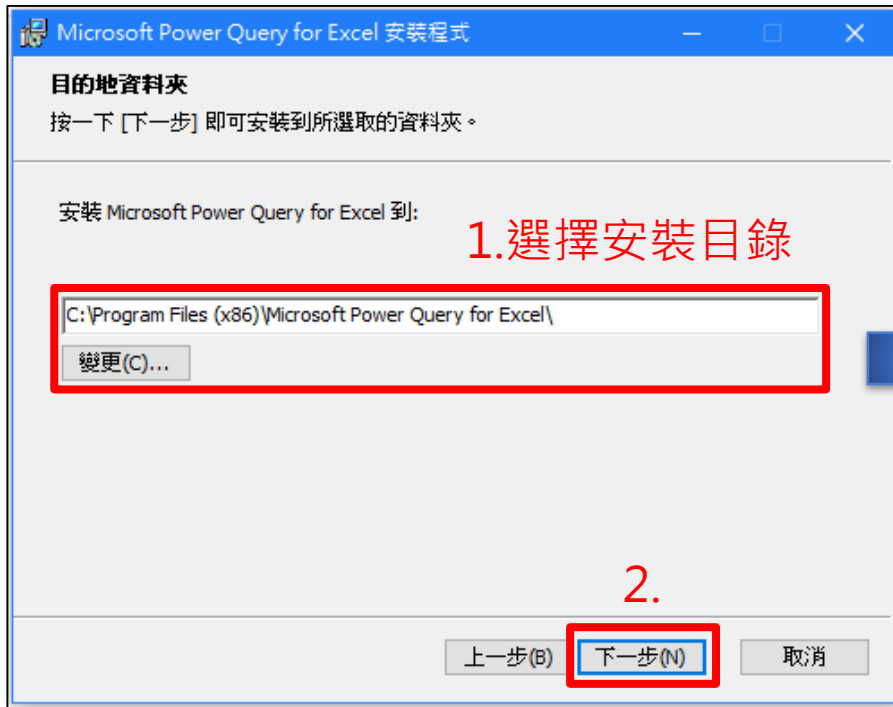
- Power Query內建於Excel 2016、2019中，功能名稱為「取得及轉換」，不需額外安裝Microsoft Power Query for Excel
- 若為Excel 2010或2013，需至微軟官網下載Microsoft Power Query for Excel，並進行安裝
 - <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>





安裝Microsoft Power Query for Excel(2/3)

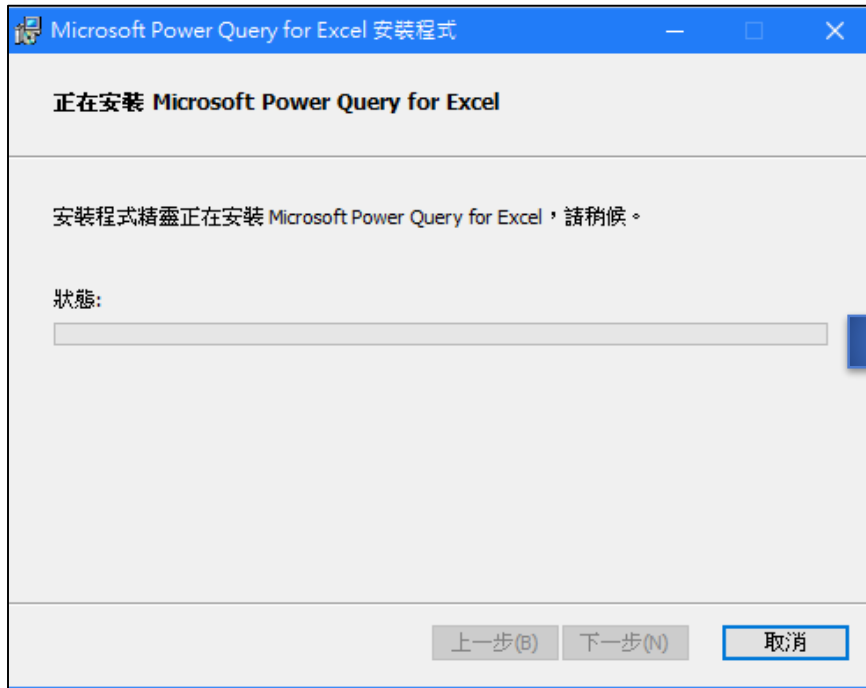
- 選擇安裝目錄，準備安裝





安裝Microsoft Power Query for Excel(3/3)

- 進行安裝





報告完畢
敬請指教