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

【內部公開】

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

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

- 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	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 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
		C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 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

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

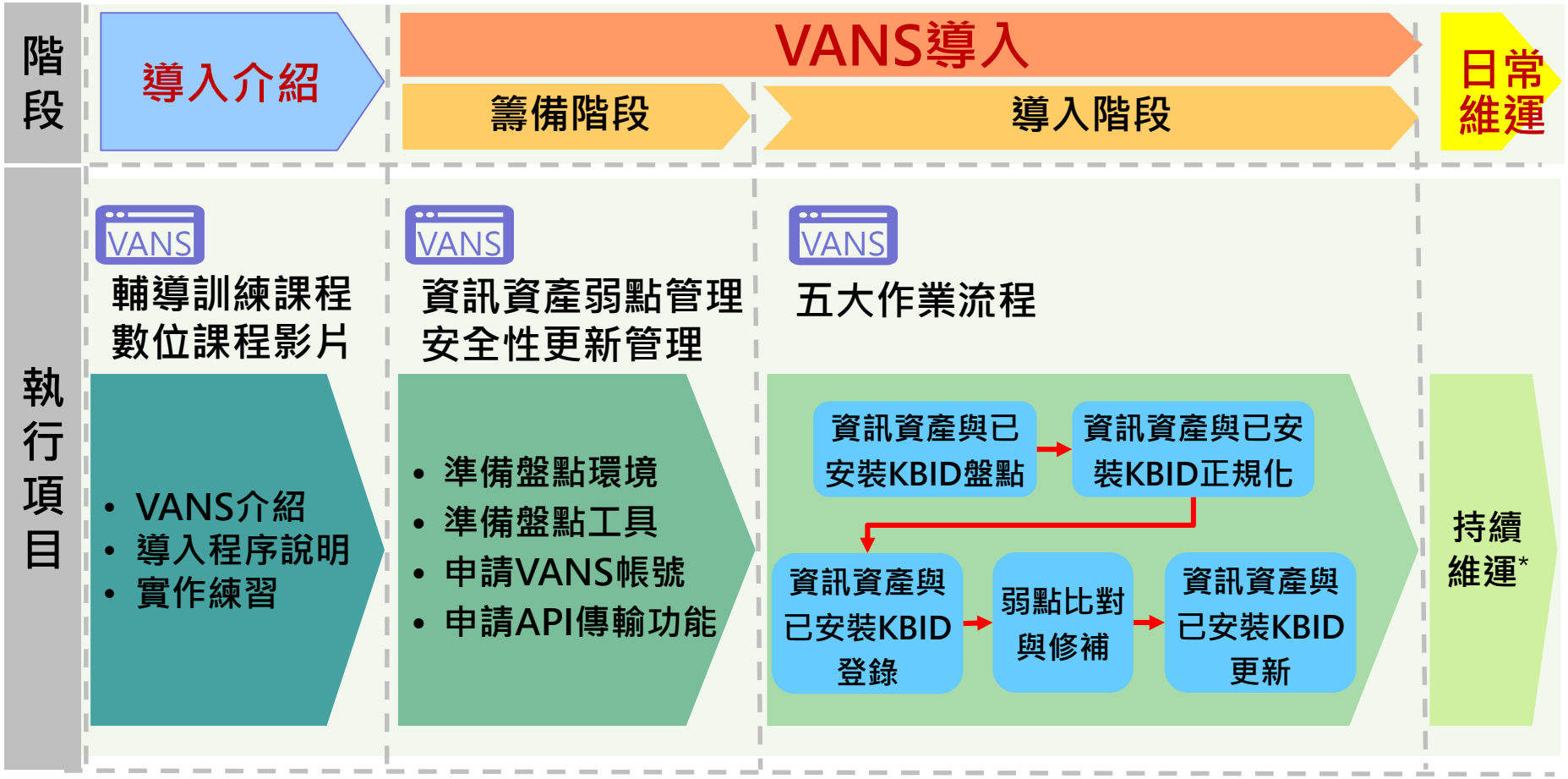
資通安全弱點通報機制

- 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

VANS目標

- 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



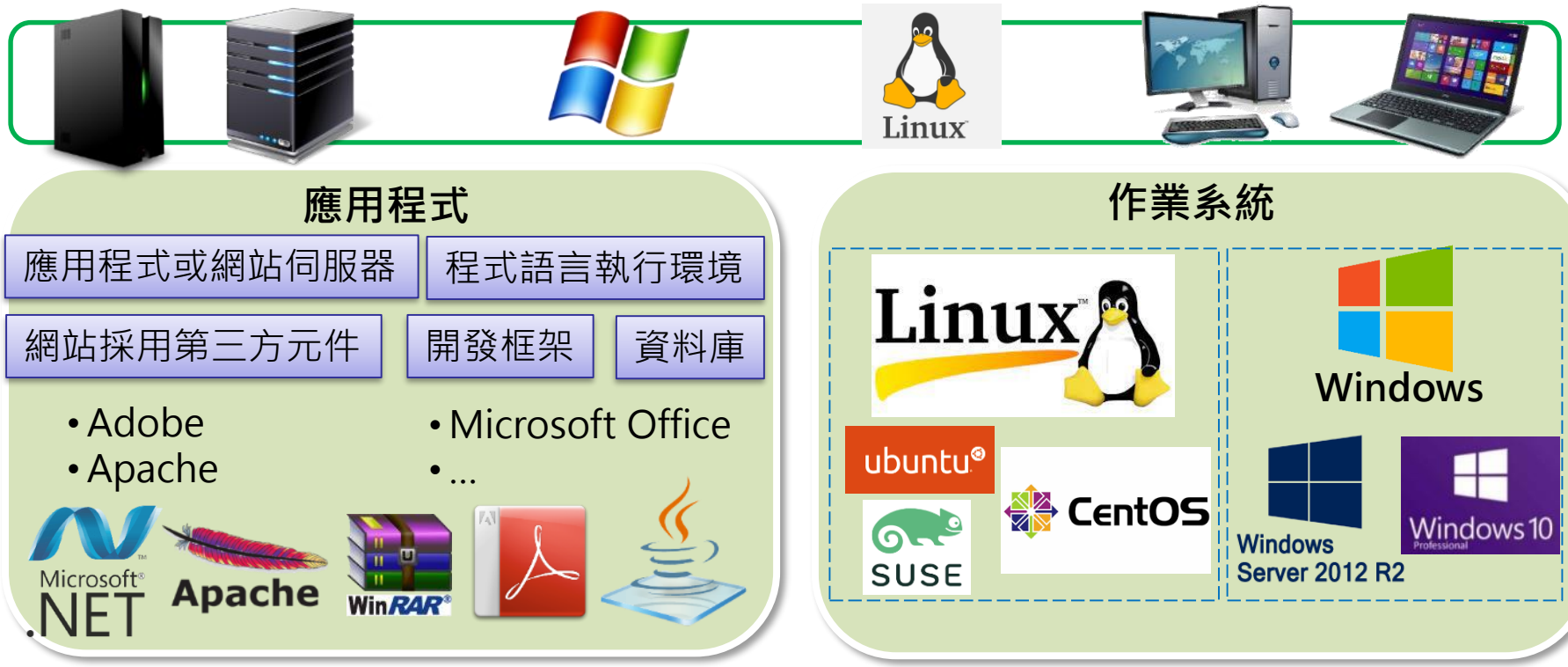
*持續維運：包含定期執行及不定期執行(例如資產異動時)

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



- 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)

CPE common platform enumeration

資訊資產呈現方式(3/3)

- CPE條目範例
  - Microsoft Windows Server 2012 R2 Service Pack 1 on X64

  - Oracle JDK 1.8.0 Update 92

common platform enumeration

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

弱點資料庫

- 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

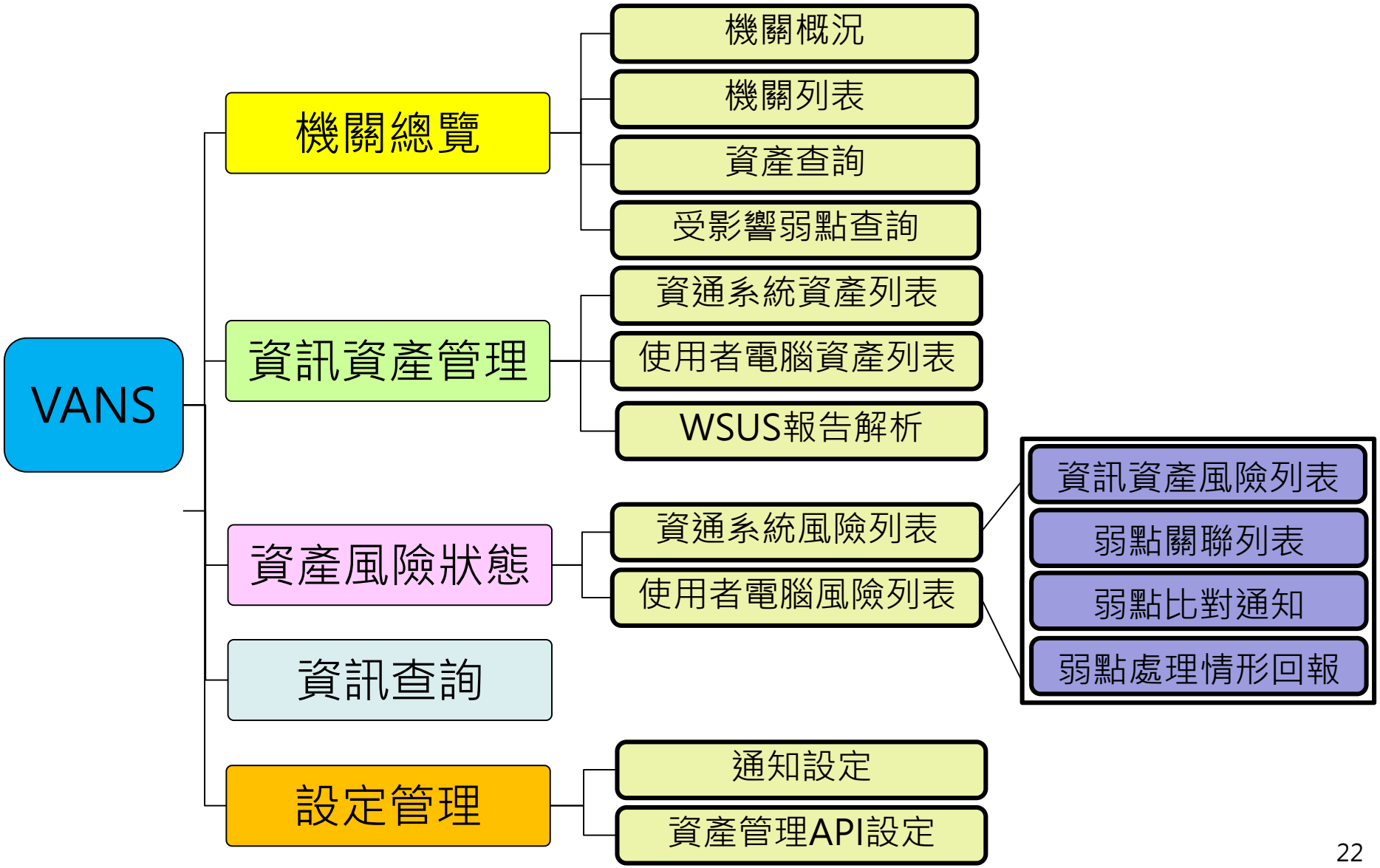
微軟安全性更新(2/2)

- 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

系統功能總覽


VANS
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
資通系統資產列表
使用者電腦資產列表
WSUS報告解析
資產風險狀態
資通系統風險列表
使用者電腦風險列表
資訊資產風險列表
弱點關聯列表
弱點比對通知
弱點處理情形回報
資訊查詢
設定管理
通知設定
資產管理API設定

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
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
顯示/隱藏
功能選單列
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
1, 50.0%
1, 50.0%
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)
0, 0.0%
344, 100.0
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

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

參閱操作手冊

- 操作諮詢
- 服務說明

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

- ✓ 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

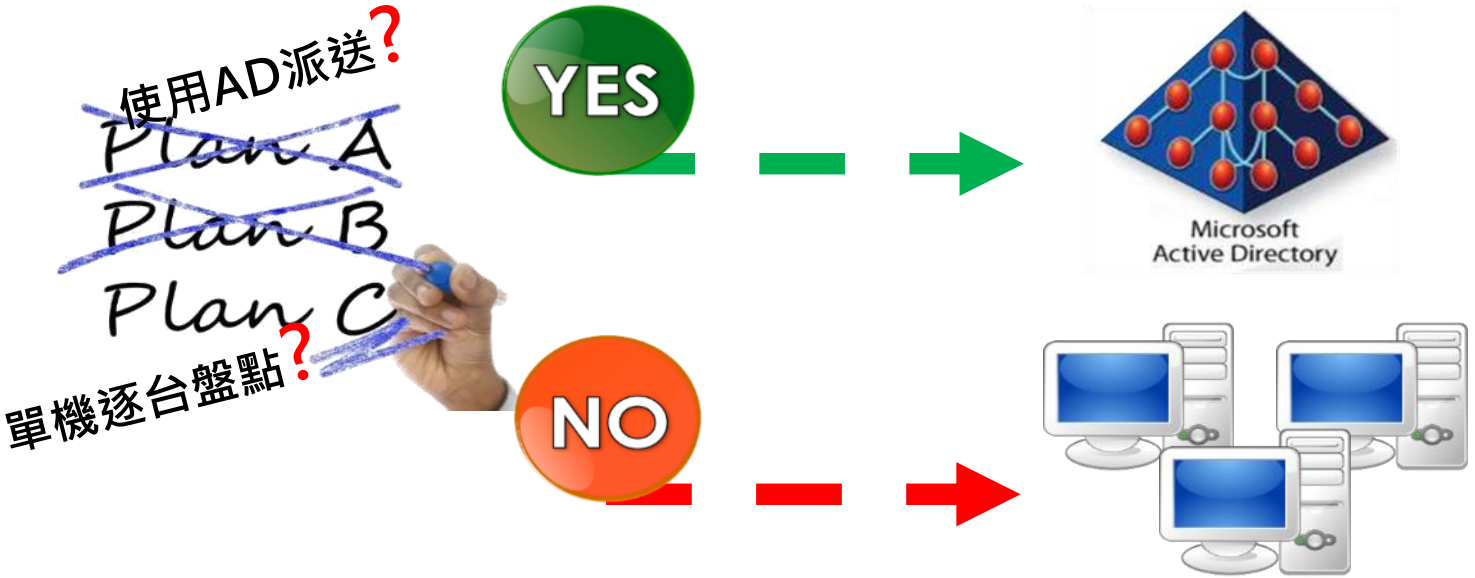
- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視機關各帳號資產異動紀錄
- ✓ **檢視**API Key

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

執行規劃

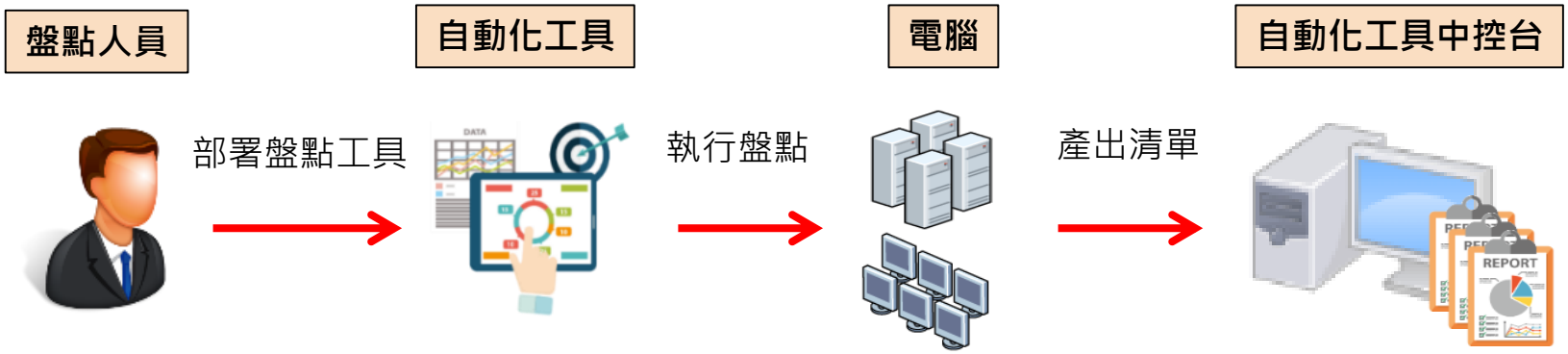
- 依據機關環境擬定導入執行規劃
  - 執行範圍：本部/本部與所屬、資通系統/使用者電腦
  - 執行時程：人力評估、導入測試起訖時間、正式導入起訖時間
  - 執行方式：單機/AD派送GPO執行、第三方工具執行



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

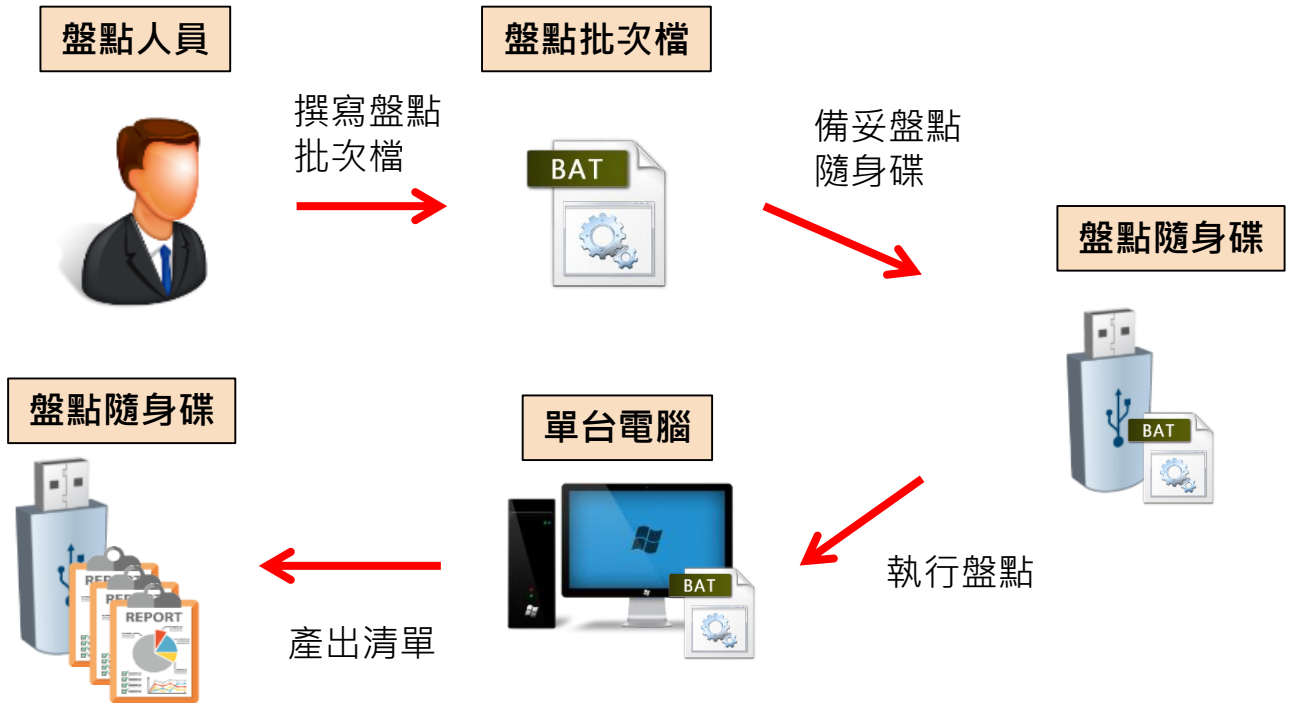


情境說明(2/3)

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

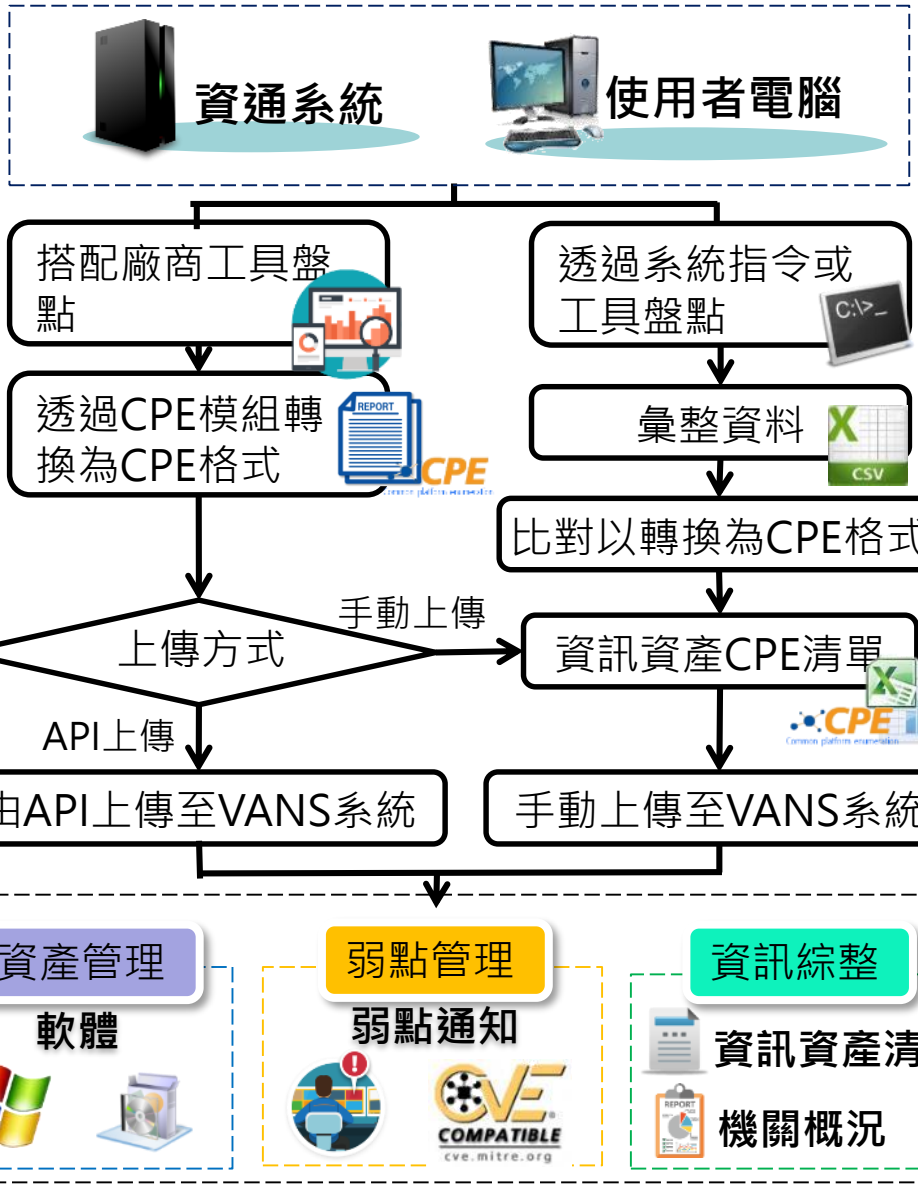
資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

資訊資產與
已安裝KBID
更新作業

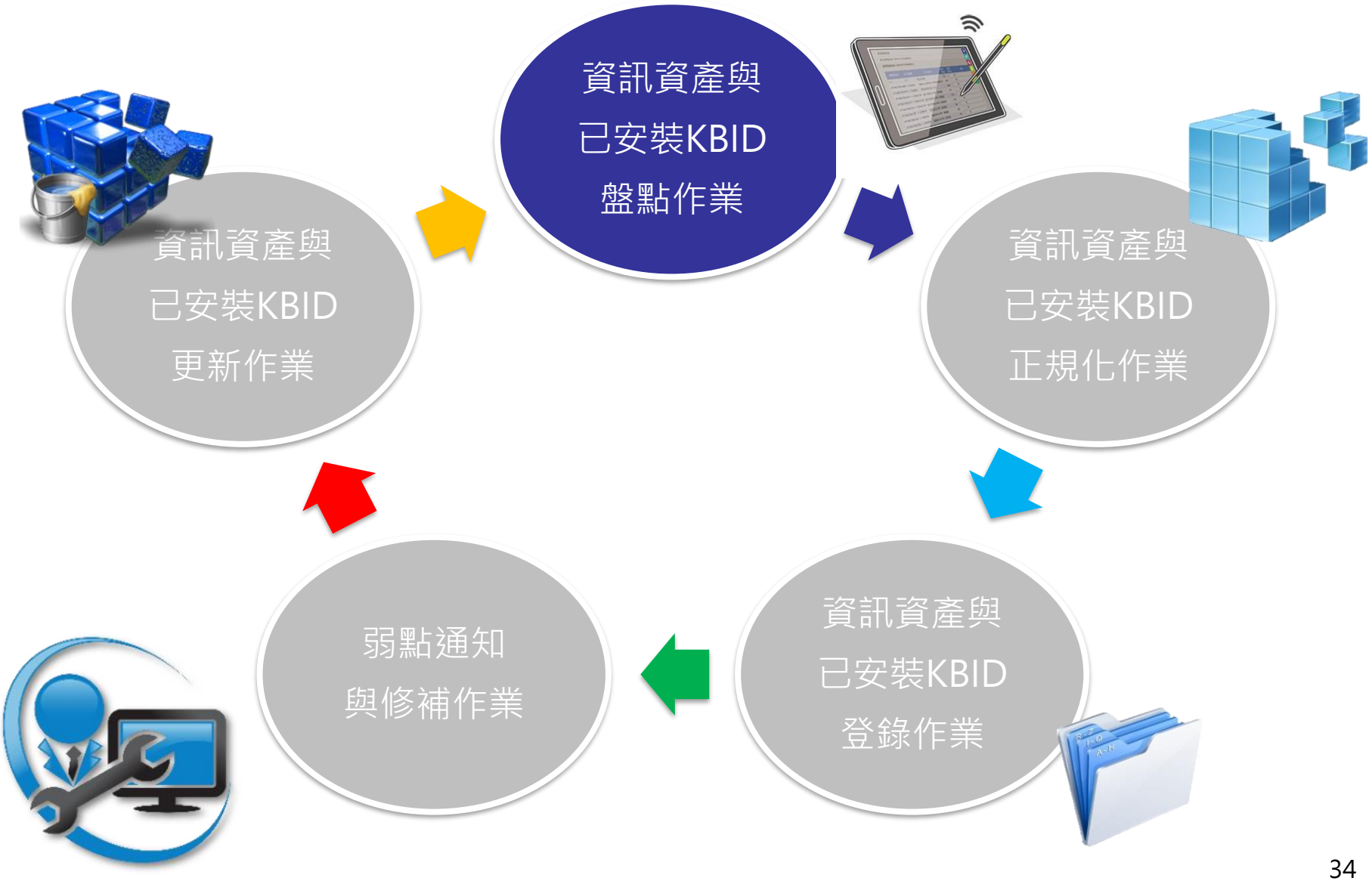
資訊資產弱點管理總覽



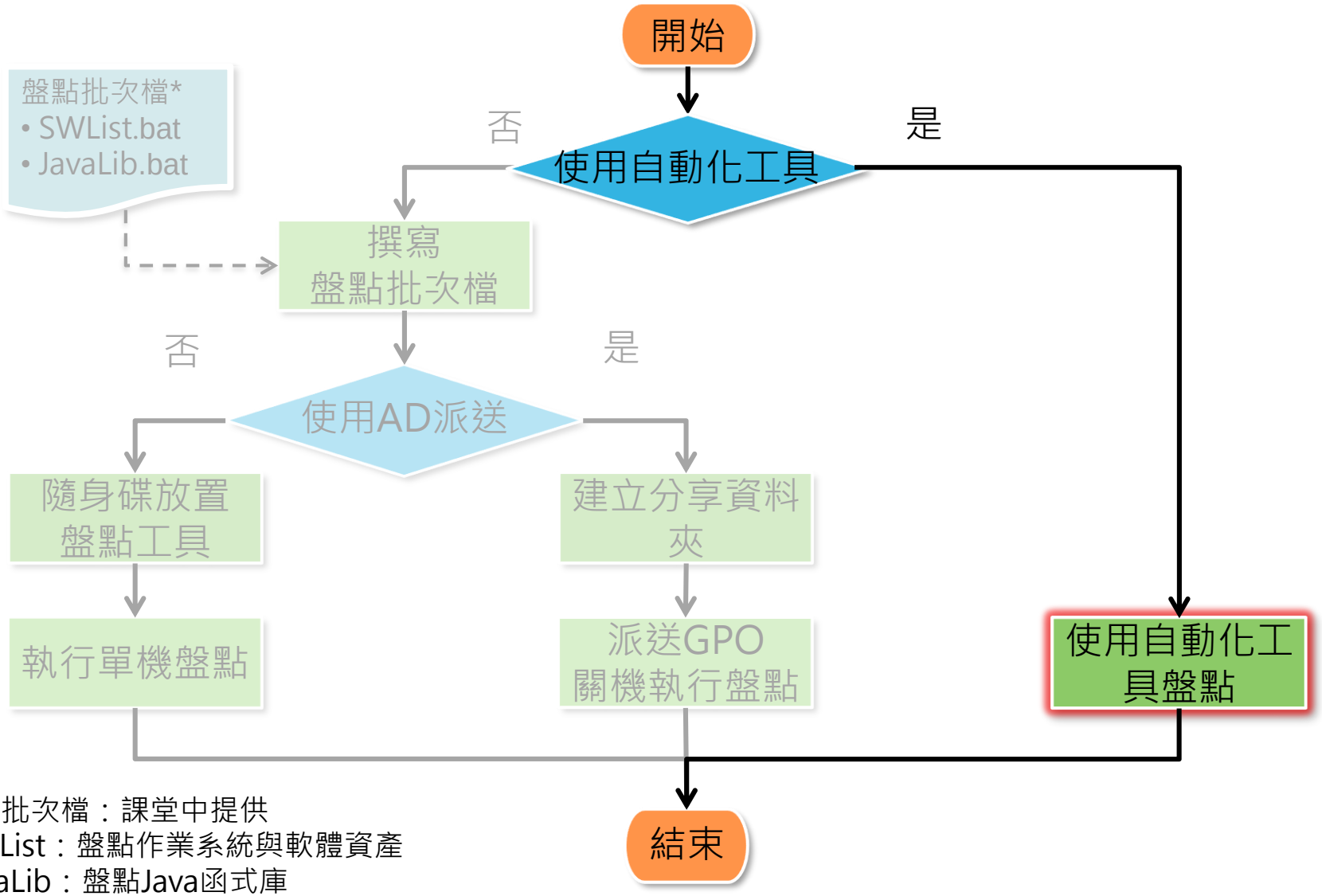
透過廠商工具產出CPE格式報表，並可透過API上傳至VANS系統

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


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
弱點通知
與修補作業
資訊資產與
已安裝KBID
更新作業

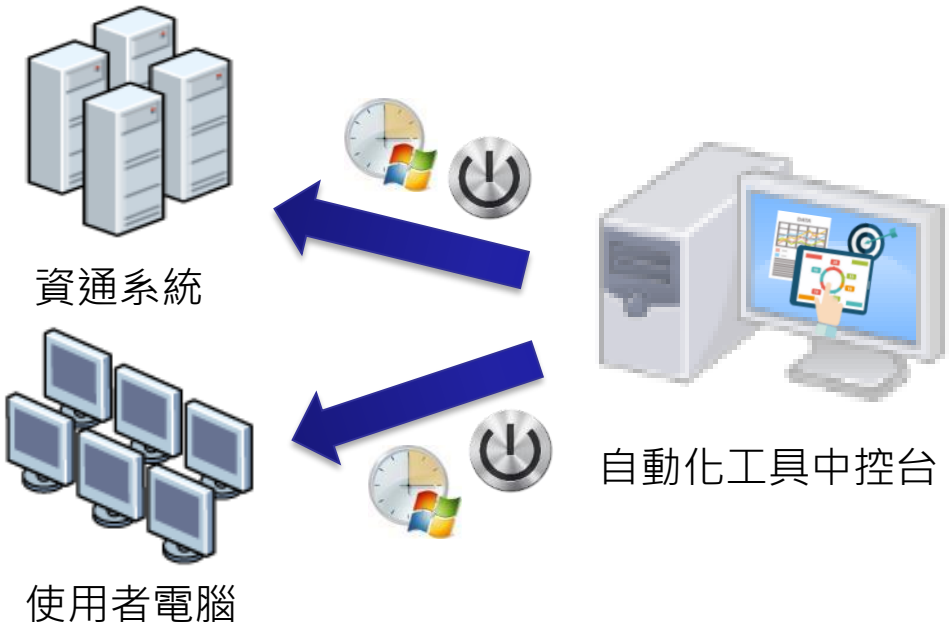
盤點作業流程



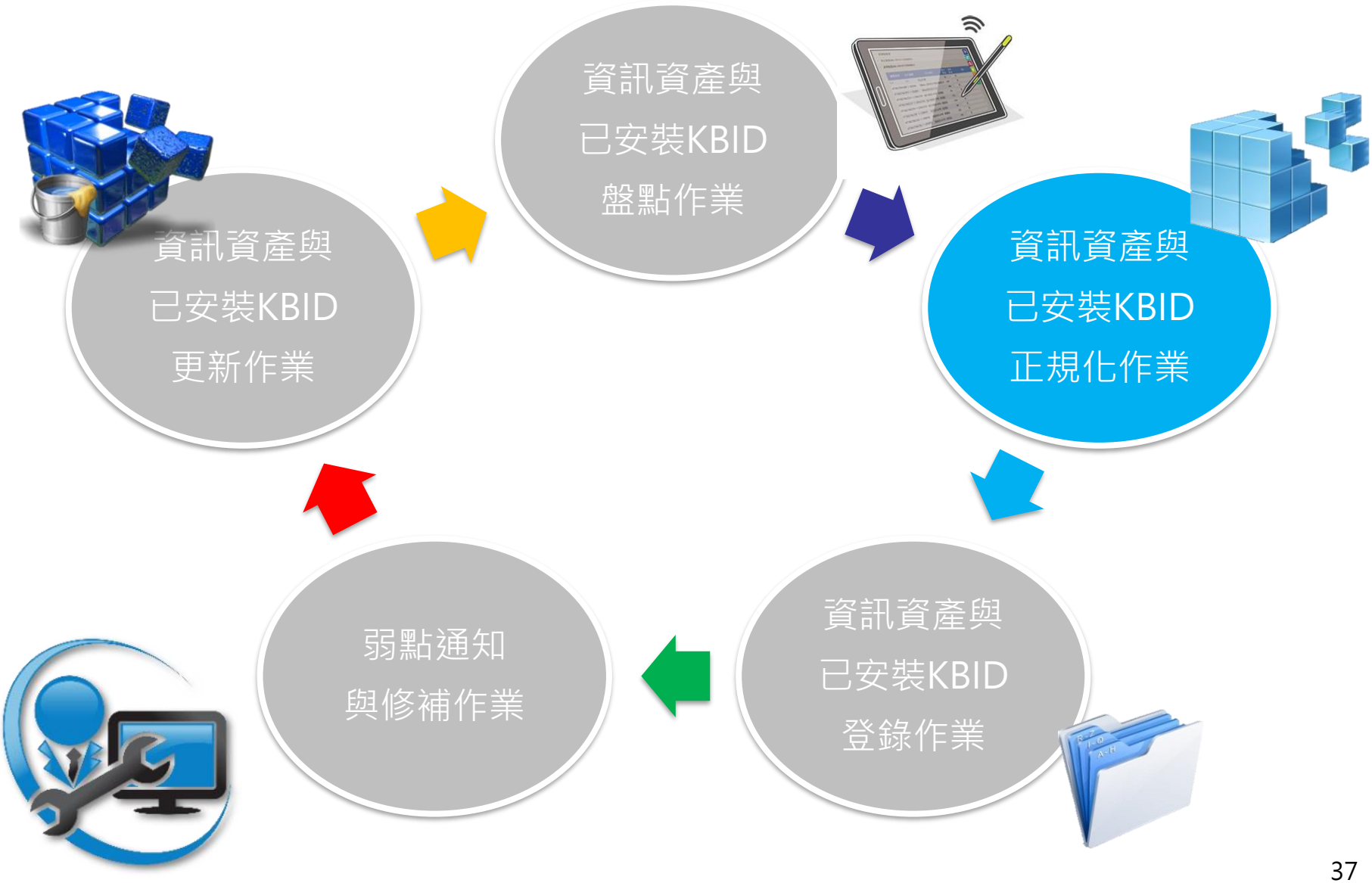
*盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

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

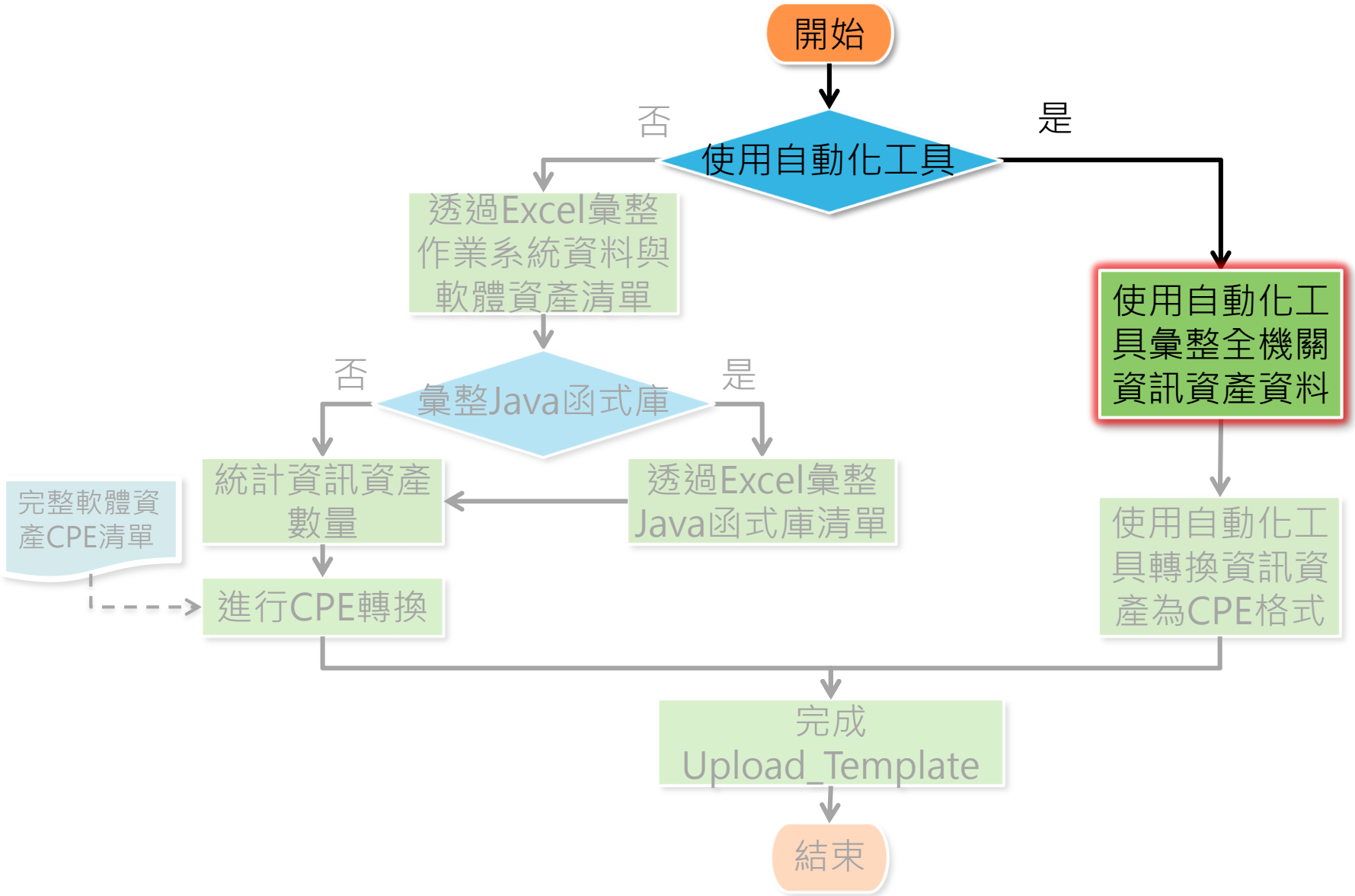


導入作業流程


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
弱點通知
與修補作業
資訊資產與
已安裝KBID
更新作業

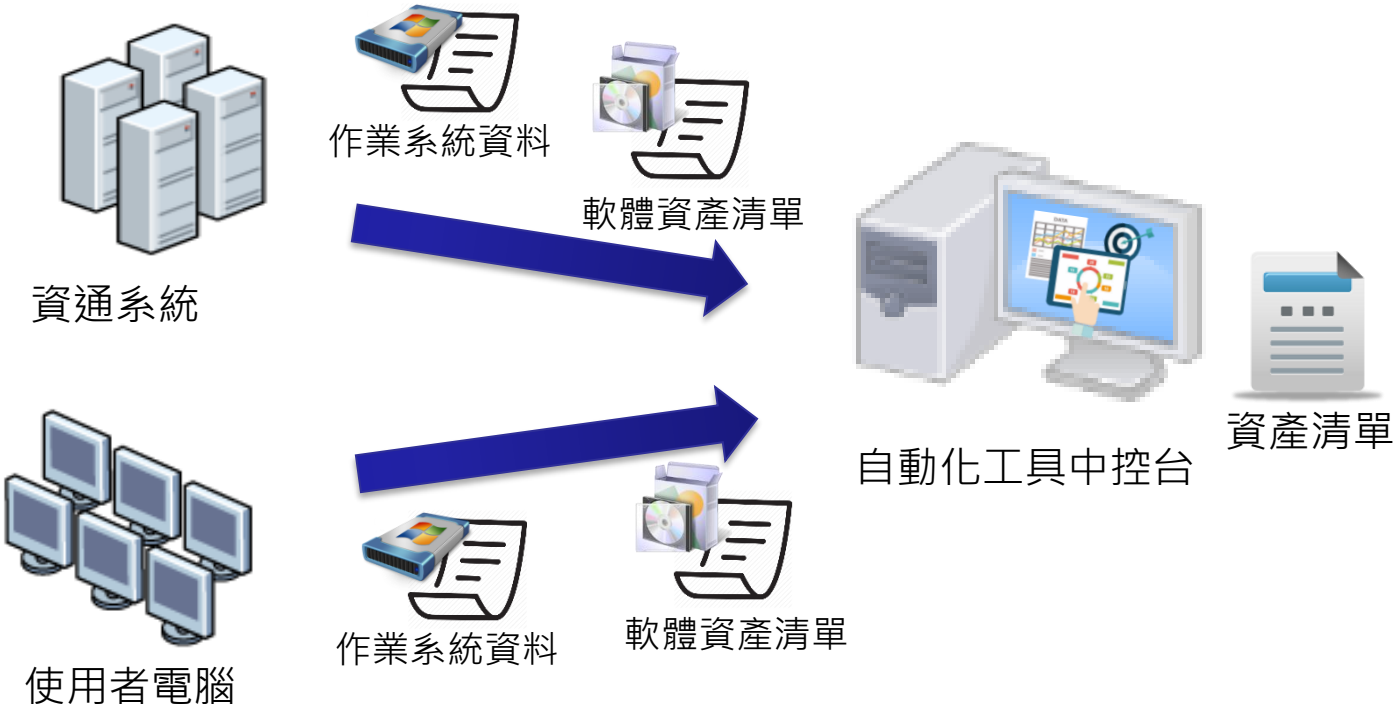
資訊資產正規化作業流程

資訊資產正規化作業流程

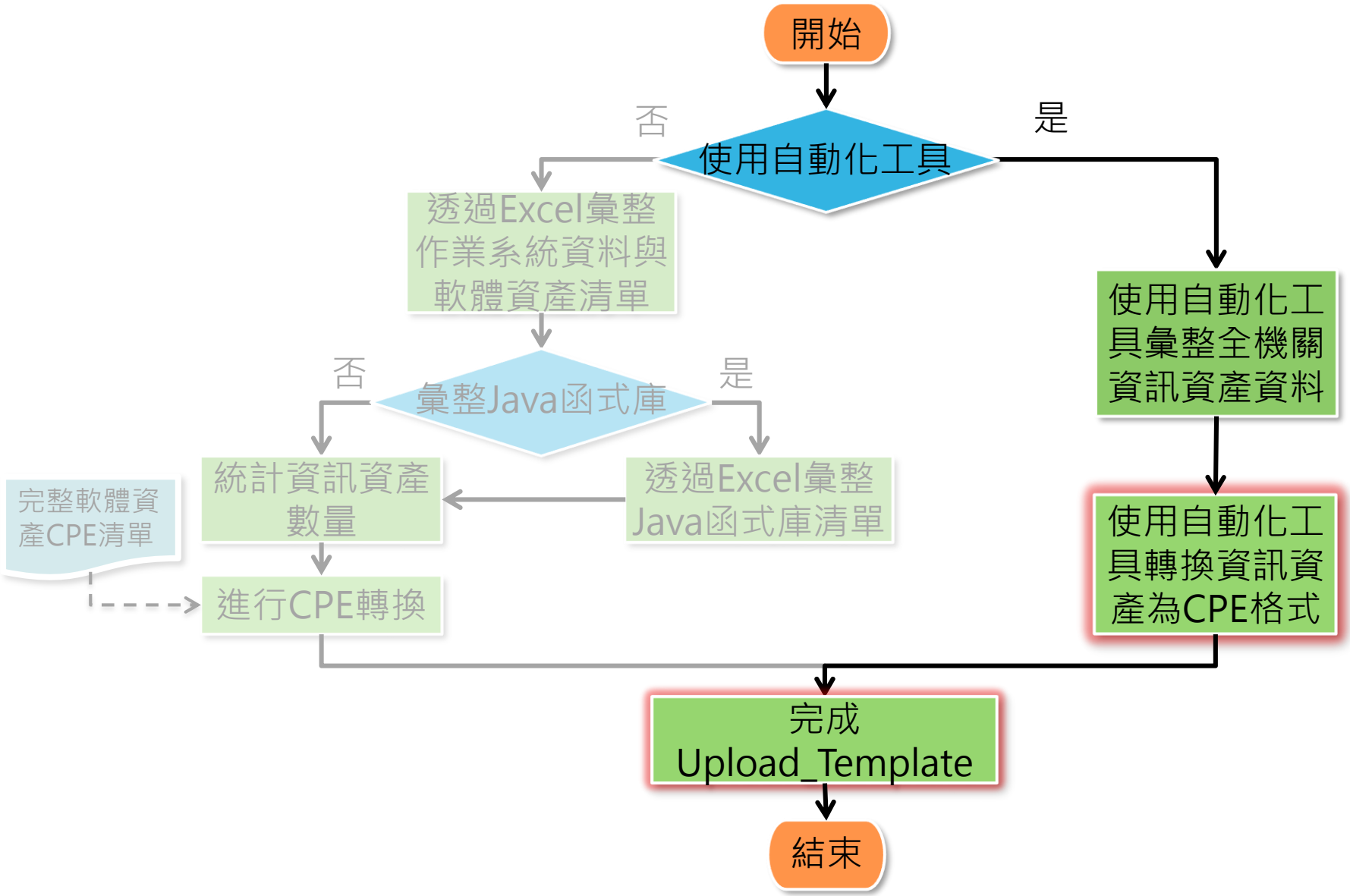


使用自動化工具彙整資訊資產

- 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

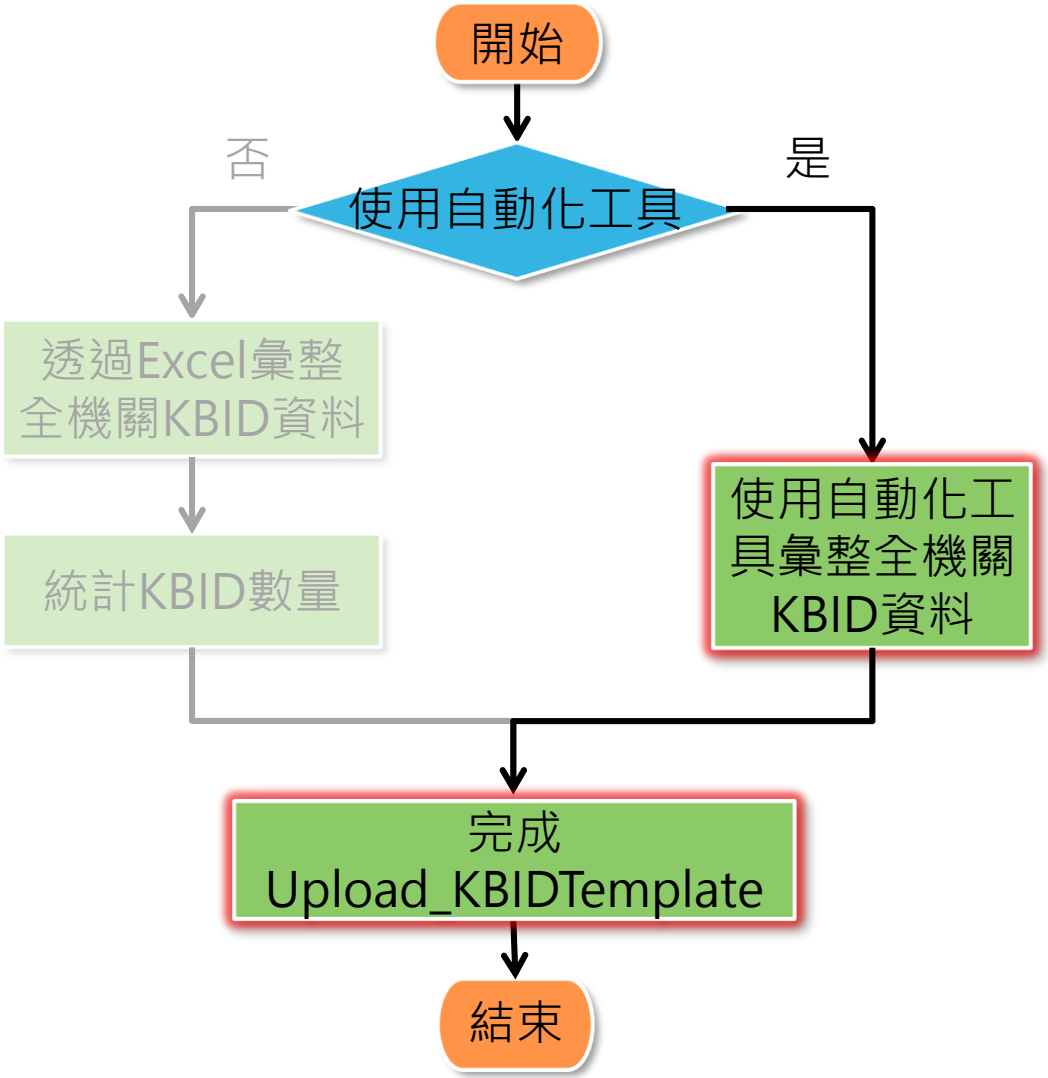


使用自動化工具轉換資訊資產格式

- 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

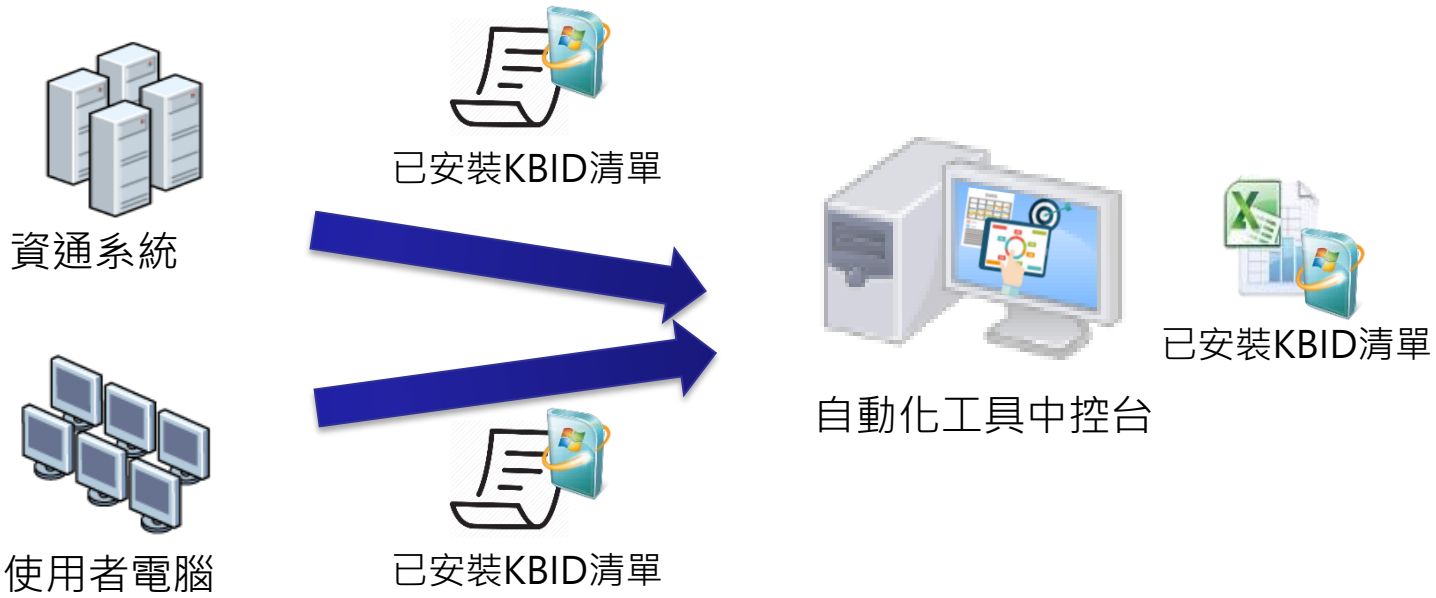
已安裝KBID正規化作業

已安裝KBID正規化作業流程



使用自動化工具彙整已安裝KBID

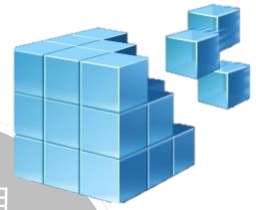
- 自動化蒐集與彙整資通系統與使用者電腦之已安裝KBID
- 透過排程定時回傳盤點結果予自動化工具中控台
- 自動去識別化整併為全機關已安裝KBID清單，並提供反查對照功能，便於機關管理已安裝KBID清單
- 完成已安裝KBID清單



導入作業流程

資訊資產與
已安裝KBID
更新作業

資訊資產與
已安裝KBID
盤點作業

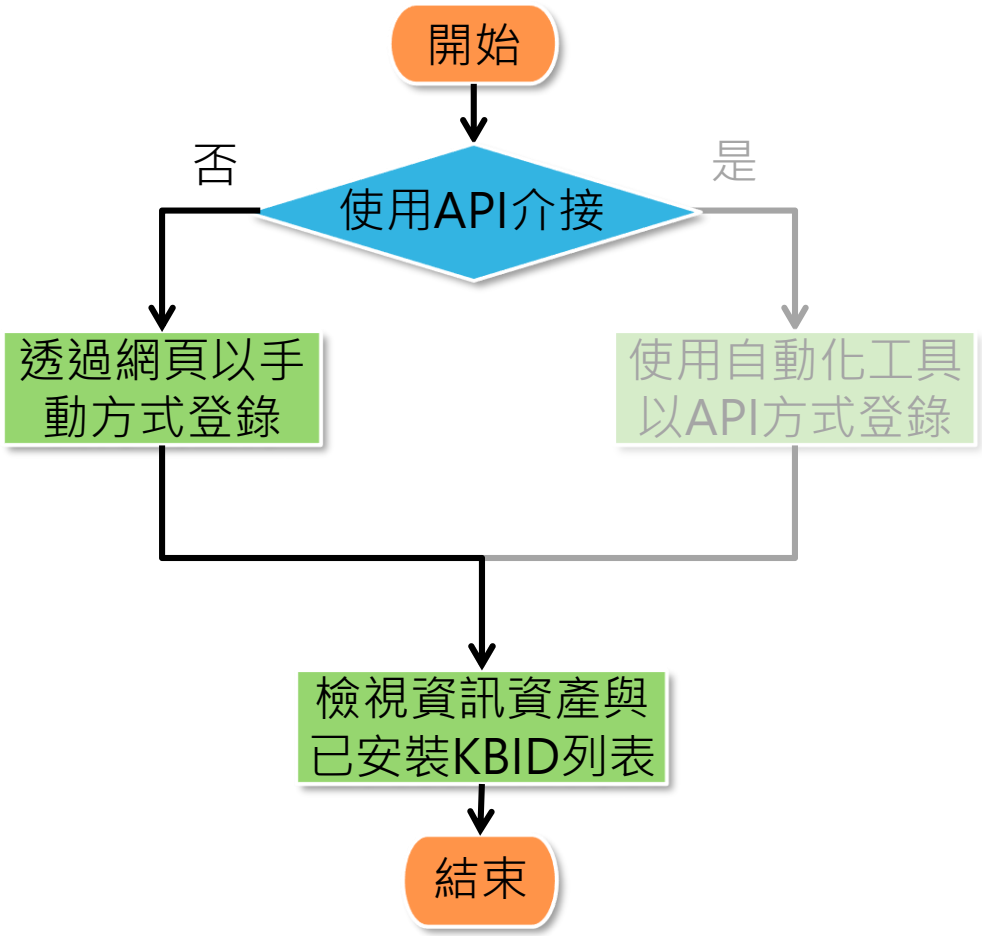


資訊資產與
已安裝KBID
正規化作業

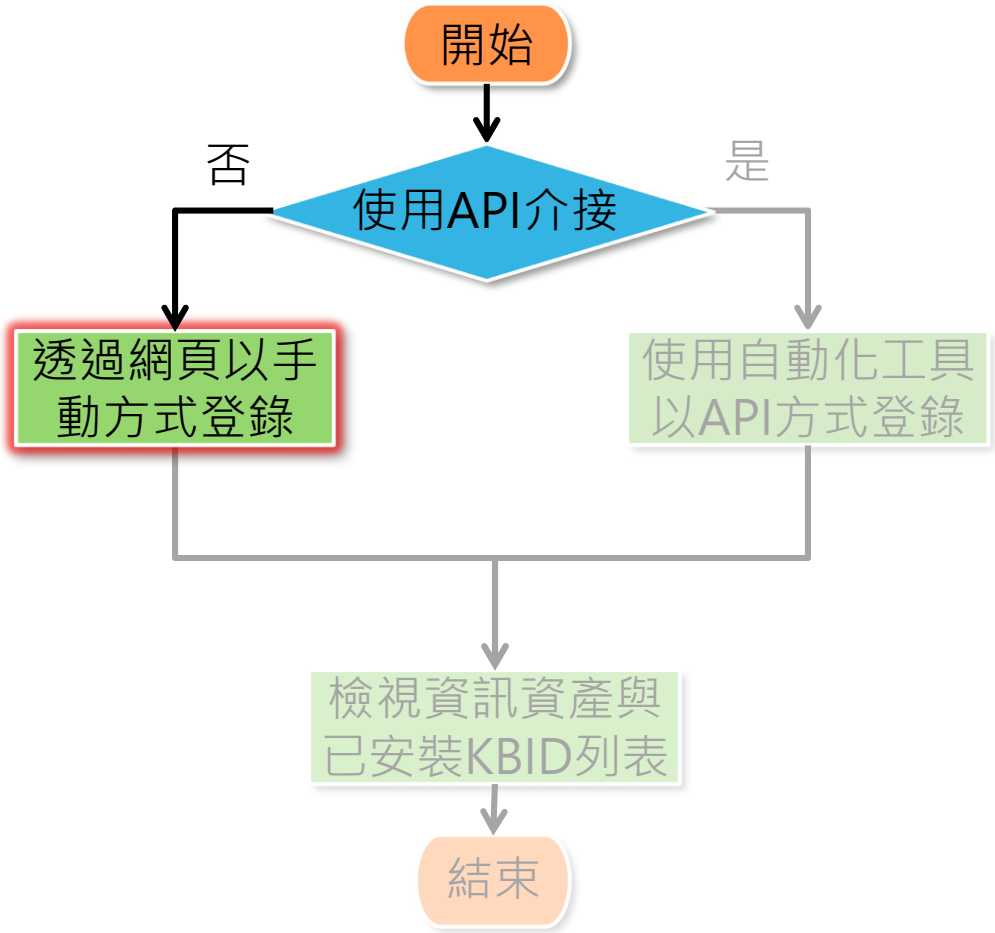
資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

登錄作業流程


開始
使用API介接
否
是
透過網頁以手動方式登錄
使用自動化工具以API方式登錄
檢視資訊資產與已安裝KBID列表
結束

登錄作業流程


開始
使用API介接
否
是
透過網頁以手動方式登錄
使用自動化工具以API方式登錄
檢視資訊資產與已安裝KBID列表
結束

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

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

網頁登錄-已安裝KBID(2/2)

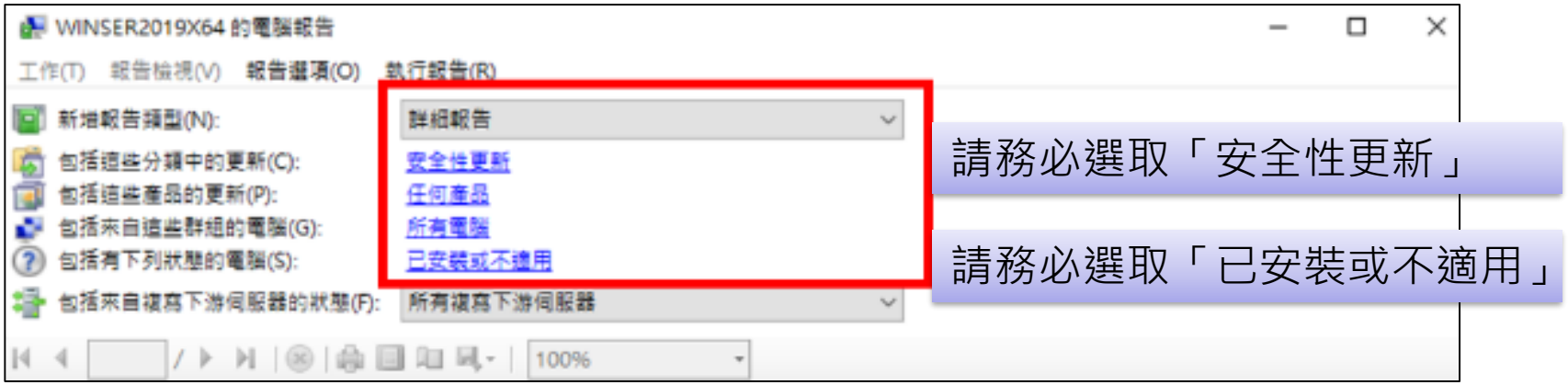
- STEP3：點選「上傳」，等待系統解析請單
- STEP4：待收到解析完成通知信，即完成登錄

WSUS解析-已安裝KBID(1/3)

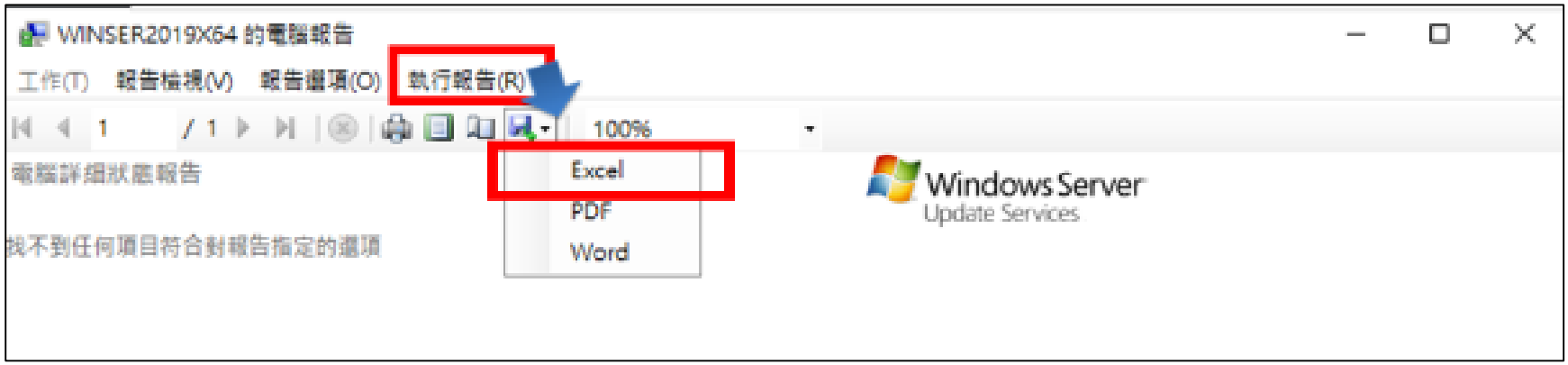
- 透過解析從WSUS匯出之電腦報告，產出已安裝KBID清單，供使用者逕行上傳至資通系統/使用者電腦資產列表
- STEP1：請點選「報告」→選擇「電腦詳細狀態」

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」

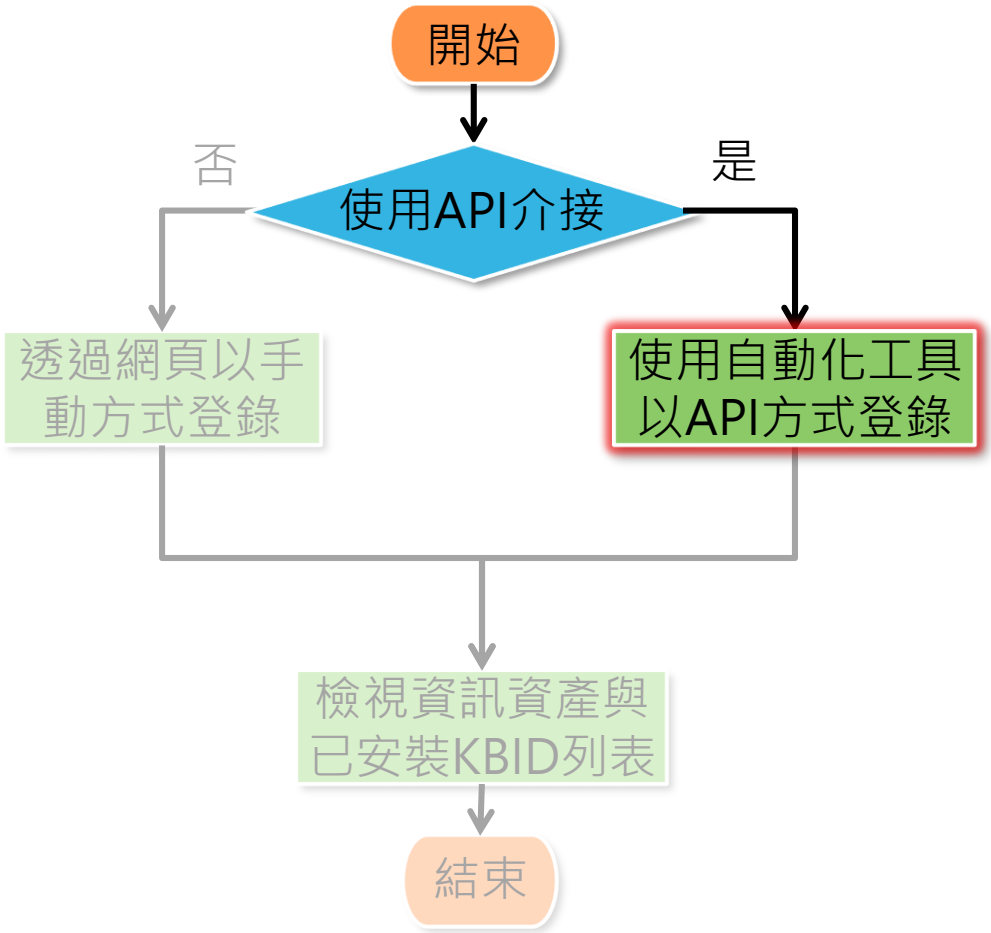


WSUS解析-已安裝KBID(3/3)

- 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」

- 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


開始
使用API介接
否
是
透過網頁以手動方式登錄
使用自動化工具以API方式登錄
檢視資訊資產與已安裝KBID列表
結束

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)

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

VANS_API_KBID_Sample.json .json 檔案 | VANS_API_Sample.json .json 檔案 | VANS系統API功能說明v0.8_1120204.pdf .pdf 檔案

您好:

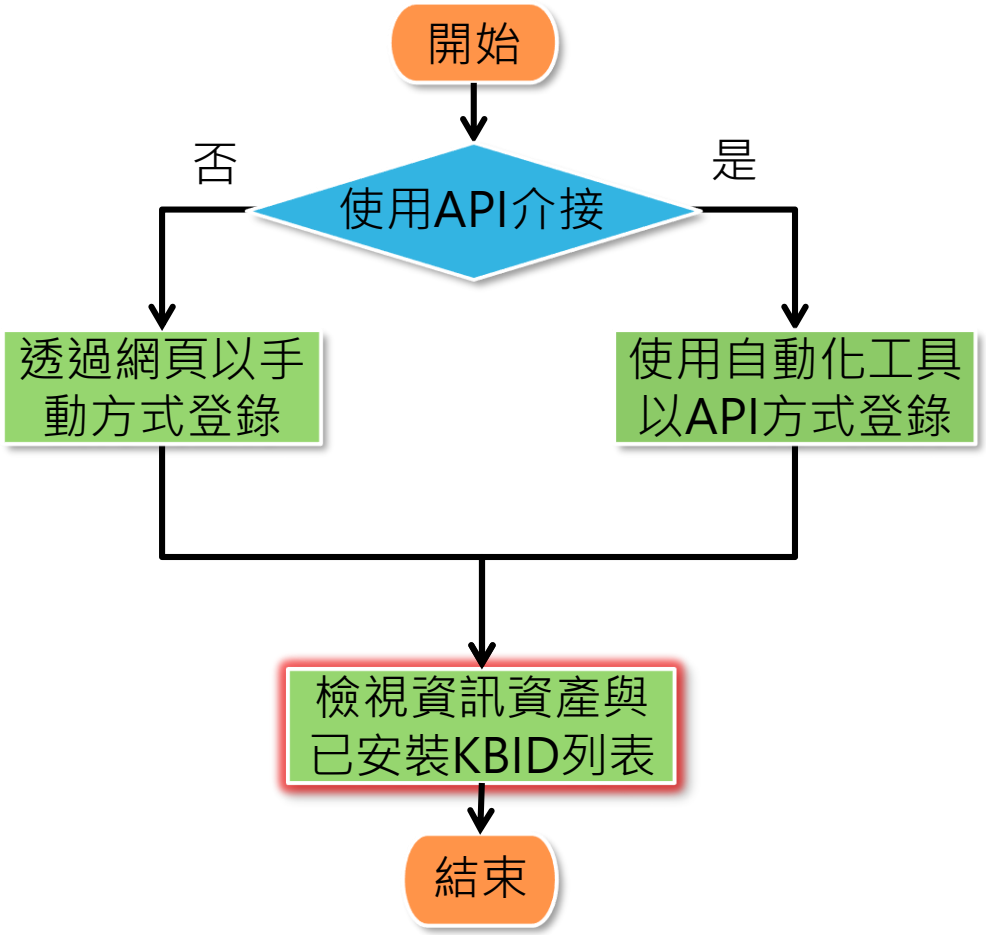
1.貴單位的 VANS API 介接 IP 已完成開通，可透過 API 方式傳輸資訊資產至 VANS 系統。

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
資通系統(System)：
https://vans.nat.gov.tw[redacted]
使用者電腦(Computer)：
https://vans.nat.gov.tw[redacted]
b.已安裝 KBID
資通系統(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。

登錄作業流程


開始
使用API介接
否
是
透過網頁以手動方式登錄
使用自動化工具以API方式登錄
檢視資訊資產與已安裝KBID列表
結束

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

檢視資訊資產與已安裝KBID列表(2/3)

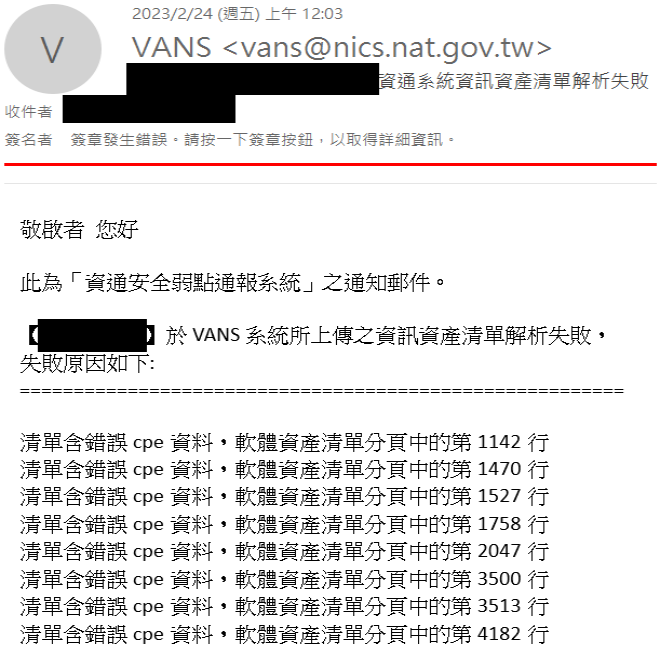
- 資訊資產與已安裝KBID尚未解析或弱點尚未比對完成，暫不提供上傳功能

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


2023/2/24 (週五) 上午 12:03

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

[redacted]資通系統資訊資產清單解析失敗

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：

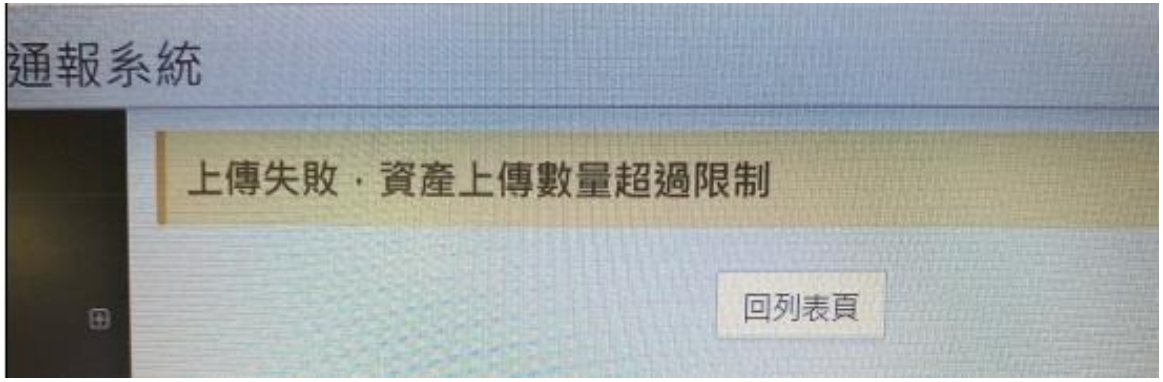
  4.上傳時間：

  5.錯誤訊息截圖：

  6.補充說明：

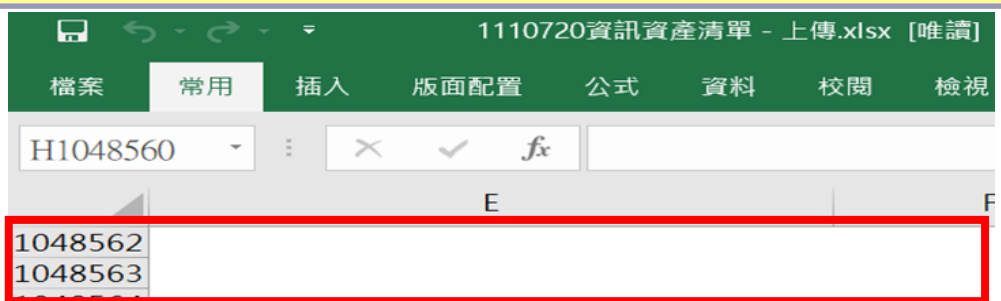
上傳失敗案例與解決方式(2/4)

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？

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

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 遠端桌面",
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

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	進行通知設定 • 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	檢視設定接收通知之信箱 

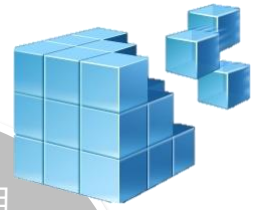
實作練習1(2/2)

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) • 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) • 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

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

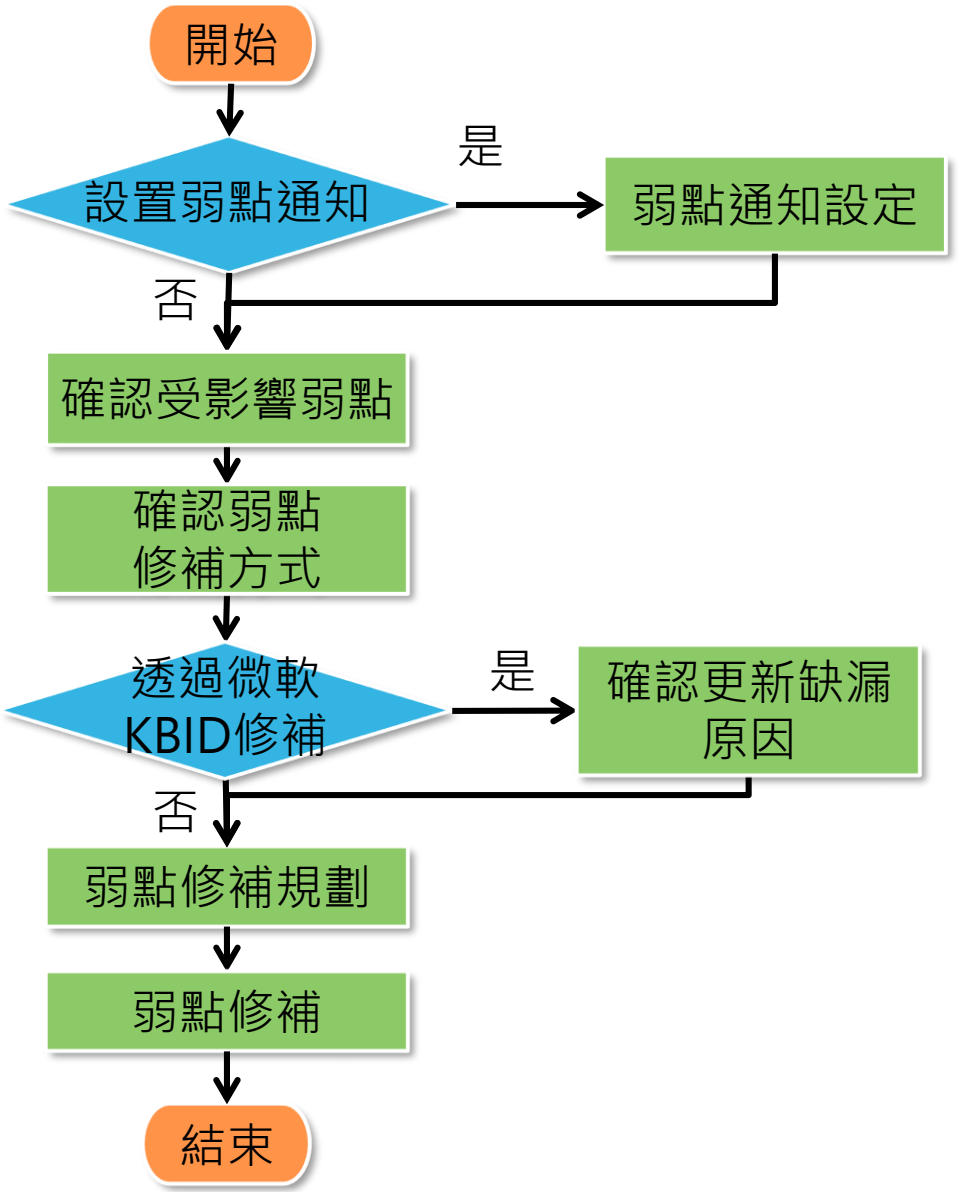


資訊資產與
已安裝KBID
登錄作業

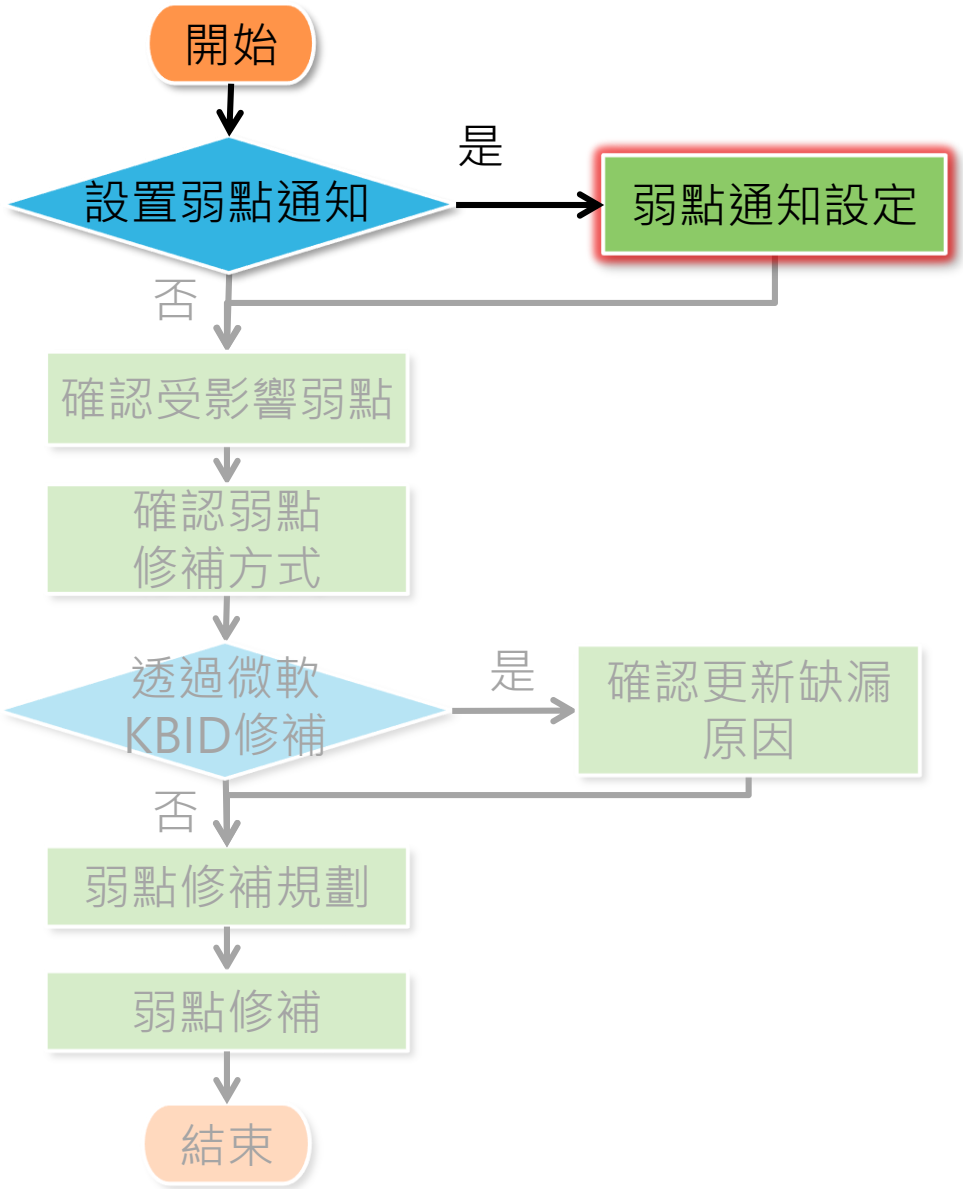
弱點通知
與修補作業

資訊資產與
已安裝KBID
更新作業

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)

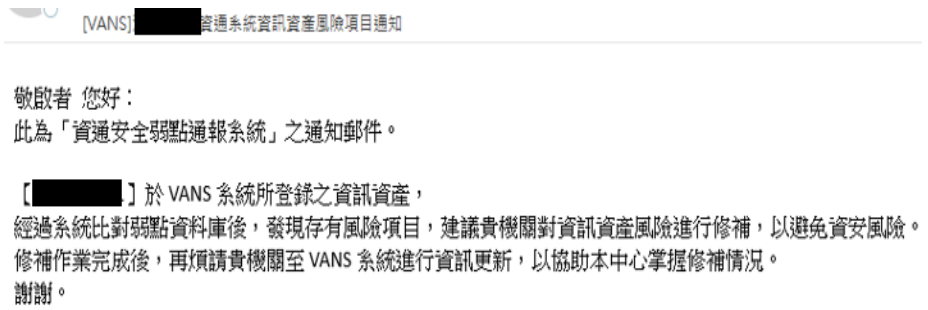
- 首次登入VANS系統，需先進行弱點通知設定
  - 弱點通知設定包含通知開關、CVSS分數門檻及接收通知Email

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

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

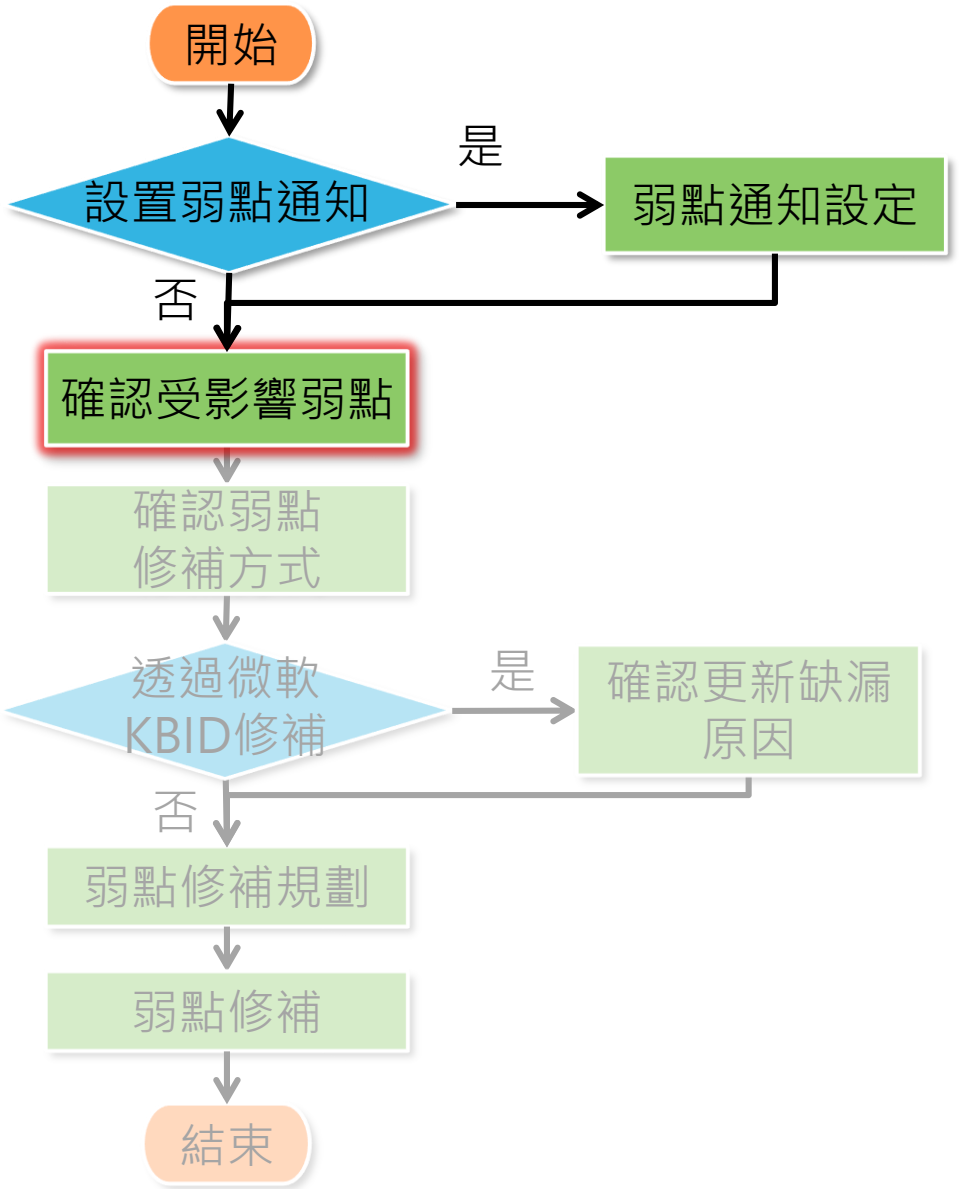

[VANS][redacted]資通系統資訊資產風險項目通知

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 系統所登錄之資訊資產，
經過系統比對弱點資料庫後，發現存有風險項目，建議貴機關對資訊資產風險進行修補，以避免資安風險。
修補作業完成後，再煩請貴機關至 VANS 系統進行資訊更新，以協助本中心掌握修補情況。
謝謝。

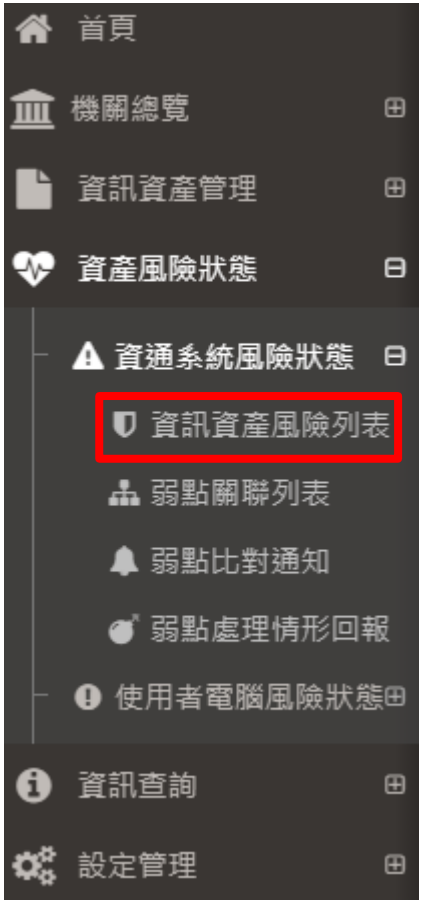
- 同一項資產的同一個弱點只會於首次比對到時進行1次通知，之後不會再出現相同之弱點通知

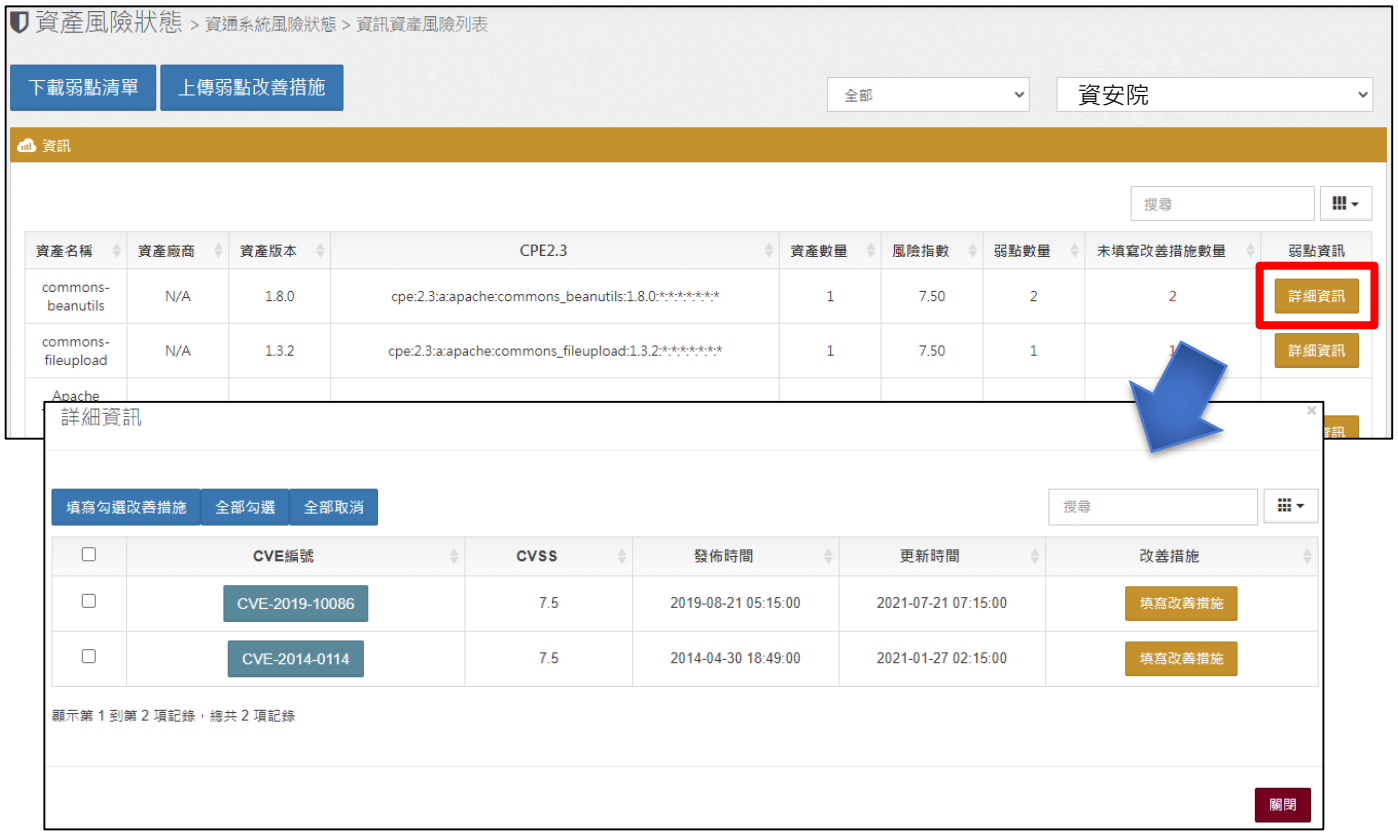
弱點通知與修補規劃作業流程



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

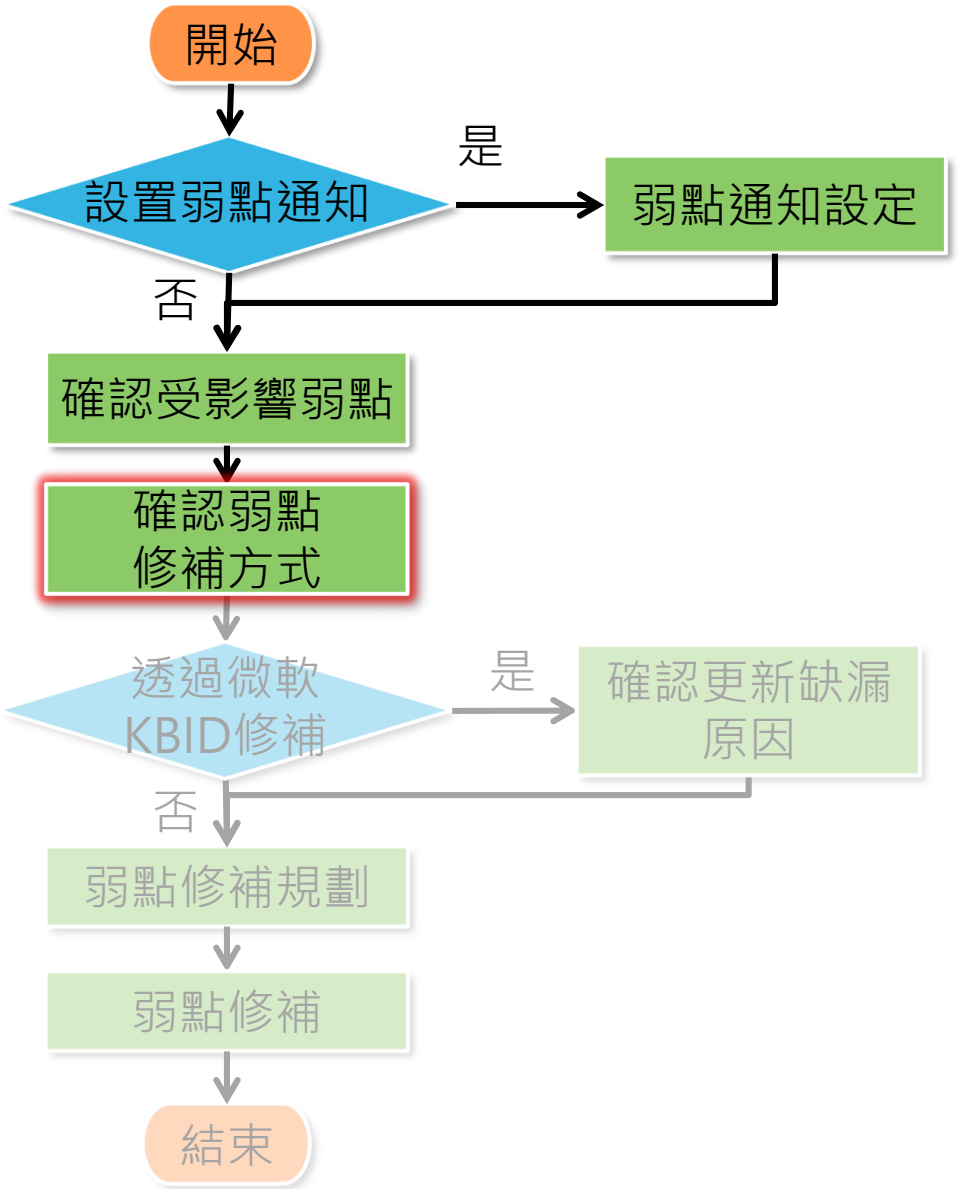




確認受影響弱點–弱點關聯列表

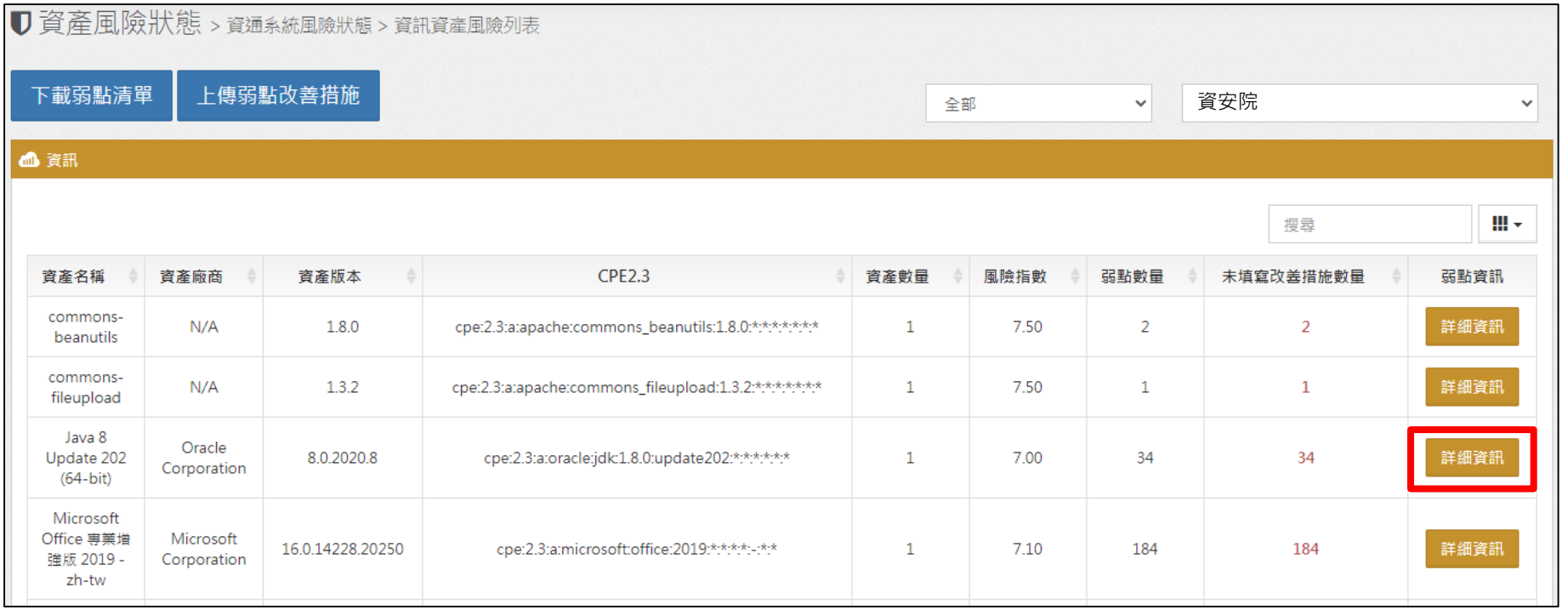
- 若欲查詢特定弱點，透過弱點關聯列表搜尋CVE編號或查詢弱點爆發時間區間，以確認受影響之資訊資產與範圍
  - 資產風險狀態>資通系統風險狀態/使用者電腦風險狀態>弱點關聯列表

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



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

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

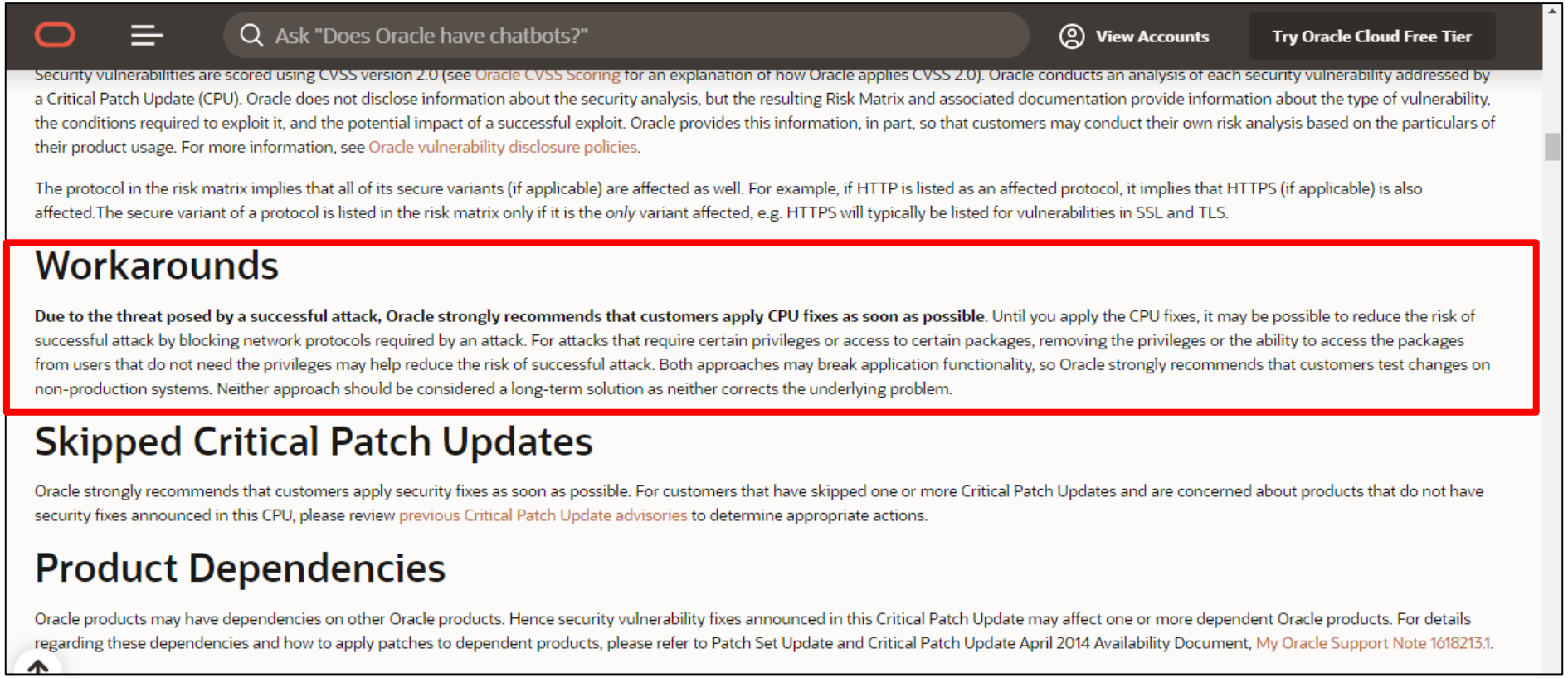
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites 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	
http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html	Vendor Advisory
http://www.securityfocus.com/bid/66856	

原廠說明連結

確認弱點修補方式(4/4)

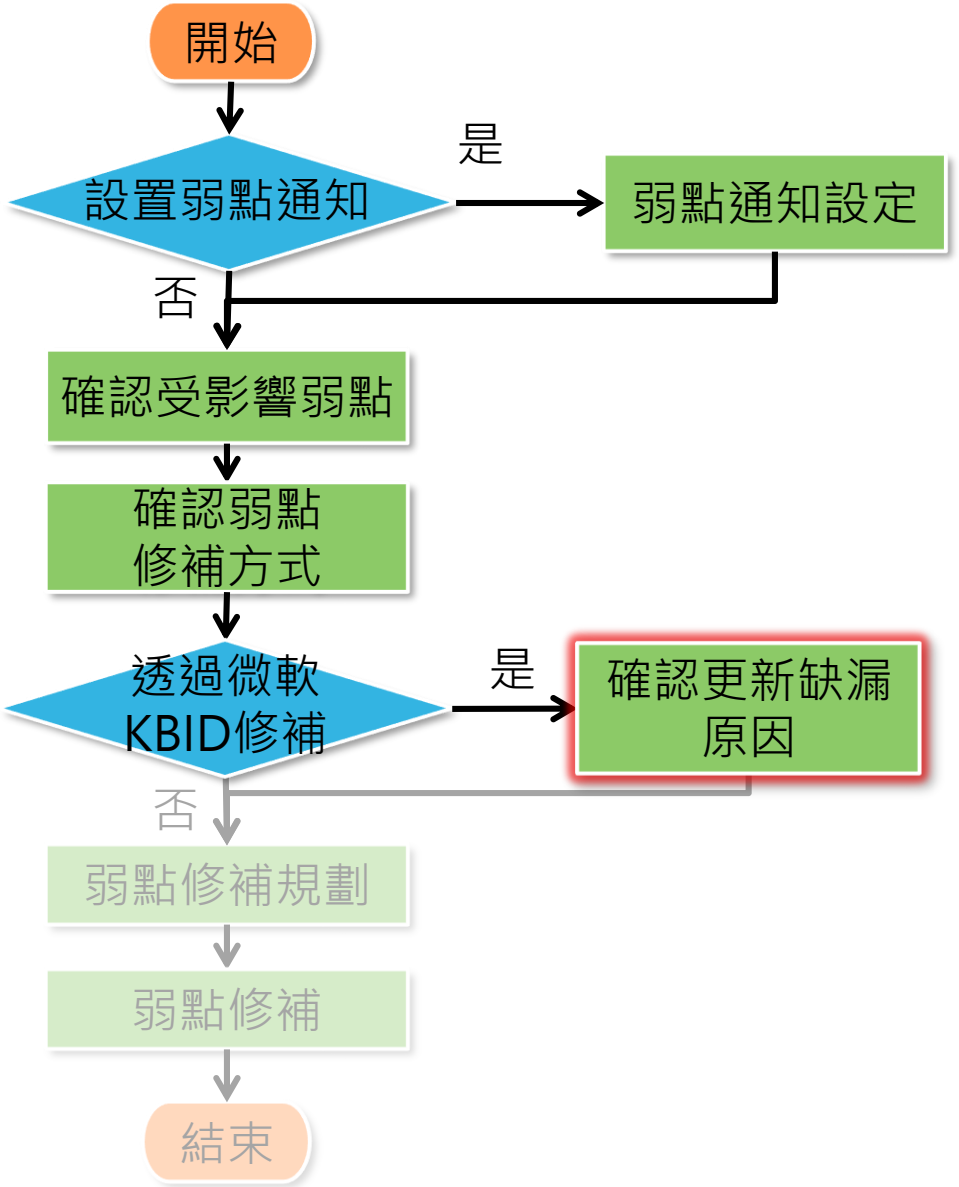
- 透過弱點詳細資訊中的連結，查閱原廠或相關廠商建議弱點修補方式



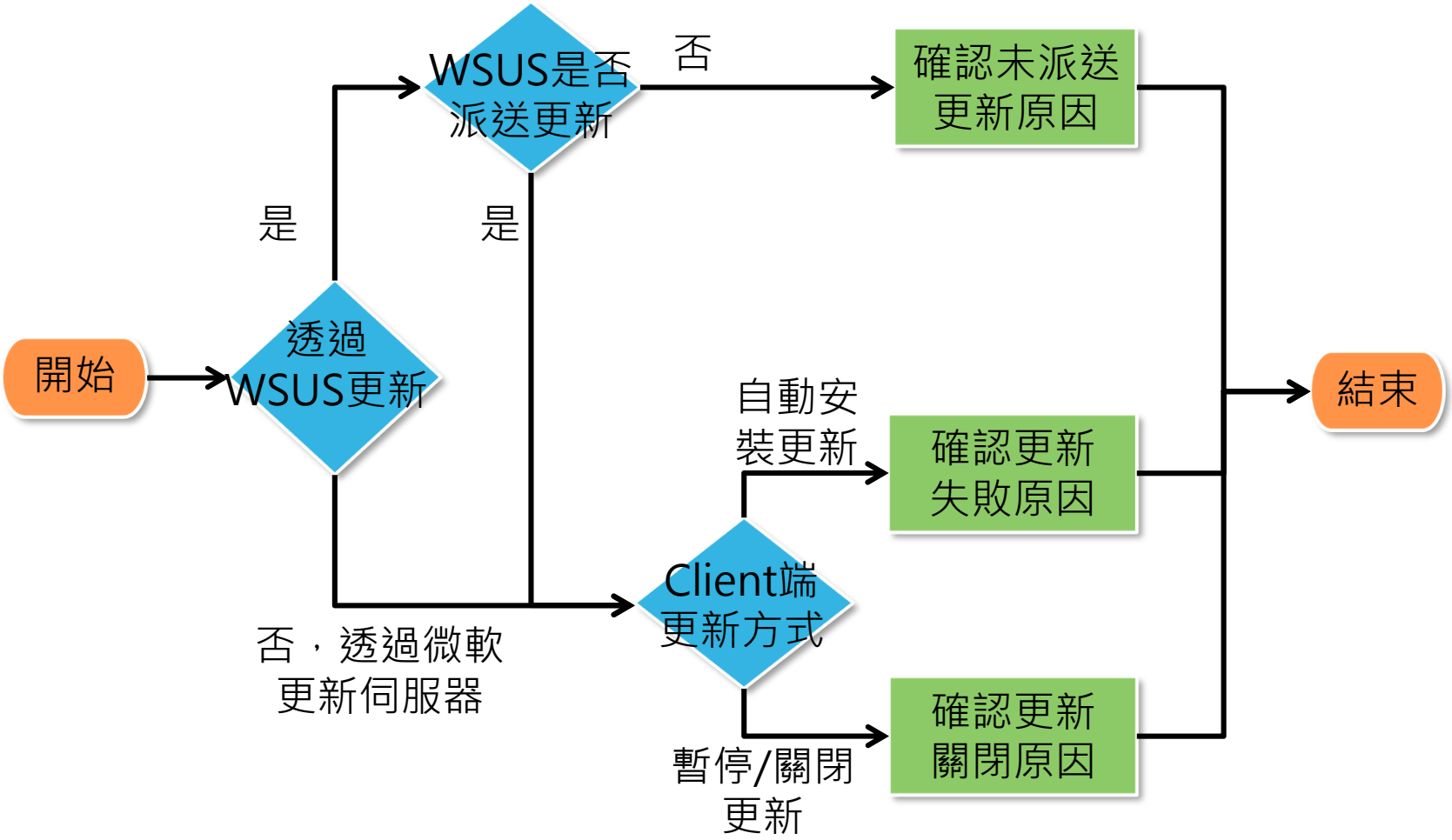
確認弱點修補方式-微軟類

- 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

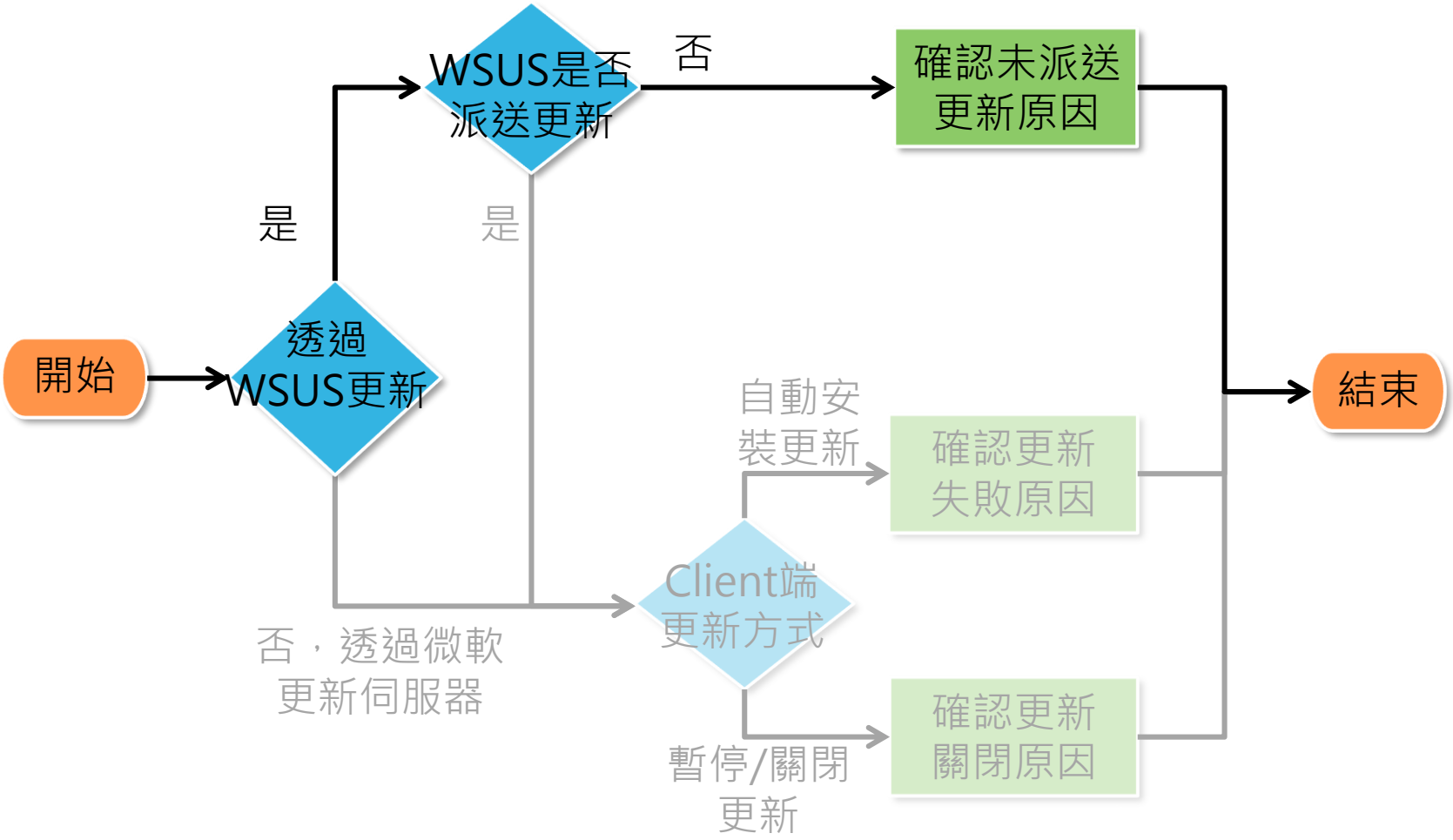
弱點通知與修補規劃作業流程



確認更新缺漏原因


開始
透過WSUS更新
是
WSUS是否派送更新
否
確認未派送更新原因
是
否，透過微軟更新伺服器
Client端更新方式
自動安裝更新
確認更新失敗原因
暫停/關閉更新
確認更新關閉原因
結束

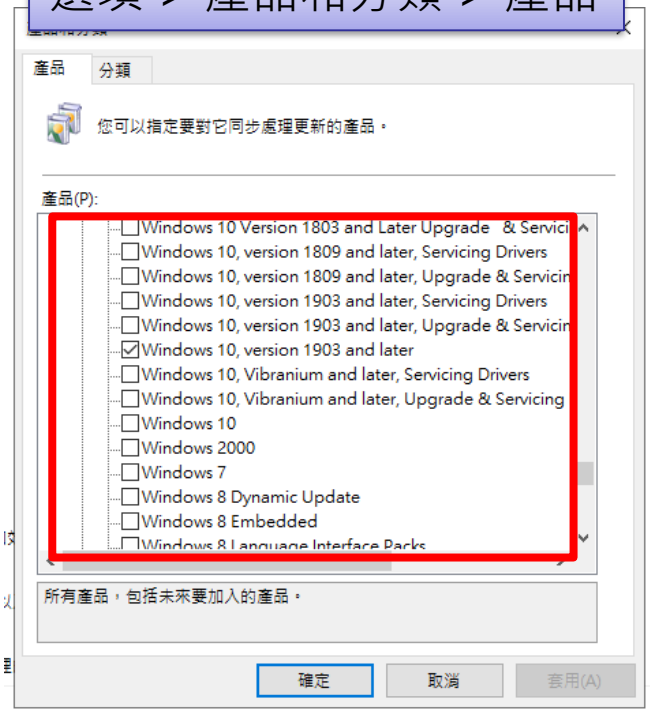
確認更新缺漏原因


開始
透過WSUS更新
是
WSUS是否派送更新
否
確認未派送更新原因
是
否，透過微軟更新伺服器
Client端更新方式
自動安裝更新
確認更新失敗原因
暫停/關閉更新
確認更新關閉原因
結束

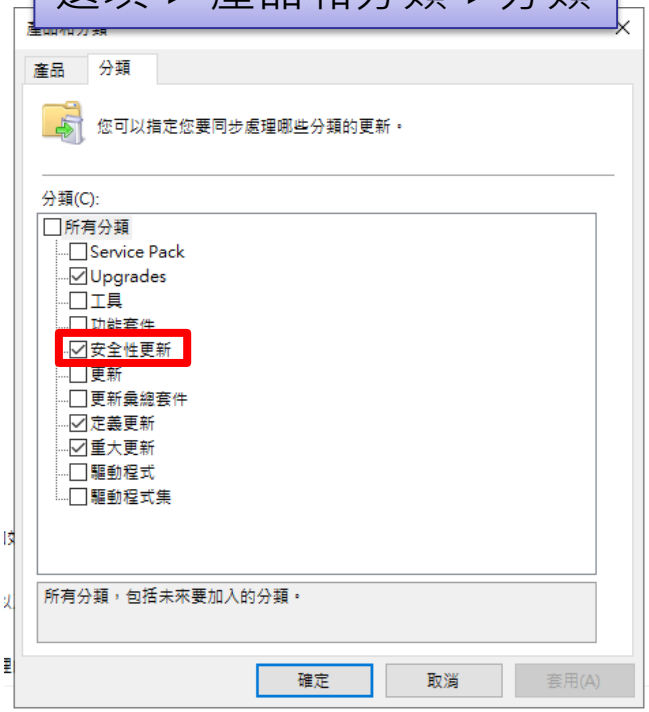
確認WSUS更新派送狀態(1/2)

- 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

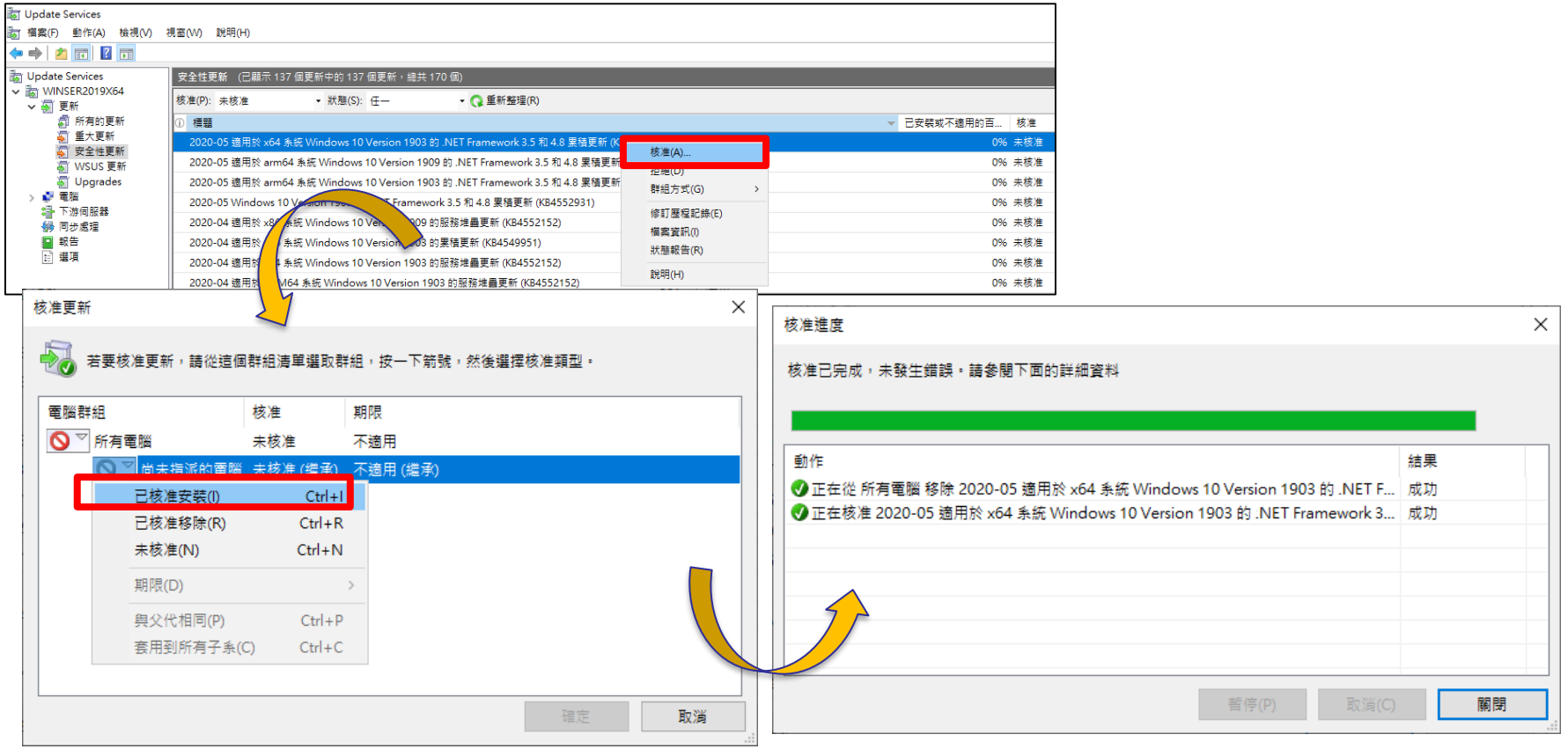


選項 > 產品和分類 >分類



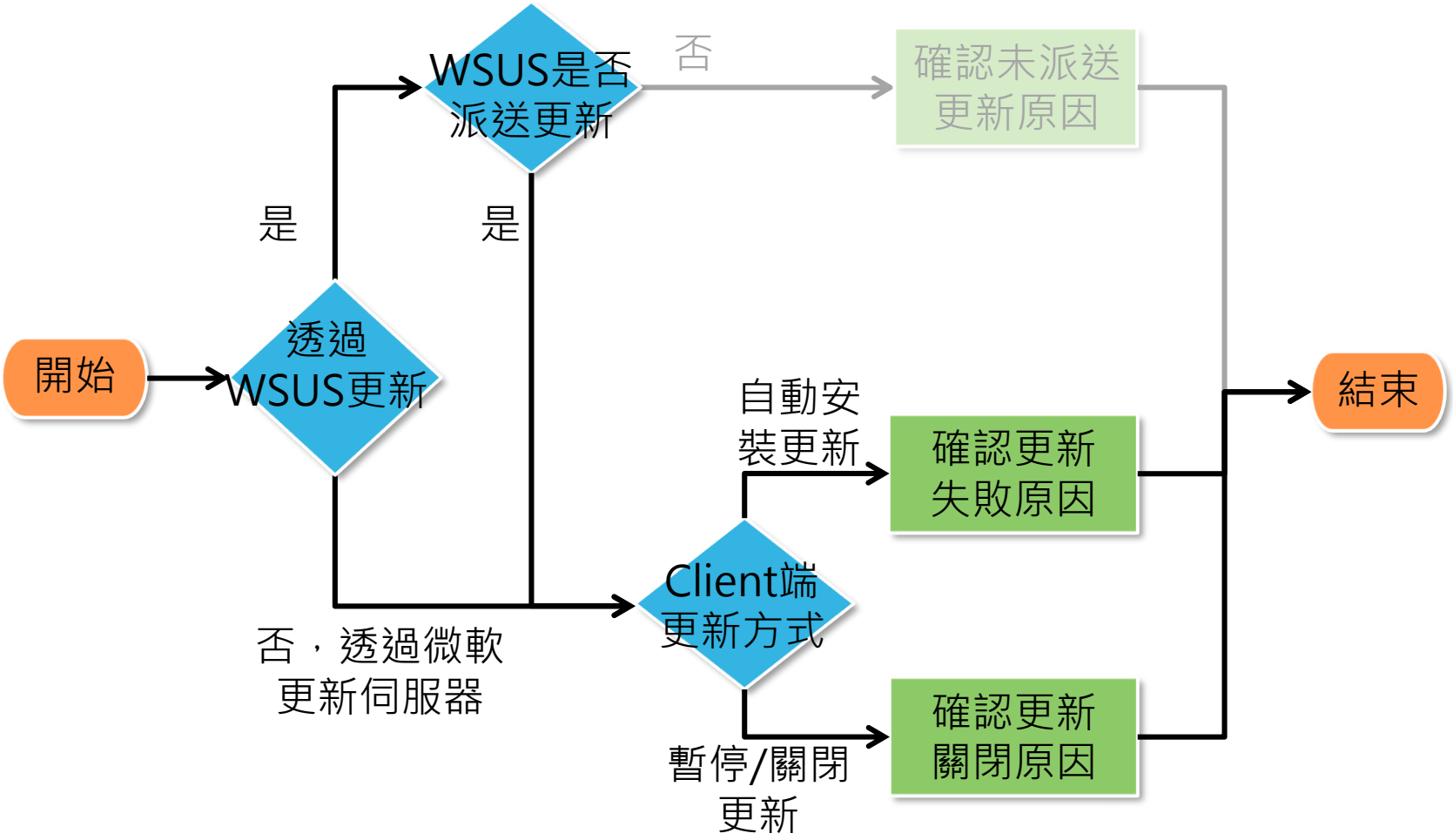
確認WSUS更新派送狀態(2/2)

- 確認缺漏更新是否已於WSUS核准派送



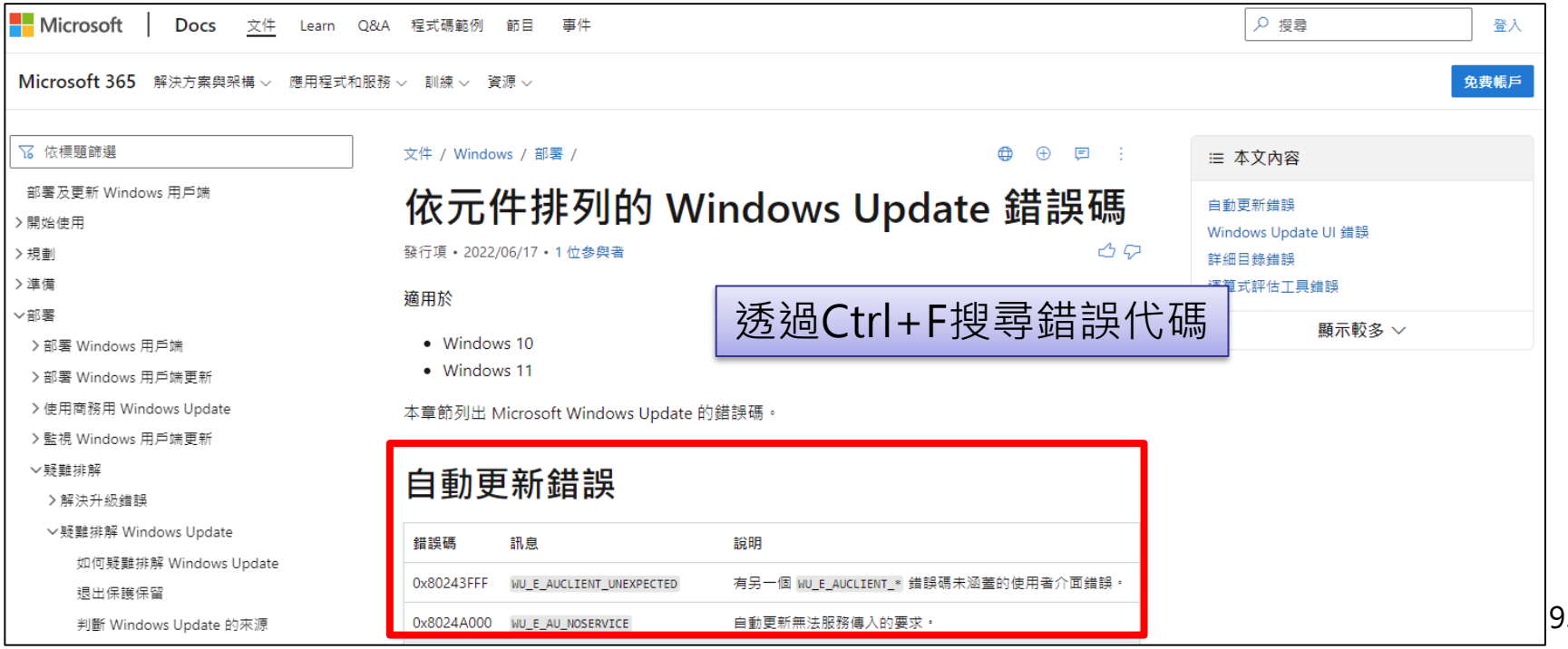
- 若上述確認完畢後，仍有缺漏更新，則需確認是否為Client端問題

確認更新缺漏原因

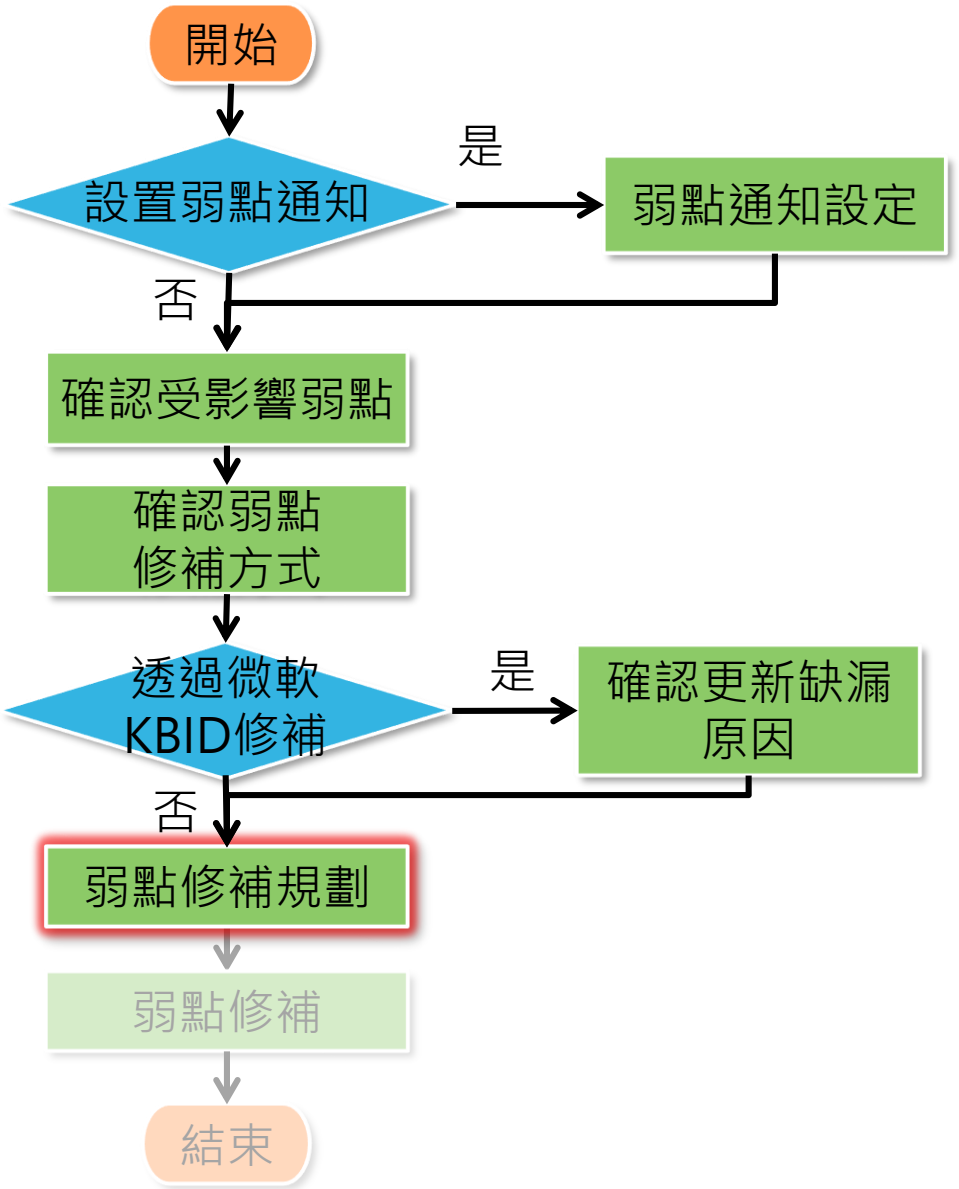

開始
透過WSUS更新
是
WSUS是否派送更新
否
確認未派送更新原因
是
否，透過微軟更新伺服器
Client端更新方式
自動安裝更新
確認更新失敗原因
暫停/關閉更新
確認更新關閉原因
結束

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



弱點通知與修補規劃作業流程



弱點修補規劃(1/6)

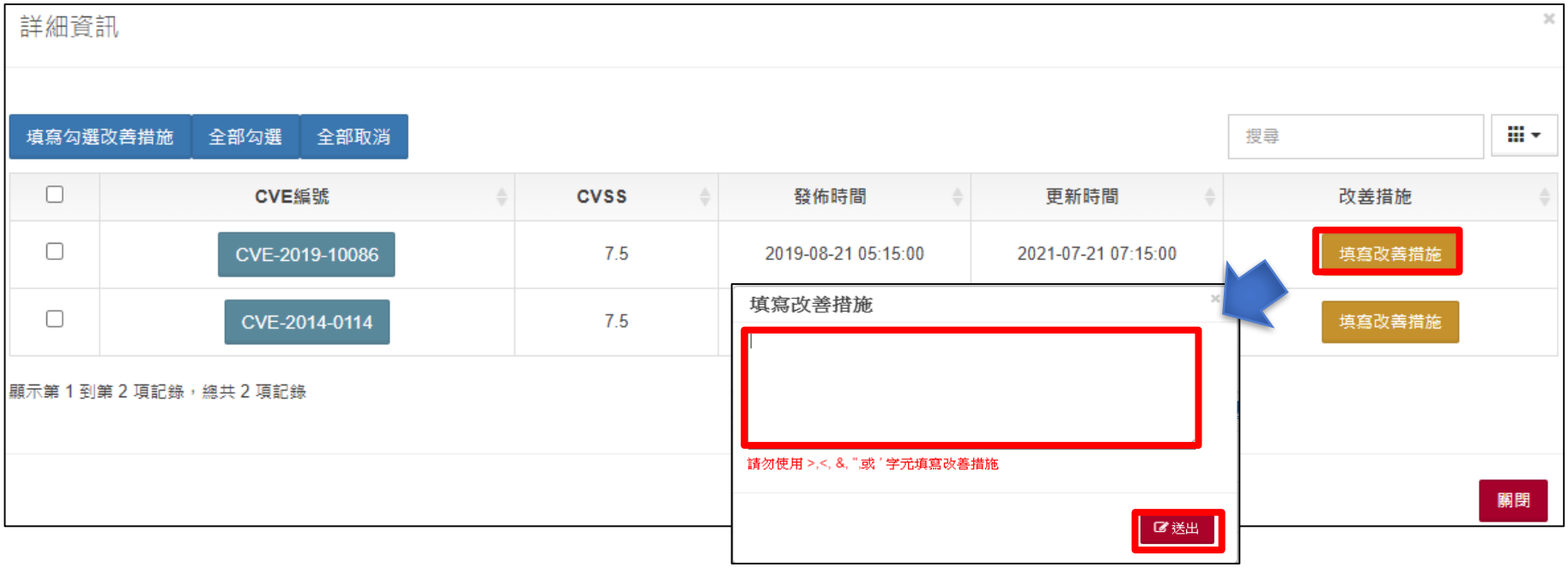
- 依據機關ISMS政策訂定弱點修復基準與修復時程，若無法立即修補、安裝安全性更新或須接受風險之弱點，可針對該風險填寫改善措施
- 針對達到弱點修復基準之弱點進行修補規劃
  - 確認是否可透過更新方式修補弱點？
  - 是否有其他替代修補措施？
  - 預計修補時程

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

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



弱點修補規劃(4/6)

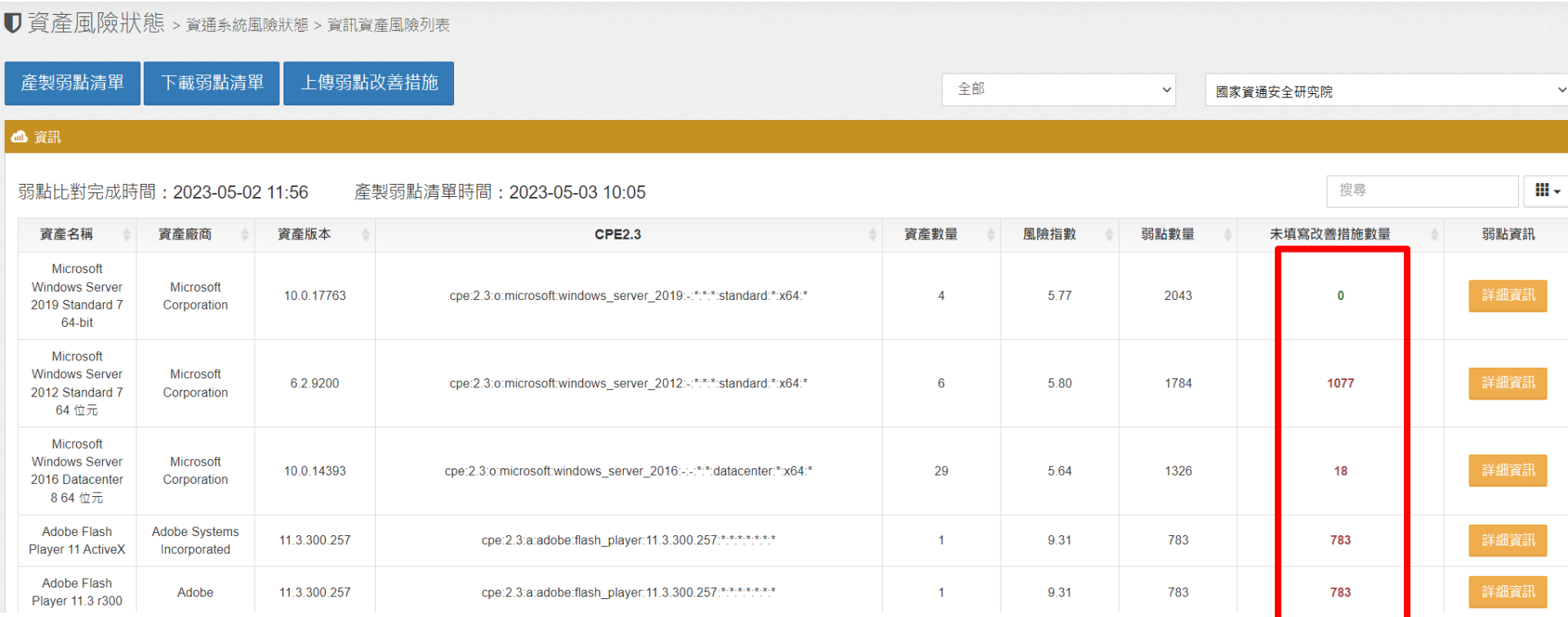
- 批次填寫：可針對同樣修補方式之弱點進行批次弱點修補規劃
  - STEP1：確認弱點後，勾選左方的方格並點選填寫勾選改善措施，以進行多筆CVE之弱點修補規劃
  - STEP2：點選「送出」即完成填寫改善措施
  - 填寫改善措施請避免使用 >、<、 &、"或'等特殊字元)

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

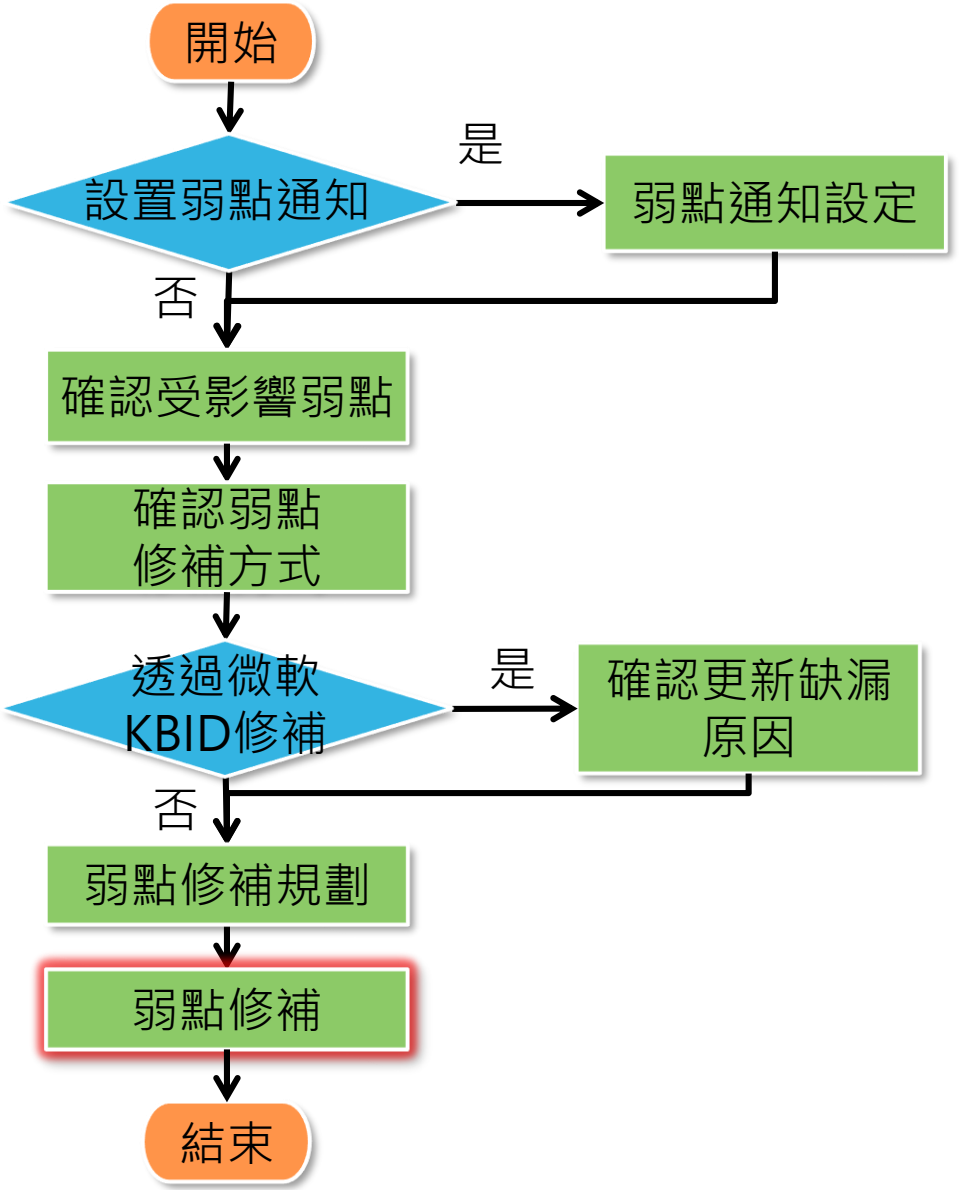
弱點修補規劃(6/6)

- 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



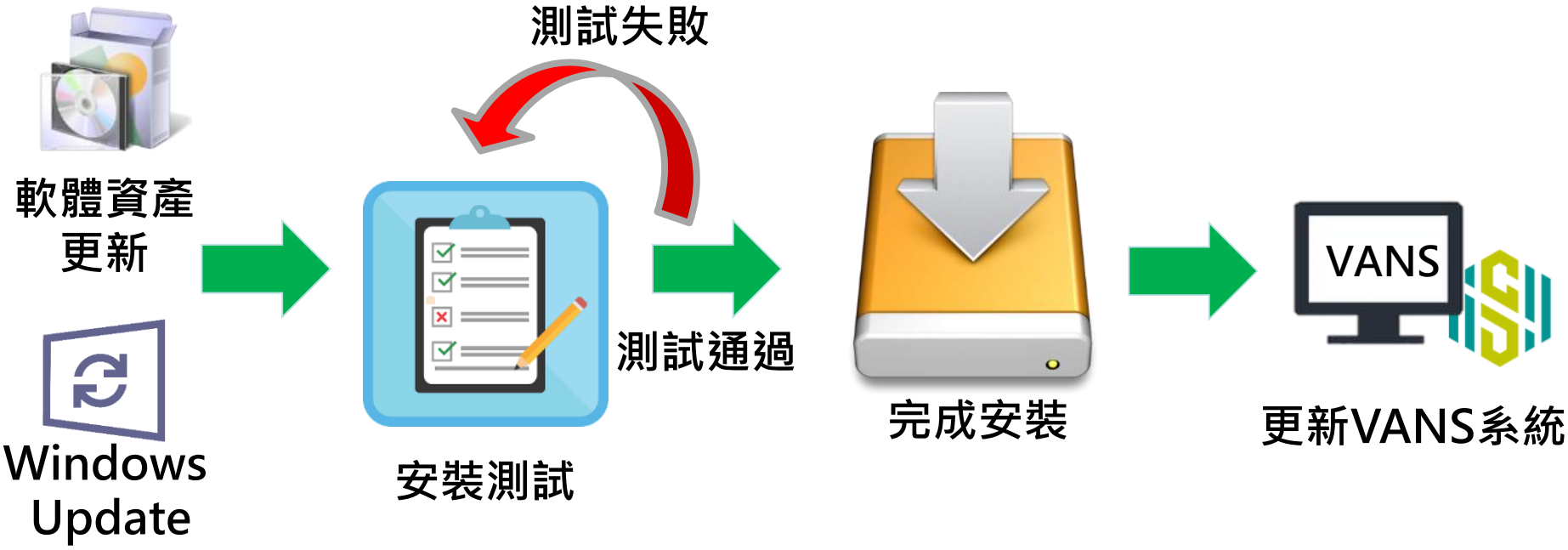
資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
Microsoft Windows Server 2019 Standard 7 64-bit	Microsoft Corporation	10.0.17763	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:standard:*:x64:*	4	5.77	2043	0	詳細資訊
Microsoft Windows Server 2012 Standard 7 64 位元	Microsoft Corporation	6.2.9200	cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:standard:*:x64:*	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

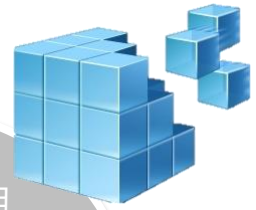
- 檢視弱點通知，並進行弱點修補規劃
- 本項練習時間20分鐘

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	• 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	• 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

資訊資產與
已安裝KBID
盤點作業

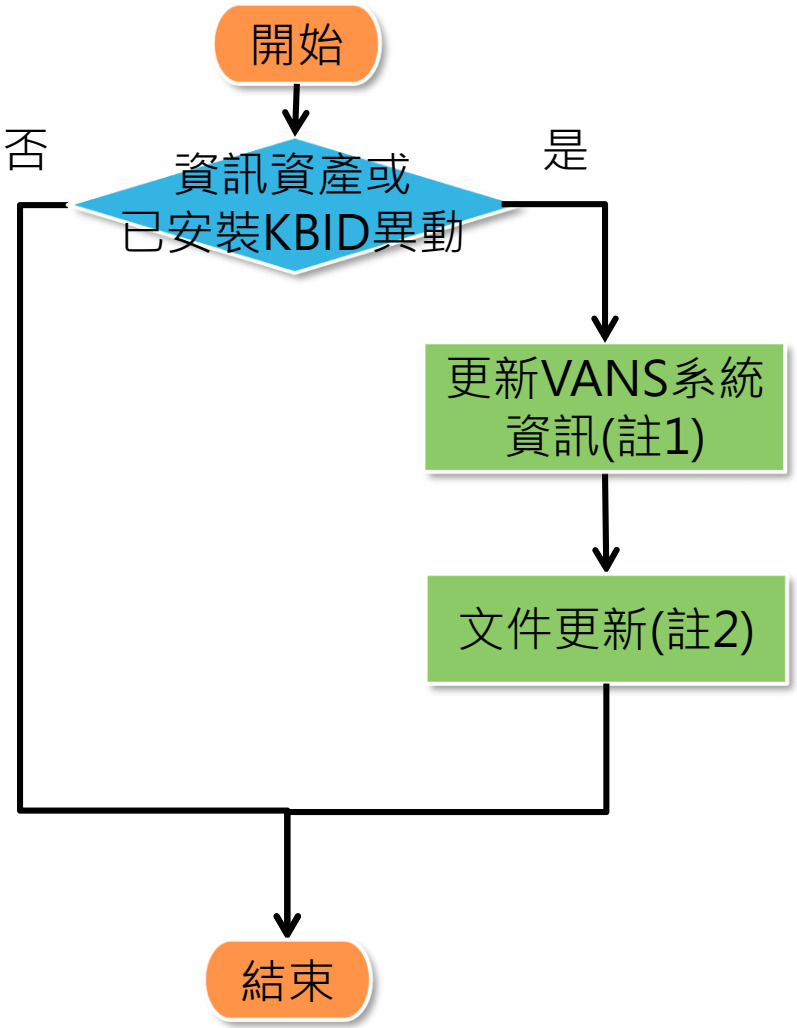


資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

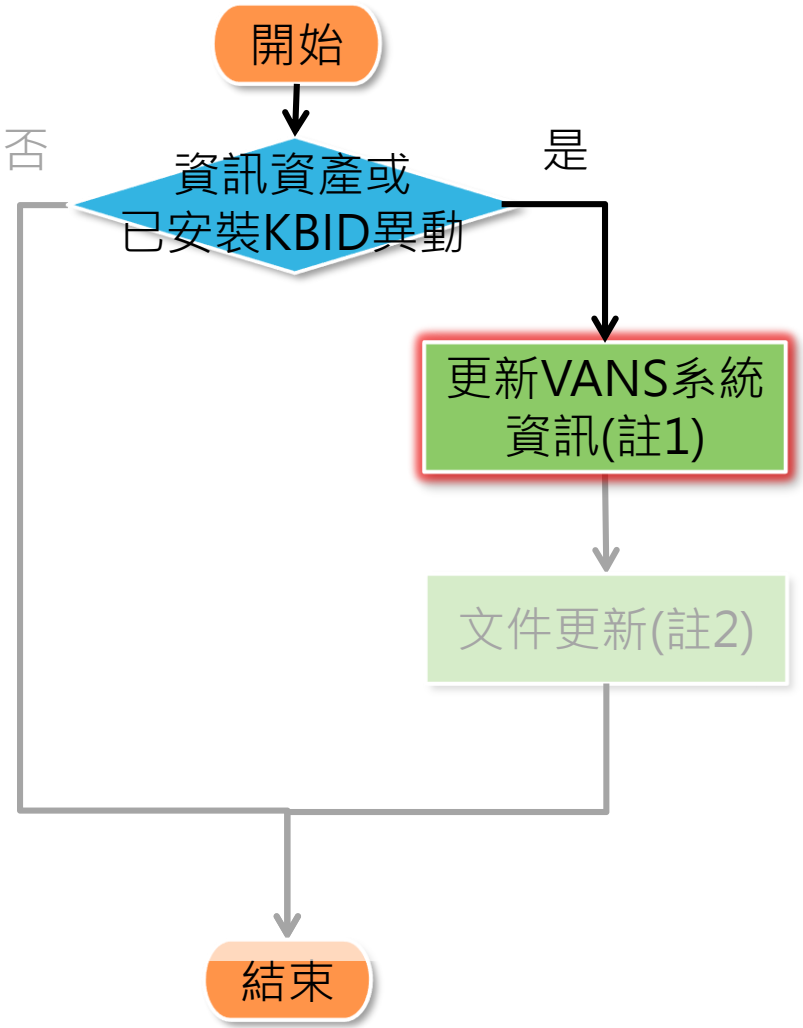
資訊資產與已安裝KBID更新作業流程



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

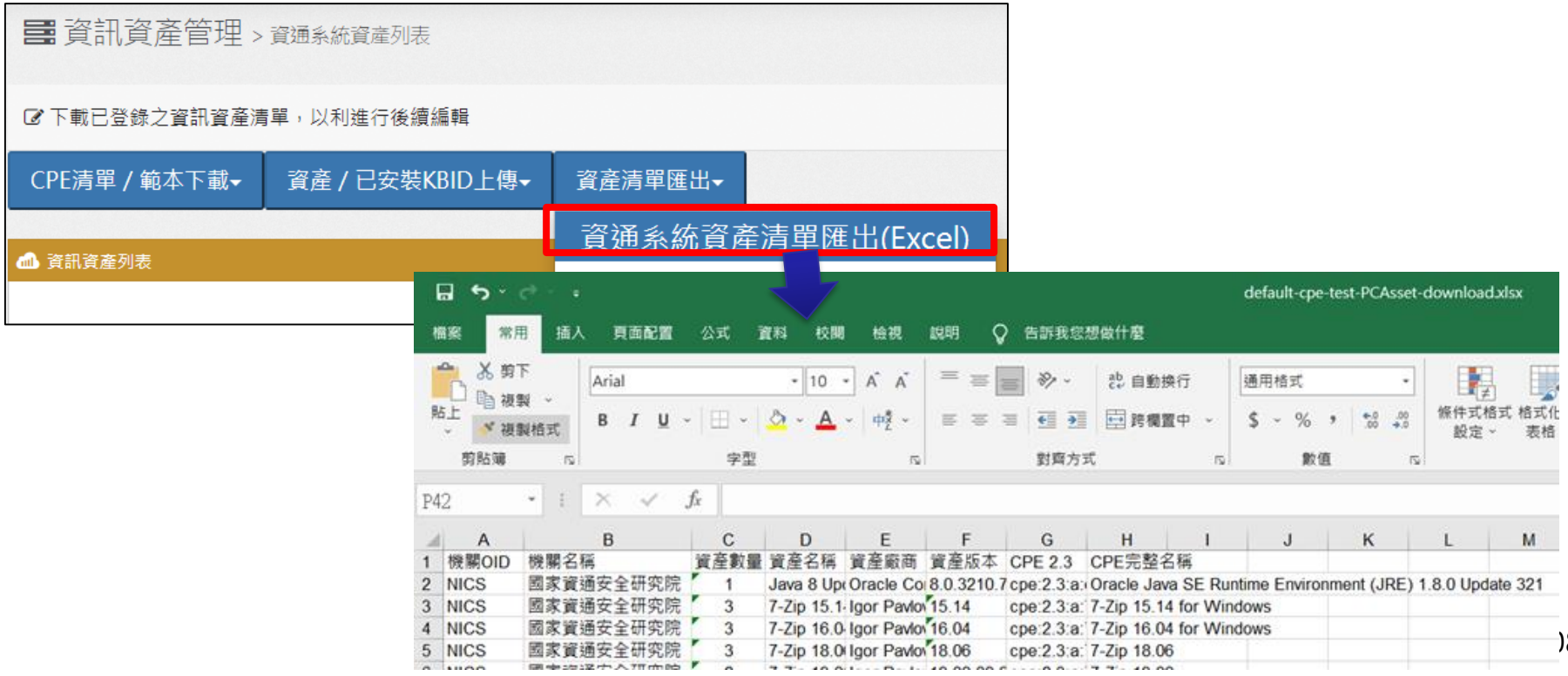


註1更新VANS系統資訊：
新增、修改及刪除VANS系統資訊

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



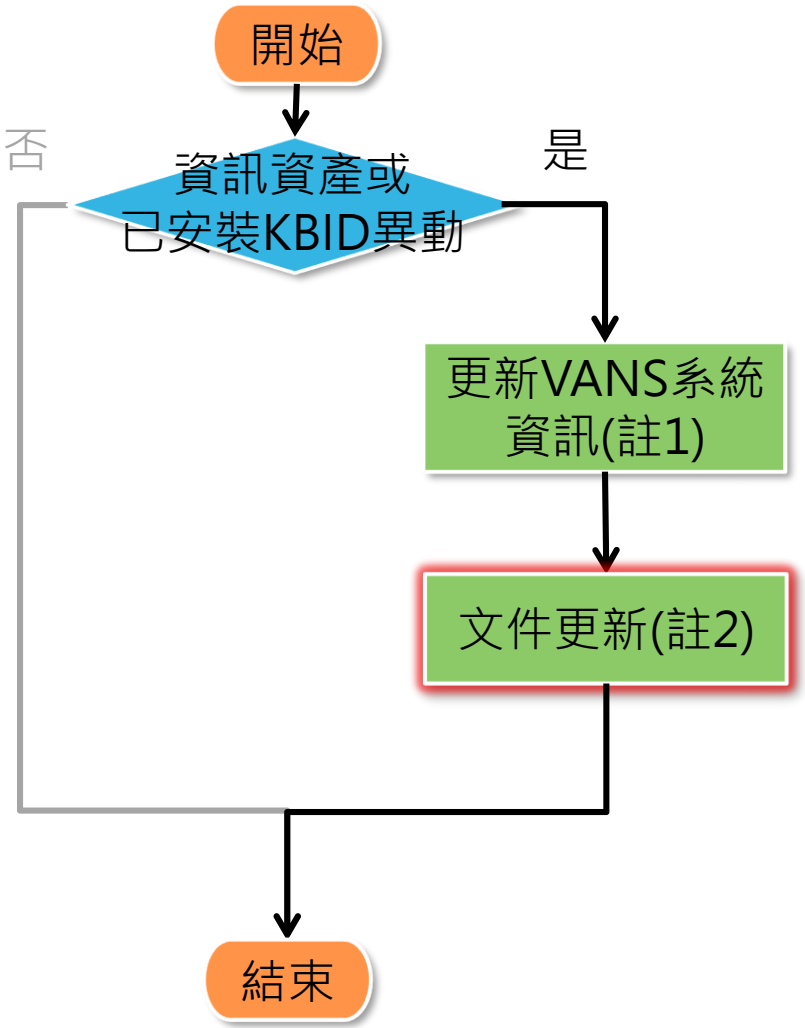
更新VANS系統資訊-單筆更新(1/2)

- 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

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

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 FileUploa	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 Corparation	N/A	Windows Server 2012 R2 Standa	1
3	1	Windows Server 2019 Datacenter x64	Microsoft Corparation	1809	Windows Server 2019 Datacente	1
4	1	Microsoft Visual C++ 2008 Redistributal	Microsoft Corporation	9.0.30729.6161	Microsoft Visual C++ 2008 Redis	1
5	2	Microsoft Silverlight	Microsoft Corporation	5.1.50918.0	Microsoft SilverlightMicrosoft C	2
6	1	VMware Tools	VMware, Inc.	11.0.0.14549434	VMware Tools VMware, Inc. 11.	1

資訊資產清冊 | 資產數量統計

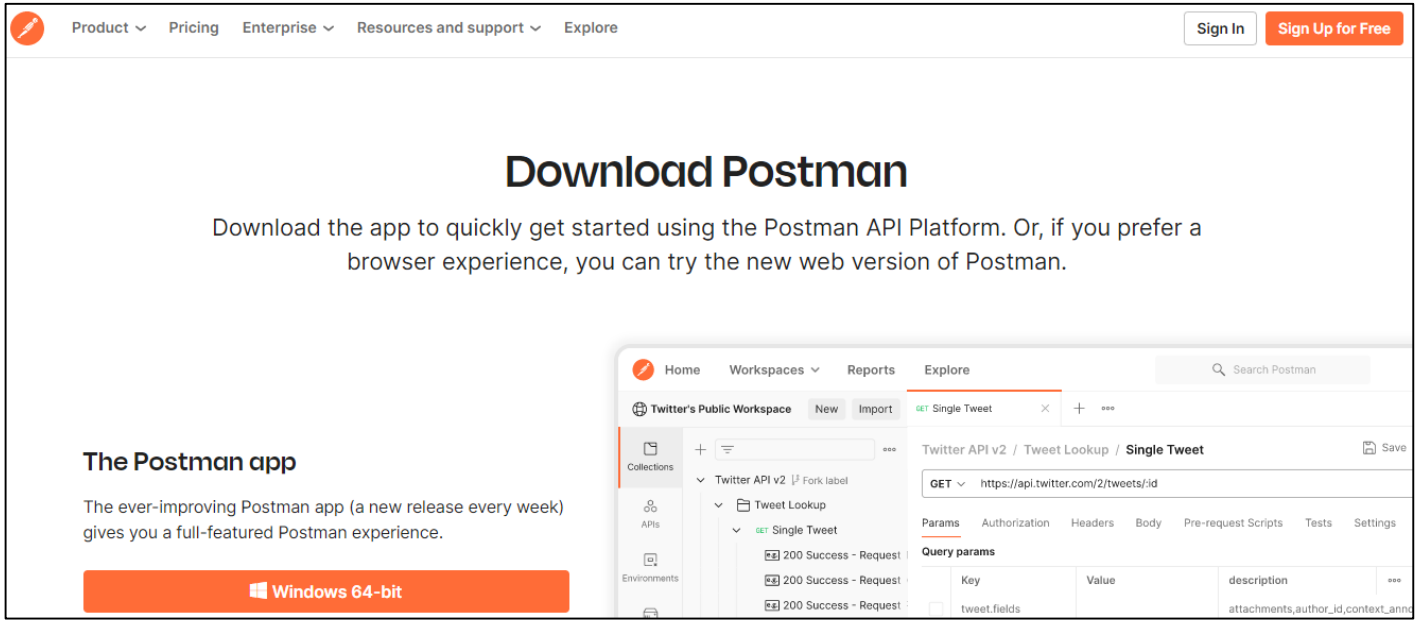
弱點清單

	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	icrosoft:office:2019:*:	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	x, 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	icrosoft: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	icrosoft: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

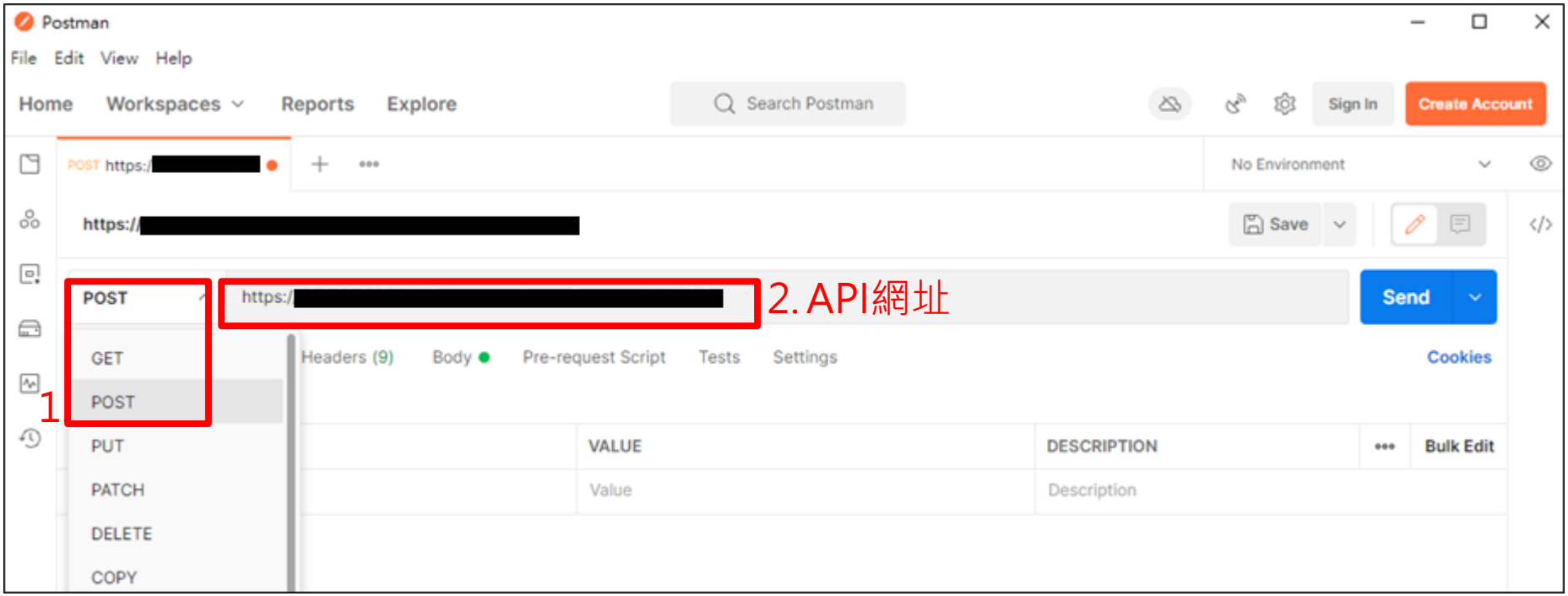
實作練習3(工具說明)(1/5)

- 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



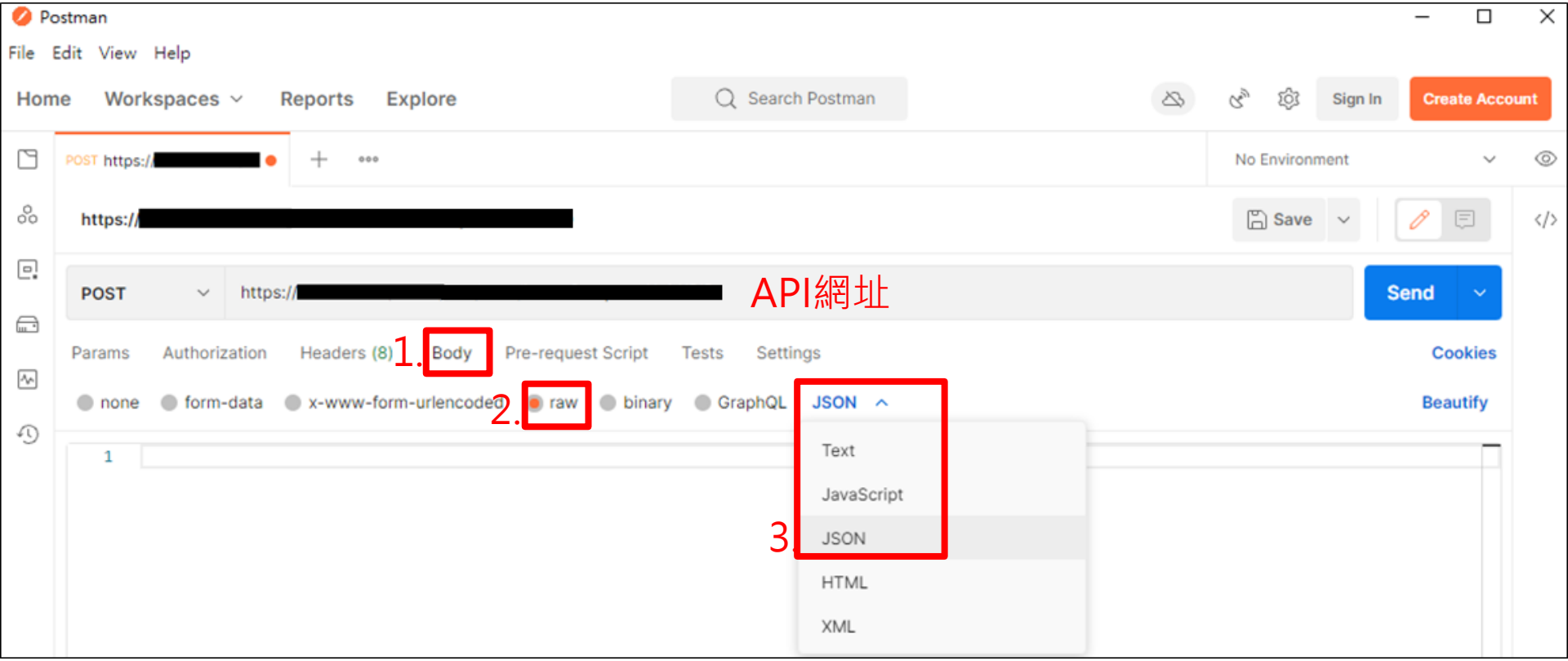
實作練習3(工具說明)(2/5)

- 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

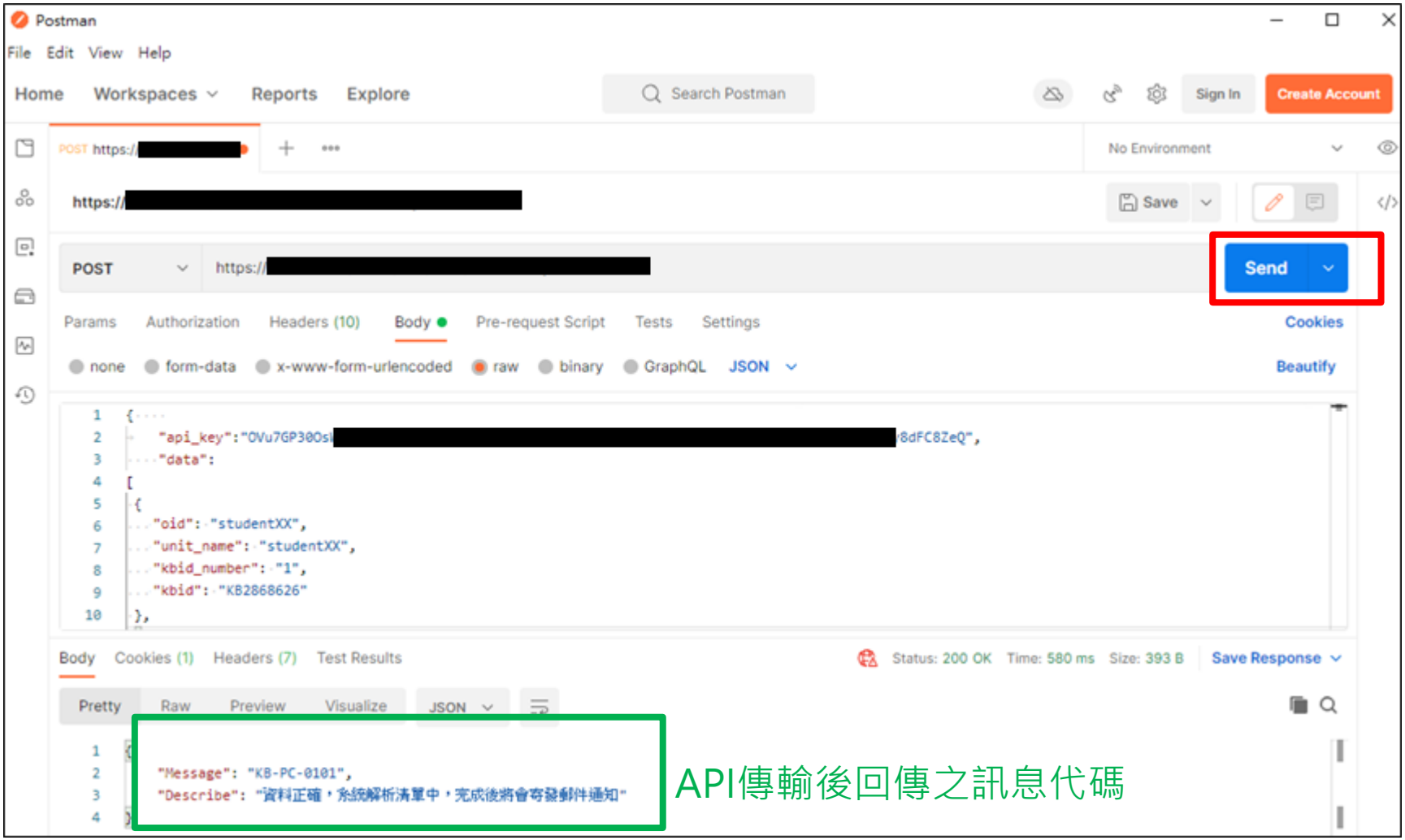


實作練習3(工具說明)(4/5)

- 設定API KEY、OID及機關名稱(unit_name)

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



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	透過API方式，上傳已安裝KBID • 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	• 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

VANS常見問答(1/10)

政策規範

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

VANS常見問答(2/10)

作業程序

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)

作業程序

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。

VANS常見問答(4/10)

系統操作

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)

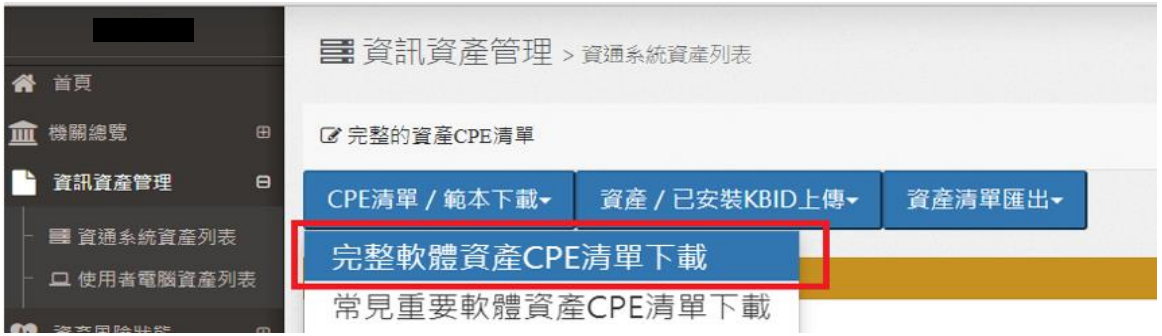
VANS常見問答(6/10)

系統操作

5.

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」



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**」

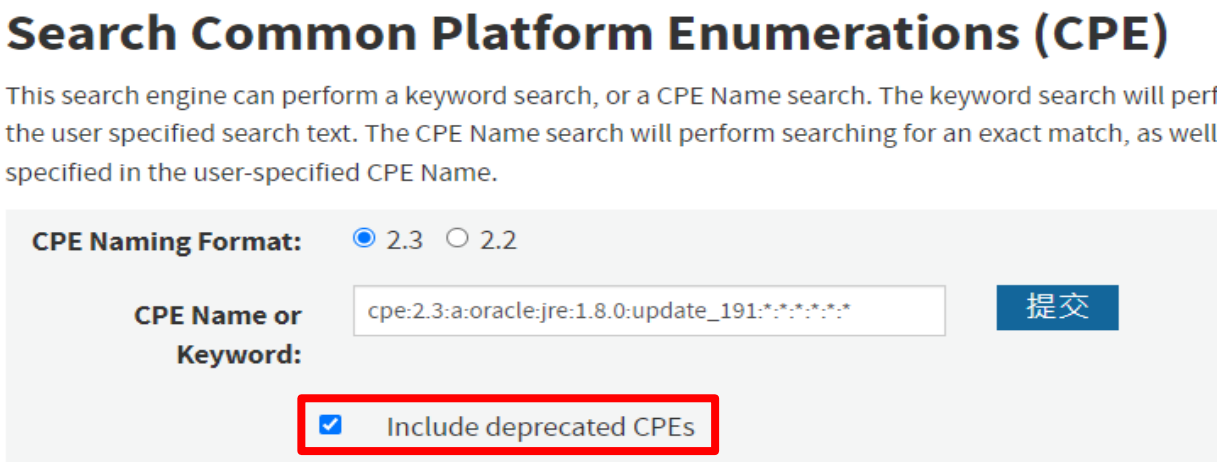
- **有找到相同「CPE2.3」與「CPE完整名稱」**時，應為**正確**之CPE條目。若仍無法上傳請透過VANS服務信箱(VansService@nics.nat.gov.tw)反映
- **未找到相同「CPE2.3」與「CPE完整名稱」**時，應為**錯誤**之CPE條目，無法上傳至VANS系統。請依循步驟3~6至NVD官網進行確認該CPE條目是否已遭取代

VANS常見問答(7/10)

系統操作

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」



4.搜尋後，點選欲查找之CPE條目

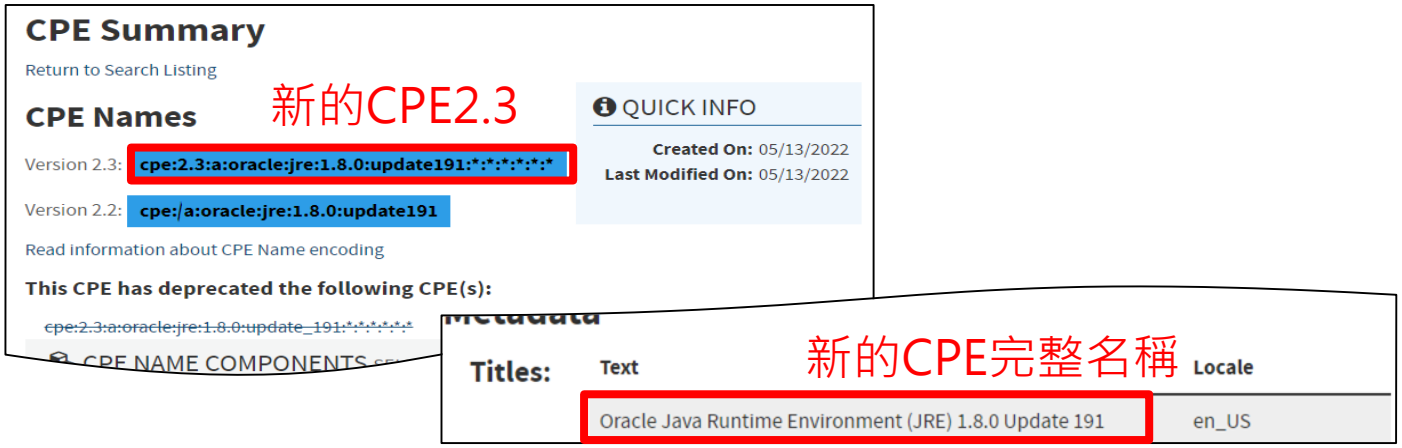
VANS常見問答(8/10)

系統操作

5.

5.依據頁面資訊確認該CPE條目是否已遭取代

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



VANS常見問答(9/10)

系統操作

6. **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?

- (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

7. **VANS系統之「查看修補KBID」功能是否已有考量KB取代關係呢？**

- 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

8. **上傳已安裝KBID至VANS系統後，要如何查看哪些弱點尚未修補？**

- 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 • 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

cpe:2.3:o:microsoft

產品類別為「o」表示為作業系統

機關OID	資產數量	資產名稱			CPE 2.3			資產格式
2.16.886.	7	Nero Info			N/A		:22	custom
2.16.886.	1	OCR			N/A		:22	custom
2.16.886.	2	VMware Player			N/A		:22	custom
2.16.886.	21	l C++ 2015-2019 Redistributable (x86)			N/A		:22	custom
2.16.886.	1	ATSignServerUser			N/A		:51:22	custom
2.16.886.	1	Microsoft Office Standard 2013			:microsoft:office:2013:*:*:*	Mi	:51:22	cpe
2.16.886.	1	Nmap 7.80			3:a:nmap:nmap:7.80:*:*:*:*	Nmap 7.80	2022-05-26 10:51:22	cpe
2.16.886.	1	Microsoft .NET Framework 4.8 SDK	Microsoft Corporation	4.8.03752	crosoft:.net_framework:4.8:*	rosoft .NET Framework 4.8	2022-05-26 10:51:22	cpe
2.16.886.	18	rosoft Office LTSC 標準版 2021 - zh-	Microsoft Corporation	16.0.14332.20281	crosoft:office:2021:*:*:*:lts	Term Servicing Channel (	2022-05-26 10:51:22	cpe
2.16.886.	1	Notepad++ (64-bit x64)	Notepad++ Team	8.1.9.3	N/A	N/A	2022-05-26 10:51:22	custom
2.16.886.	1	ATSignServerUser	AT Information Systems	3.2.0.2	N/A	N/A	2022-05-26 10:51:22	custom
2.16.886.	1	LINE	LINE Corporation	6.3.0.2329	corp:line:6.3.0.2329:*:*:*:*	ration LINE 6.3.0.2329 for	2022-05-26 10:51:22	cpe
2.16.886.	1	Java 8 Update 311 (64-bit)	Oracle Corporation	8.0.3110.11	oracle:jre:1.8.0:update311:*	racle JRE 1.8.0 Update 311	2022-05-26 10:51:22	cpe
2.16.886.	1	會議 Microsoft Teams	會議 Microsoft Teams	1	N/A	N/A	2022-05-26 10:51:22	custom
2.16.886.	1	System CLR Types for SQL Server 20	Microsoft Corporation	11.0.2100.60	nicrosoft:sql_server:2012:-:*	Microsoft SQL Server 2012	2022-05-26 10:51:22	cpe
2.16.886.	3	sual C++ 2008 Redistributable - x86 9.	Microsoft Corporation	9.0.30729	N/A	N/A	2022-05-26 10:51:22	custom
2.16.886.	1	WinMerge 2.16.4.0	Thingamahoochie Software	2.16.4.0	inmerge:winmerge:2.16.4:*:	WinMerge 2.16.4	2022-05-26 10:51:22	cpe

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

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


Q
&
A

参考資料

參考資料(1/2)

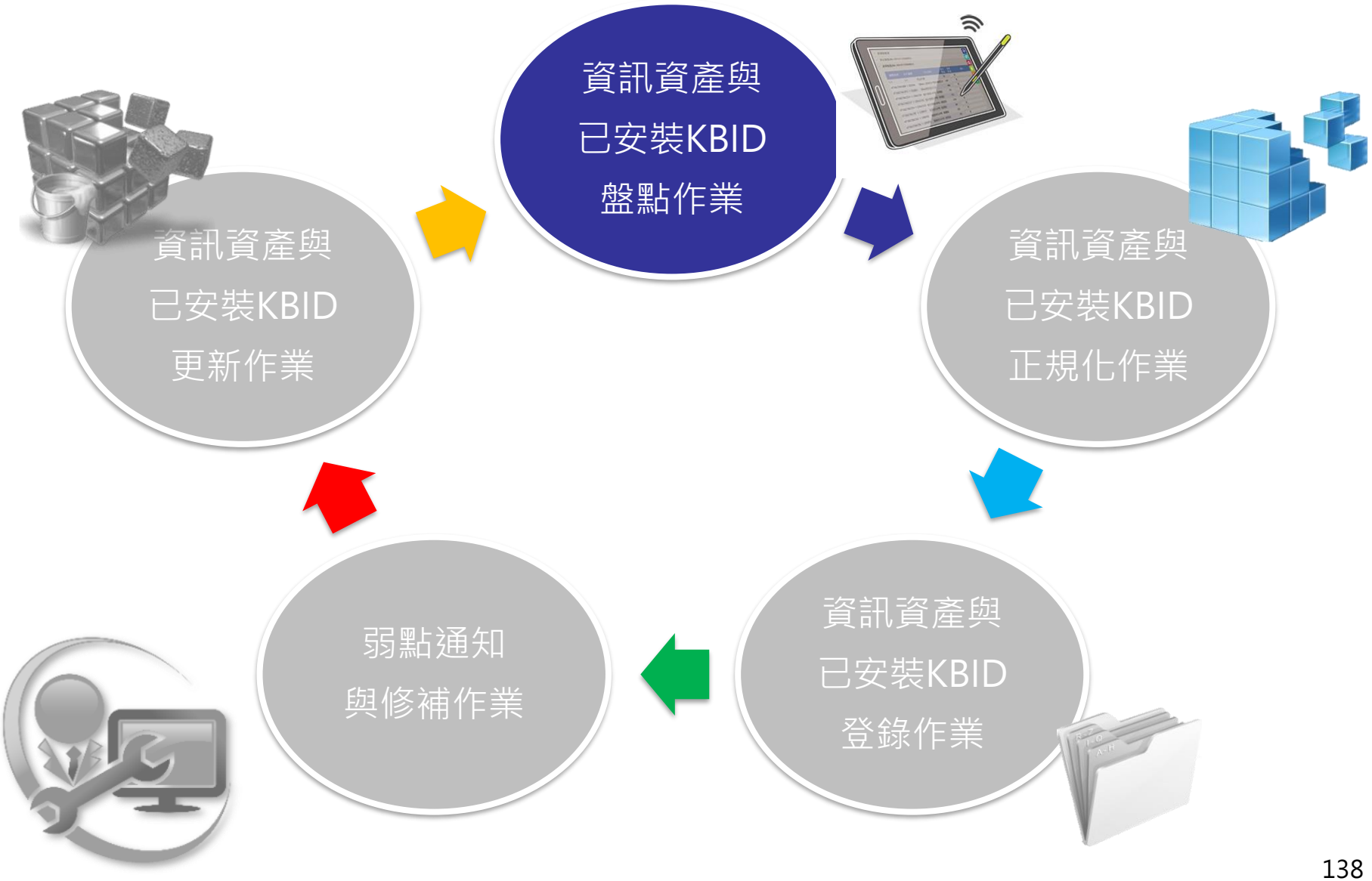
- Windows Management Instrumentation
  - https://docs.microsoft.com/zh-tw/windows/desktop/wmisdk/wmi-start-page
- How to find the Windows version using Registry?
  - https://mivilisnet.wordpress.com/2020/02/04/how-to-find-the-windows-version-using-registry/
- Microsoft Docs - Dir
  - https://docs.microsoft.com/zh-tw/windows-server/administration/windows-commands/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)

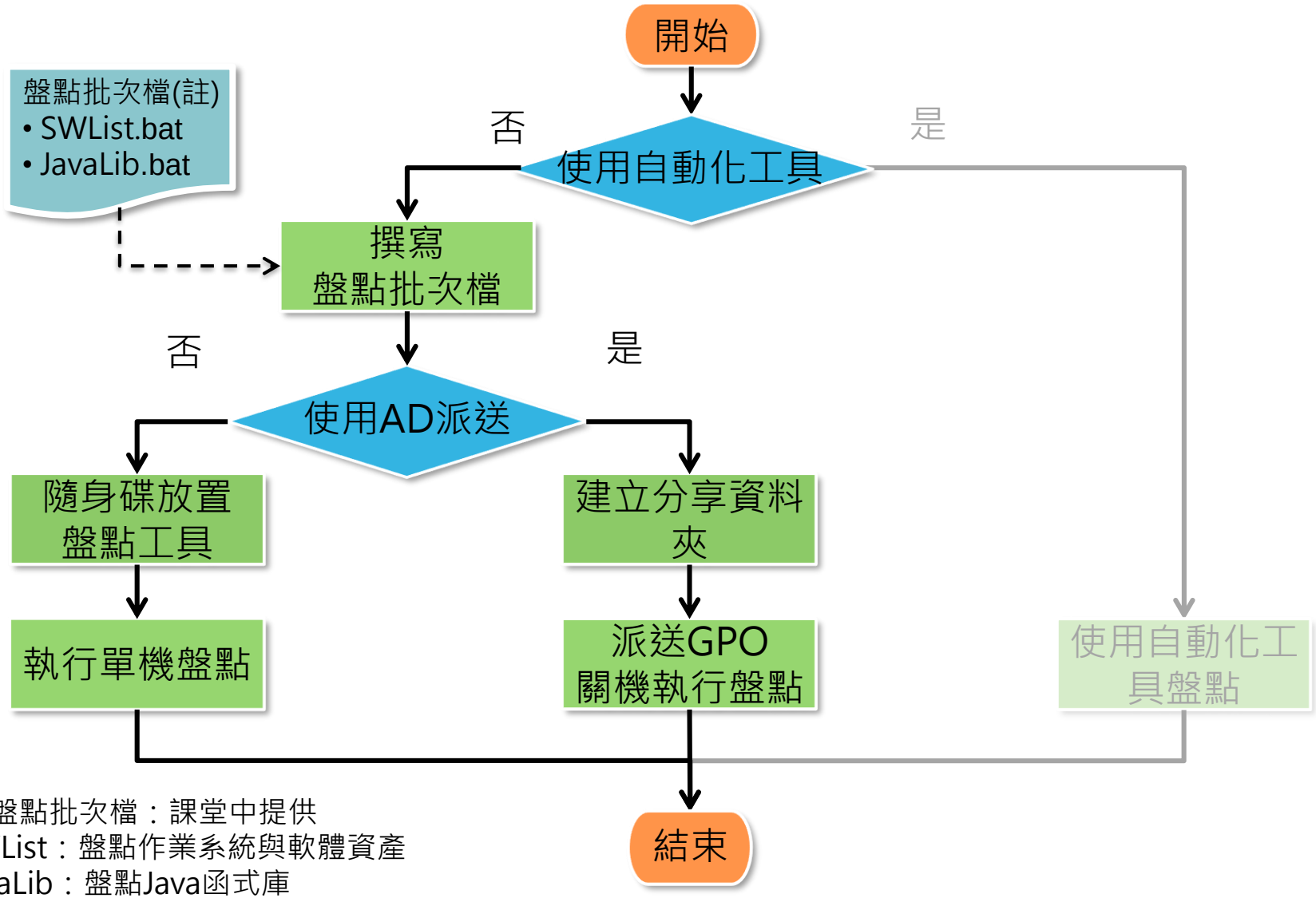
- 用來描述 Microsoft 軟體更新標準術語的說明
  - https://support.microsoft.com/zh-tw/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro
- Microsoft Power Query for Excel
  - https://www.microsoft.com/zh-TW/download/details.aspx?id=39379
- 關於 Excel 中的 Power Query
  - https://support.office.com/zh-tw/article/Power-Query-%E5%BF%AB%E9%80%9F%E5%85%A5%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

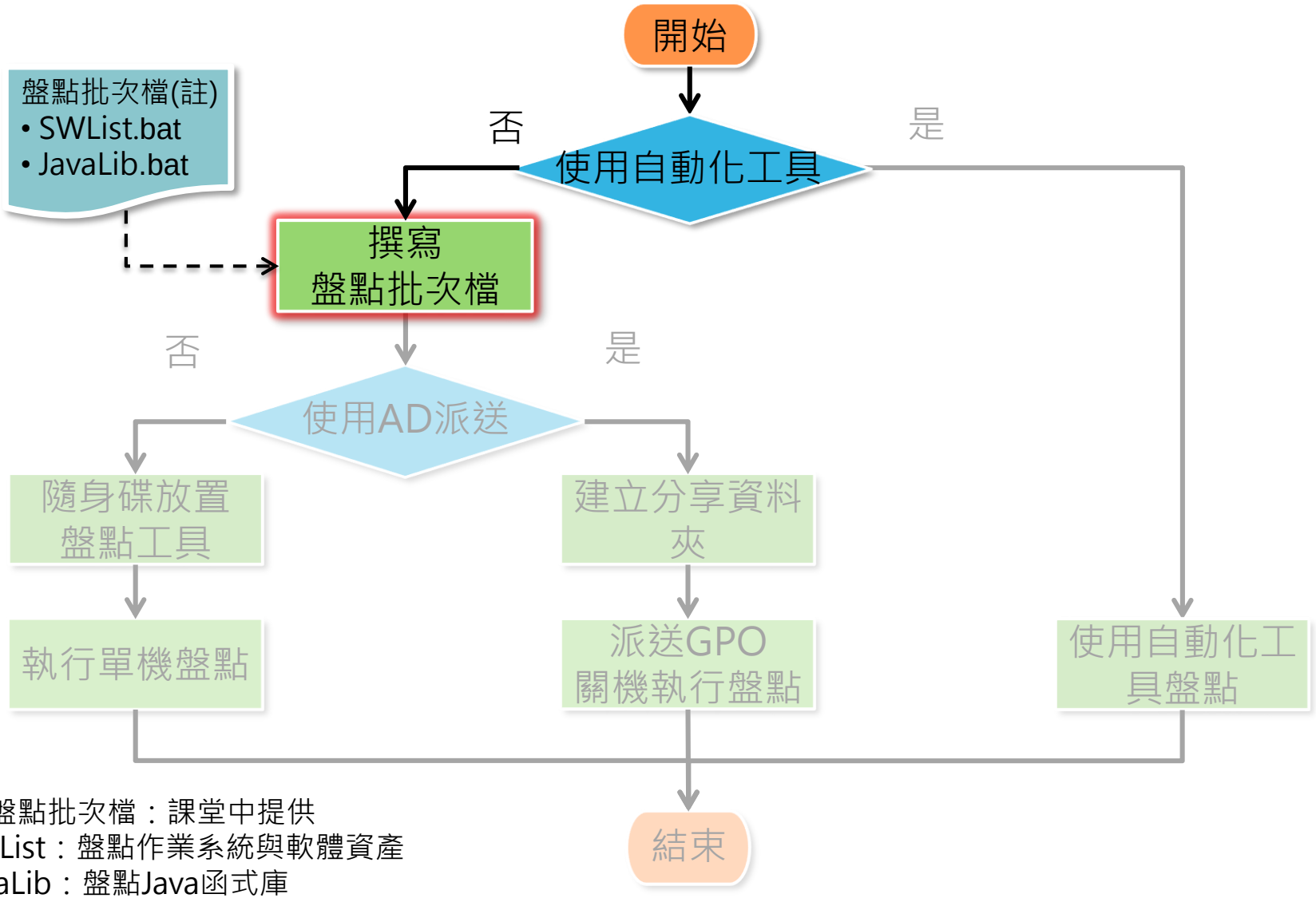

資訊資產與
已安裝KBID
盤點作業
資訊資產與
已安裝KBID
正規化作業
資訊資產與
已安裝KBID
登錄作業
弱點通知
與修補作業
資訊資產與
已安裝KBID
更新作業

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

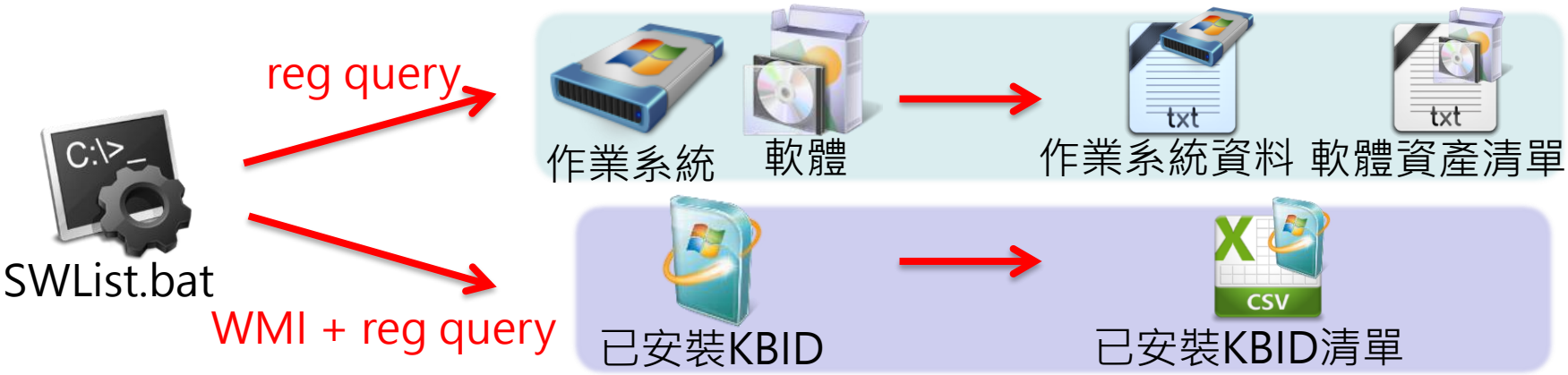
盤點作業流程



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)

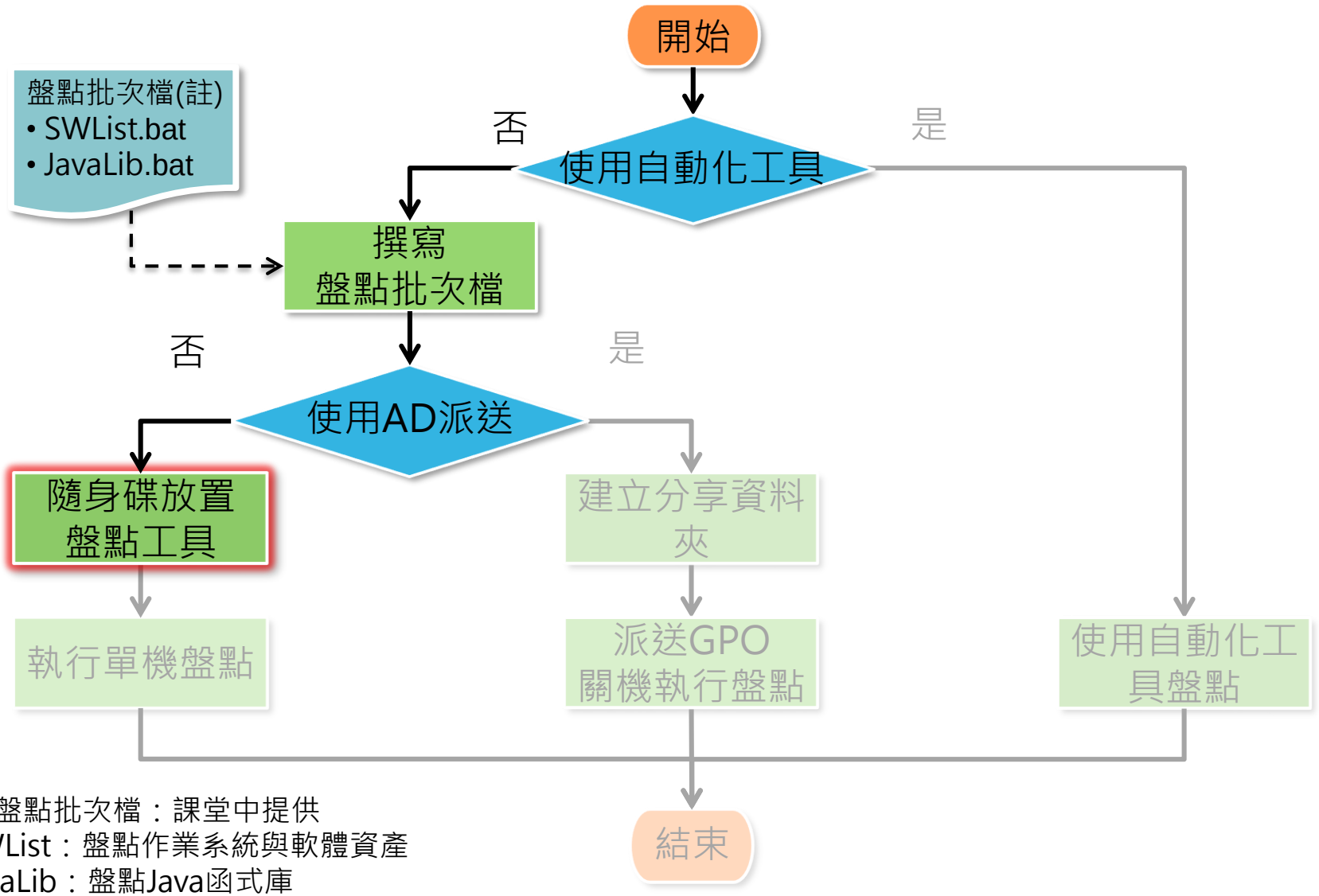
- 命令提示字元指令
  - 若機關環境有使用Java函式庫時，可透過此批次檔執行盤點
  - Tomcat Java函式庫路徑預設位置如下圖
    - cd C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\

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
```

透過系統指令單機盤點

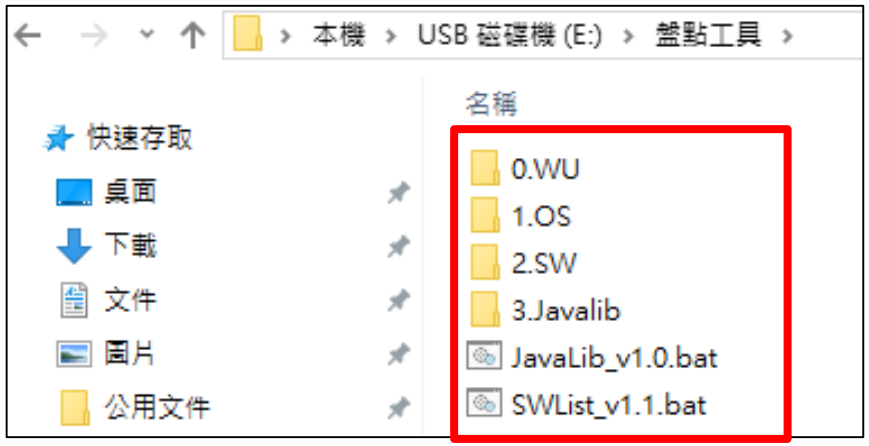
盤點作業流程



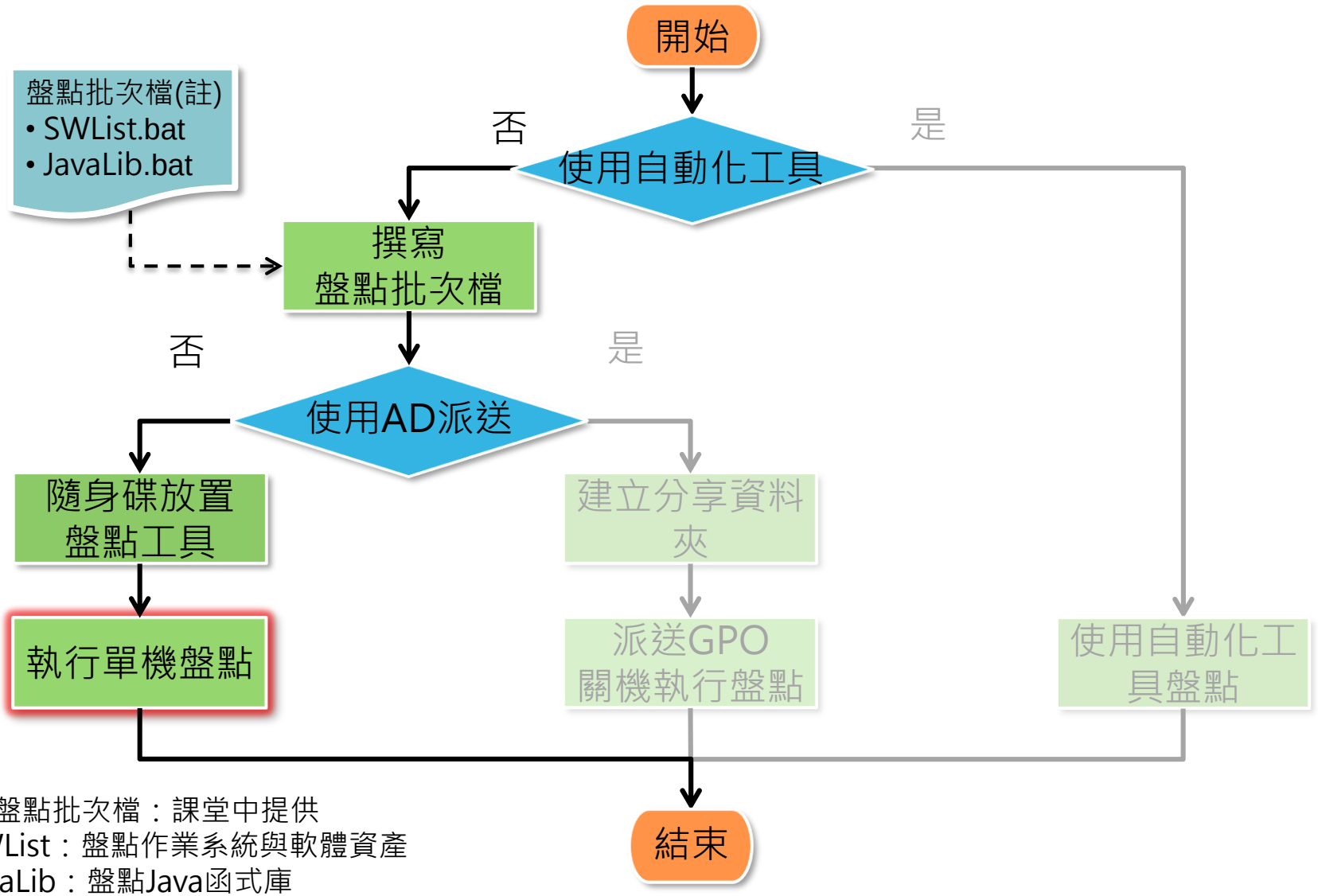
註：盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

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



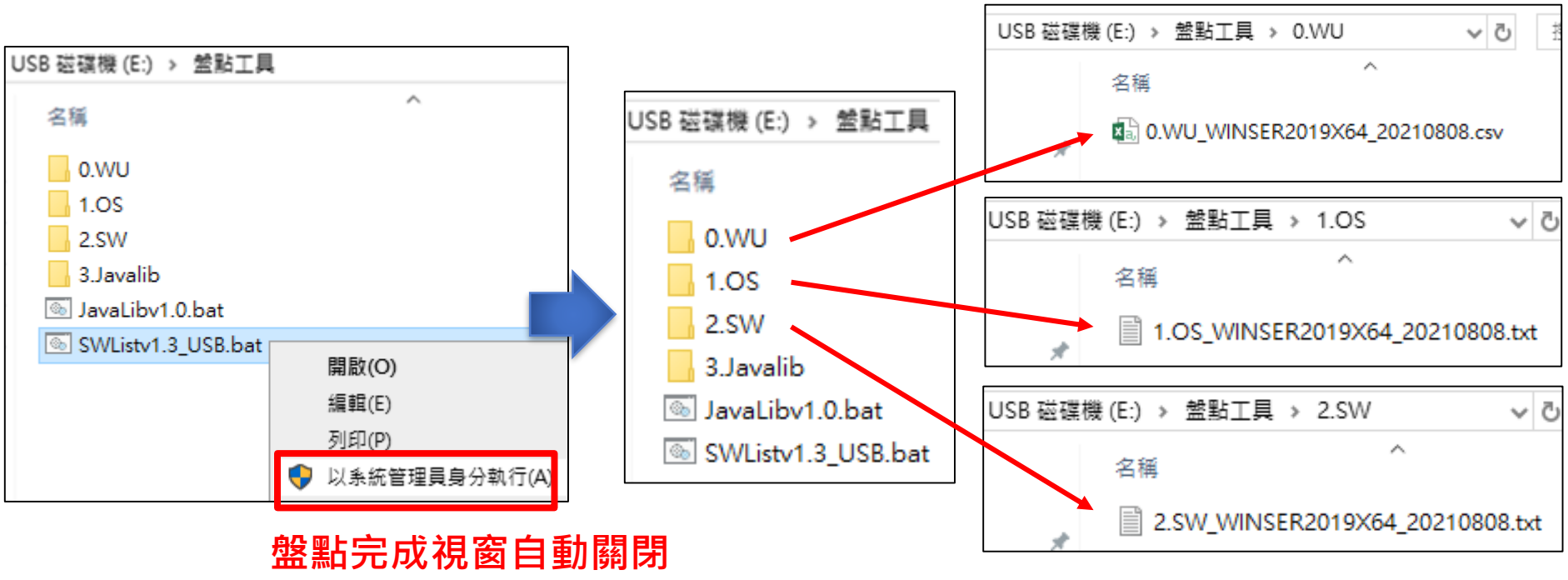
盤點作業流程



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

執行單機盤點(1/2)

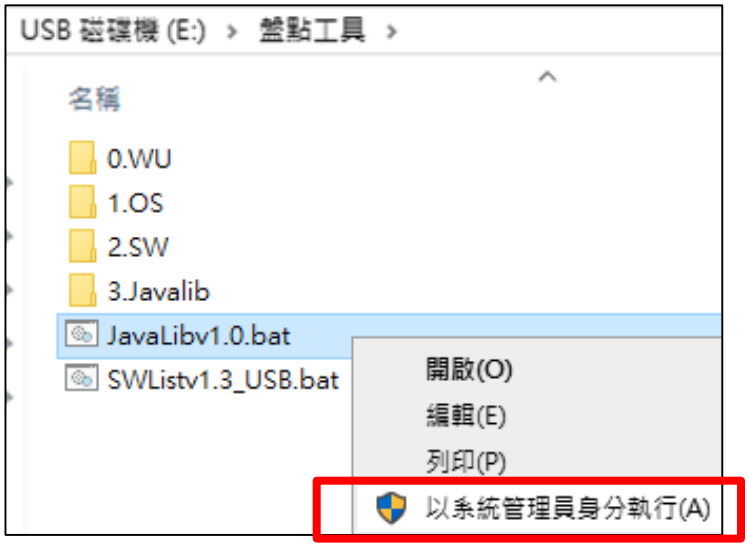
- STEP1：以系統管理員身分執行SWList批次檔
- STEP2：檢視盤點結果資料夾，分別為已安裝KBID清單、作業系統資訊及軟體盤點清單

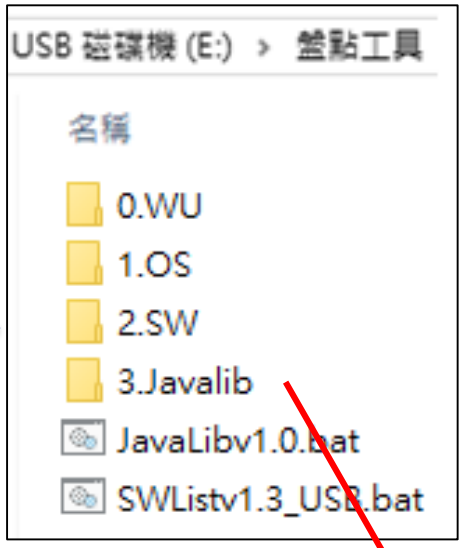


盤點完成視窗自動關閉

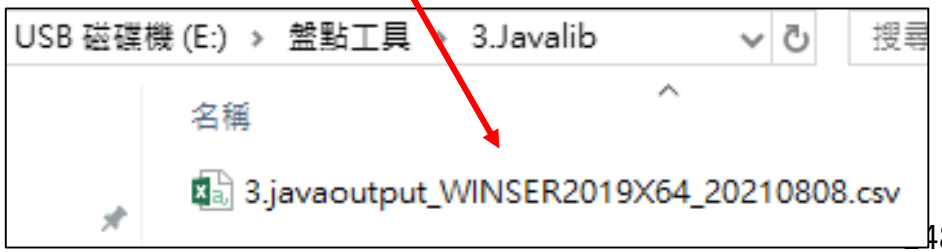
執行單機盤點(2/2)

- 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



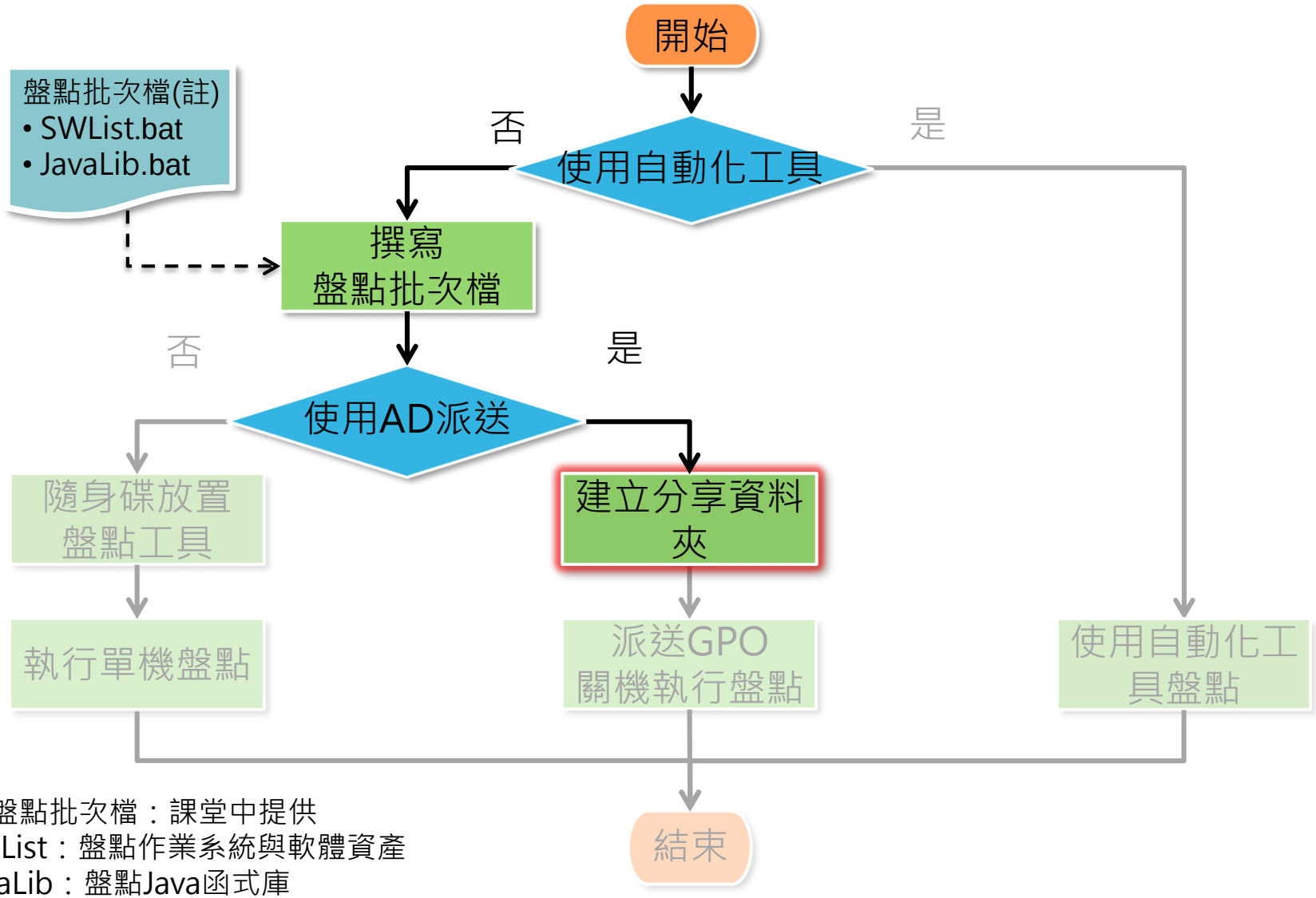


盤點完成視窗自動關閉



透過系統指令批次盤點

盤點作業流程



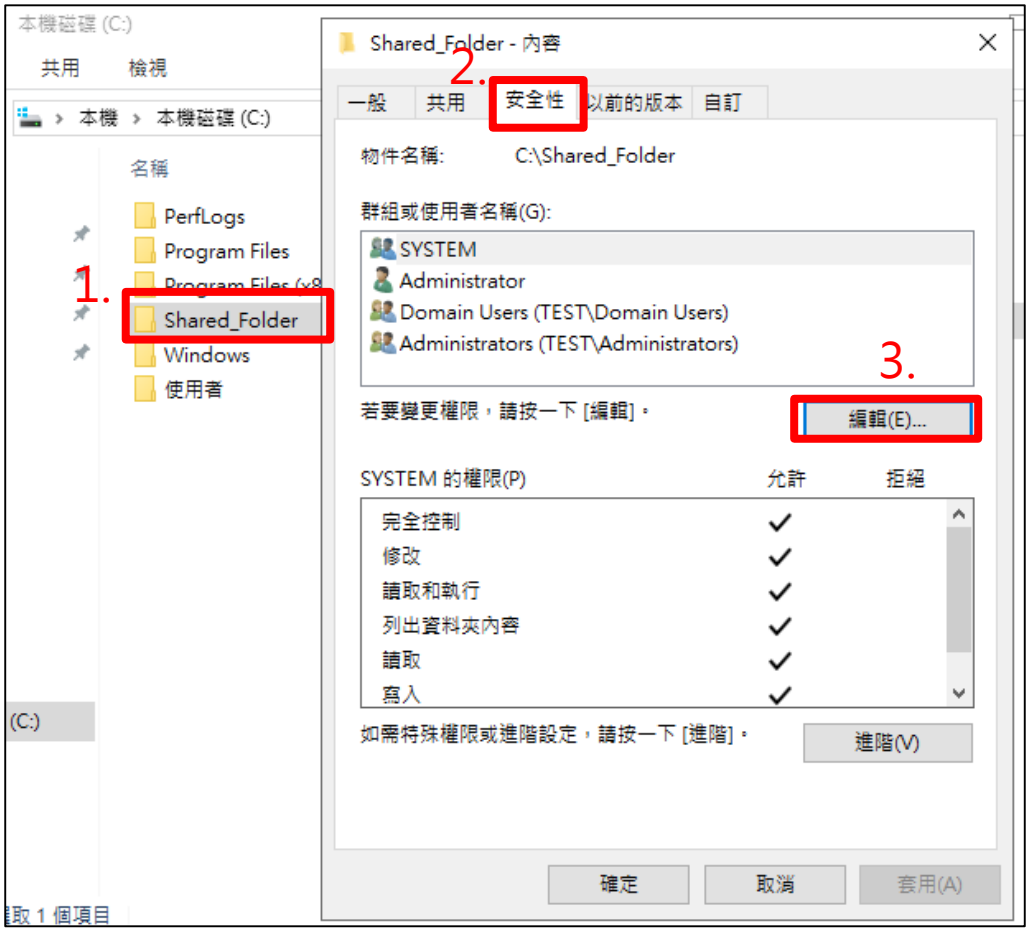
註：盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

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

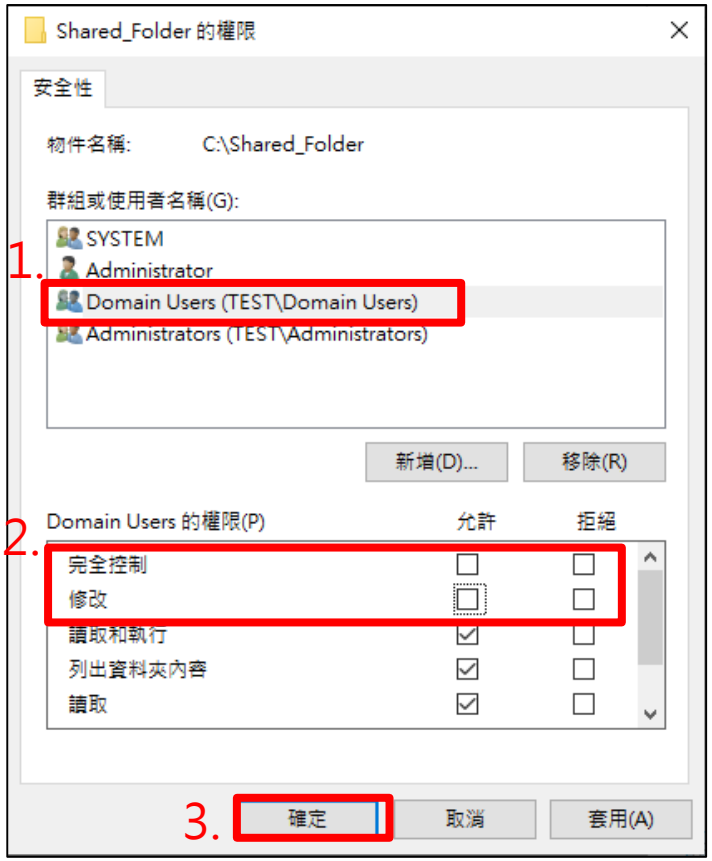
AD主機建立分享資料夾(2/3)

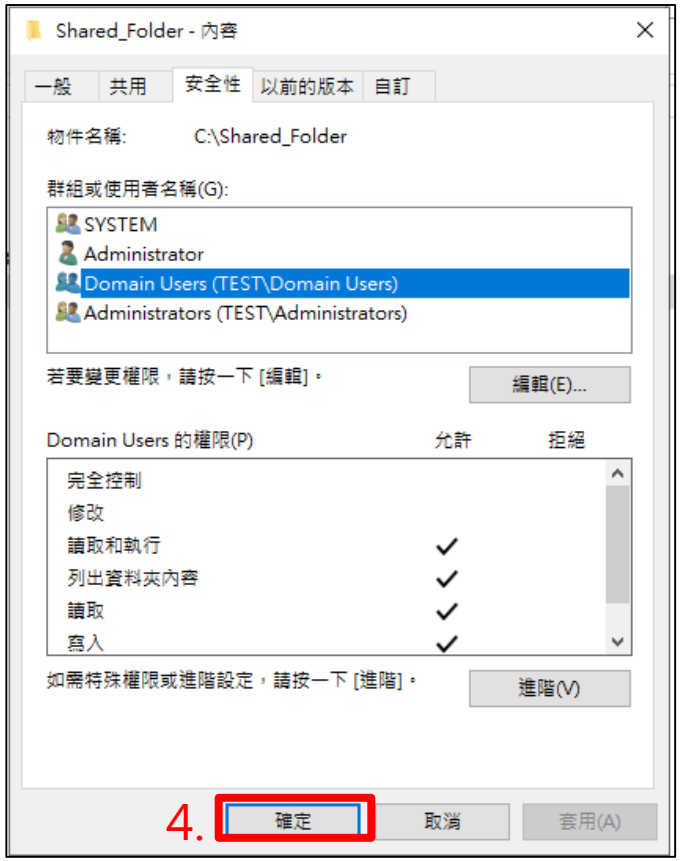
- STEP3：避免網域使用者誤刪檔案，需限縮其存取權限，切換至安全性頁籤，並點選編輯



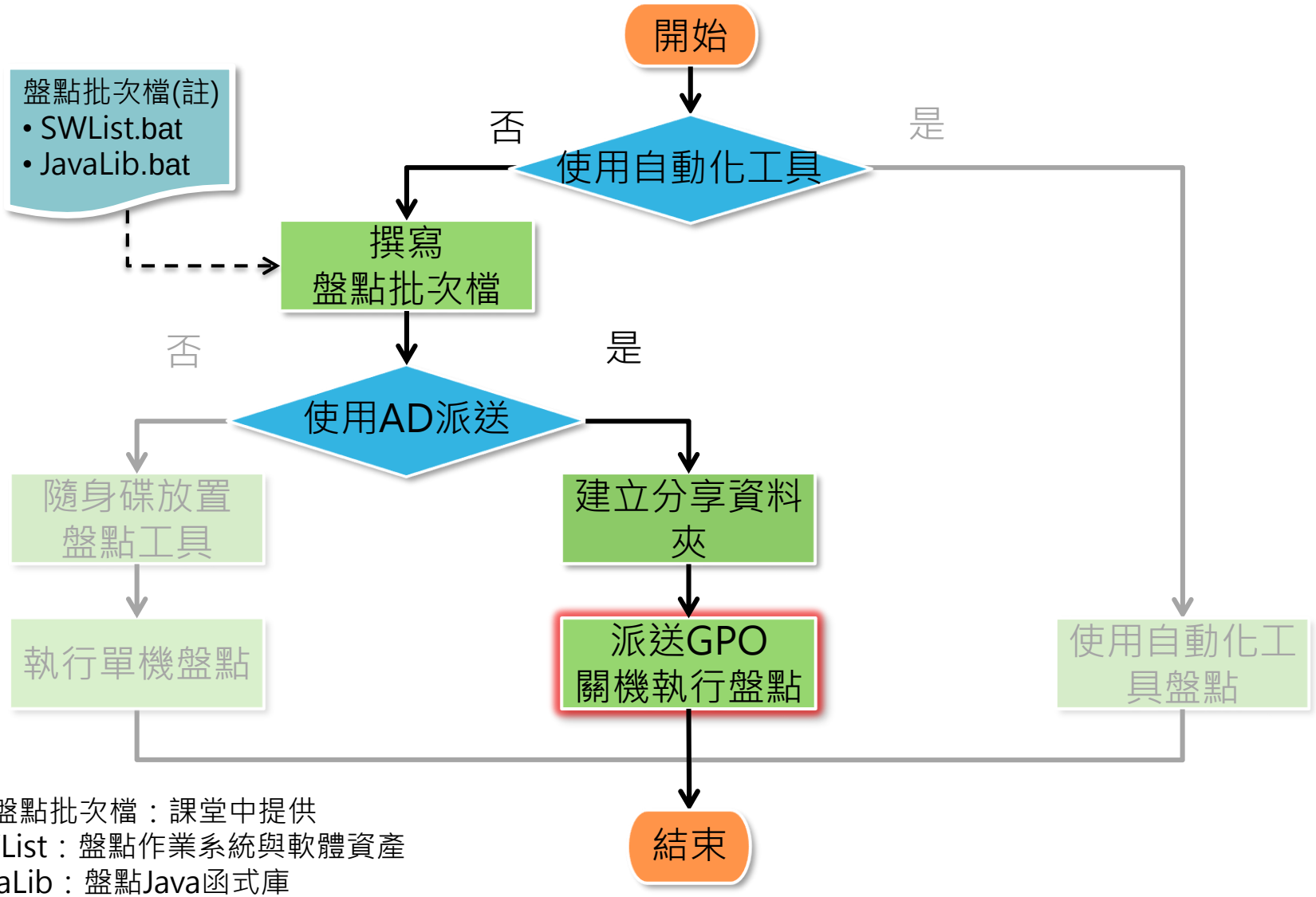
AD主機建立分享資料夾(3/3)

- 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



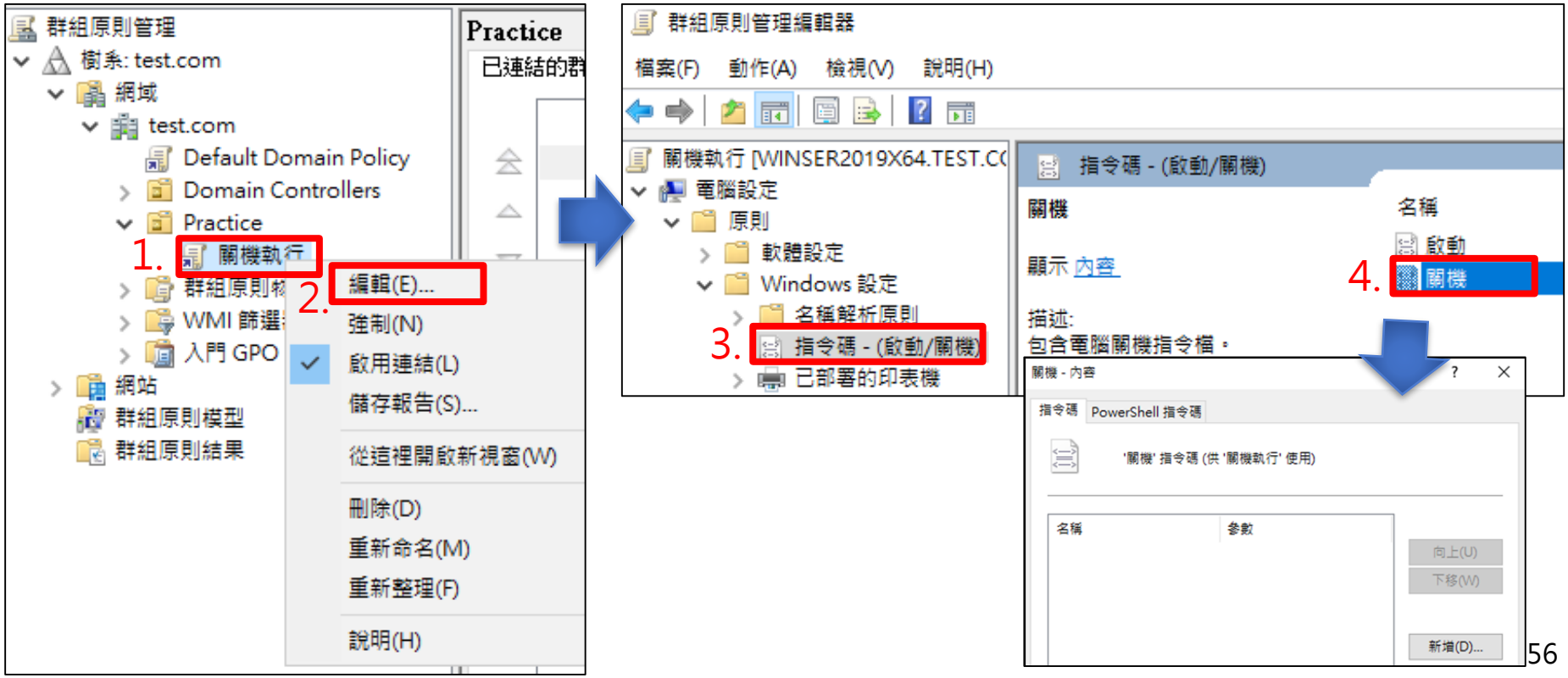
註：盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

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

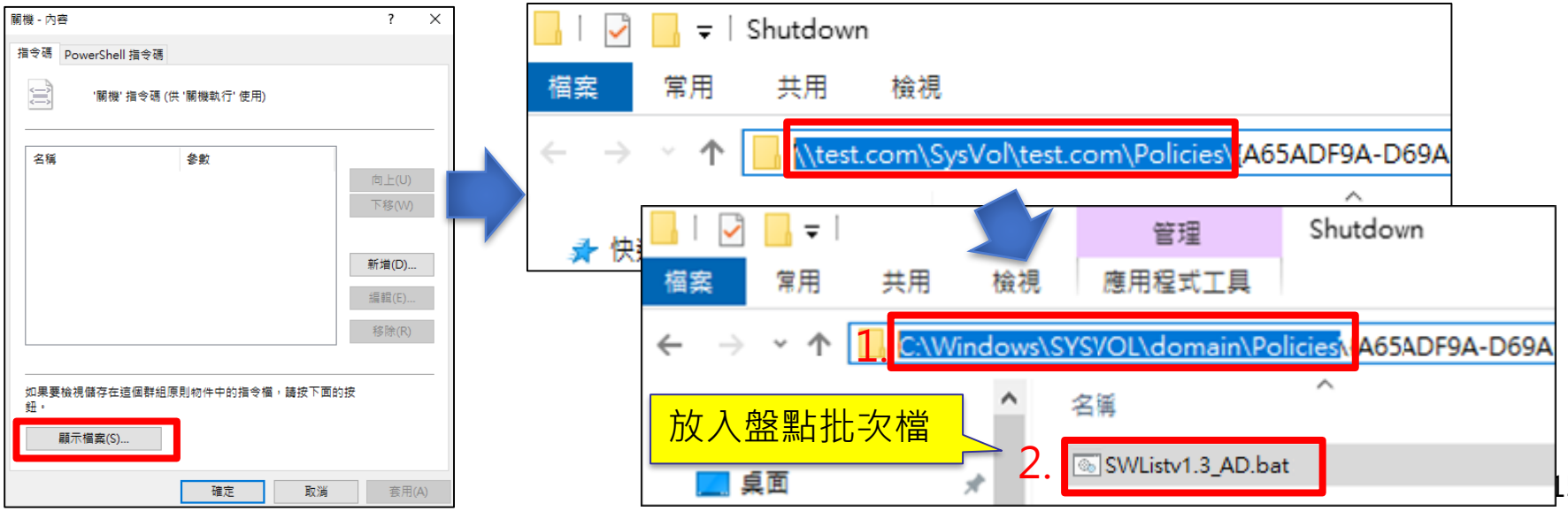
派送GPO-關機執行(2/5)

- 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」



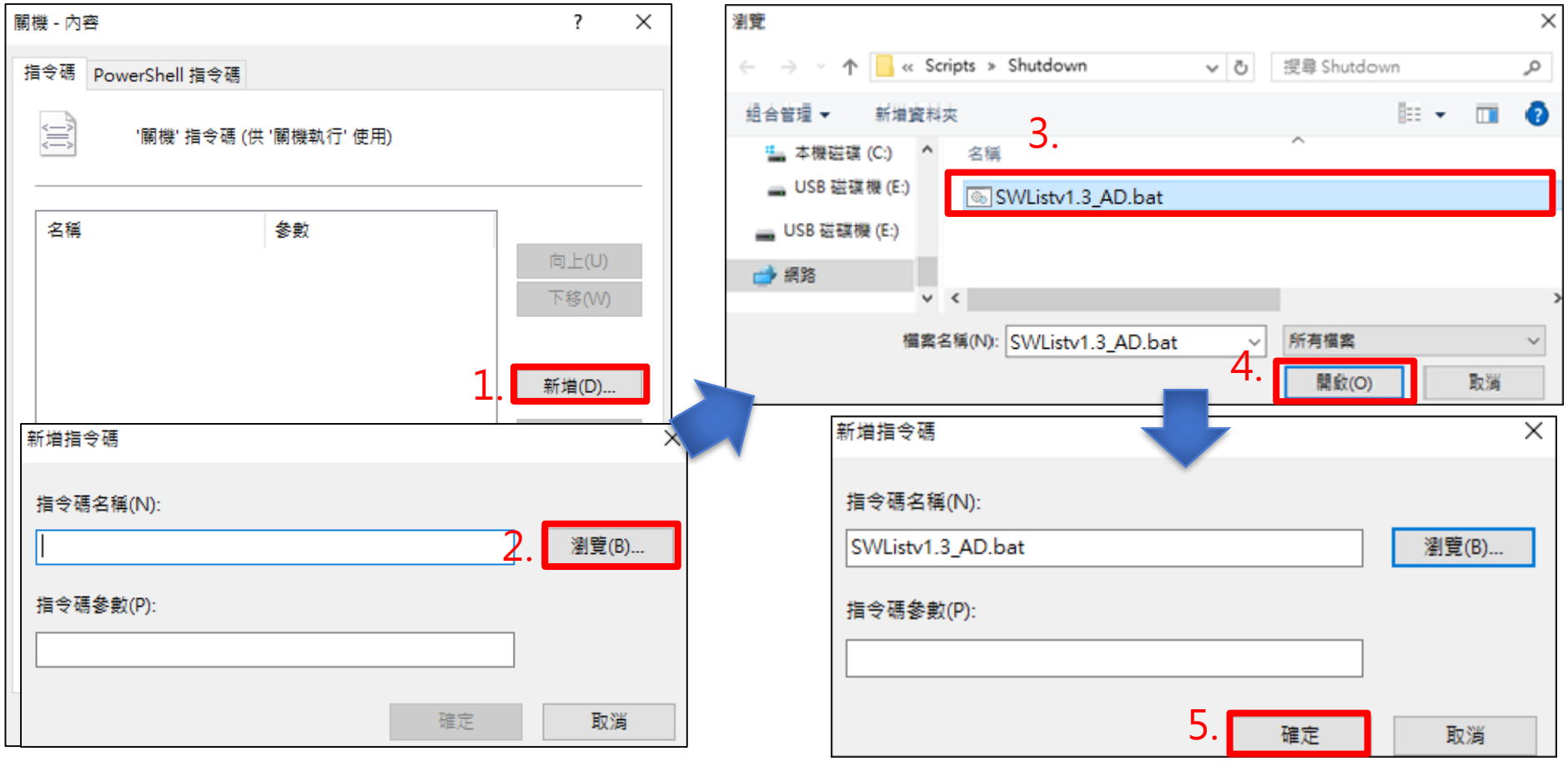
派送GPO-關機執行(3/5)

- 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 」



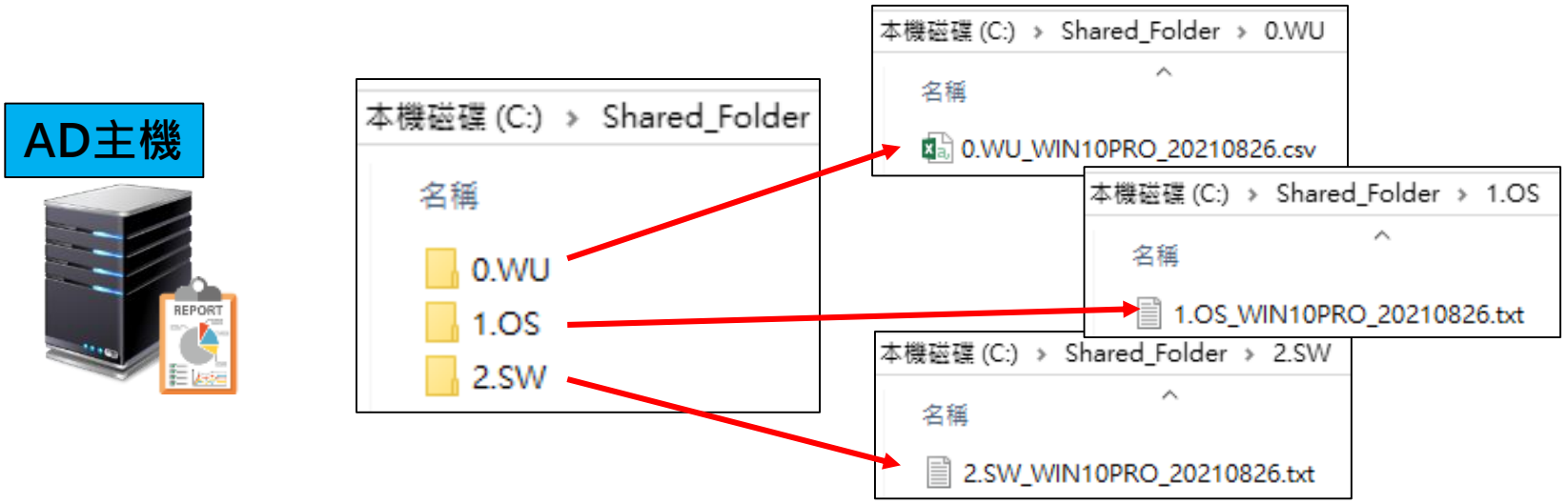
派送GPO-關機執行(4/5)

- 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



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



導入作業流程

資訊資產與
已安裝KBID
更新作業

資訊資產與
已安裝KBID
盤點作業

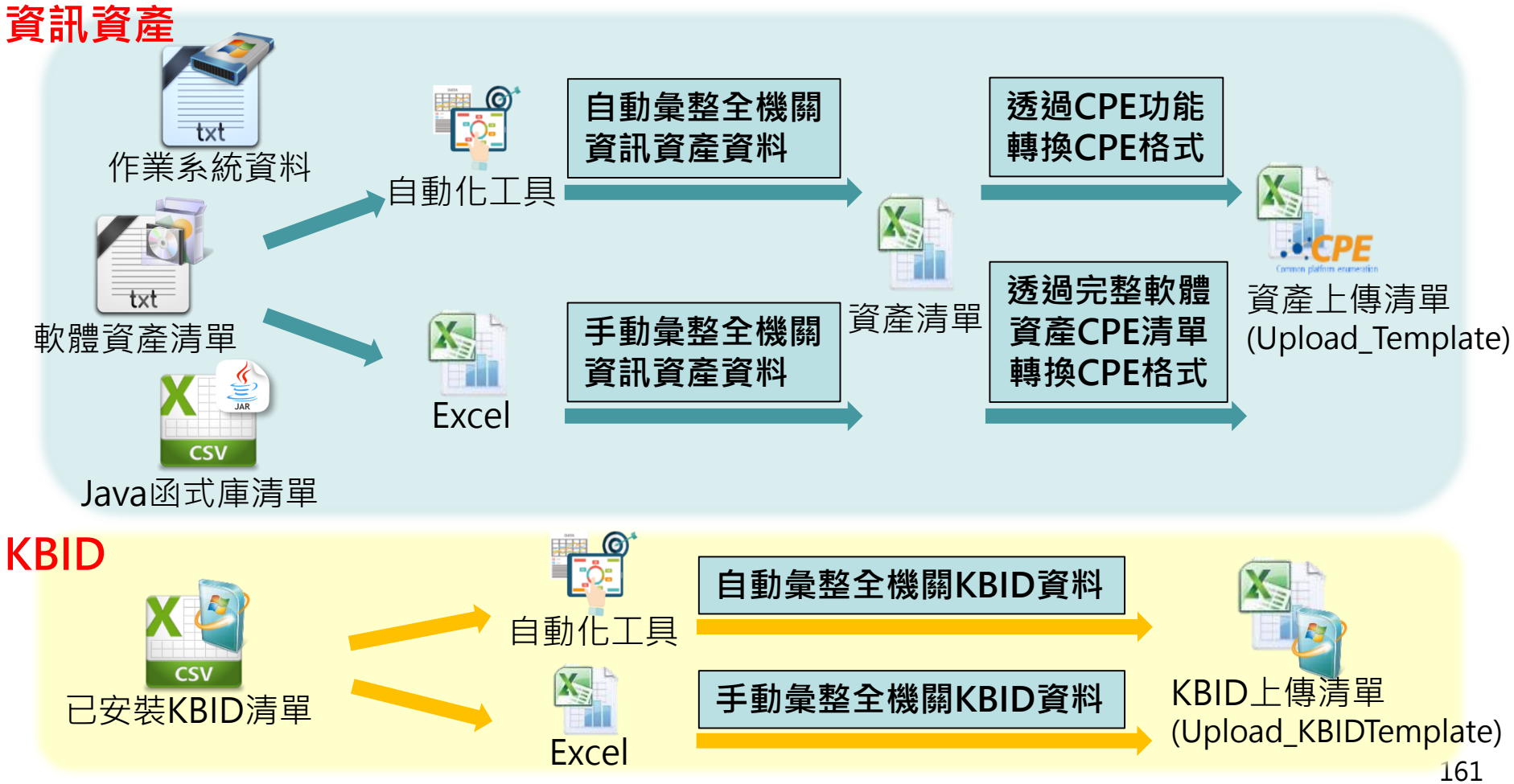
資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

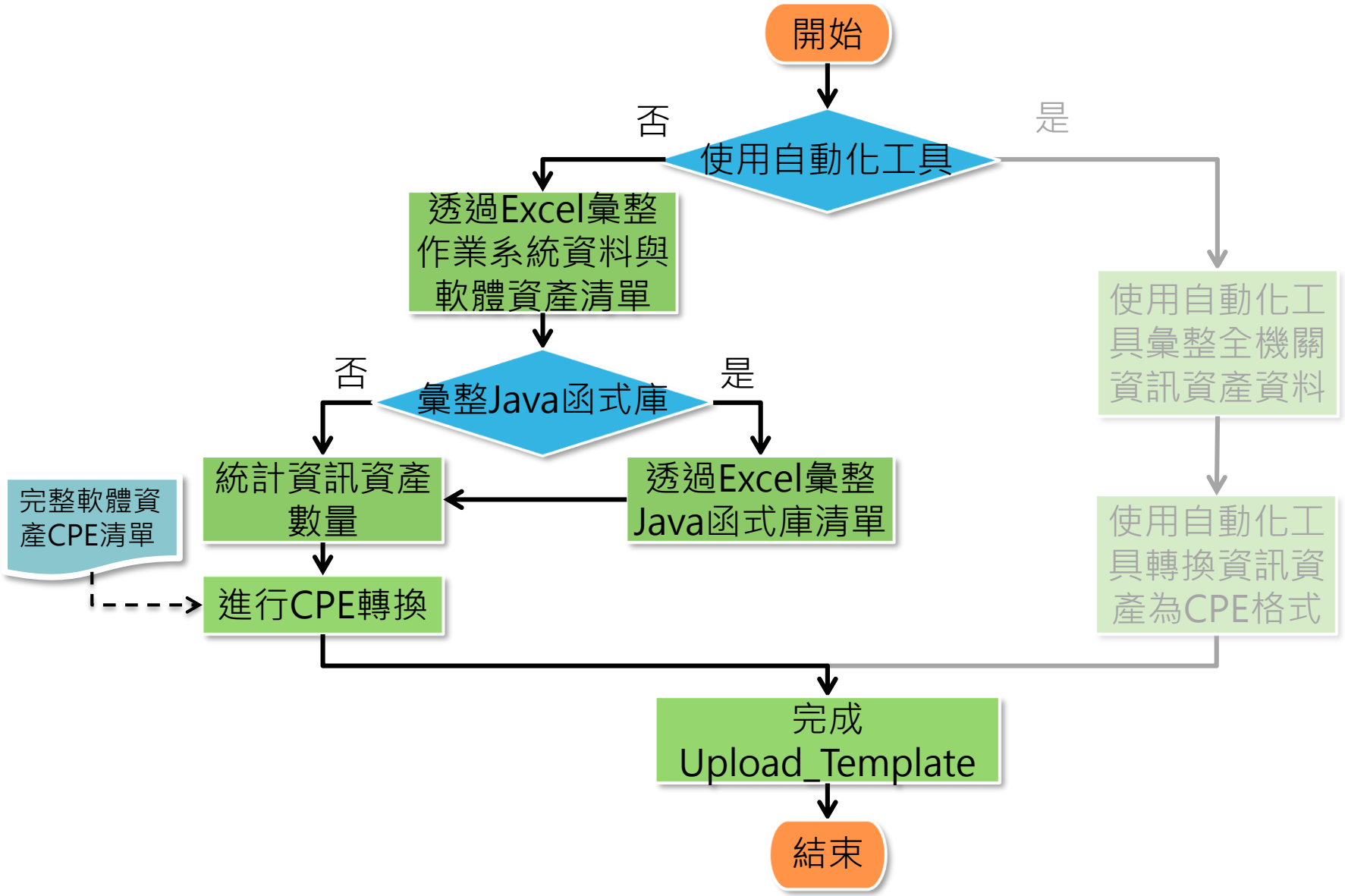
資訊資產與已安裝KBID正規化

- 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

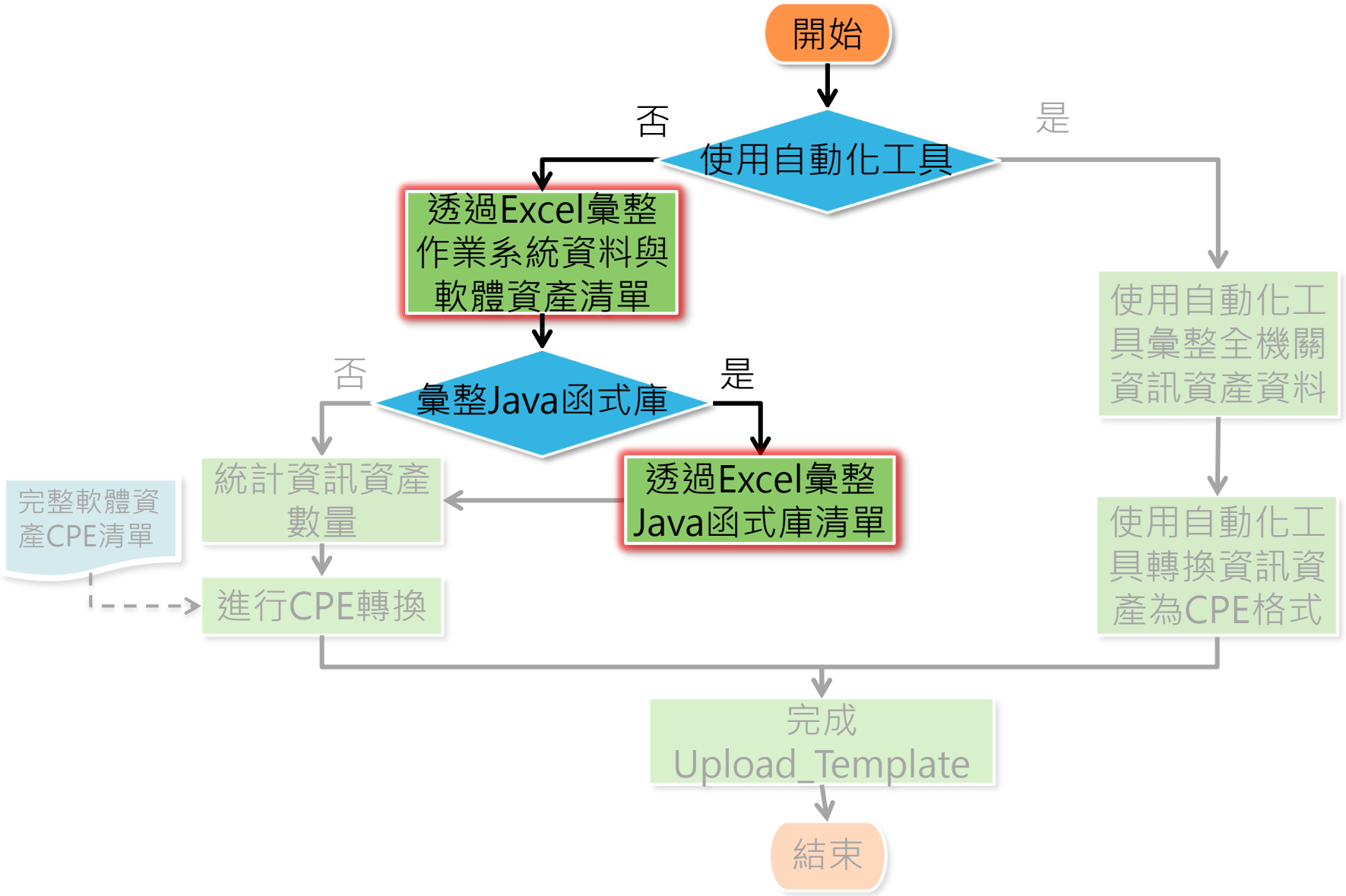


資訊資產正規化作業

資訊資產正規化作業流程



資訊資產正規化作業流程

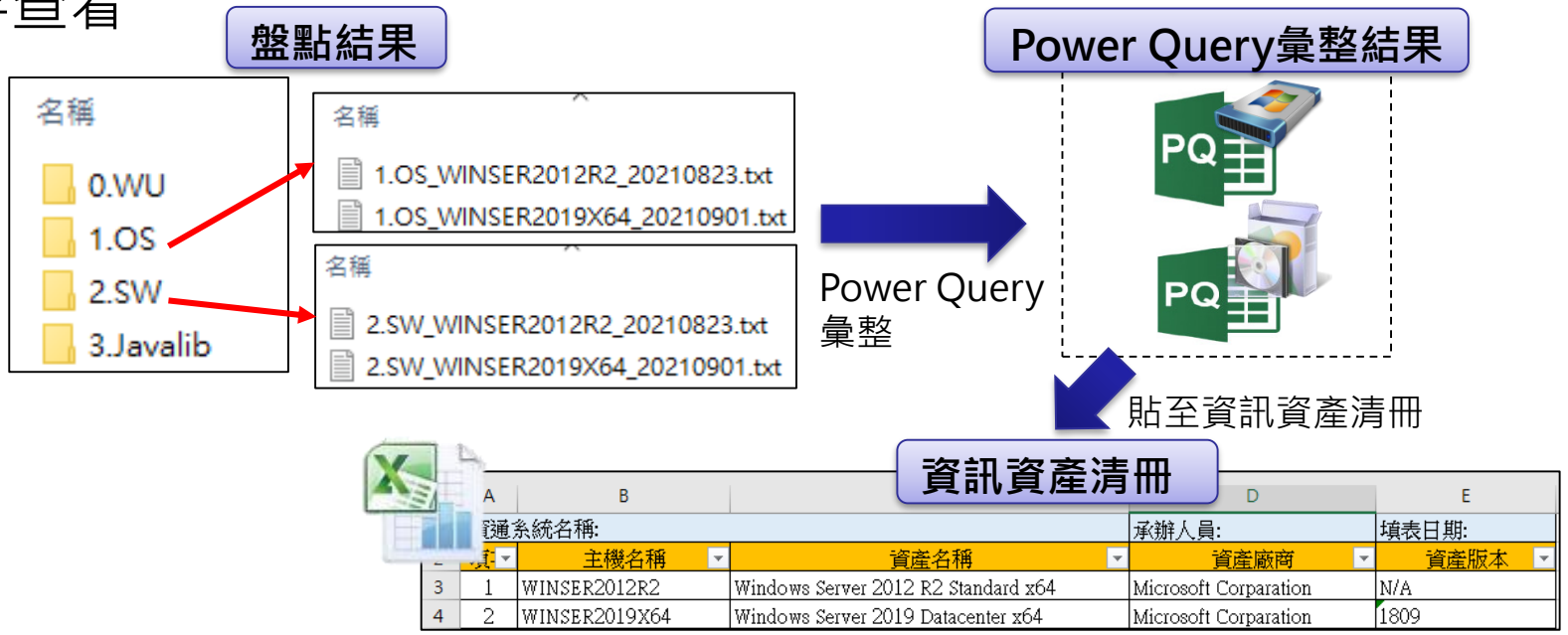


Excel彙整功能介紹

- 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

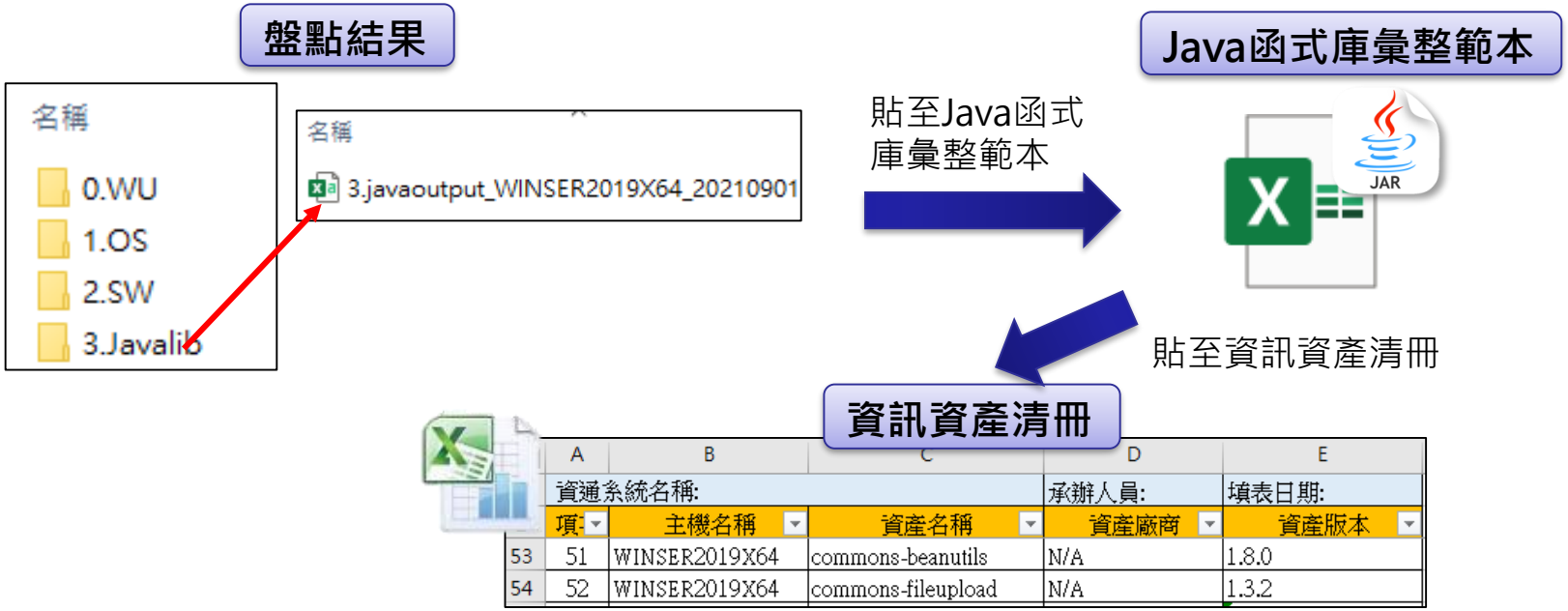
- 透過Power Query分別彙整歸類後作業系統與軟體資產之盤點結果
  - 若欲了解彙整步驟，請參閱「資通安全弱點通報系統操作手冊*」v1.8或更新版本
- 將作業系統與軟體資產彙整結果，整合至資訊資產清冊*，以留存查看



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

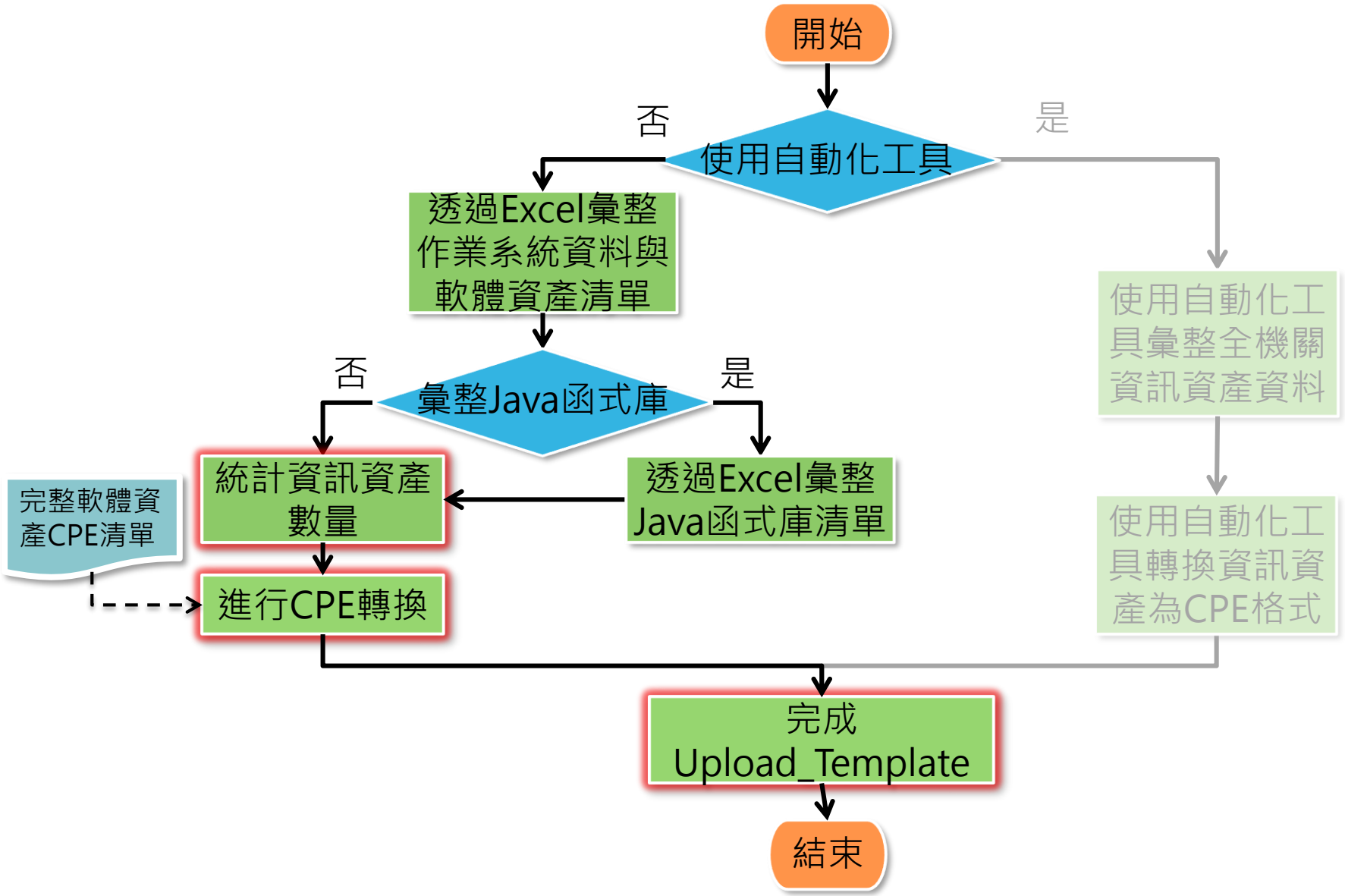
彙整資訊資產清單_Java函式庫

- 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



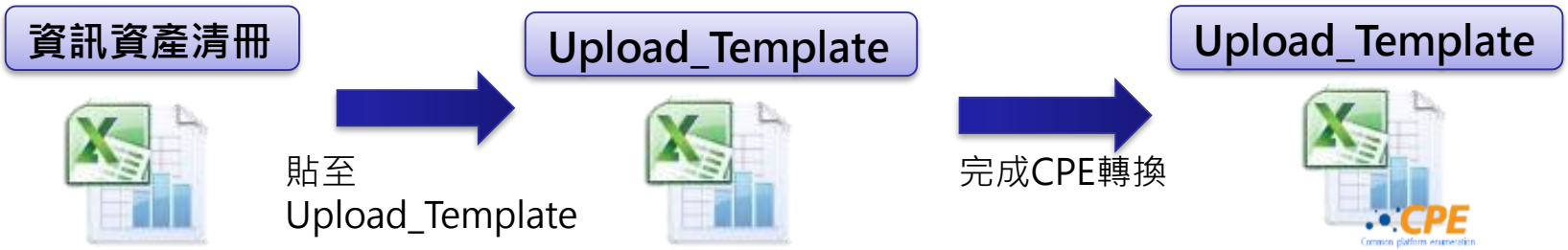
註： Java函式庫彙整範本：課堂中提供

資訊資產正規化作業流程



完成Upload_Template

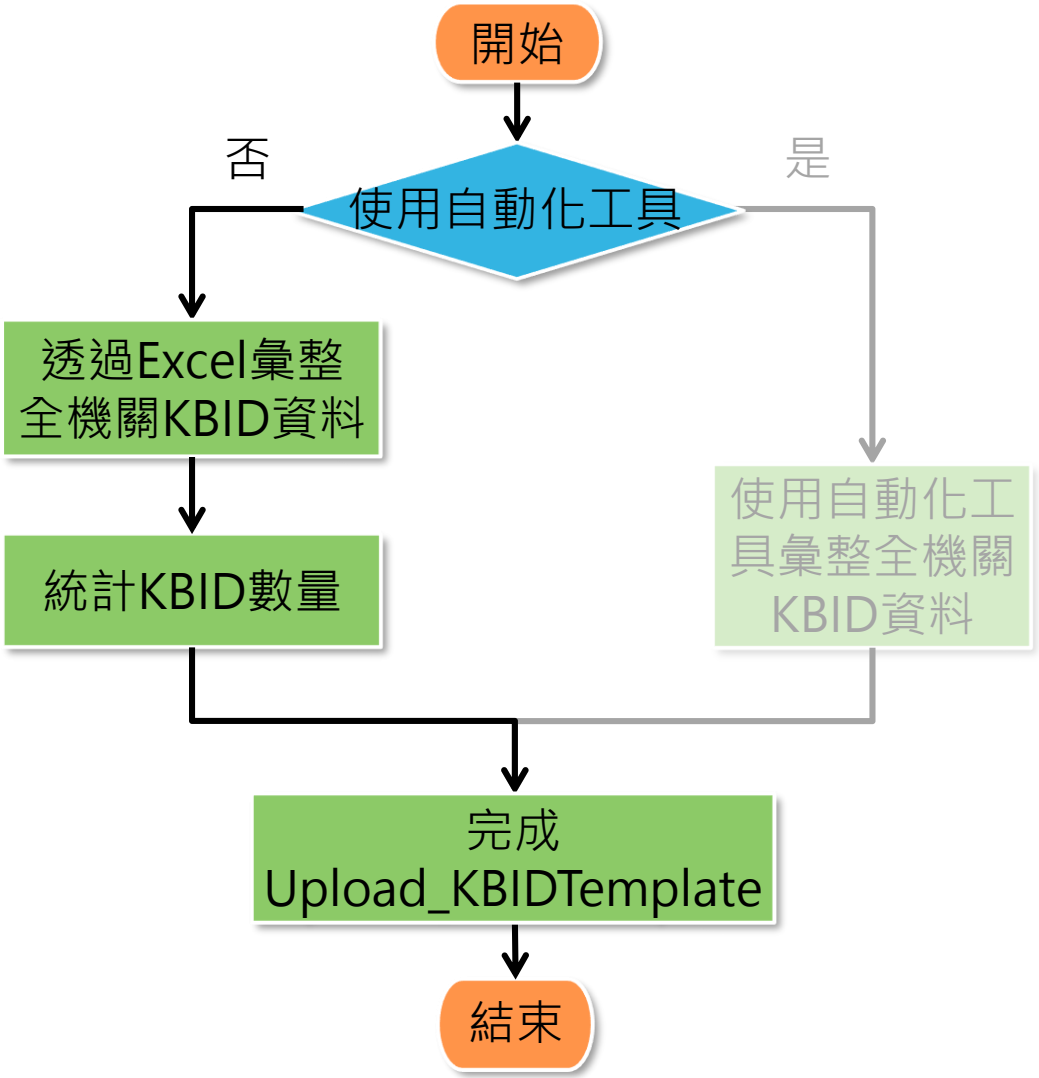
- 統計資訊資產數量
  - 資訊資產清冊自動計算資產數量
  - 利用移除重複項功能，以避免上傳相同之資訊資產
- 進行CPE轉換
  - 將資訊資產清冊彙整至Upload_Template(註)
  - 於完整軟體資產CPE清單*搜尋，並於Upload_Template填入資訊資產對應之CPE格式，若無則填入N/A
- 完成Upload_Template
  - 填寫機關OID與機關名稱



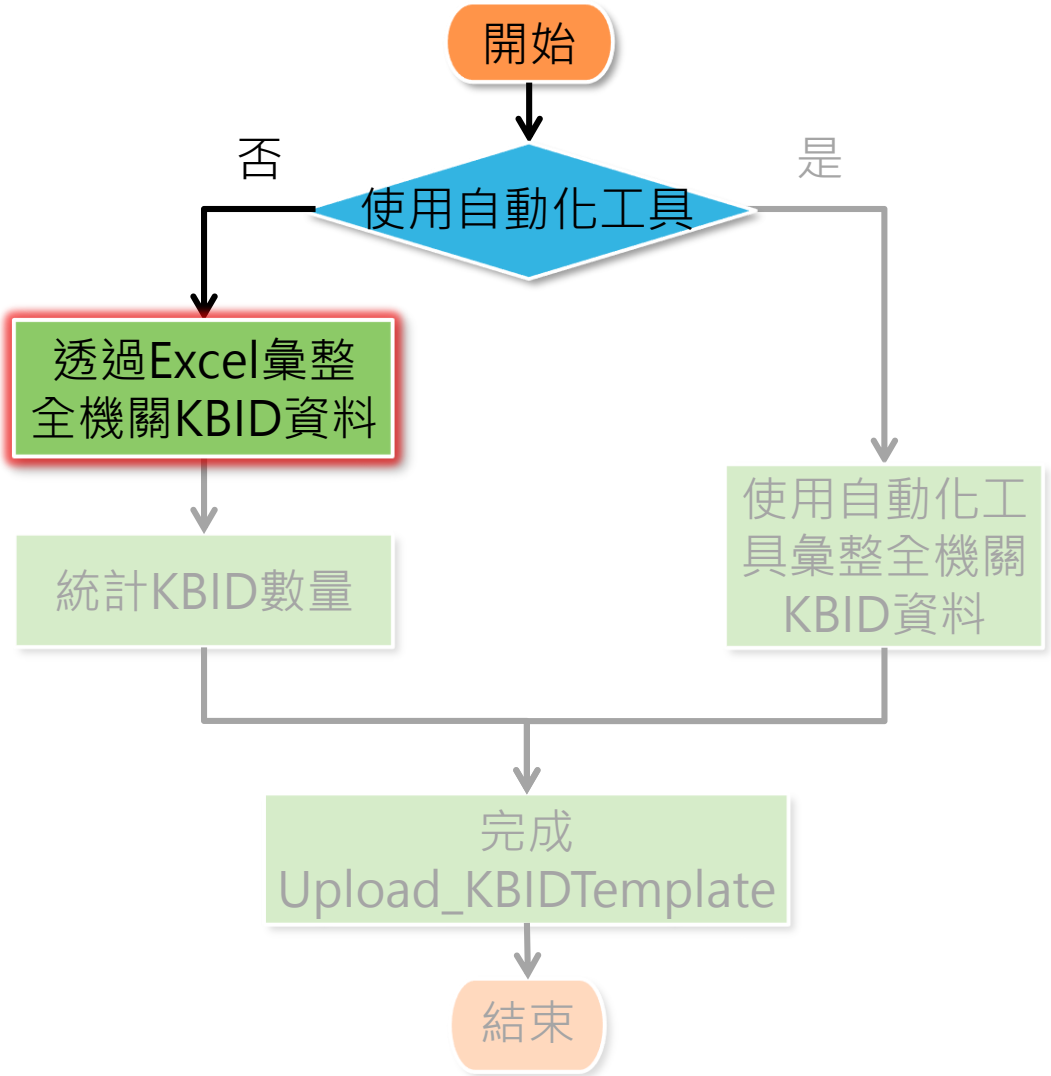
註：於VANS系統下載

已安裝KBID正規化作業

已安裝KBID正規化作業流程

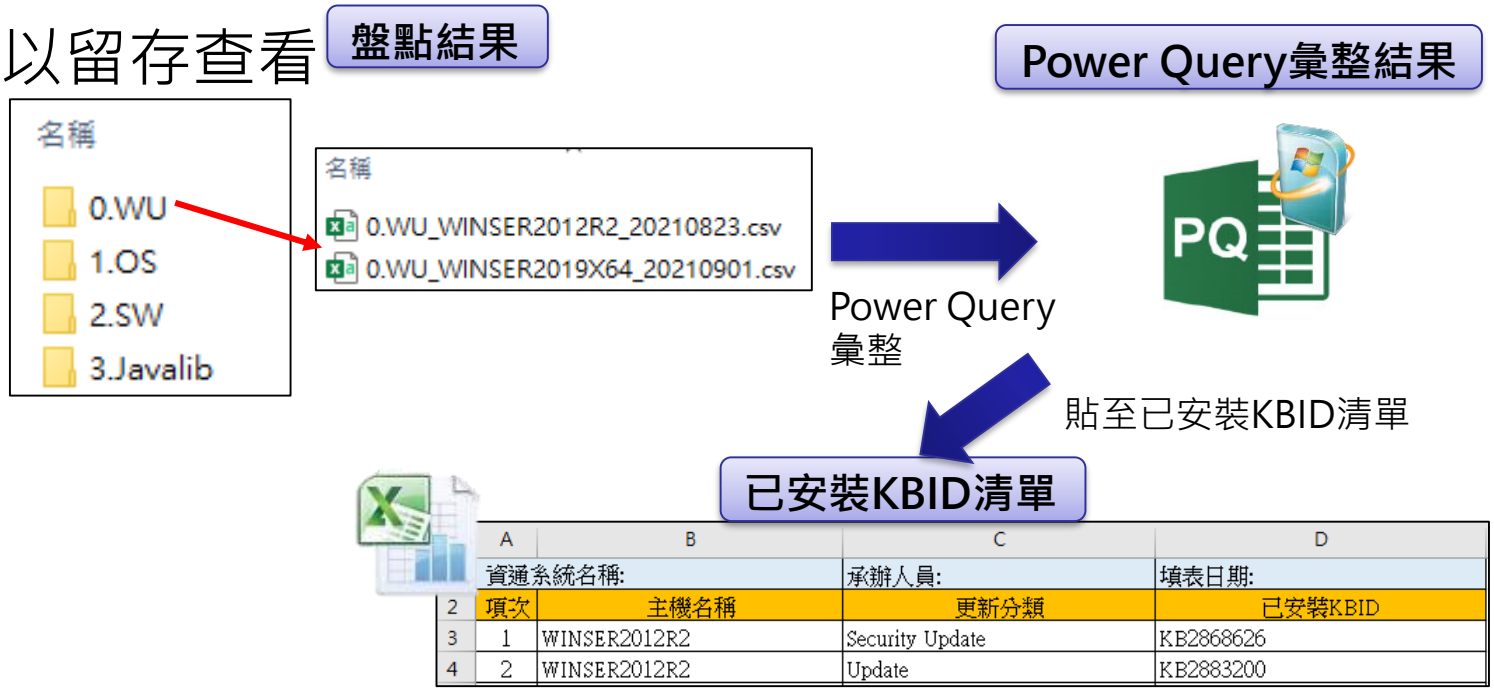


已安裝KBID正規化作業流程



彙整KBID清單

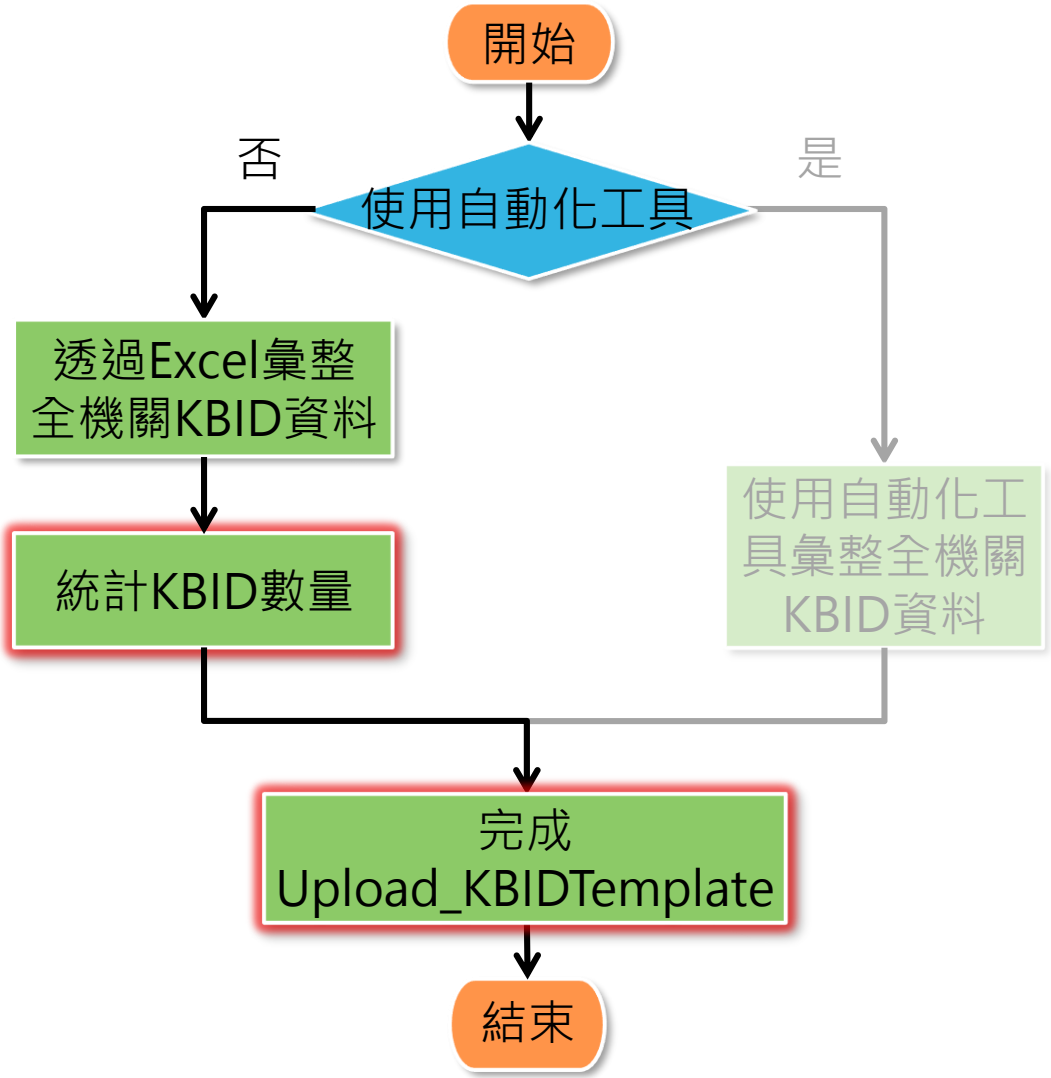
- 透過Power Query彙整歸類後已安裝KBID之盤點結果
  - 若欲了解彙整步驟，請參閱「資通安全弱點通報系統操作手冊(註1)」v1.9或更新版本
- 將已安裝KBID彙整結果，整合至已安裝KBID清單(註2)，以留存查看



	A	B	C	D
	資通系統名稱:		承辦人員:	填表日期:
2	項次	主機名稱	更新分類	已安裝KBID
3	1	WINSER2012R2	Security Update	KB2868626
4	2	WINSER2012R2	Update	KB2883200

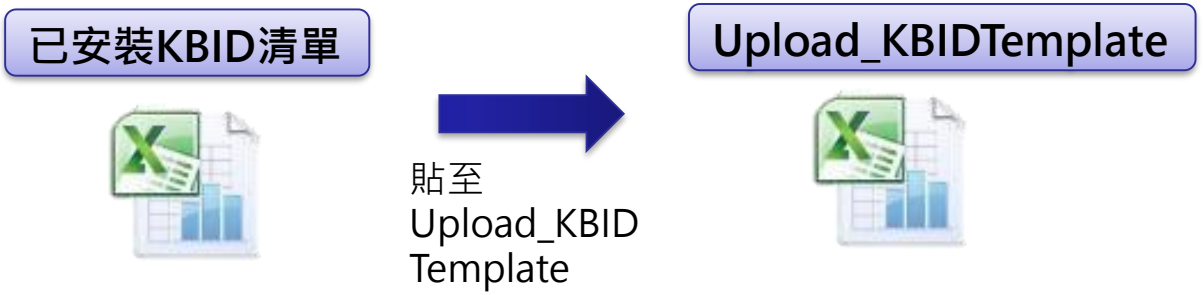
註1：操作手冊：機關管理者帳號開通之通知信提供或透過VansService服務信箱索取
註2：已安裝KBID清單：課堂中提供

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

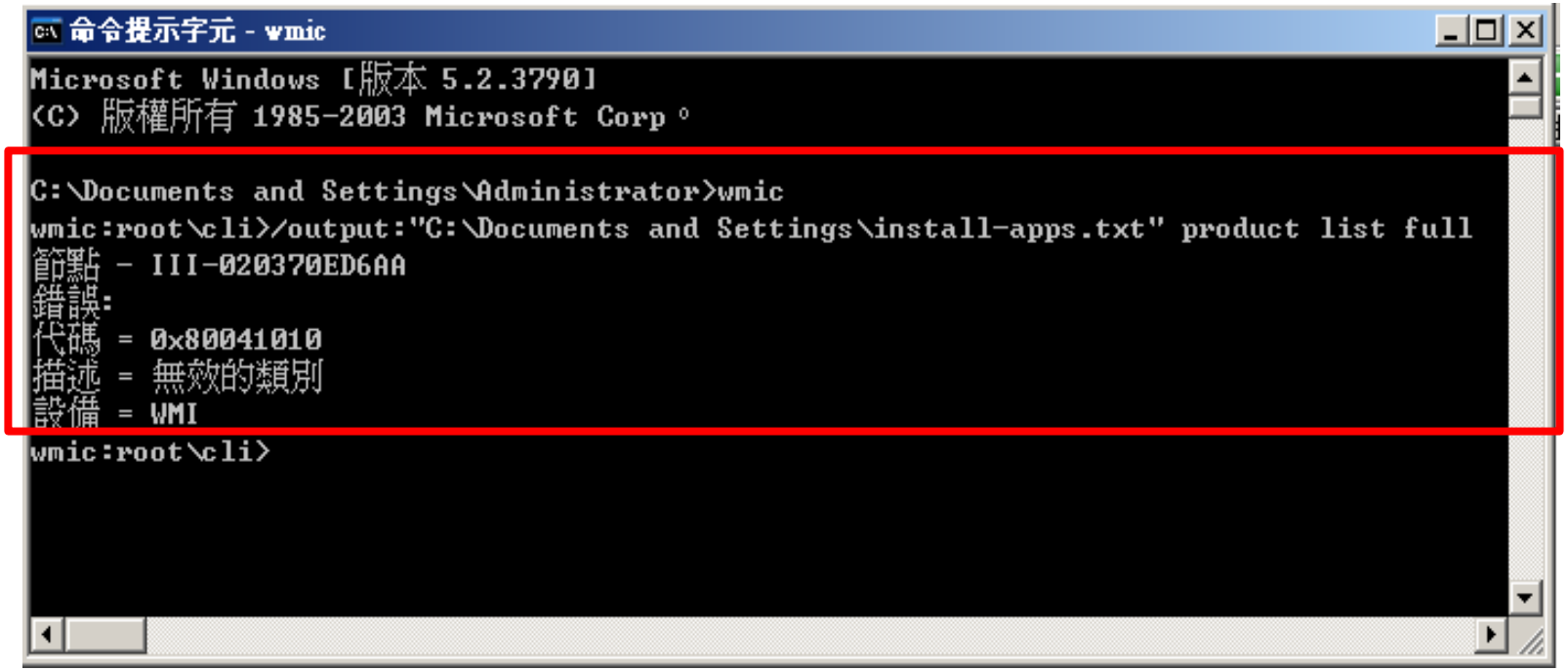


註：Upload_KBIDTemplate：於VANS系統下載

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

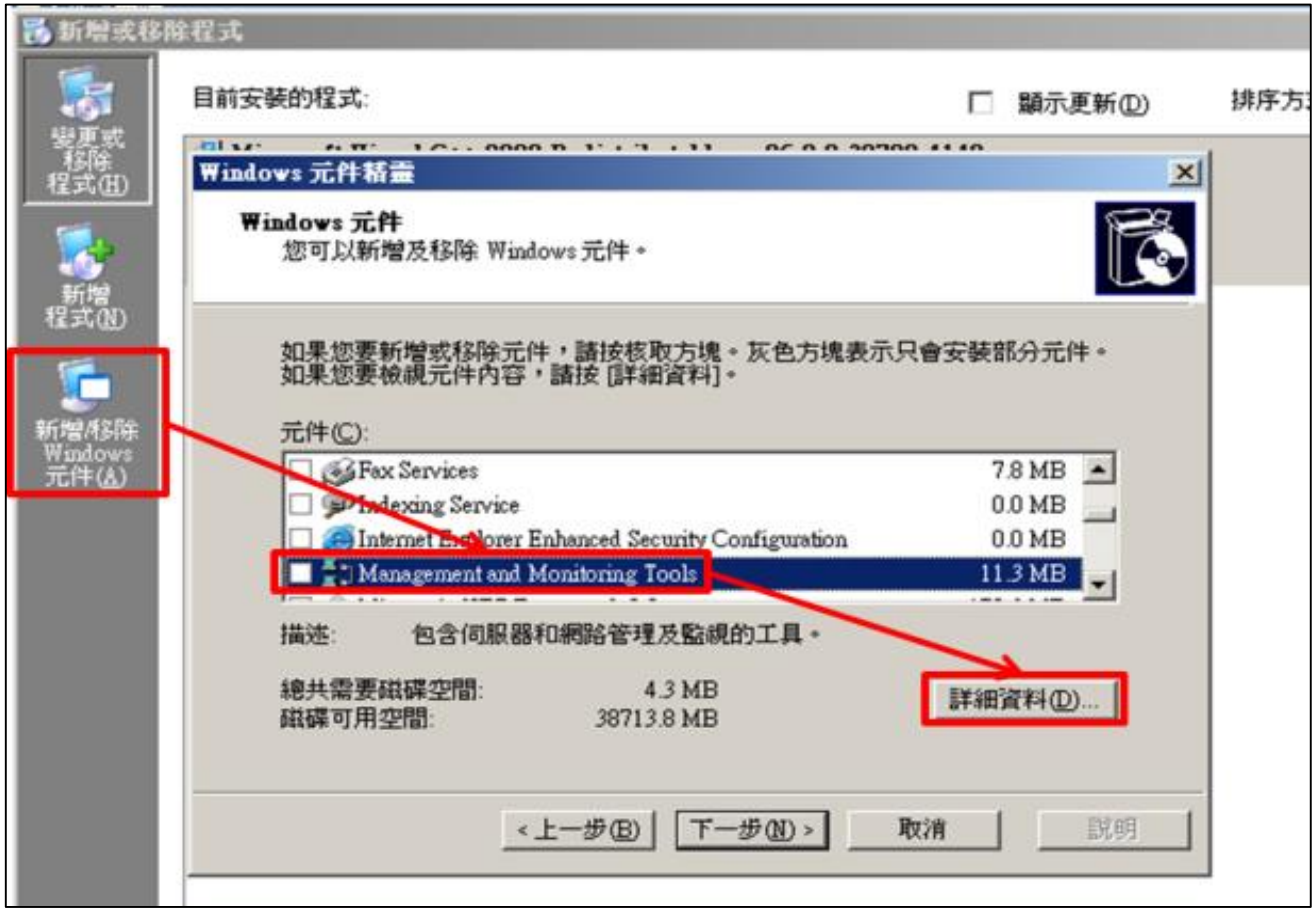


安裝WMI Windows Installer(2/7)

- 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」

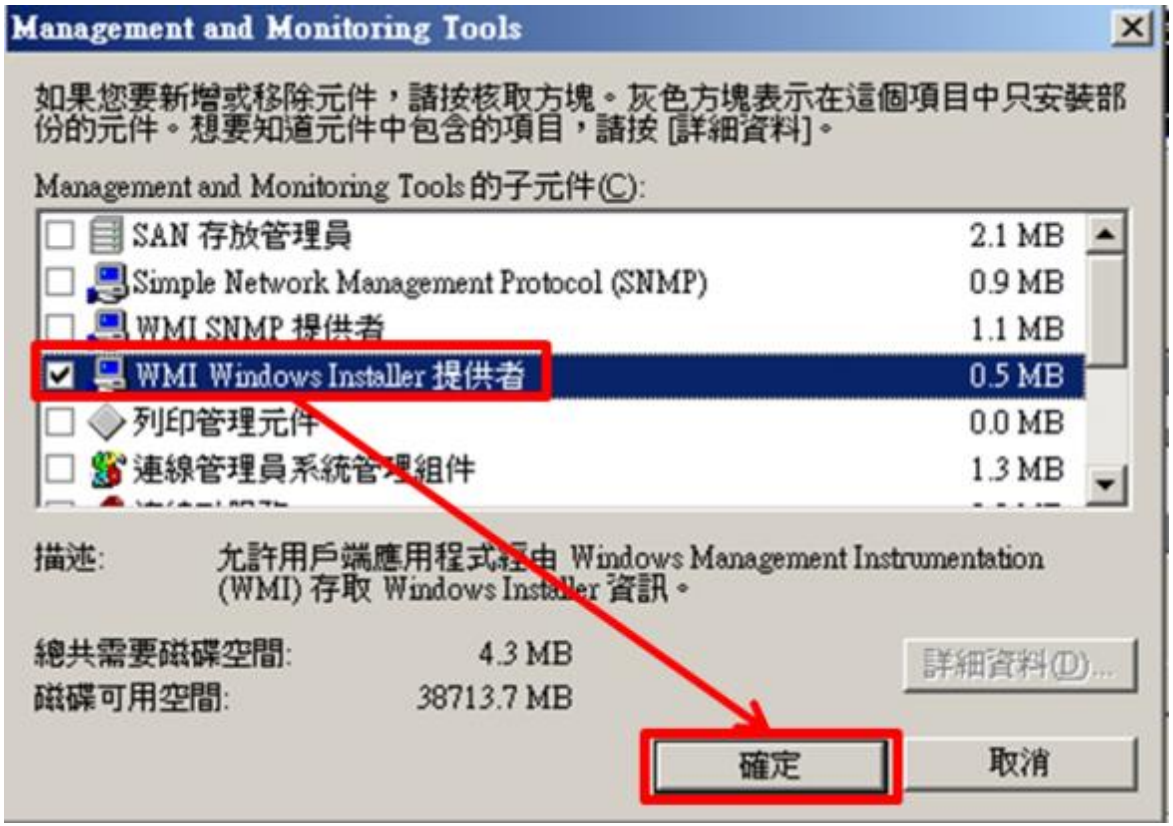
安裝WMI Windows Installer(3/7)

- 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



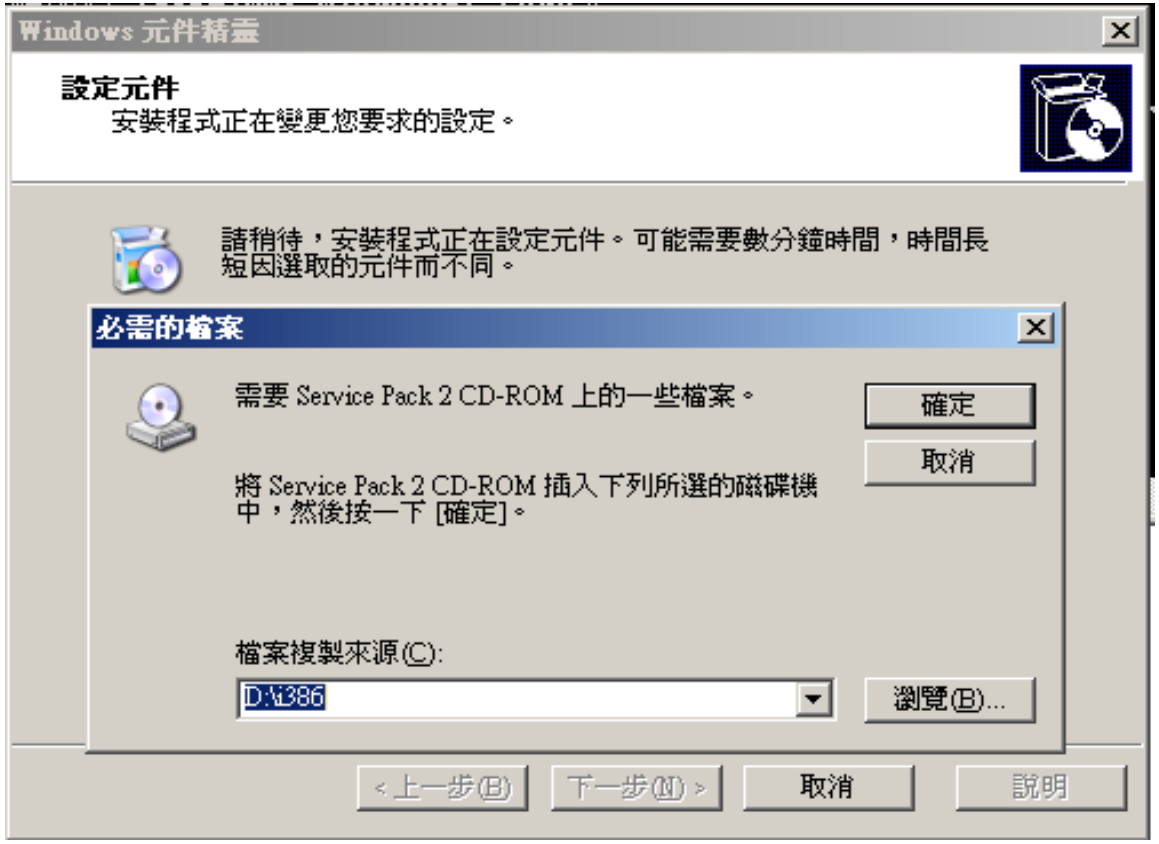
安裝WMI Windows Installer(4/7)

- 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」



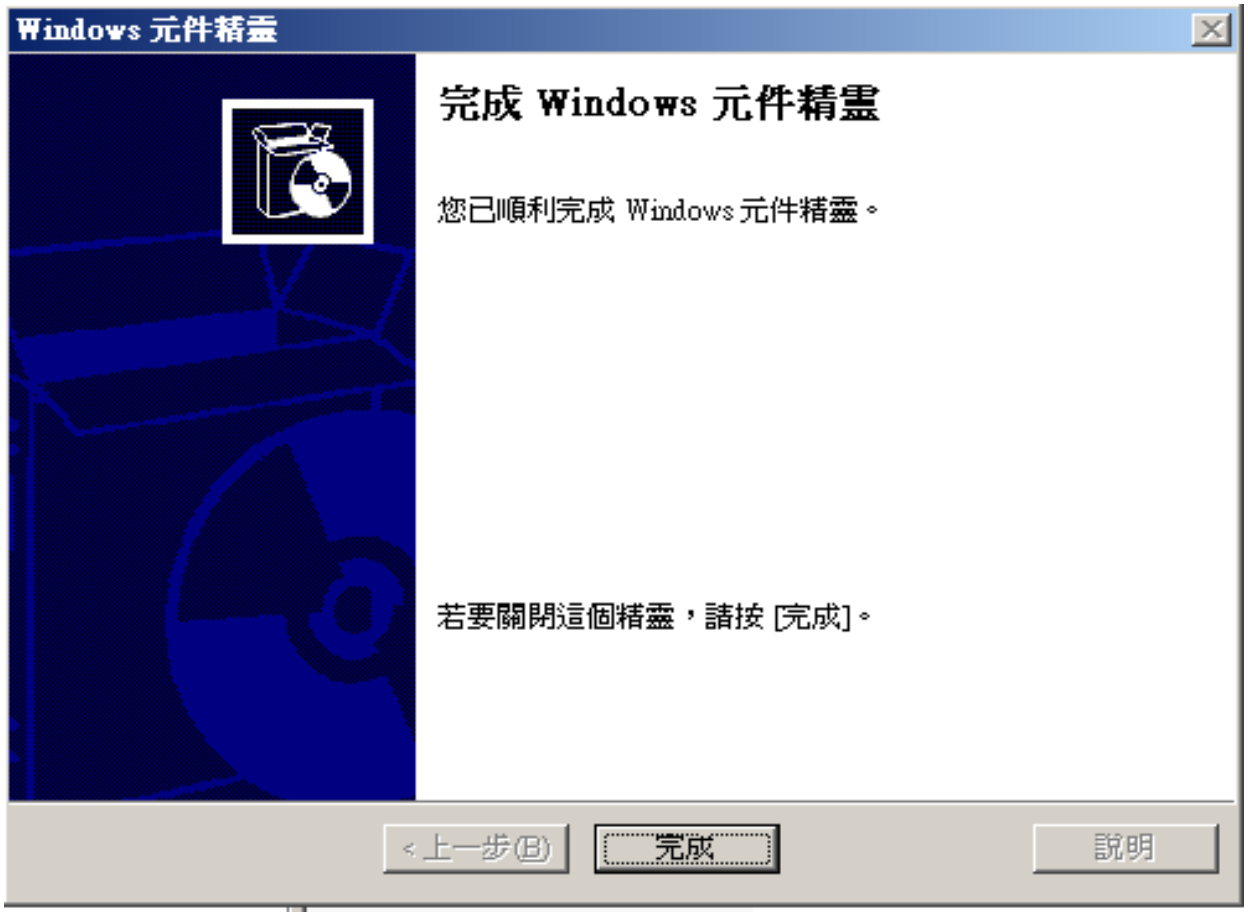
安裝WMI Windows Installer(5/7)

- 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



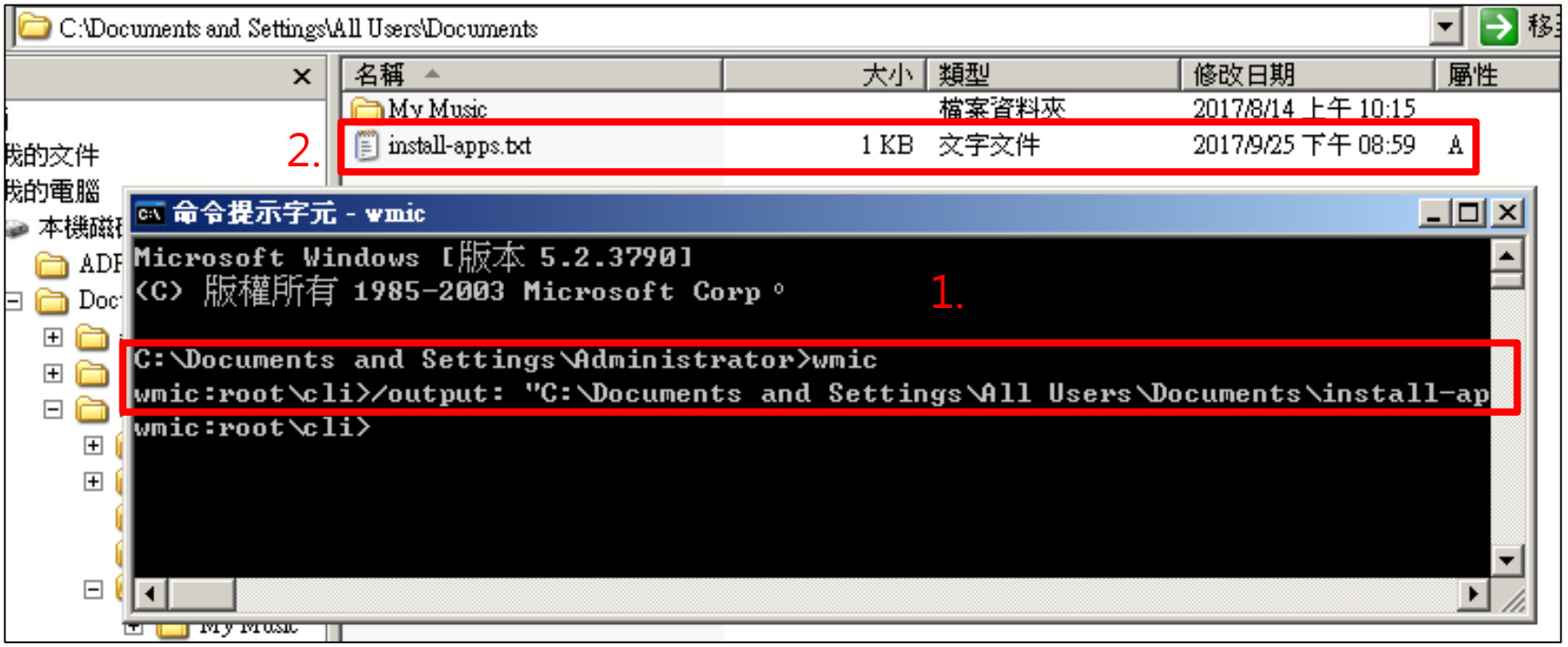
安裝WMI Windows Installer(6/7)

- 步驟五：完成安裝



安裝WMI Windows Installer(7/7)

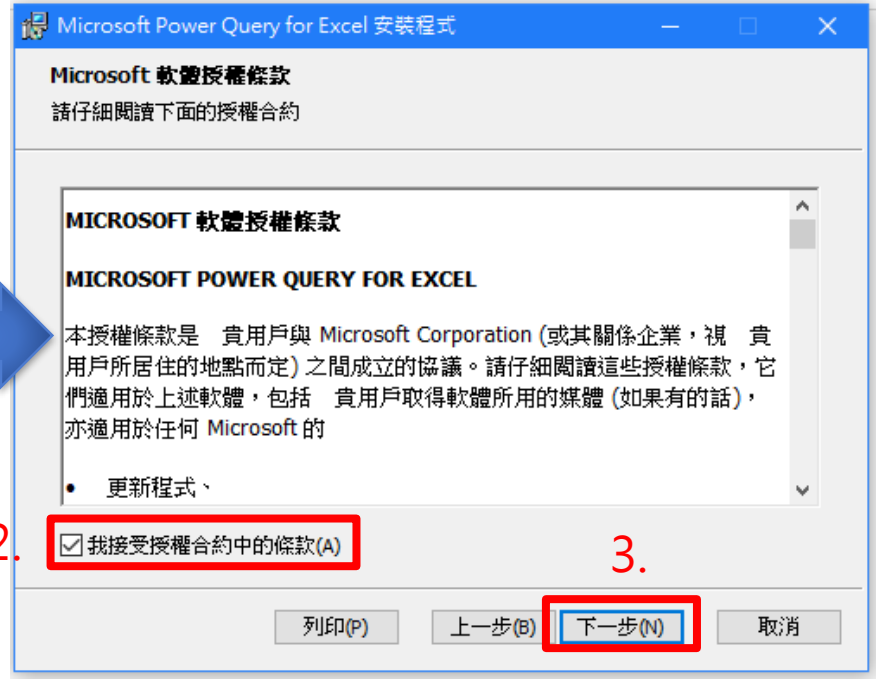
- 步驟六：安裝完成後，即可執行WMIC



附件3
Microsoft Power Query for Excel
安裝步驟

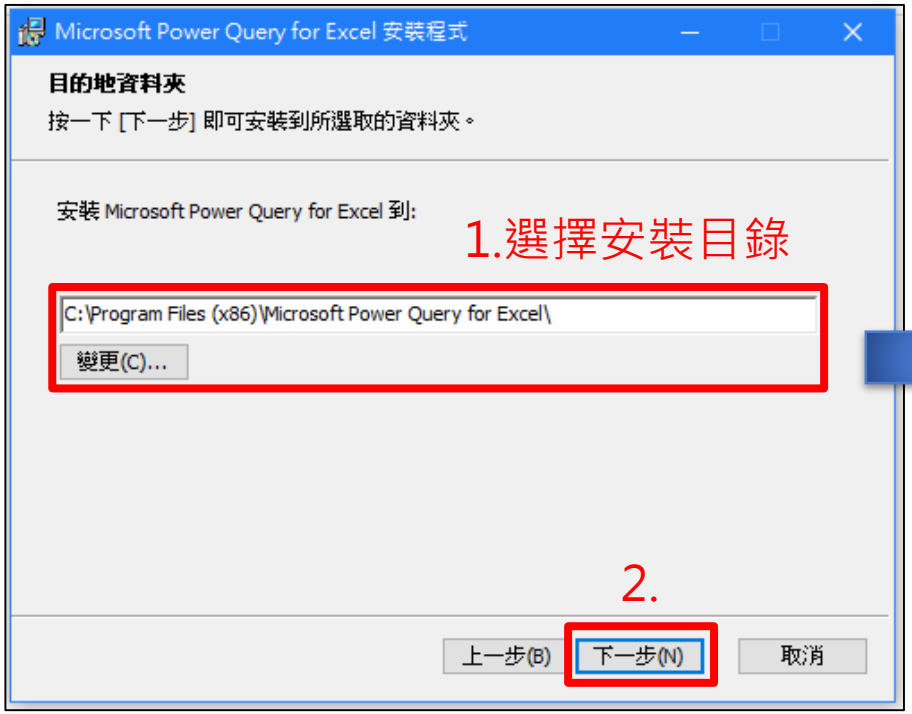
安裝Microsoft Power Query for Excel(1/3)

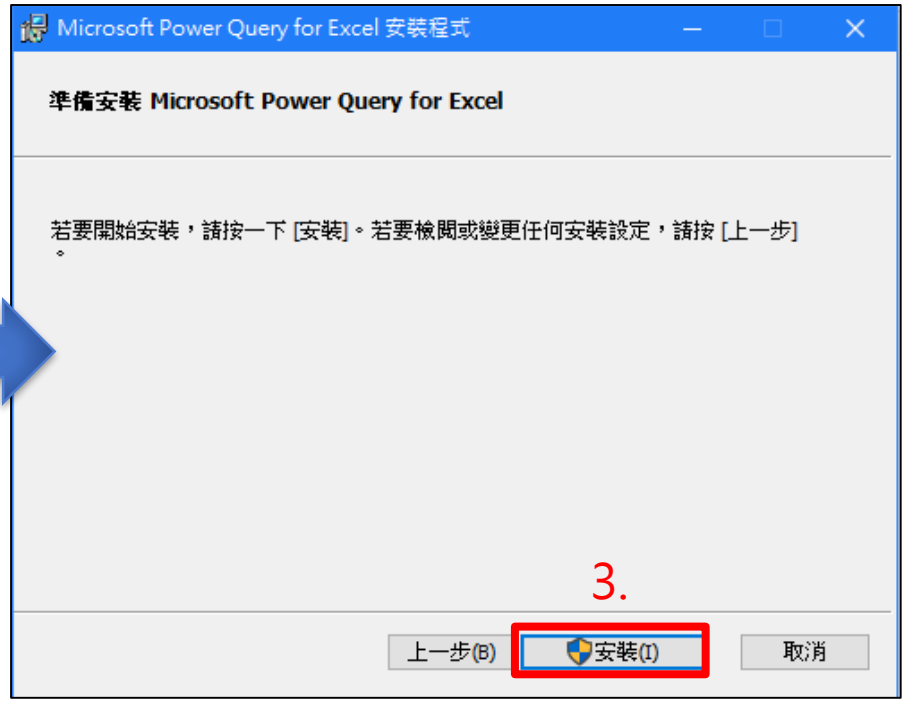
- Power Query內建於Excel 2016、2019中，功能名稱為「取得及轉換」，不需額外安裝Microsoft Power Query for Excel
- 若為Excel 2010或2013，需至微軟官網下載Microsoft Power Query for Excel，並進行安裝
  - https://www.microsoft.com/zh-TW/download/details.aspx?id=39379



安裝Microsoft Power Query for Excel(2/3)

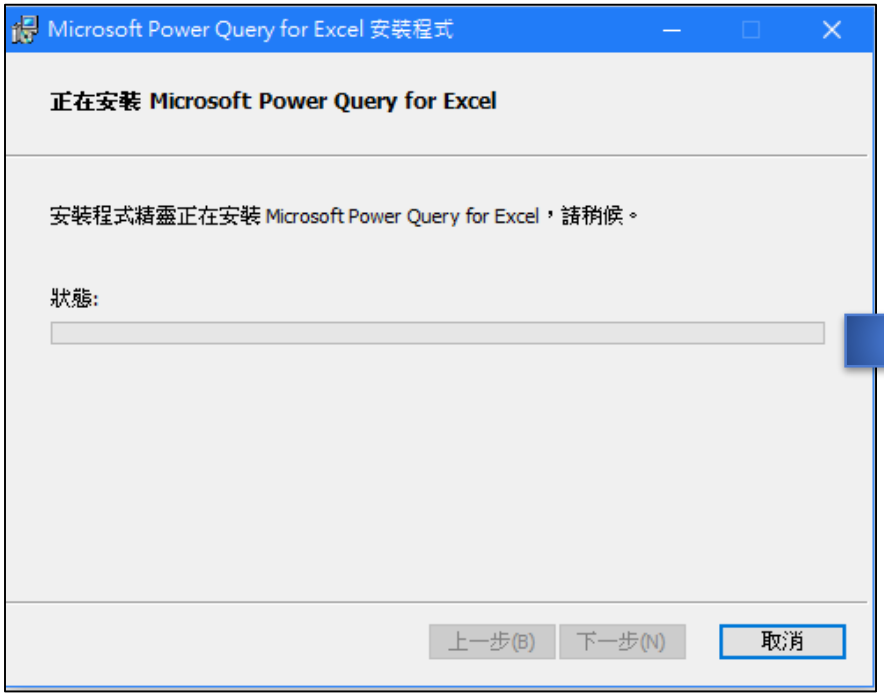
- 選擇安裝目錄，準備安裝

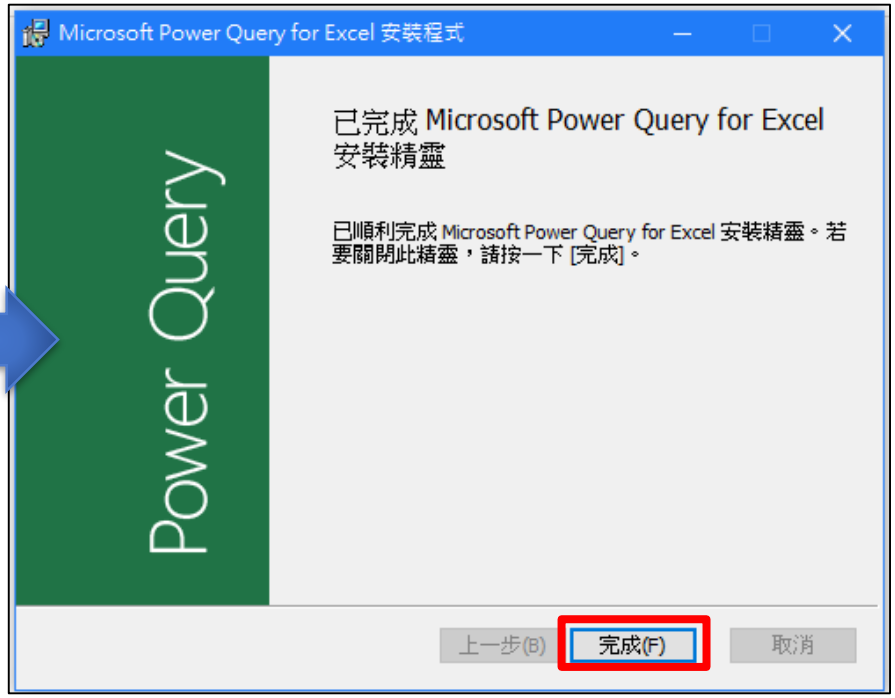




安裝Microsoft Power Query for Excel(3/3)

- 進行安裝





報告完畢
敬請指教