政府機關資安弱點通報機制(VANS)實作訓練

行政院國家資通安全會報技術服務中心

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
  - 09:00~09:15：政府機關資安弱點通報系統說明
  - 09:15~11:30：政府機關資安弱點通報系統實作
  - 11:30~12:00：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
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
  - 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
    - 實作練習1
  - 資訊資產與已安裝KBID登錄作業
    - 實作練習2
  - 弱點通知與修補作業
    - 實作練習3
  - 資訊資產與已安裝KBID更新作業
    - 實作練習4

課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
  - 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
    - 實作練習1
  - 資訊資產與已安裝KBID登錄作業
    - 實作練習2
  - 弱點通知與修補作業
    - 實作練習3
  - 資訊資產與已安裝KBID更新作業
    - 實作練習4

前言

- 不定期爆發之重大弱點，若未能即時反應，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

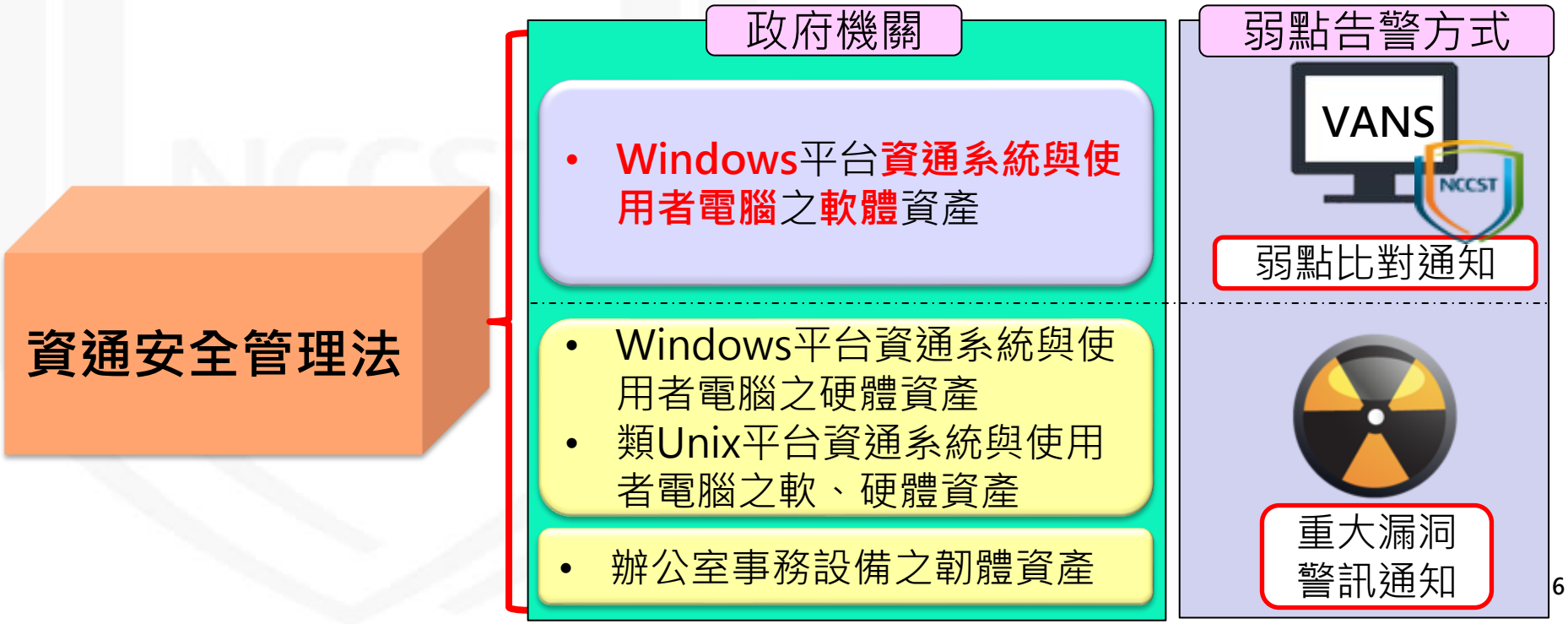
確認範圍
- 如何在確認受影響版本後，可確實掌握受影響範圍

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

資通安全管理法相關規定(1/3)

- 資通安全管理法第十條/第十六條第二項
  - 公務機關/關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫
- 資通安全管理法施行細則第六條規範資通安全維護計畫應包含之項目
  - 第六款規範機關應盤點資通系統，並標示核心資通系統與相關資產
  - 第七款規範機關應建立相關風險評估機制，以針對盤點之資產進行資通安全風險評估



資通安全管理法相關規定(2/3)

- 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安弱點通報機制

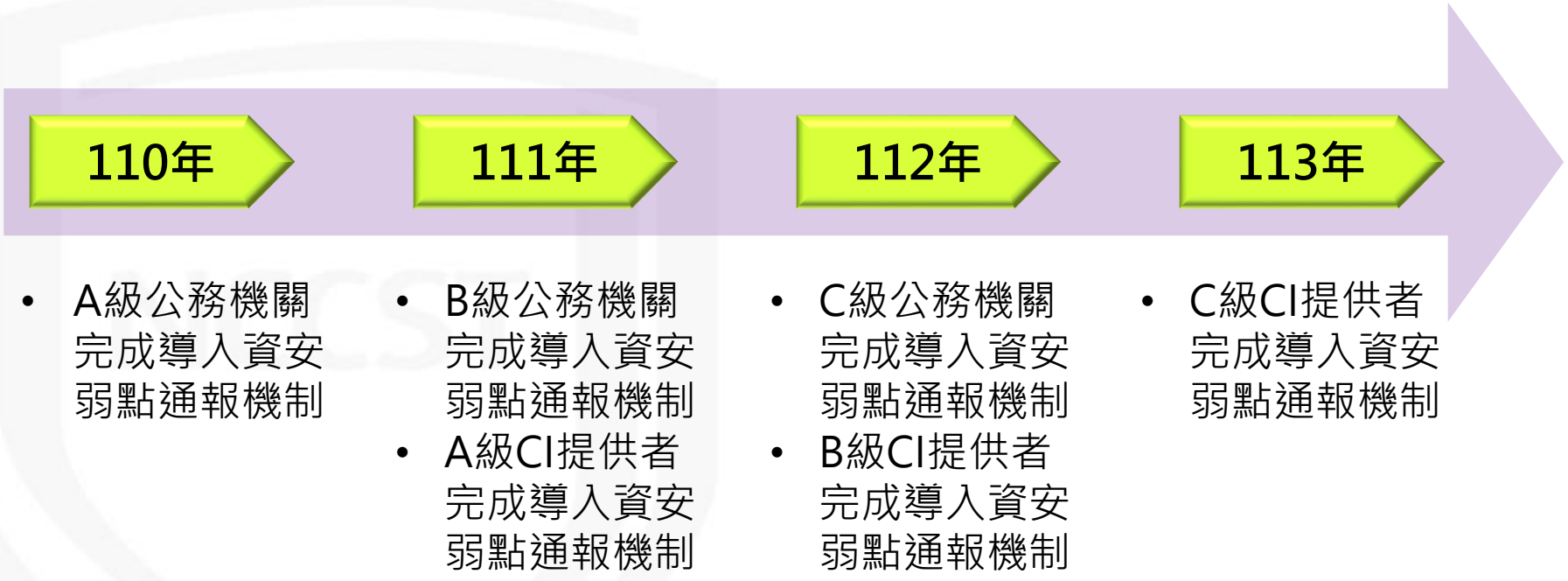
制度面向	辦理項目	資安責任等級	辦理內容
技術面	資安弱點通報機制	A、B級 公務機關	一、初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料
		A、B級 特定非公務機關	一、關鍵基礎設施提供者初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式完成提交資訊資產盤點資料 二、本辦法中華民國一百十年八月二十三日修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

資通安全管理法相關規定(3/3)

制度面向	辦理項目	資安責任等級	辦理內容
技術面	資安弱點通報機制	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

國家資通安全發展方案

- 「國家資通安全發展方案(110年至113年)」策略三之「1-2 建立資通系統弱點之主動發掘、通報及修補機制」工作項目之分年重要進程



課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
  - 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
    - 實作練習1：資訊資產正規化
    - 實作練習2：已安裝KBID正規化
  - 資訊資產與已安裝KBID登錄作業
    - 實作練習3：資訊資產登錄
  - 弱點通知與修補作業
  - 資訊資產與已安裝KBID更新作業
    - 實作練習4：弱點修補規劃與更新
    - 實作練習5：已安裝KBID更新

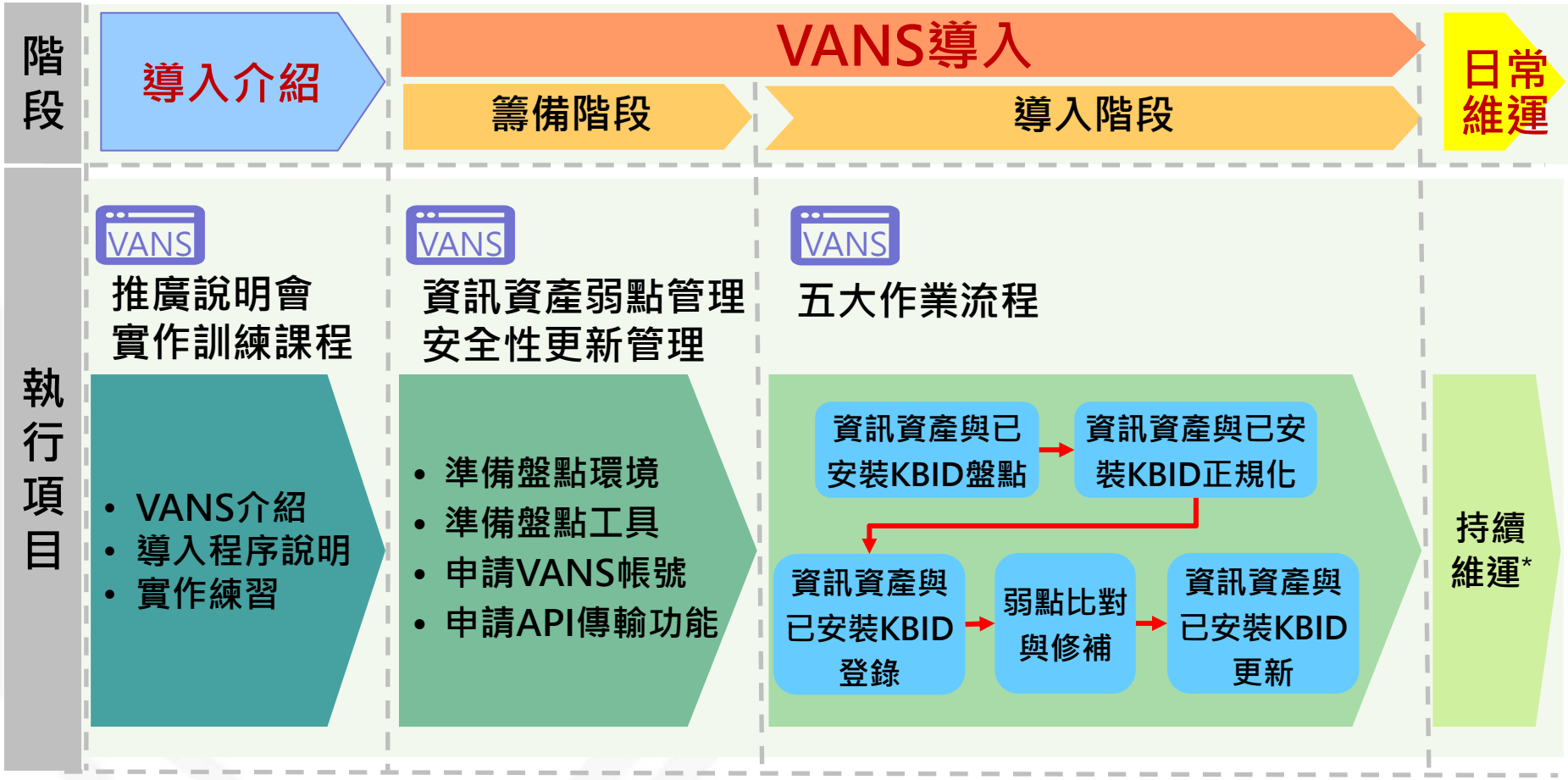
政府機關資安弱點通報機制

- 政府機關資安弱點通報機制(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
  - 蒐集政府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，提供政府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

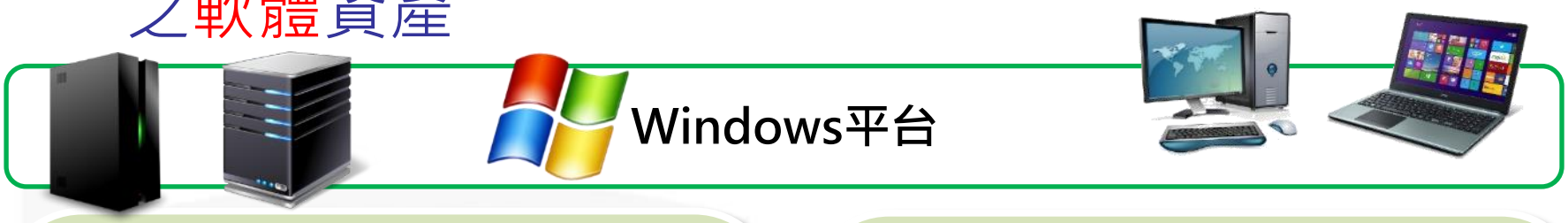
- VANS系統提供機關登錄資訊資產，藉由系統自動與NVD弱點資料庫比對，羅列出資訊資產之弱點，俾利機關掌握可能面臨之資安風險，以強化資訊資產之資安管理

NVD CVE cve.mitre.org CPE common platform enumeration

Windows Update

資訊資產盤點標的

- 蒐集範圍：Windows平台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

Windows Server

Windows Server 2012 R2

Windows Server 2016 Datacenter

Windows

Windows 8

Windows 10 Professional

- 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(1/2)

- 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)

資訊資產呈現方式(2/2)

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

廠商名稱　　版本　　版次

➢ cpe:2.3:o:microsoft:windows_server_2012:r2:sp1:*:*:*:*:x64:*

產品類別　　產品名稱　　更新

  - Oracle JDK 1.8.0 Update 92

廠商名稱　　版本

➢ cpe:2.3:a:oracle:jdk:1.8.0:update92:*:*:*:*:*:*:*

產品類別　產品名稱　　更新

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CVE都賦予一個專屬編號，格式如下：

  –CVE-YYYY-NNNN

  西元紀年 流水號

弱點資料庫

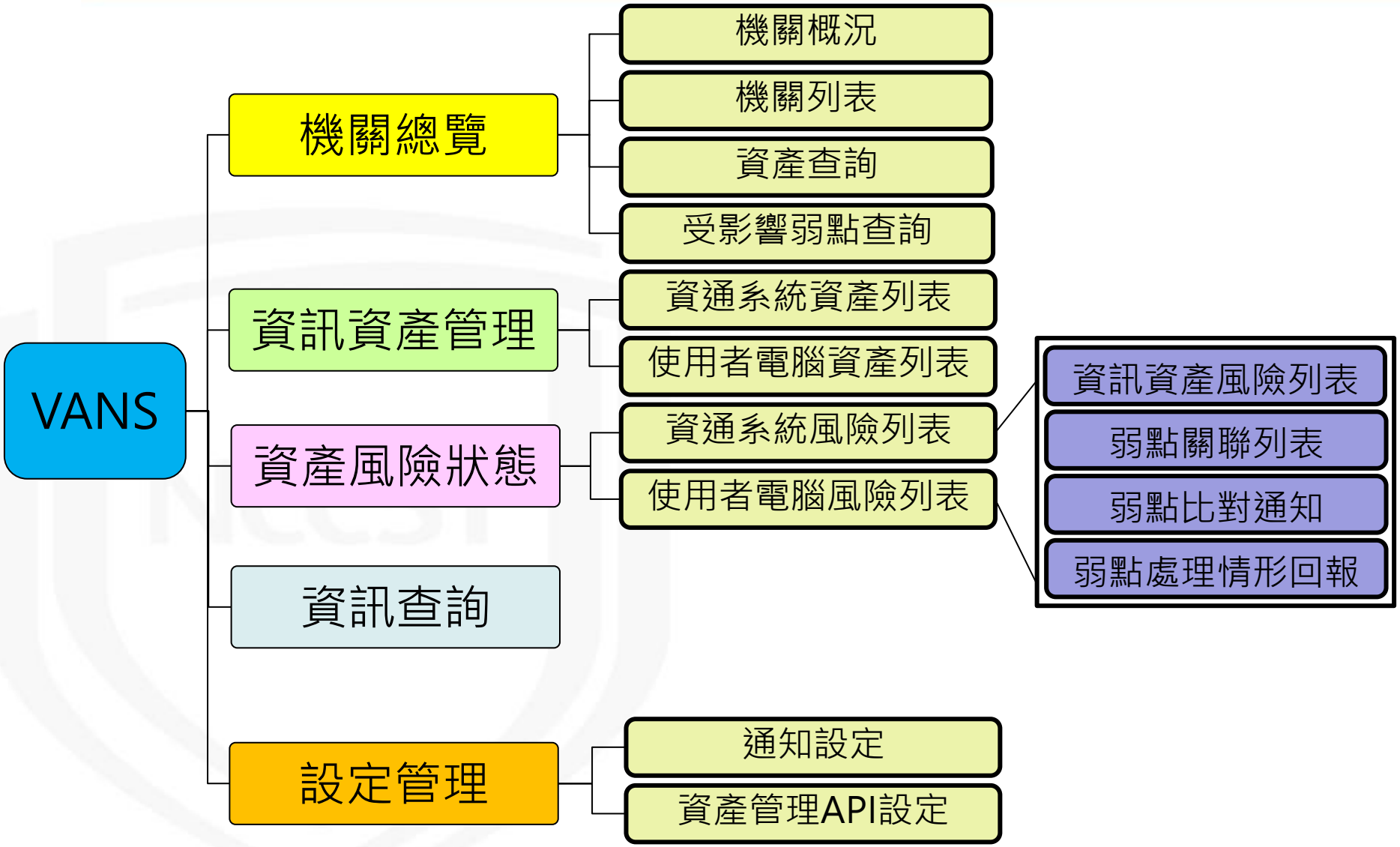
- National Vulnerability Database(簡稱NVD)為NIST所建置，專門用來蒐集各種弱點資訊之資料庫網站
  - 自MITRE取得CVE列表，並增加修補建議連結、嚴重性評分(CVSS分數)及影響等級等資訊
  - 建立CPE與CVE對應關係，以解決弱點與資訊資產之對應關係
  - VANS系統每天更新1次資產與弱點資訊

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

微軟安全性更新

- 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

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
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
政府機關資安弱點通報系統
登入人員
機關總覽 > 機關概況
功能路徑
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
功能頁面
檢視方式
資通系統
使用者電腦
資通系統資產類別統計
2, 40.0%
3, 60.0%
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)
2, 0.1%
3765, 99.9%
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)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

申請個人帳號

- 於iAuth系統申請個人帳號

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

機關提出申請

- 於iAuth系統提出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予資安處

技服中心VANS專區
https://www.nccst.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.nccst.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予資安處，審核通過後，技服中心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
  - 重新啟用步驟如下圖

說明帳號遭閒置鎖定，並提供：

- 機關名稱
- iAuth帳號名稱
- 人員姓名
- 連絡電話
- Email

資料核對無誤後，協助啟用帳號

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

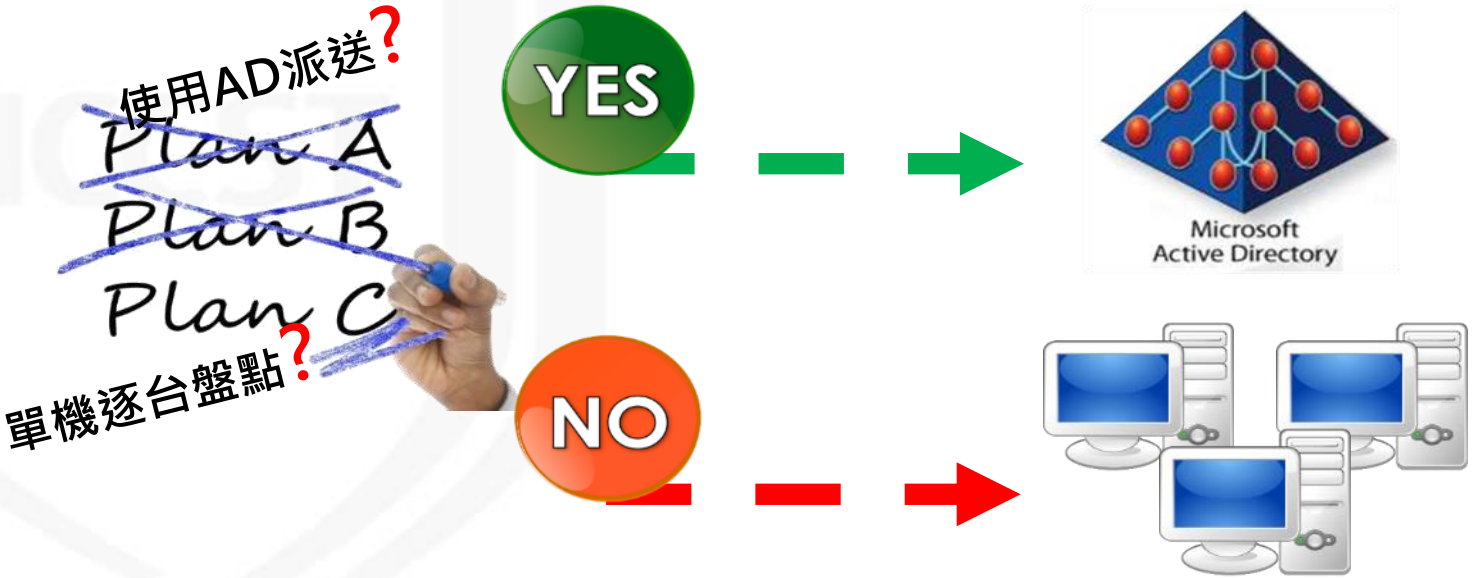
- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視**自身**帳號資產異動紀錄
- ✓ **檢視**API Key

課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
  - 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
    - 實作練習1
  - 資訊資產與已安裝KBID登錄作業
    - 實作練習2
  - 弱點通知與修補作業
    - 實作練習3
  - 資訊資產與已安裝KBID更新作業
    - 實作練習4

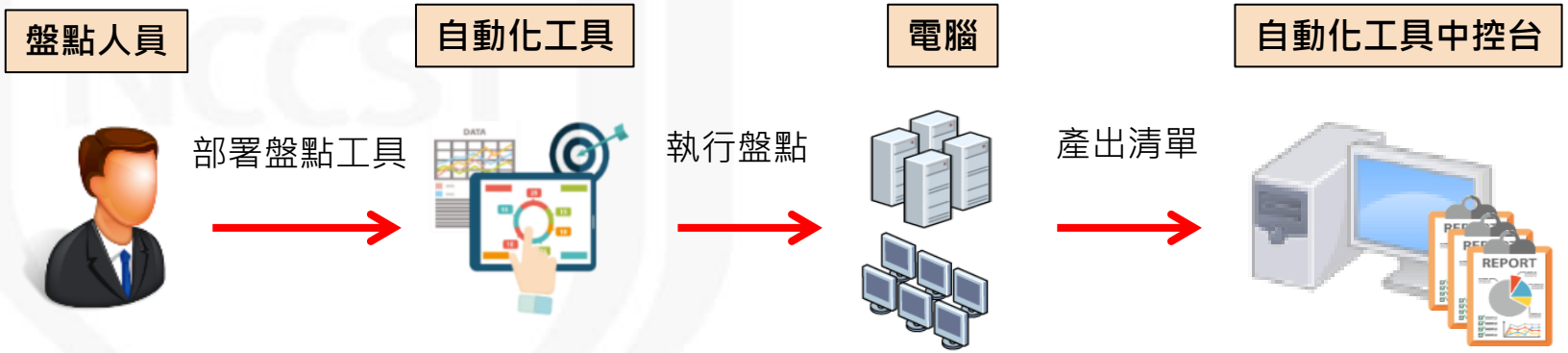
執行規劃

- 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



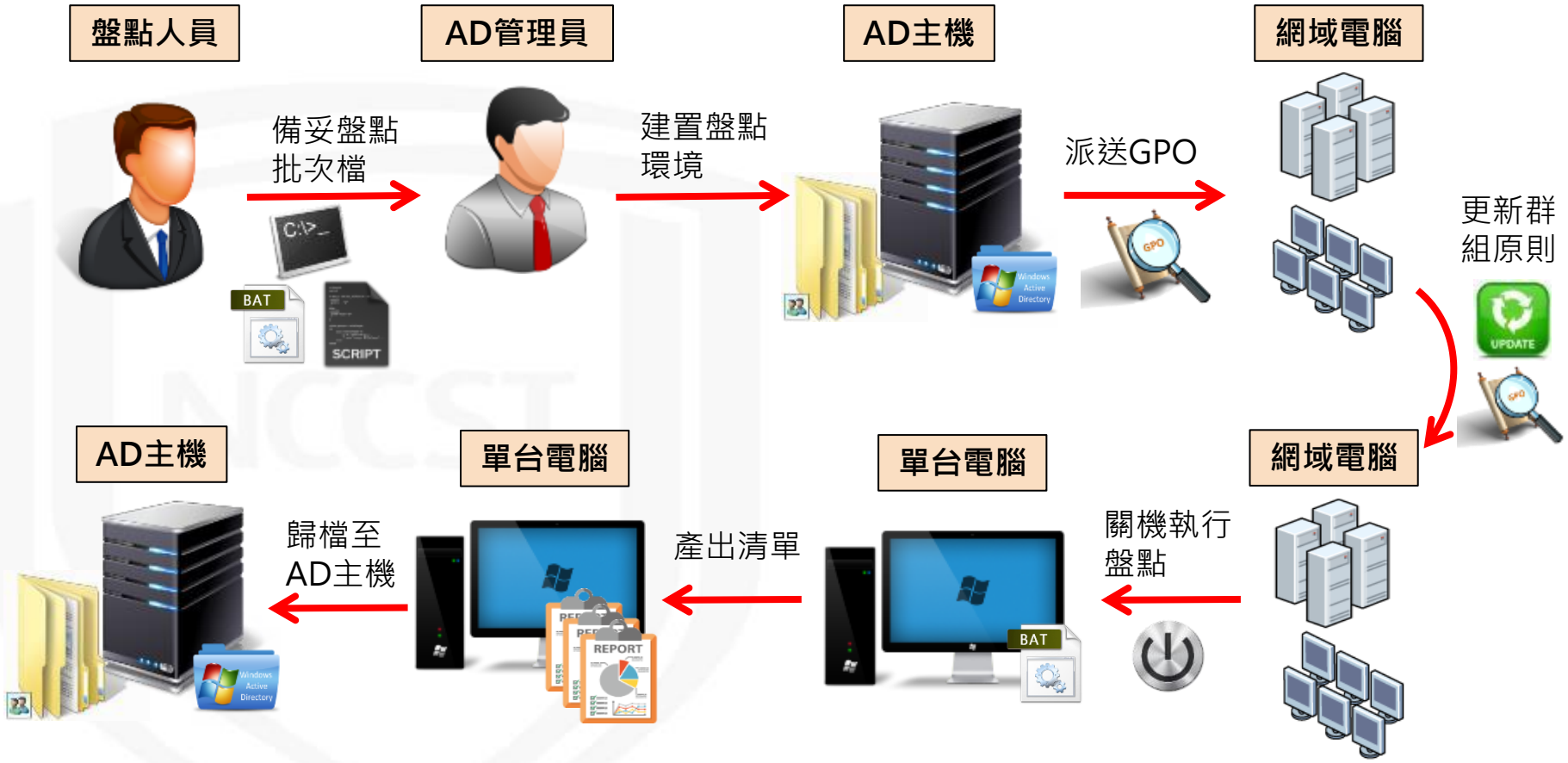
情境說明(1/3)

- 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
  - 透過自動化工具盤點



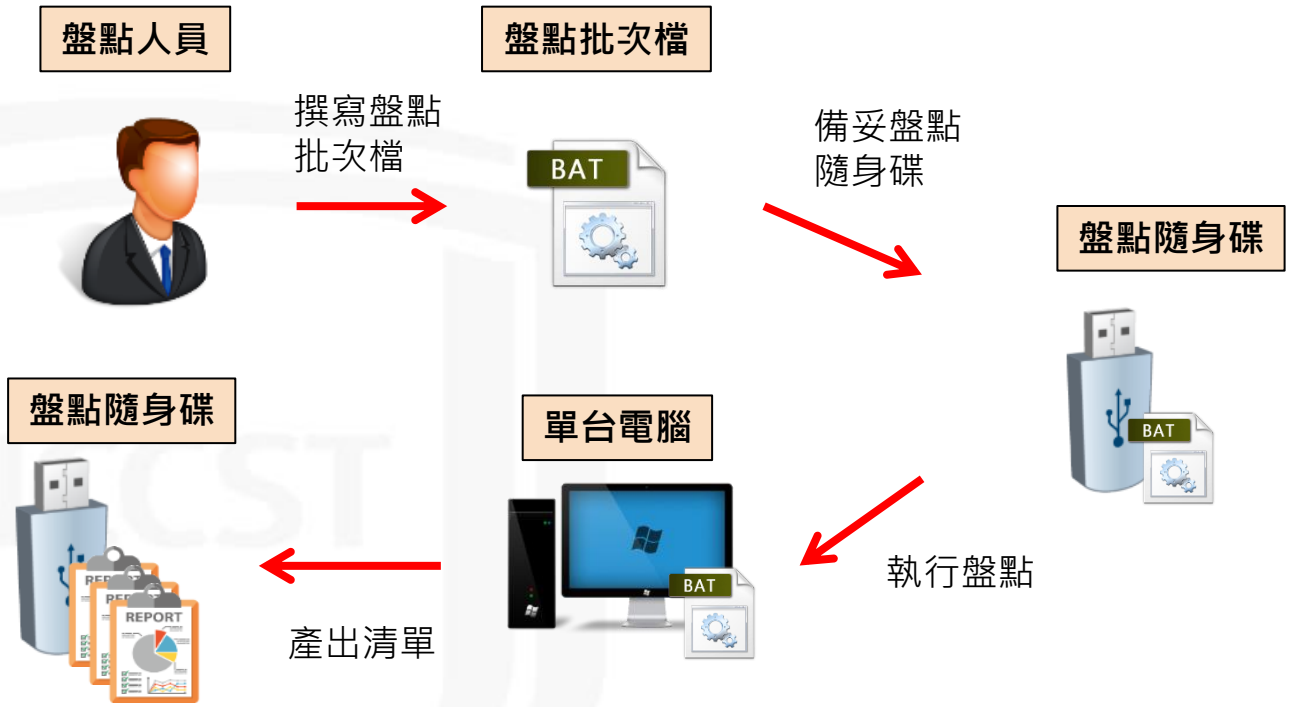
情境說明(2/3)

–透過系統指令批次盤點



情境說明(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
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

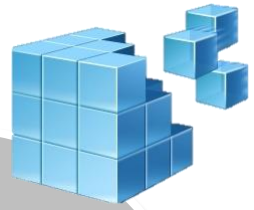
弱點通知
與修補作業

導入作業流程說明重點

編號	流程名稱	教材編排方式
1	資訊資產與已安裝KBID盤點作業	先說明手動盤點、正規化及登錄作業方式，再說明透過工具進行盤點、正規化及登錄作業方式
2	資訊資產與已安裝KBID正規化作業	
3	資訊資產與已安裝KBID登錄作業	
4	弱點通知與修補作業	說明透過VANS系統網頁介面進行修補與更新
5	資訊資產與已安裝KBID更新作業	

導入作業流程

資訊資產與
已安裝KBID
盤點作業



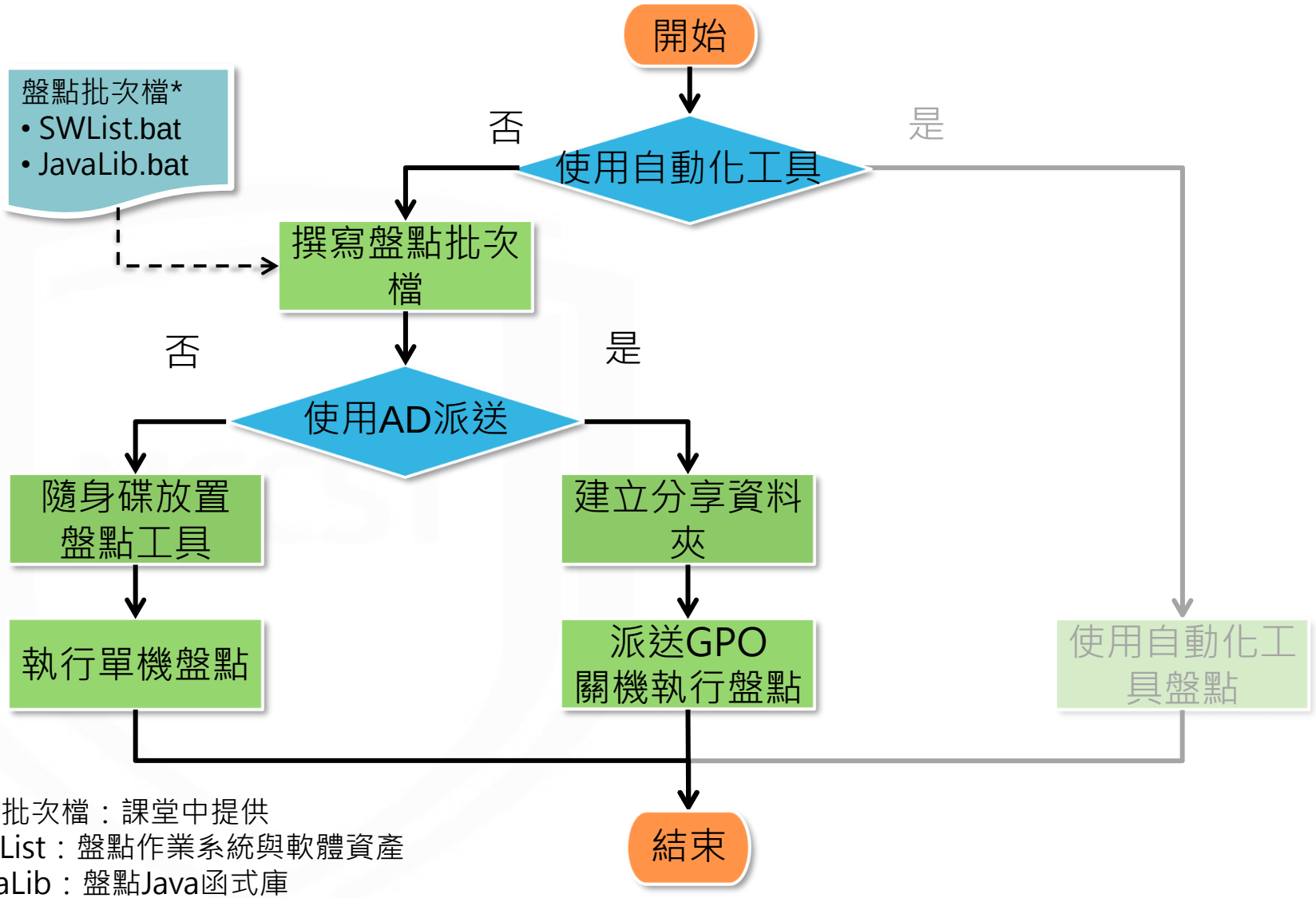
資訊資產與
已安裝KBID
更新作業

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

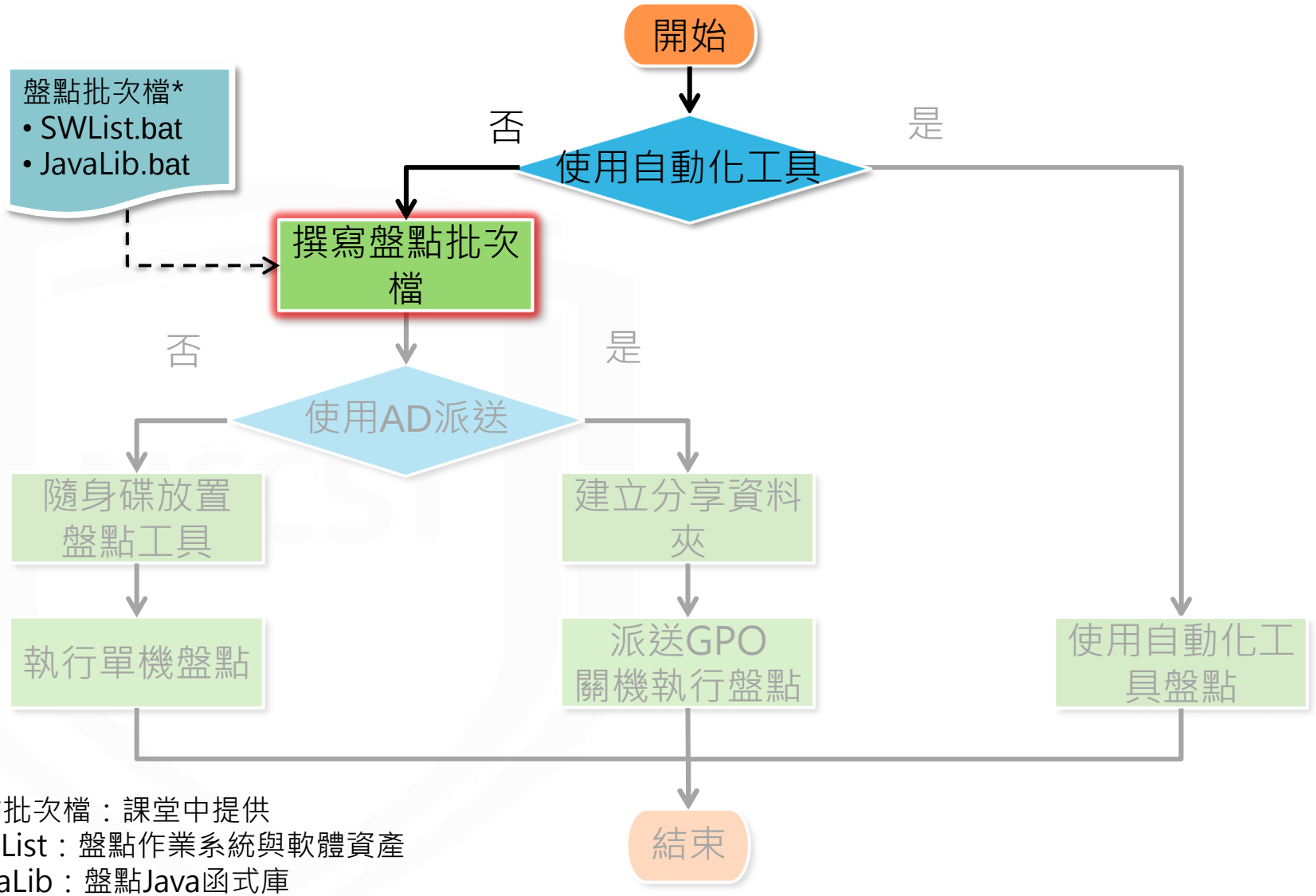
弱點通知
與修補作業

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

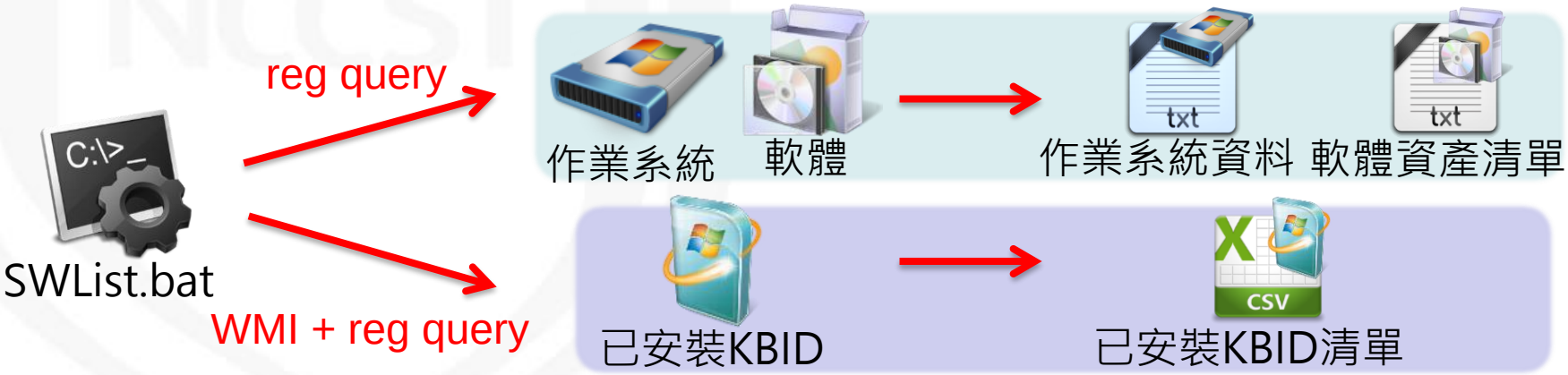
盤點作業流程



*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

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)

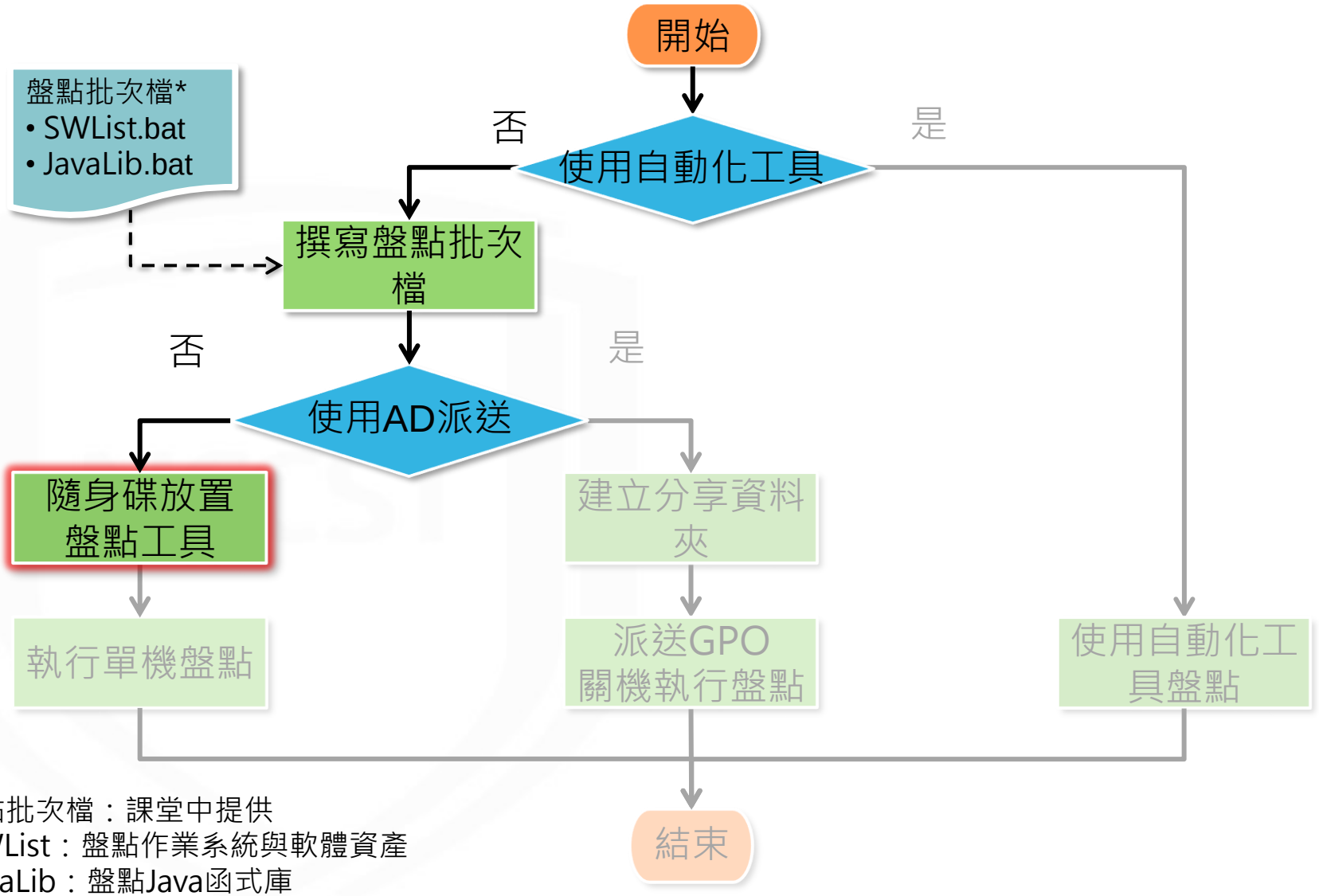
- 命令提示字元指令
  - 若機關環境有使用Java函式庫時，可透過此批次檔執行盤點
  - Tomcat Java函式庫路徑預設位置如下圖
    - cd C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\

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

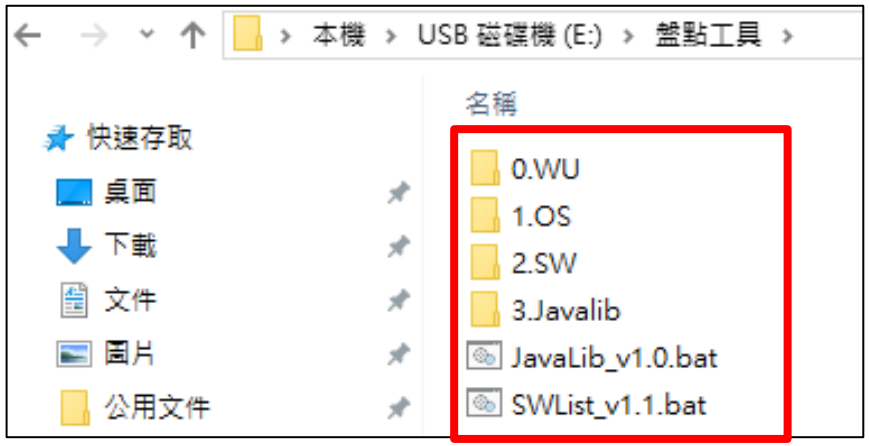
盤點作業流程



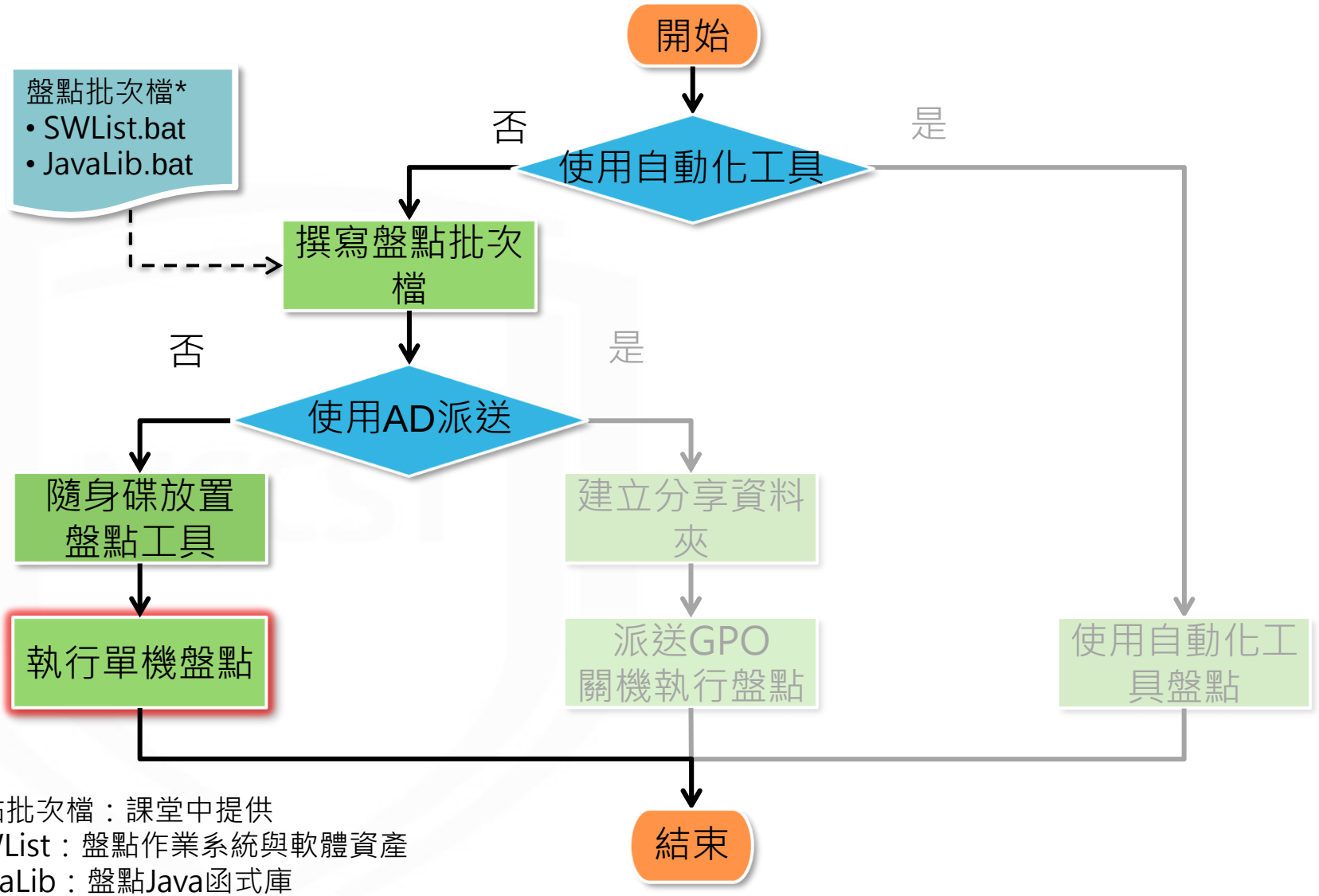
*盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

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



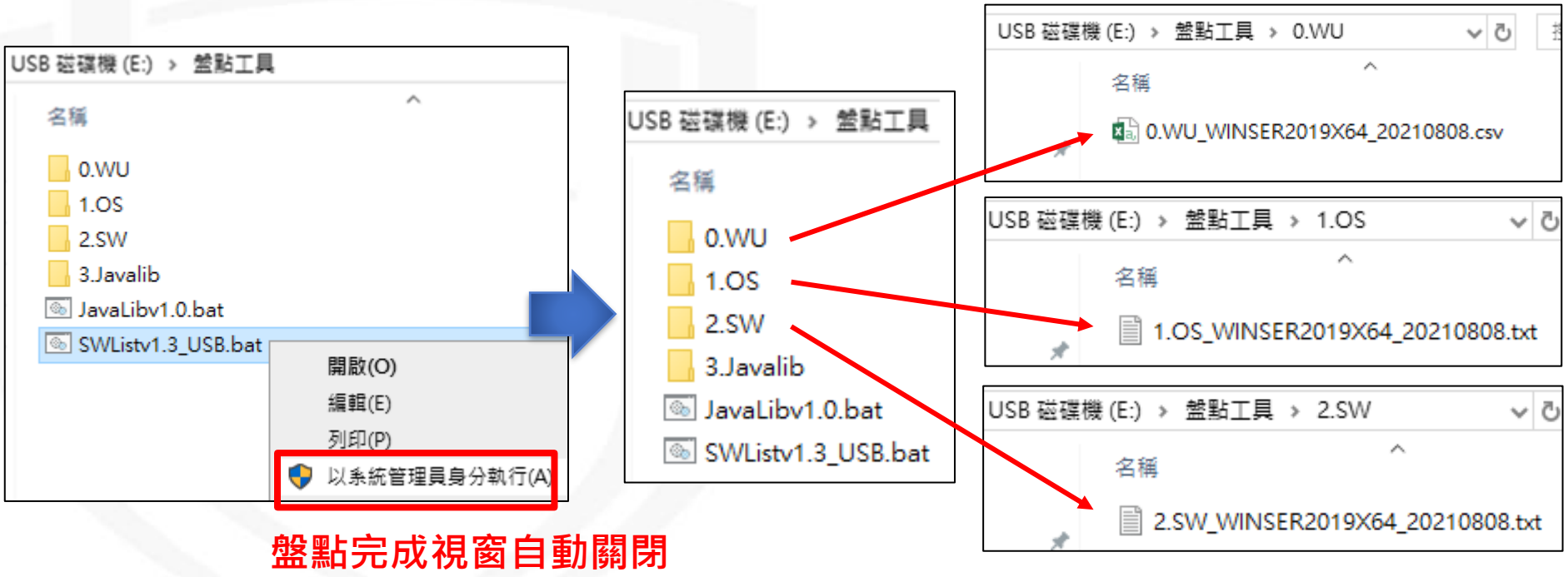
盤點作業流程



*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)

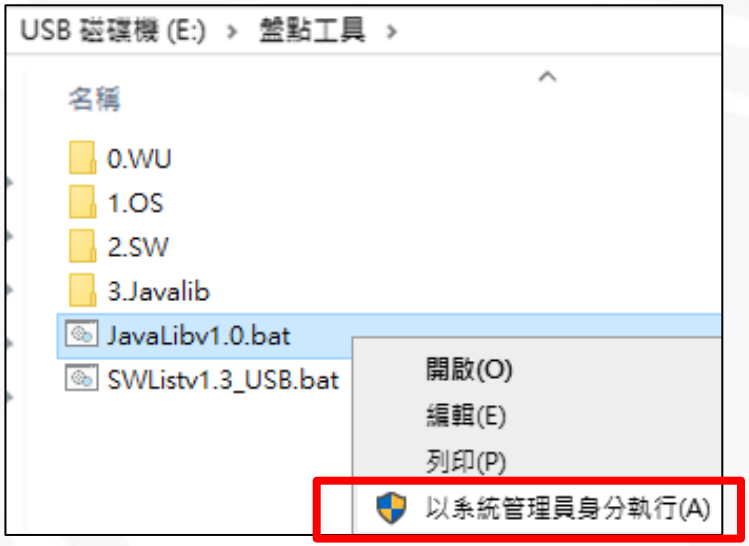
- STEP1：以系統管理員身分執行SWList批次檔
- STEP2：檢視盤點結果資料夾，分別為已安裝KBID清單、作業系統資訊及軟體盤點清單



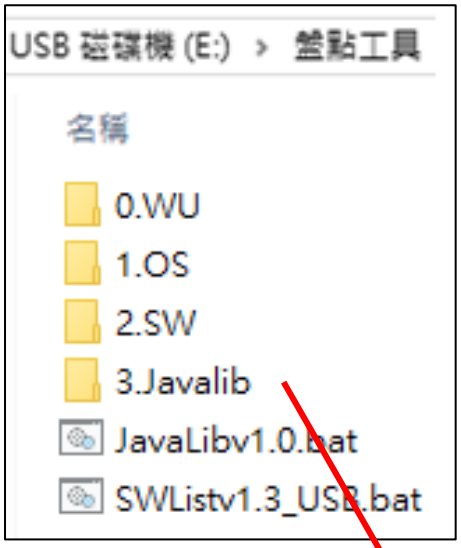
盤點完成視窗自動關閉

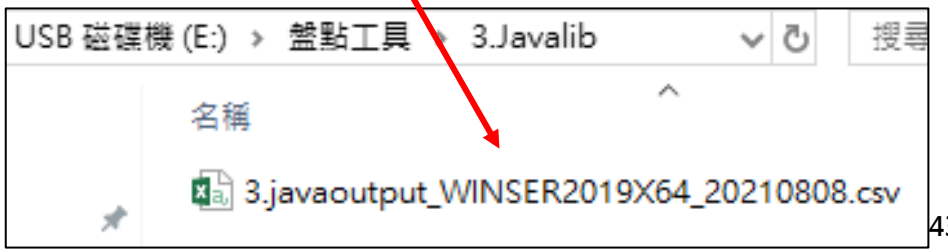
執行單機盤點(2/2)

- 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



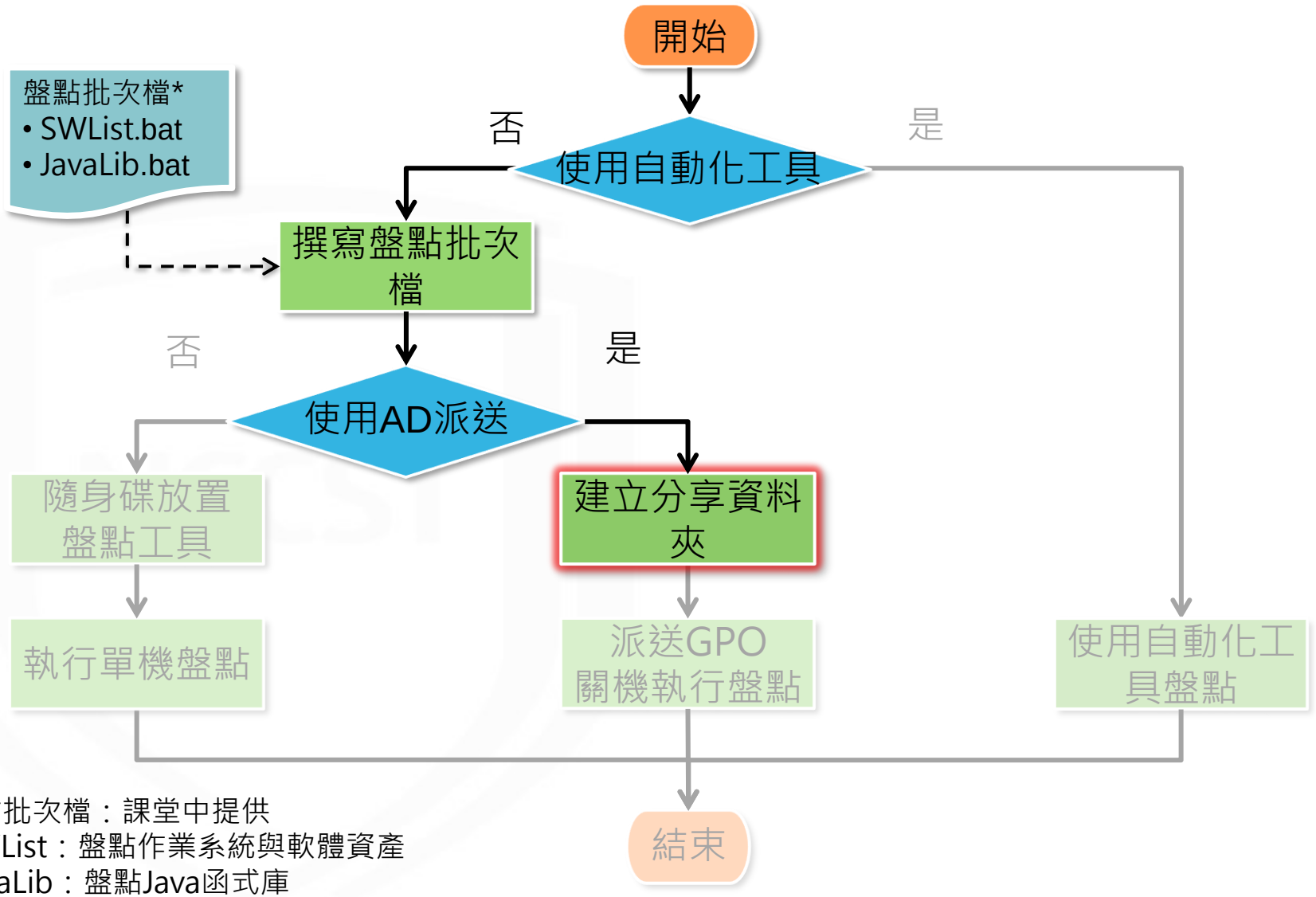
盤點完成視窗自動關閉





透過系統指令批次盤點

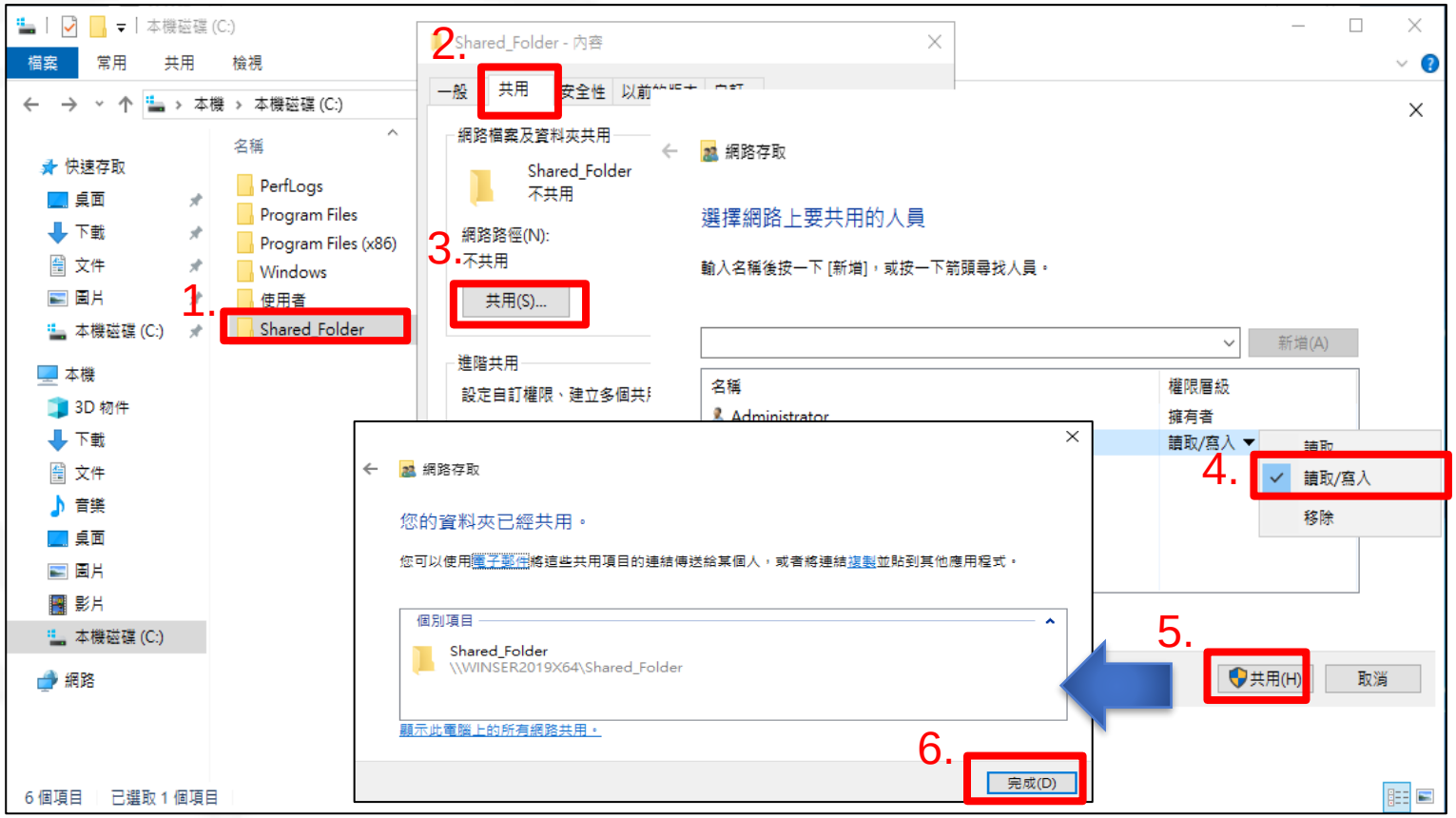
盤點作業流程



*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

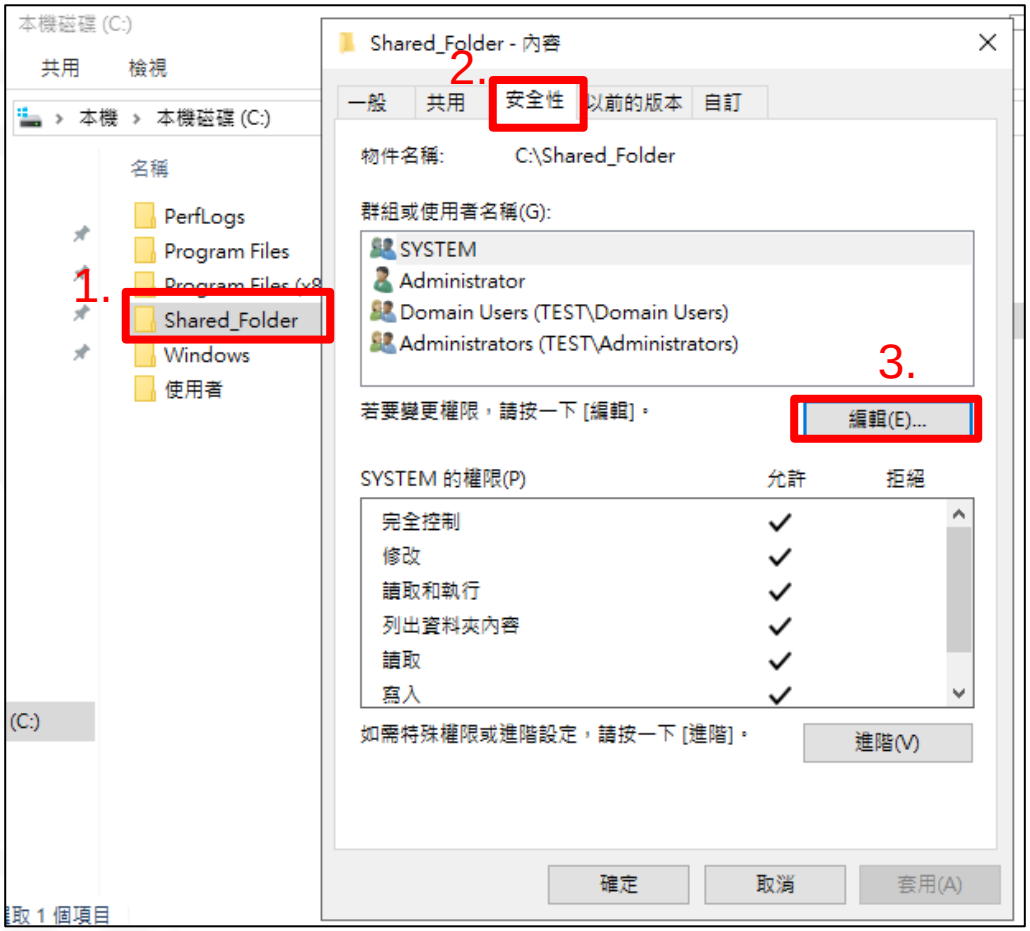
AD主機建立分享資料夾(1/3)

- 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



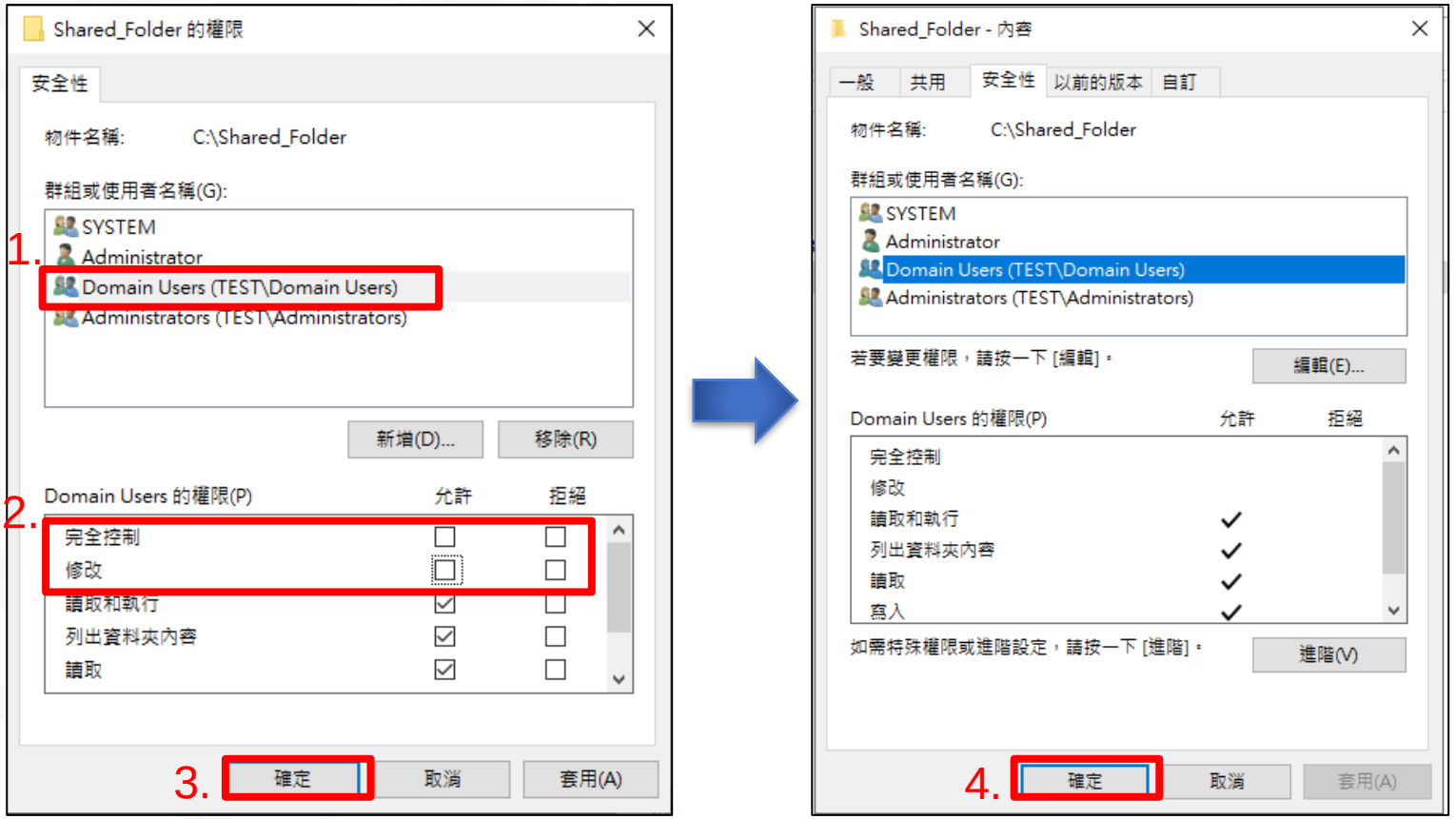
AD主機建立分享資料夾(2/3)

- 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

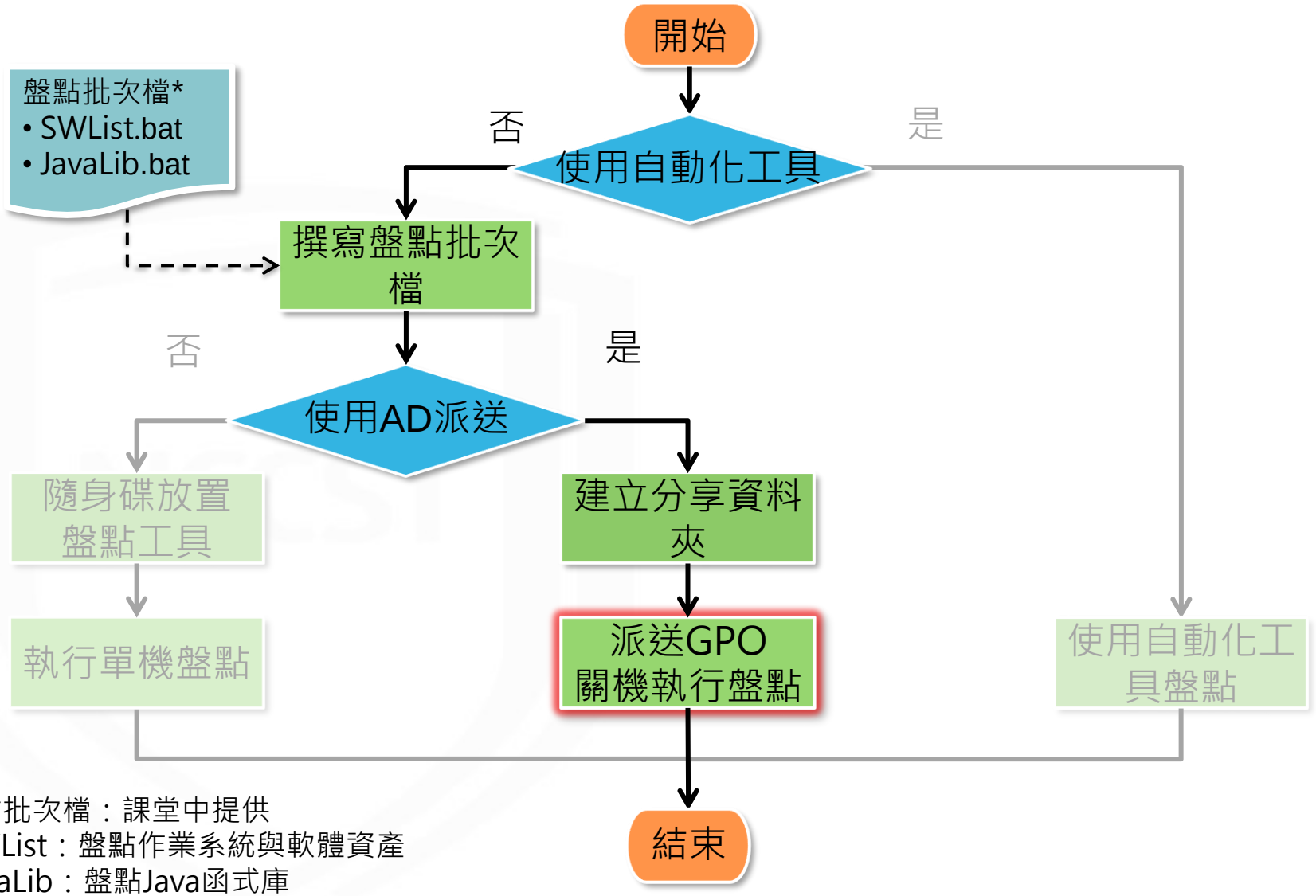


AD主機建立分享資料夾(3/3)

- 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



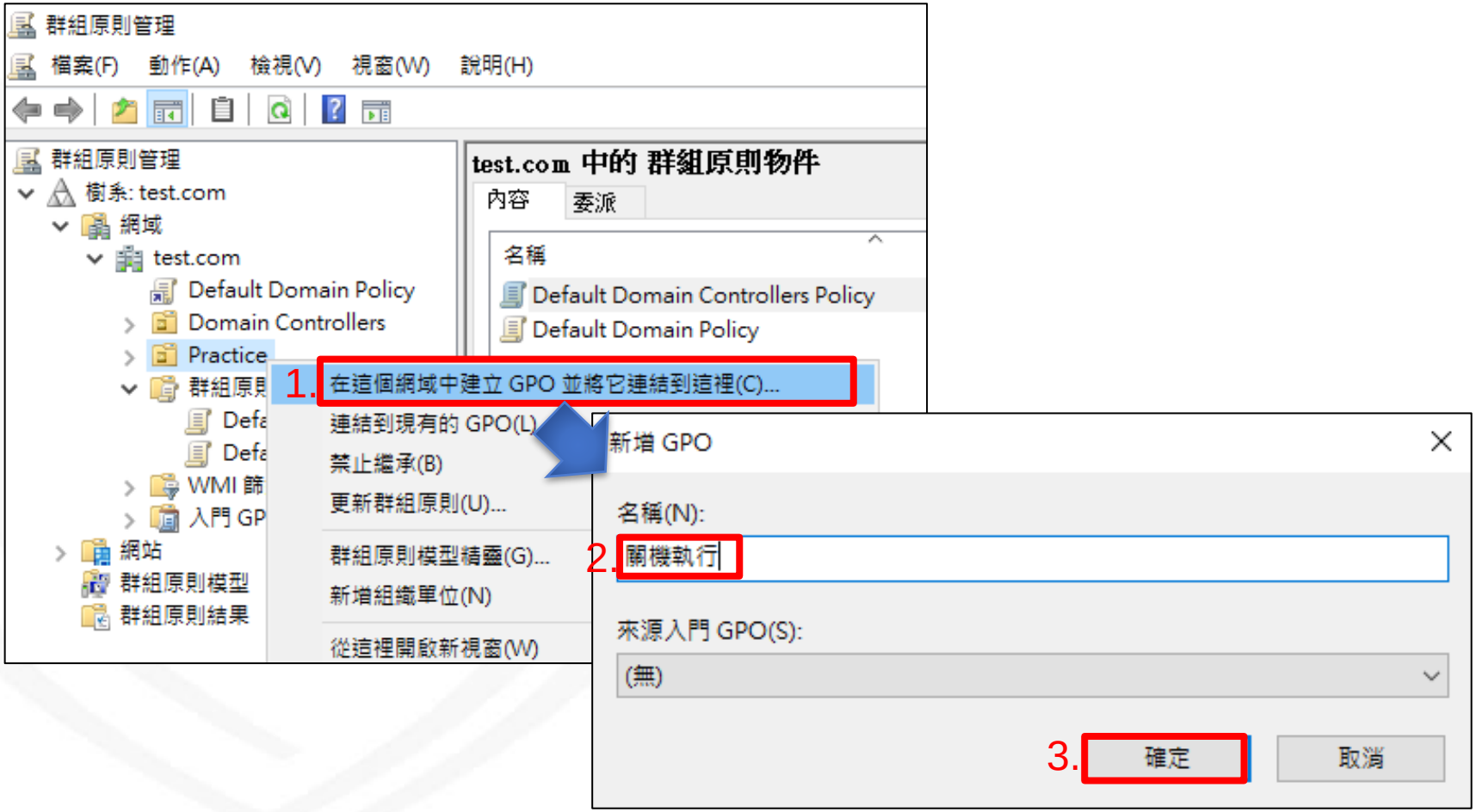
盤點作業流程



*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

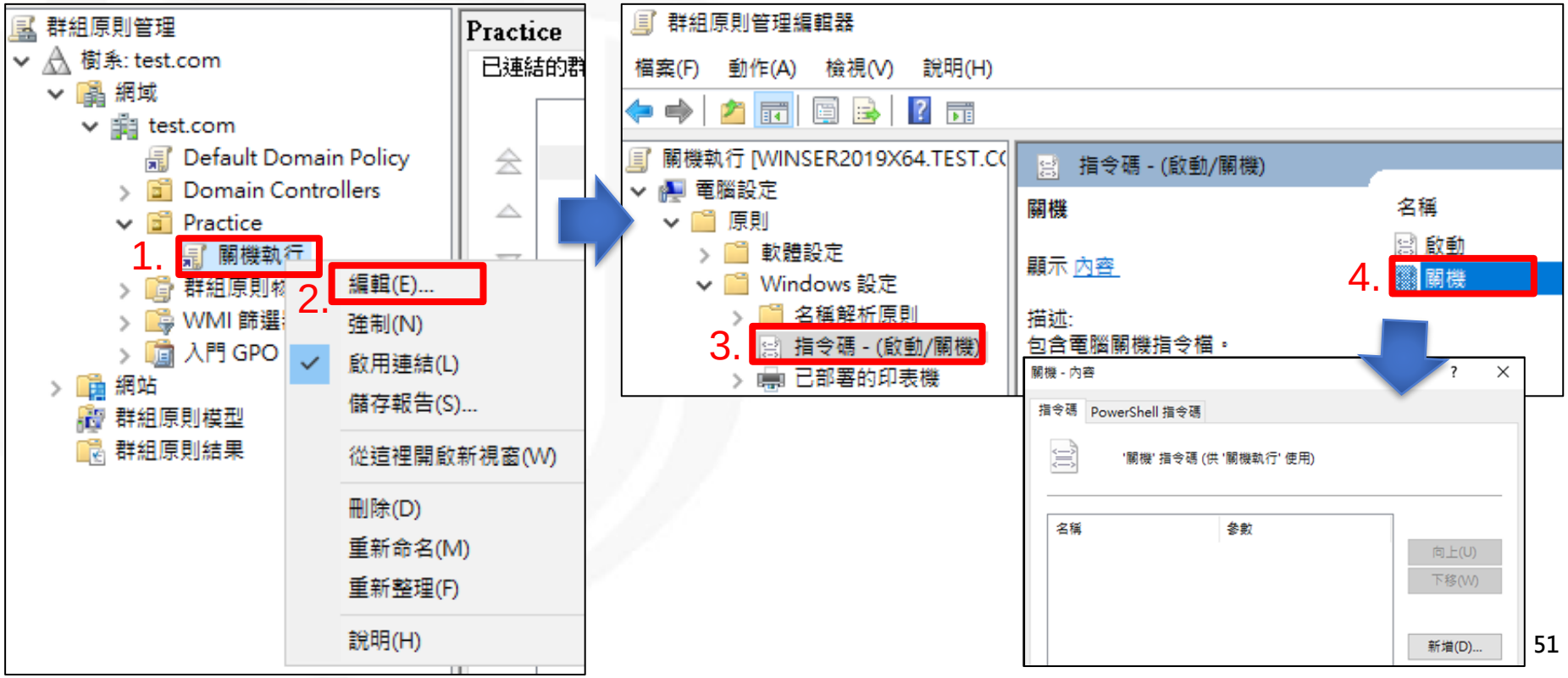
派送GPO-關機執行(1/5)

- 在目標OU點選右鍵並建立GPO
  - 新增「關機執行」GPO



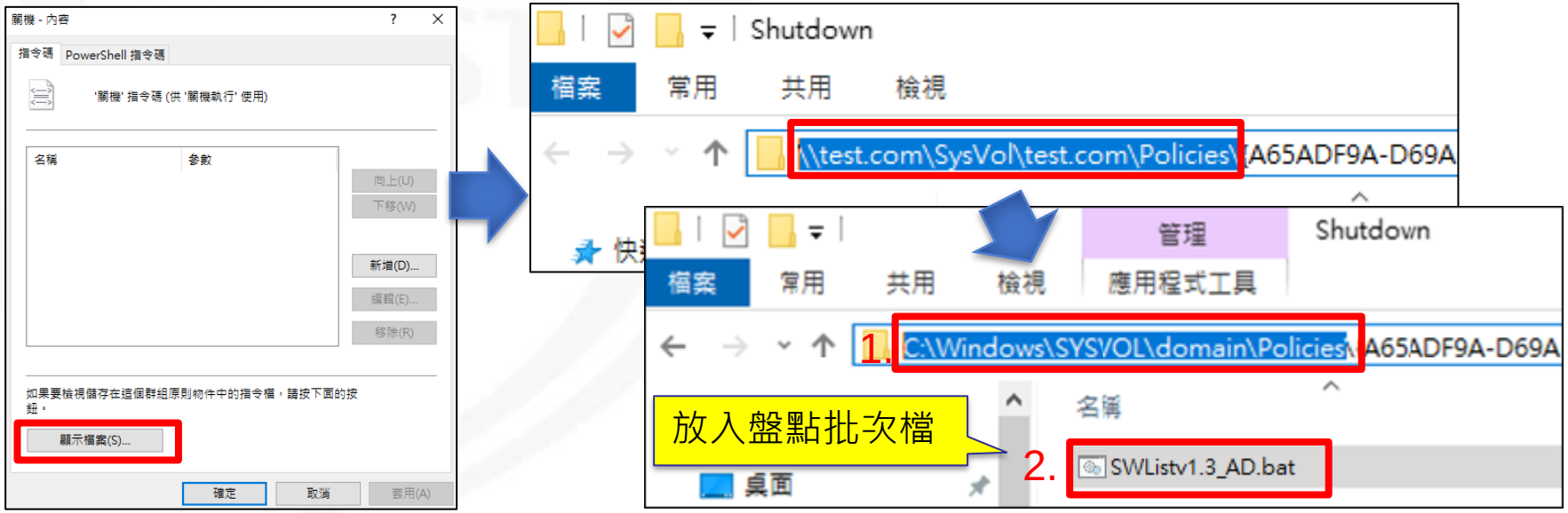
派送GPO-關機執行(2/5)

- 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」



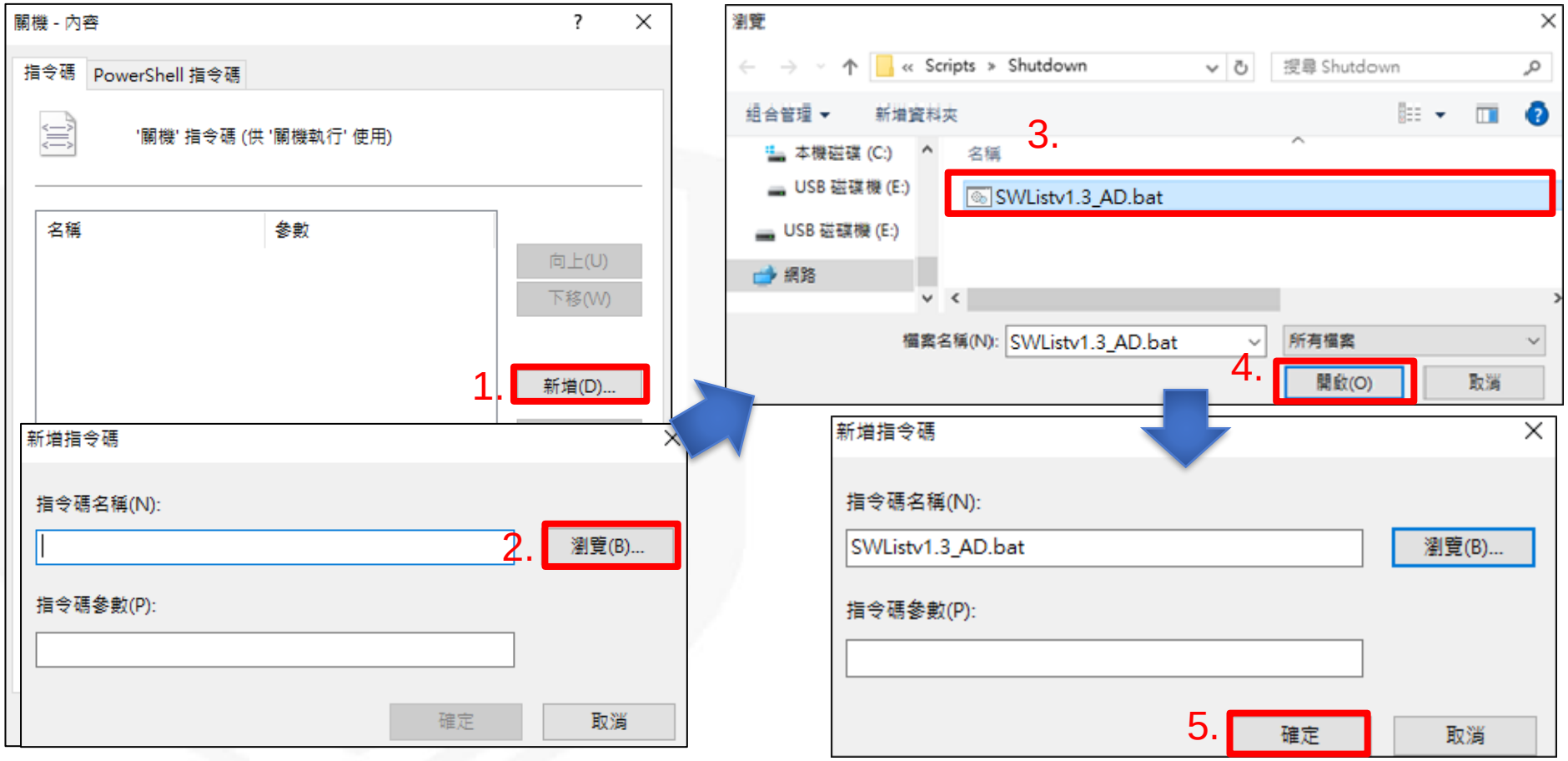
派送GPO-關機執行(3/5)

- 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 」



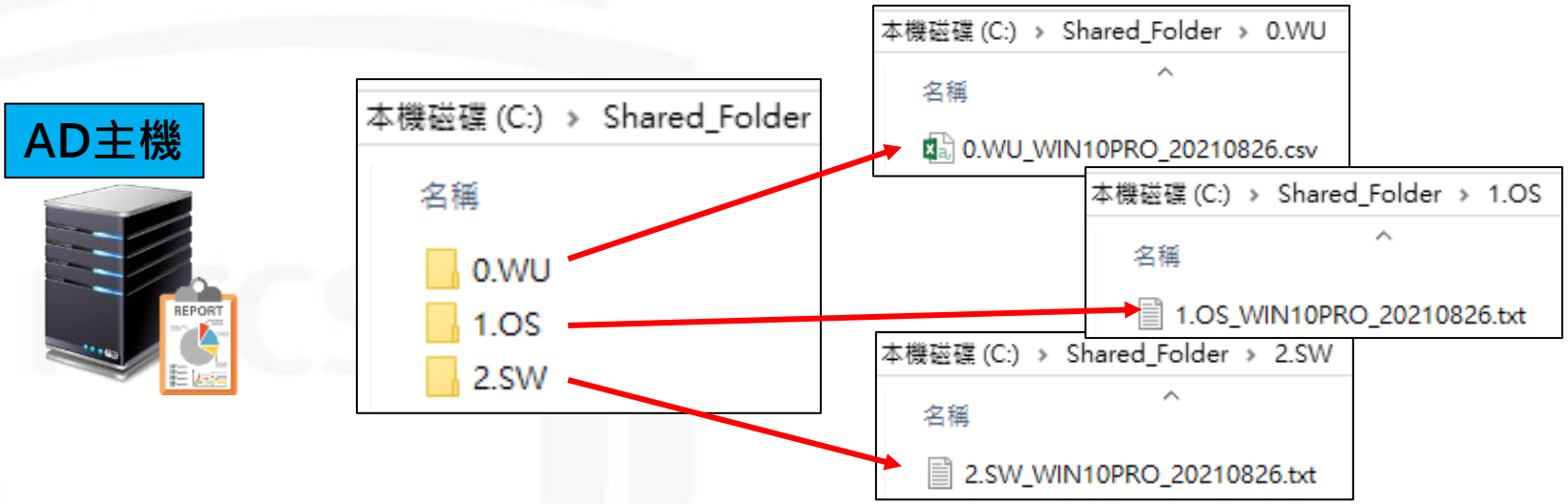
派送GPO-關機執行(4/5)

- 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

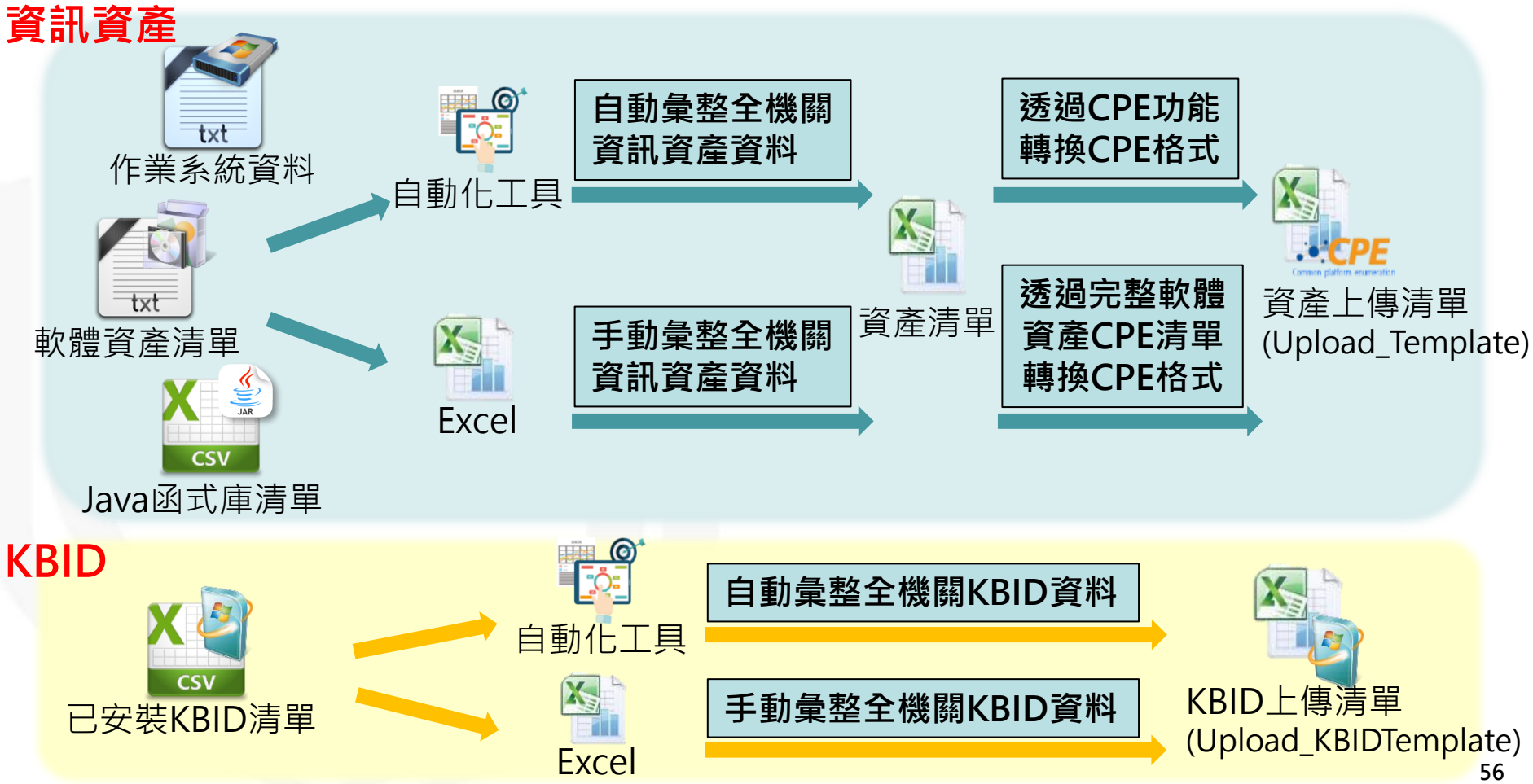
資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

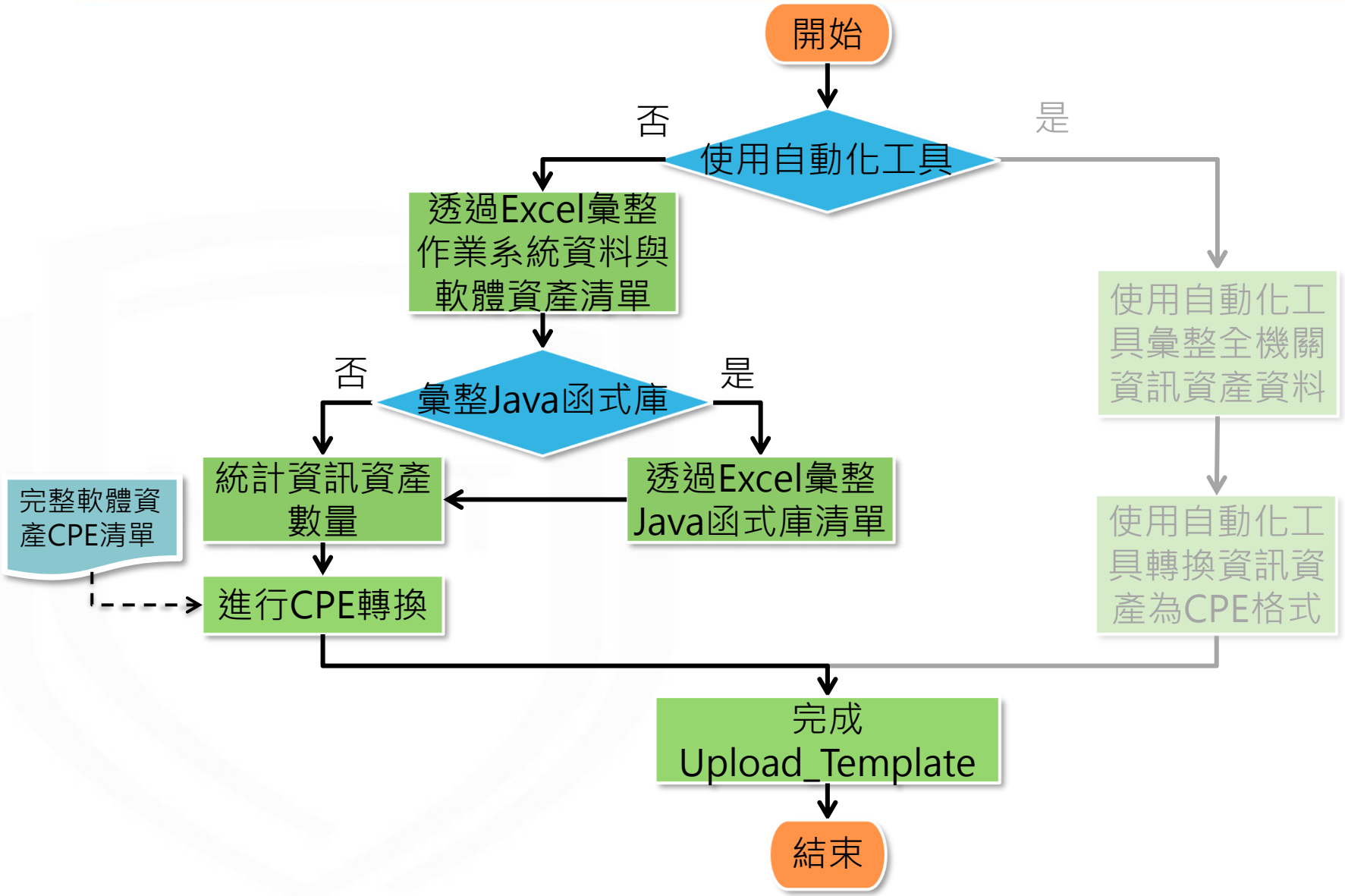
資訊資產與已安裝KBID正規化

- 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

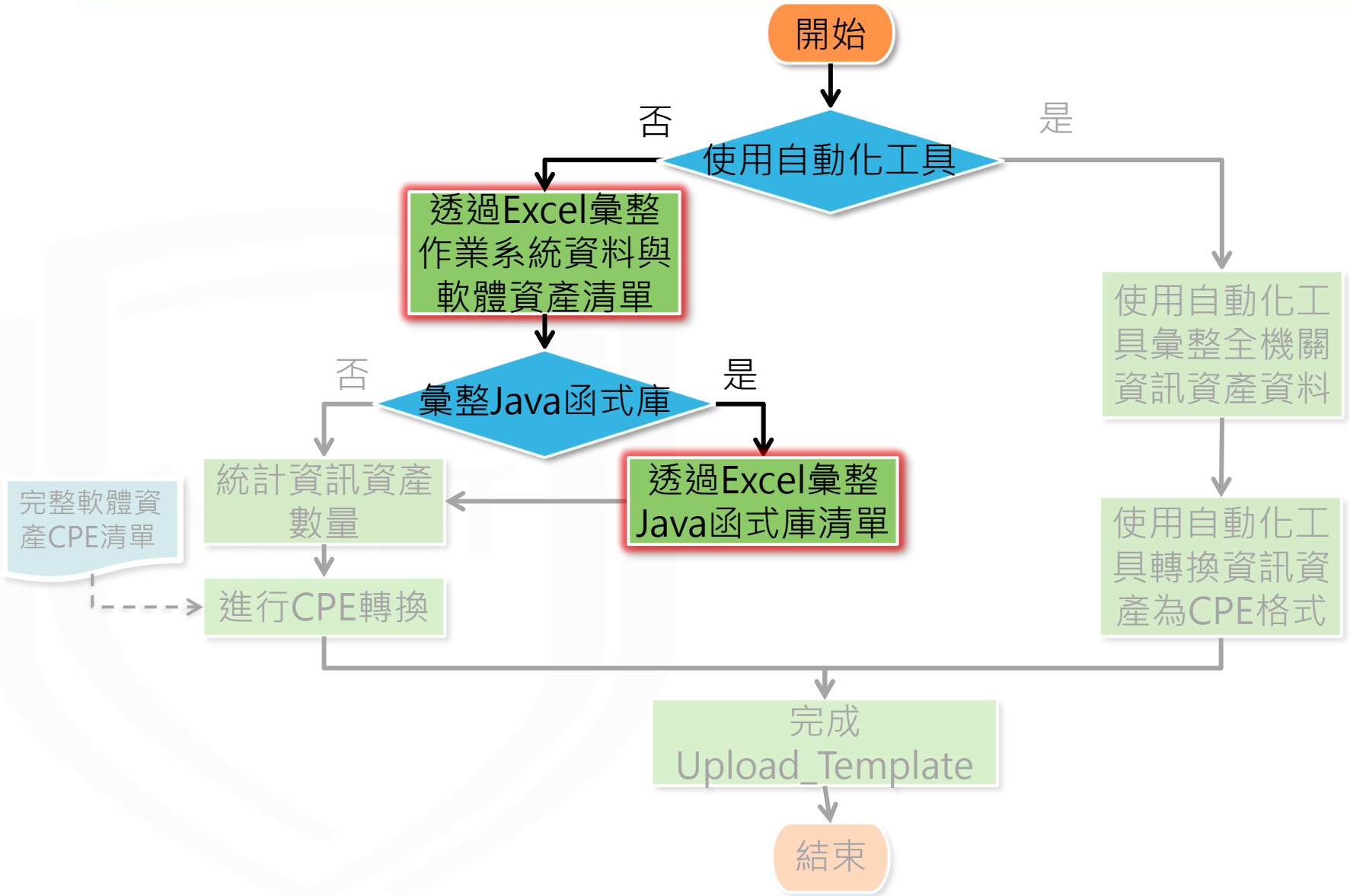


資訊資產正規化作業

資訊資產正規化作業流程



資訊資產正規化作業流程



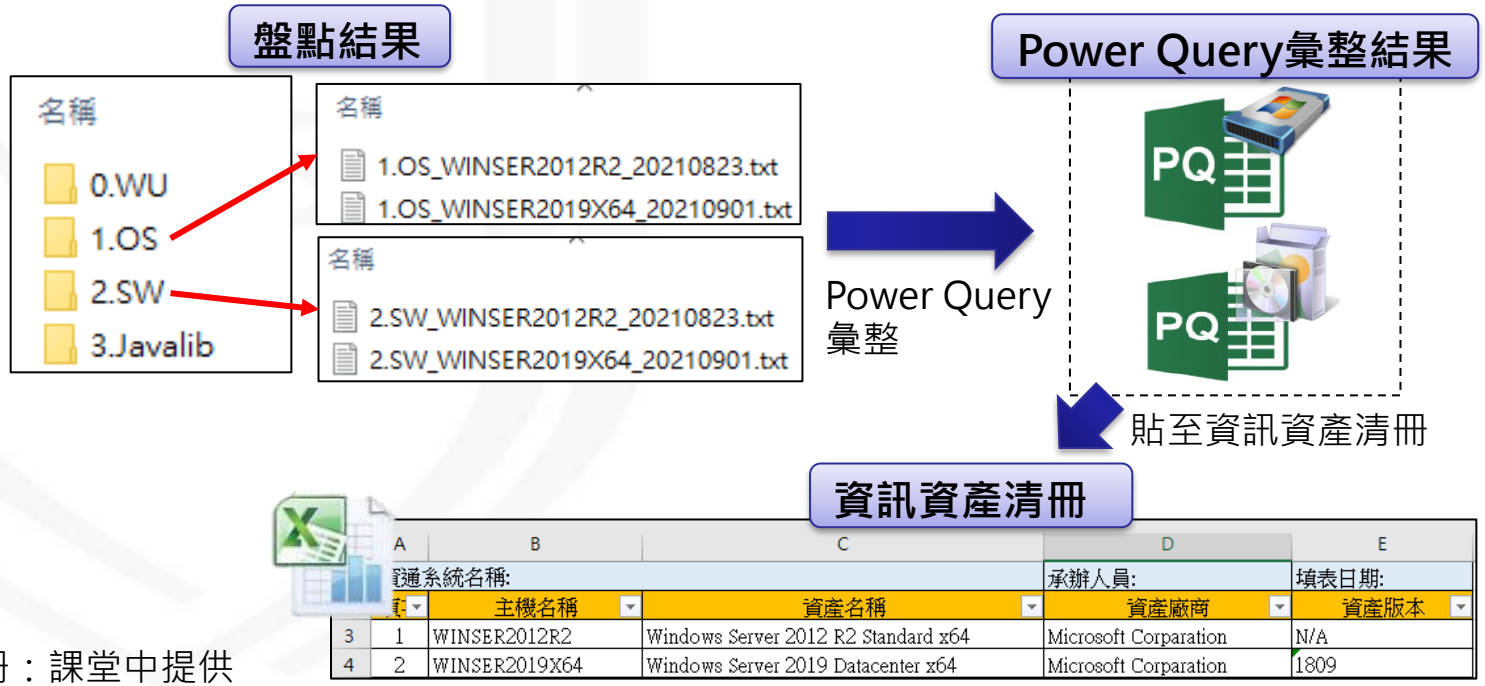
Excel彙整功能介紹

- 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

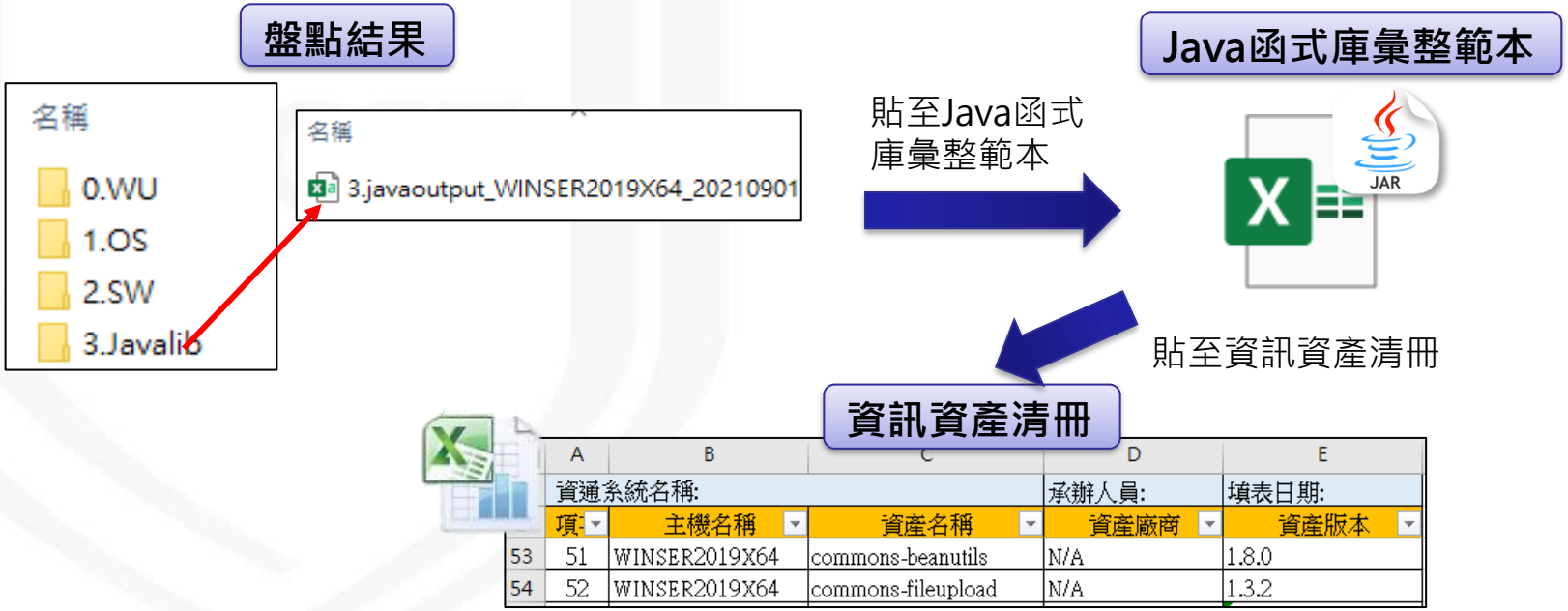
- 透過Power Query分別彙整歸類後作業系統與軟體資產之盤點結果
  - 若欲了解彙整步驟，請參閱「政府機關資安弱點通報系統操作手冊v1.8」
- 將作業系統與軟體資產彙整結果，整合至資訊資產清冊*，以留存查看



*資訊資產清冊：課堂中提供

彙整資訊資產清單_Java函式庫

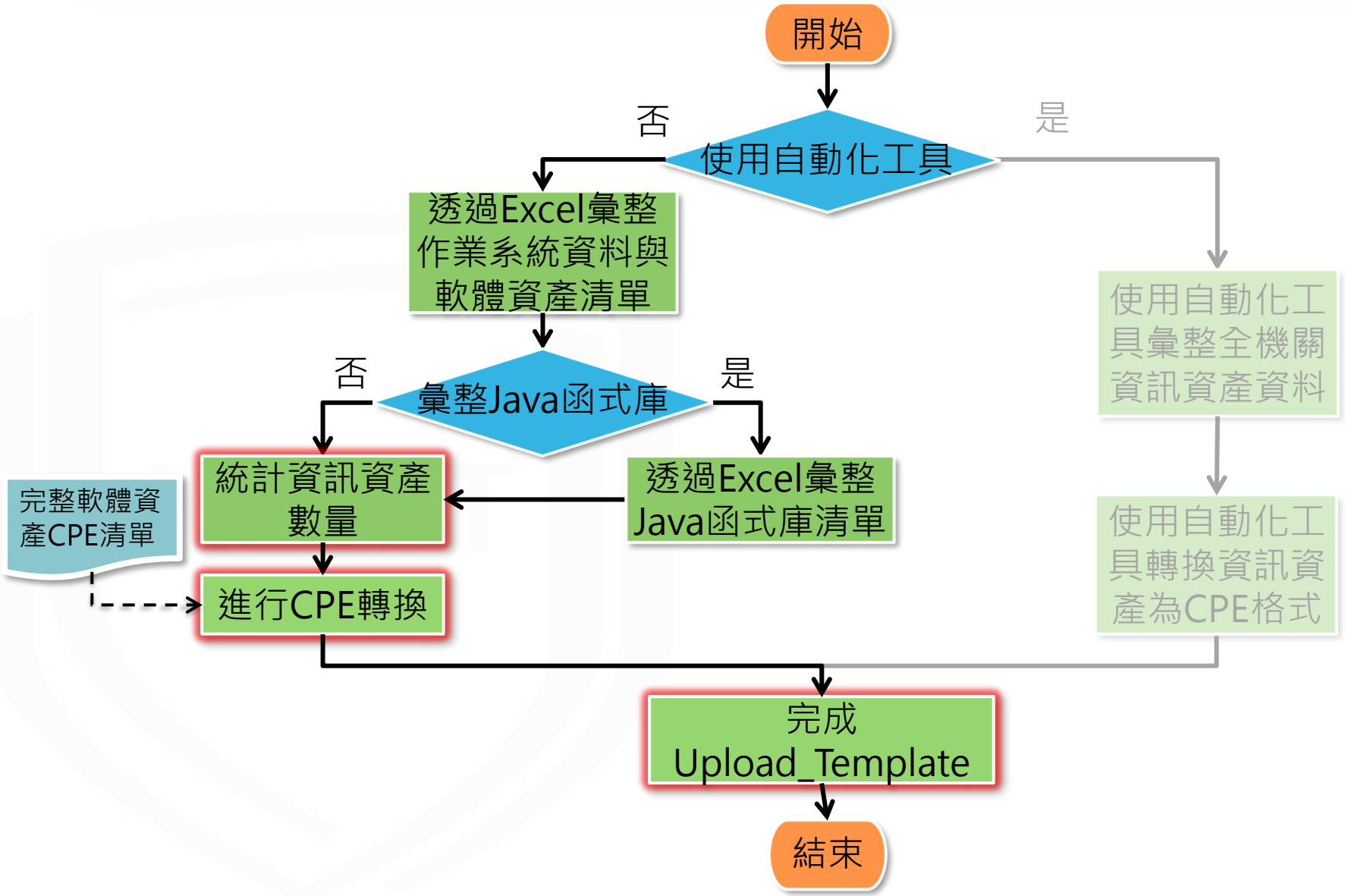
- Java函式庫盤點清單彙整至Java函式庫彙整範本*，以取得Java函式庫名稱與Java函式庫版本
- 將Java函式庫彙整結果，整合至資訊資產清冊*，並補充主機名稱與資產廠商資訊



	A	B	C	D	E
	資通系統名稱:			承辦人員:	填表日期:
	項次	主機名稱	資產名稱	資產廠商	資產版本
53	51	WINSER2019X64	commons-beanutils	N/A	1.8.0
54	52	WINSER2019X64	commons-fileupload	N/A	1.3.2

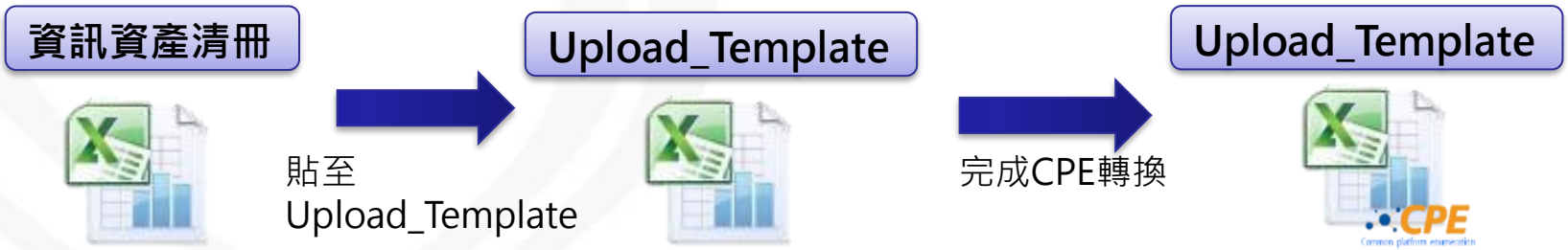
*Java函式庫彙整範本：課堂中提供

資訊資產正規化作業流程



完成Upload_Template

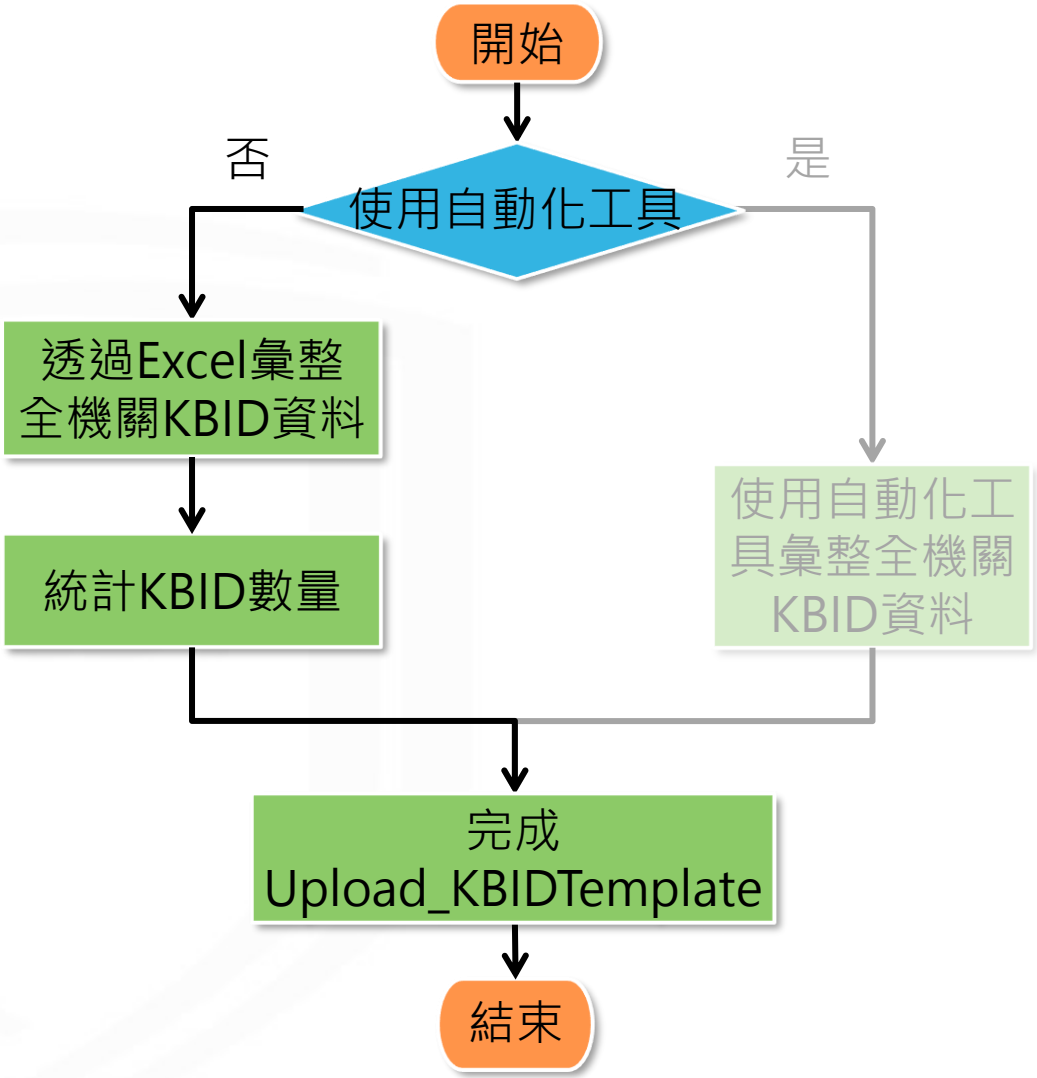
- 統計資訊資產數量
  - 資訊資產清冊自動計算資產數量
  - 利用移除重複項功能，以避免上傳相同之資訊資產
- 進行CPE轉換
  - 將資訊資產清冊彙整至Upload_Template*
  - 於完整軟體資產CPE清單*搜尋，並於Upload_Template填入資訊資產對應之CPE格式，若無則填入N/A
- 完成Upload_Template
  - 填寫機關OID與機關名稱



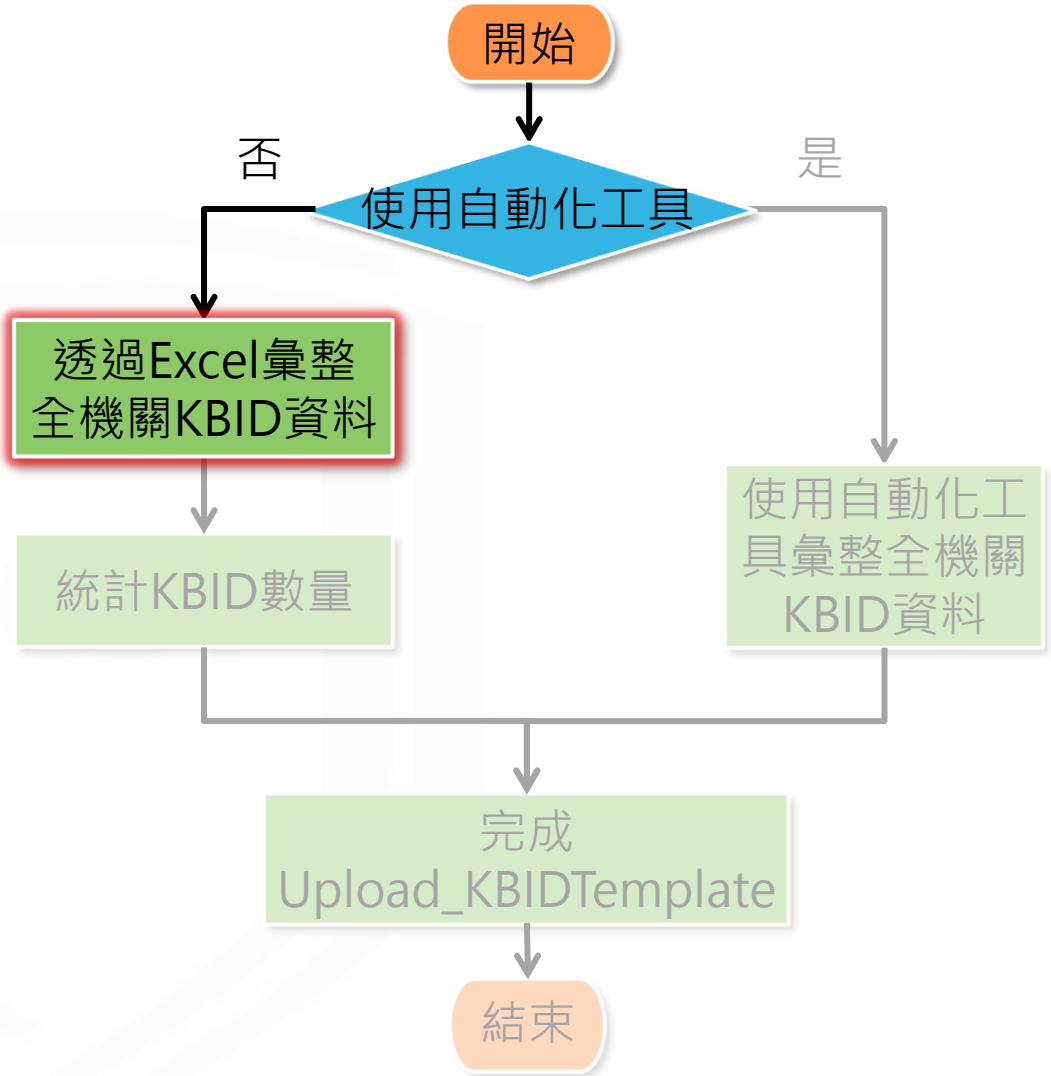
*Upload_Template：於VANS系統下載
*完整軟體資產CPE清單：於VANS系統下載

已安裝KBID正規化作業

已安裝KBID正規化作業流程

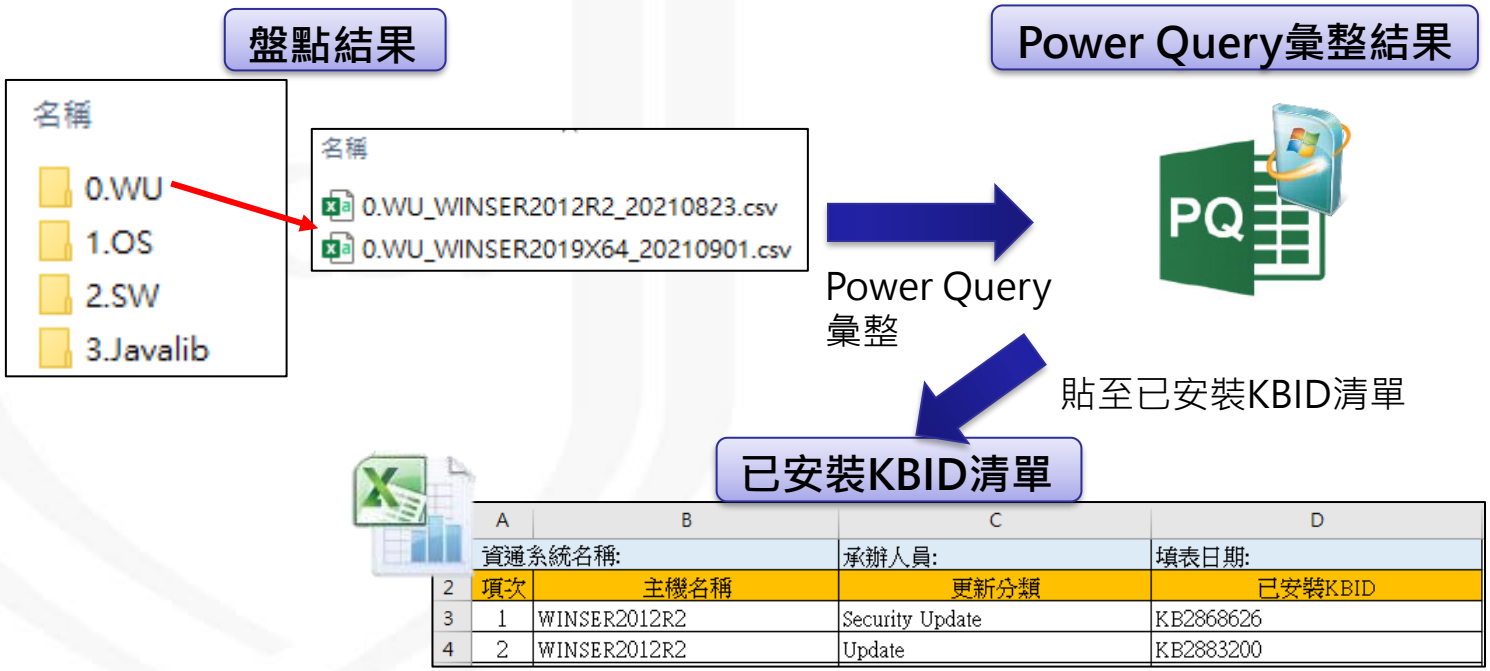


已安裝KBID正規化作業流程



彙整KBID清單

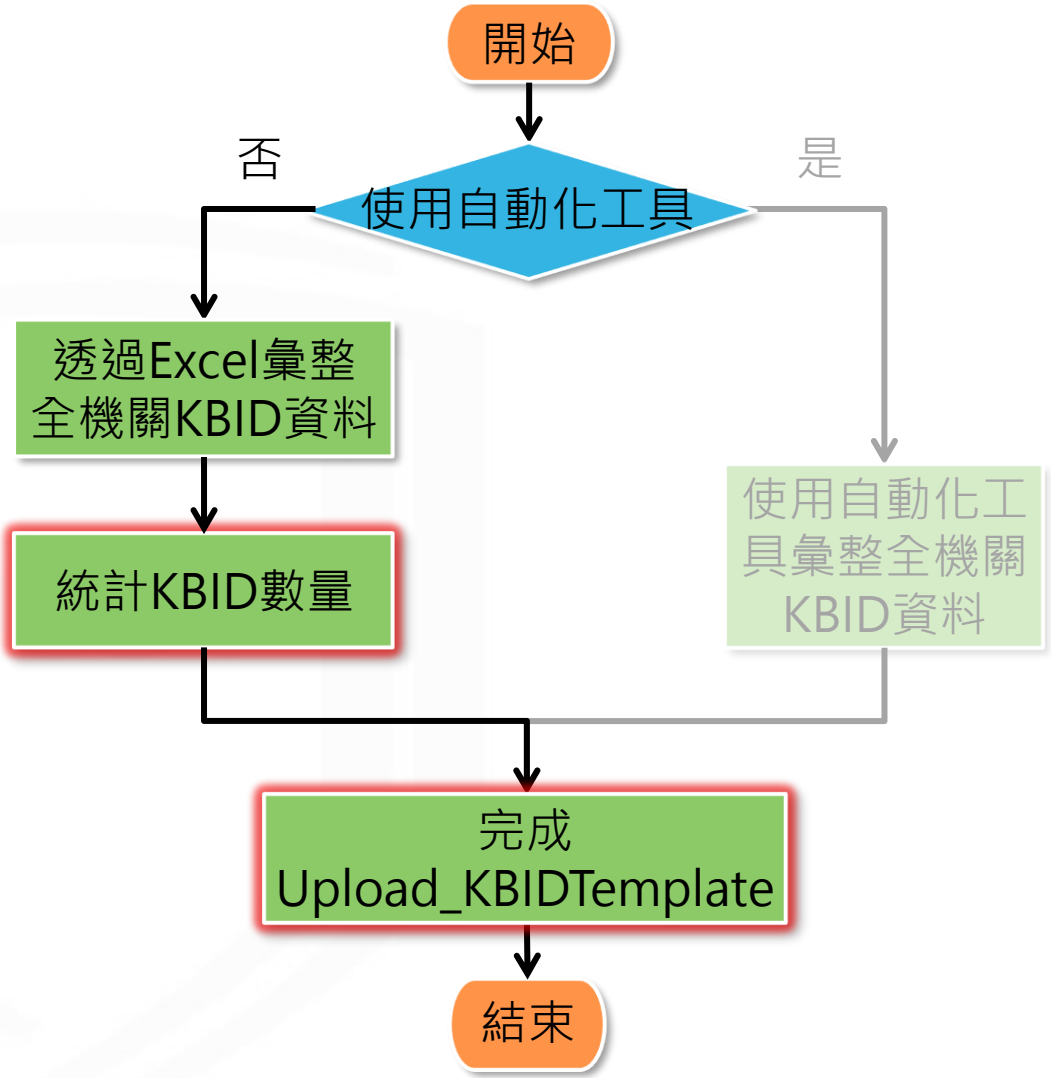
- 透過Power Query彙整歸類後已安裝KBID之盤點結果
  - 若欲了解彙整步驟，請參閱「政府機關資安弱點通報系統操作手冊v1.8」
- 將已安裝KBID彙整結果，整合至已安裝KBID清單*，以留存查看



	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

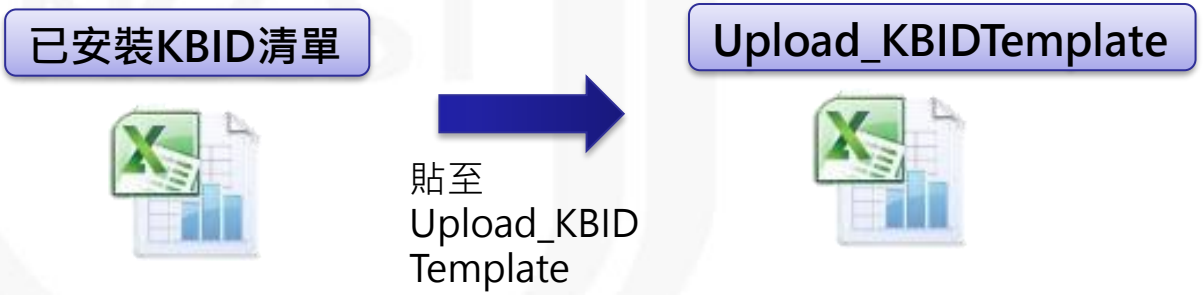
*已安裝KBID清單：課堂中提供

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*
  - 填寫機關OID與機關名稱



*Upload_KBIDTemplate：於VANS系統下載

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
  - **首次登入設定**
    - **通知設定**：ON
    - **分數設定**：4.0
    - **電子郵件設定**：請輸入欲接收弱點通知之電子郵件
  - **機關資訊**
    - **機關OID**：student01~45
    - **機關名稱**：student01~45

實作練習1

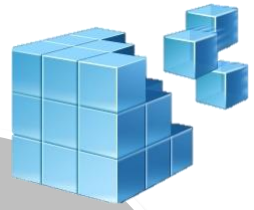
- 請將「實作練習1」提供之Upload_Template與Upload_KBIDTemplate完成正規化作業
- 本項練習時間20分鐘

項次	參考頁數	執行項目	產出項目/執行結果
1	P.63	登入VANS系統下載完整資產CPE清單	完整資產CPE清單
2	P.63	開啟Upload_Template (路徑：學員資料夾\01.實作練習\實作練習1\Upload_Template.xlsx) • 針對前3筆軟體資產進行正規化 • 針對前3筆Java函式庫清單進行正規化 • 完成Upload_Template	Upload_Template
3	P.69	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) • 完成KBID上傳清單	Upload_KBIDTemplate.xlsx

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

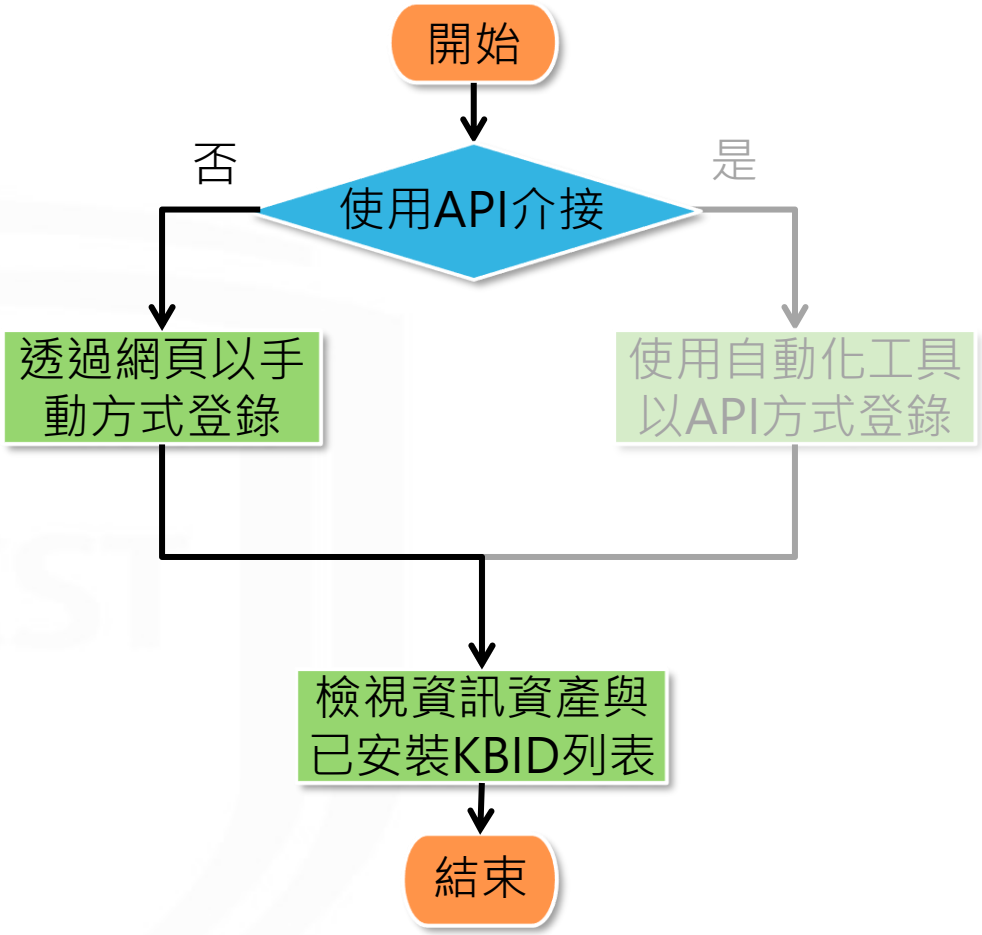


資訊資產與
已安裝KBID
正規化作業

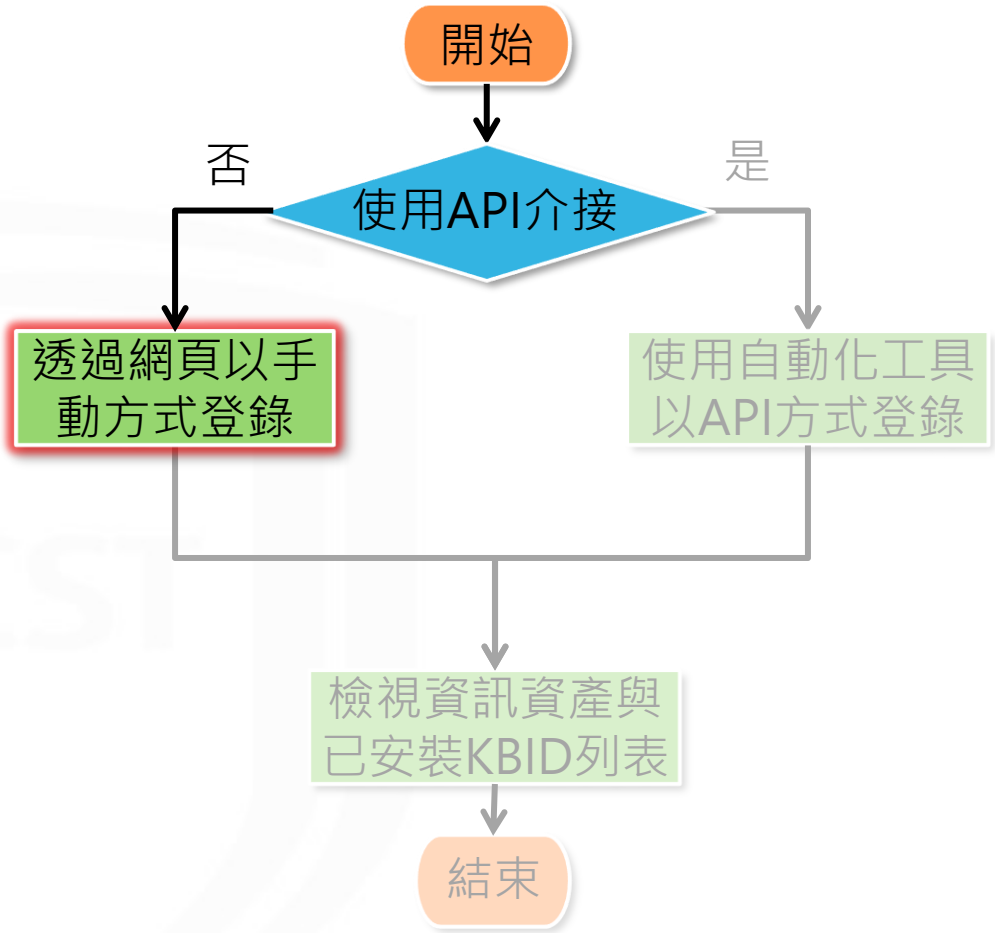
資訊資產與
已安裝KBID
登錄作業

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)

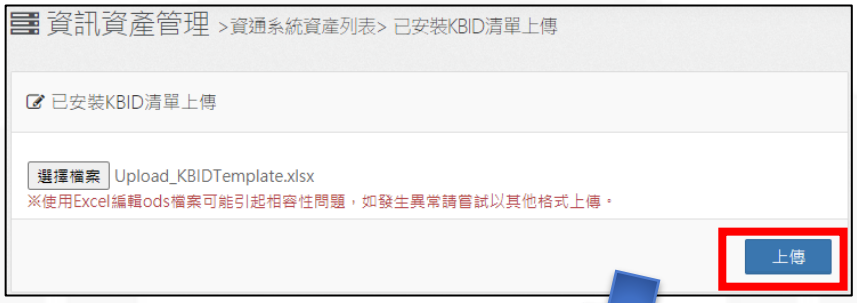
- STEP3：點選「上傳」，等待系統解析清單
- STEP4：待收到解析完成通知信，即完成登錄

網頁登錄-已安裝KBID(1/2)

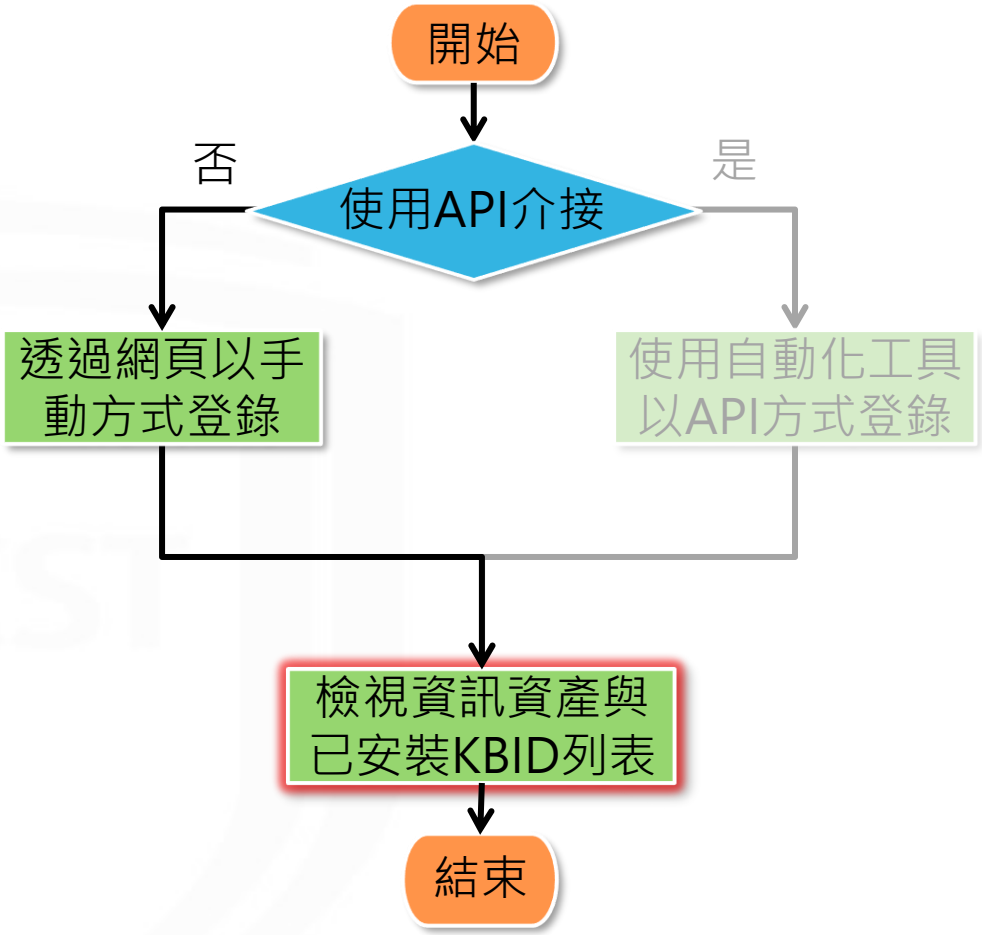
- STEP1：於VANS系統進行已安裝KBID清單上傳
  - 資訊資產管理>資通系統資產列表/使用者電腦資產列表
- STEP2：瀏覽並上傳已完成之上傳清單

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



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

- 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

實作練習2

實作練習2

- 請將「實作練習1」建立之Upload_Template執行登錄作業
- 本項練習時間5分鐘

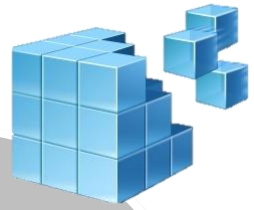
項次	參考頁數	執行項目	產出項目/執行結果
1	P.76~77	上傳Upload_Template至VANS系統	於資產列表檢視登錄資產

使用自動化工具

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



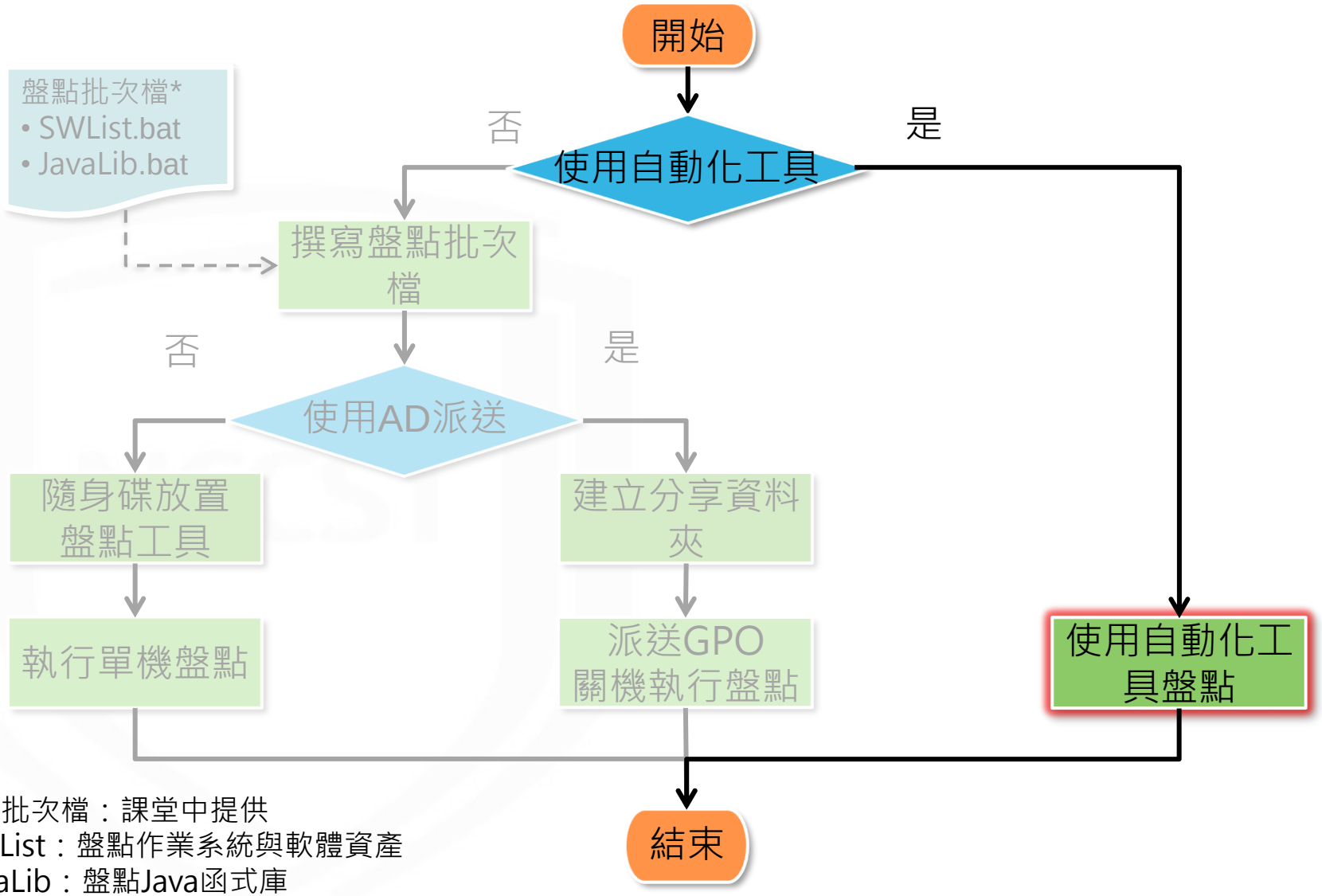
資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

資訊資產與
已安裝KBID
更新作業

自動化工具

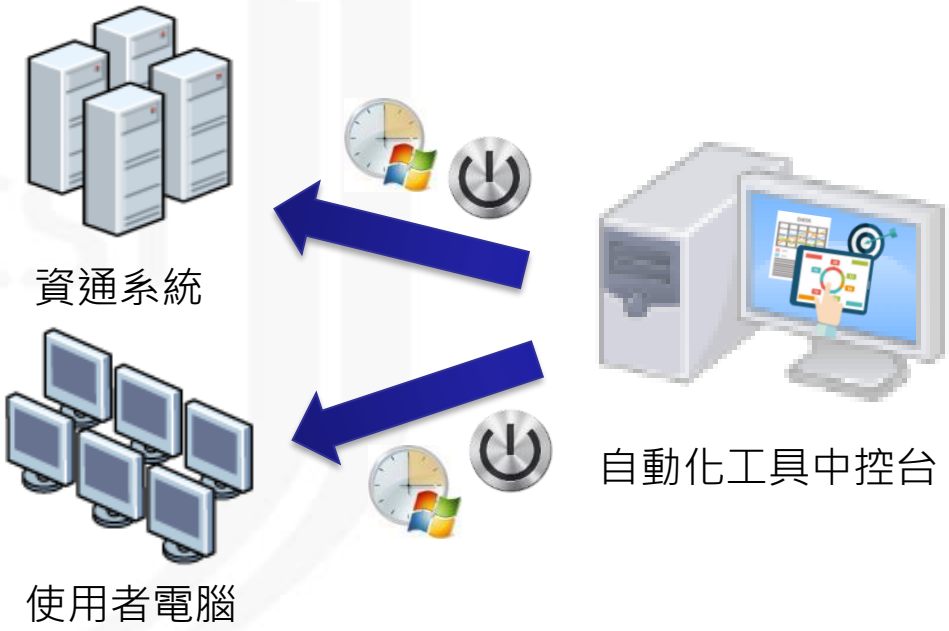
盤點作業流程



*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
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

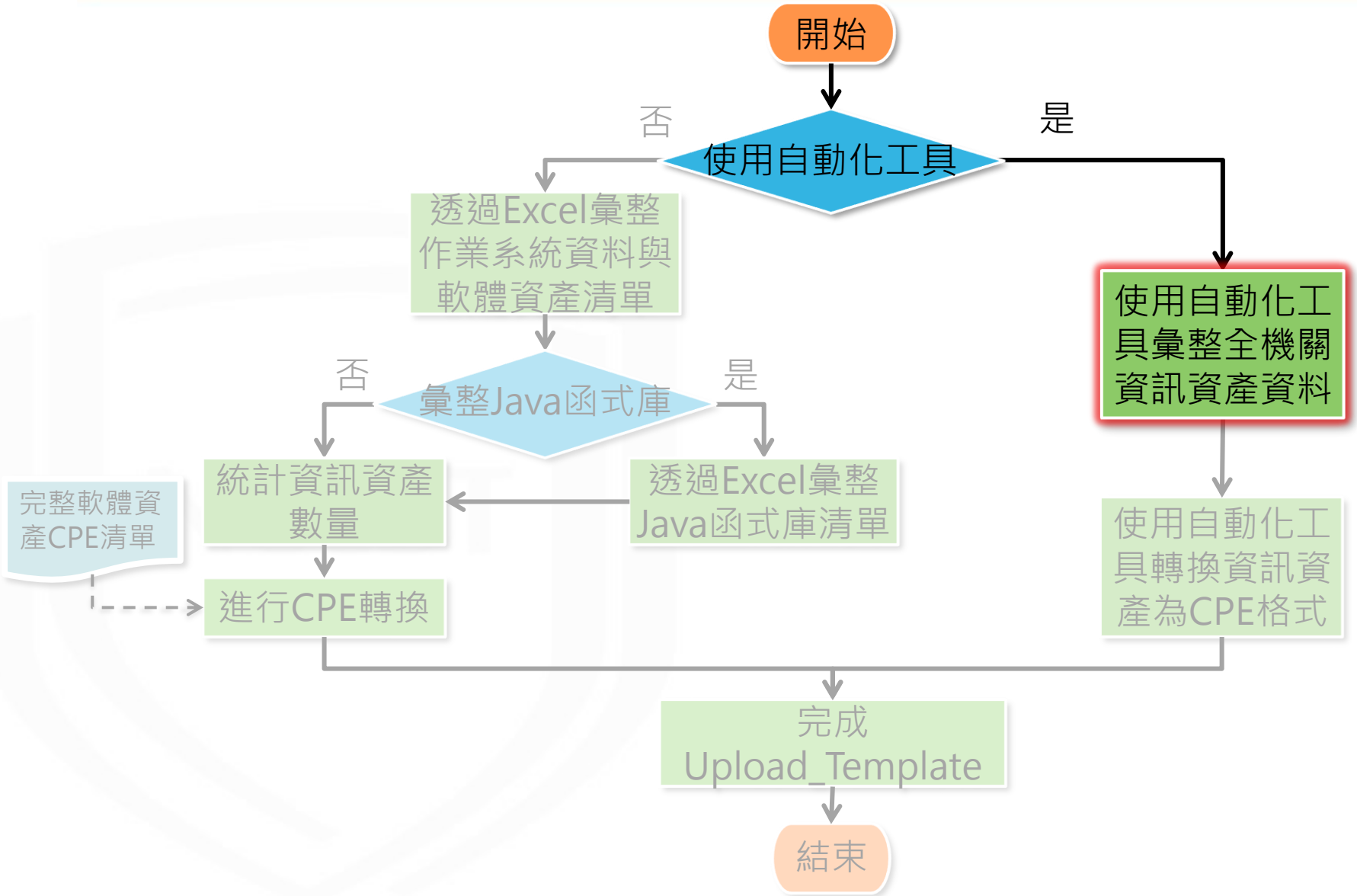
自動化工具

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

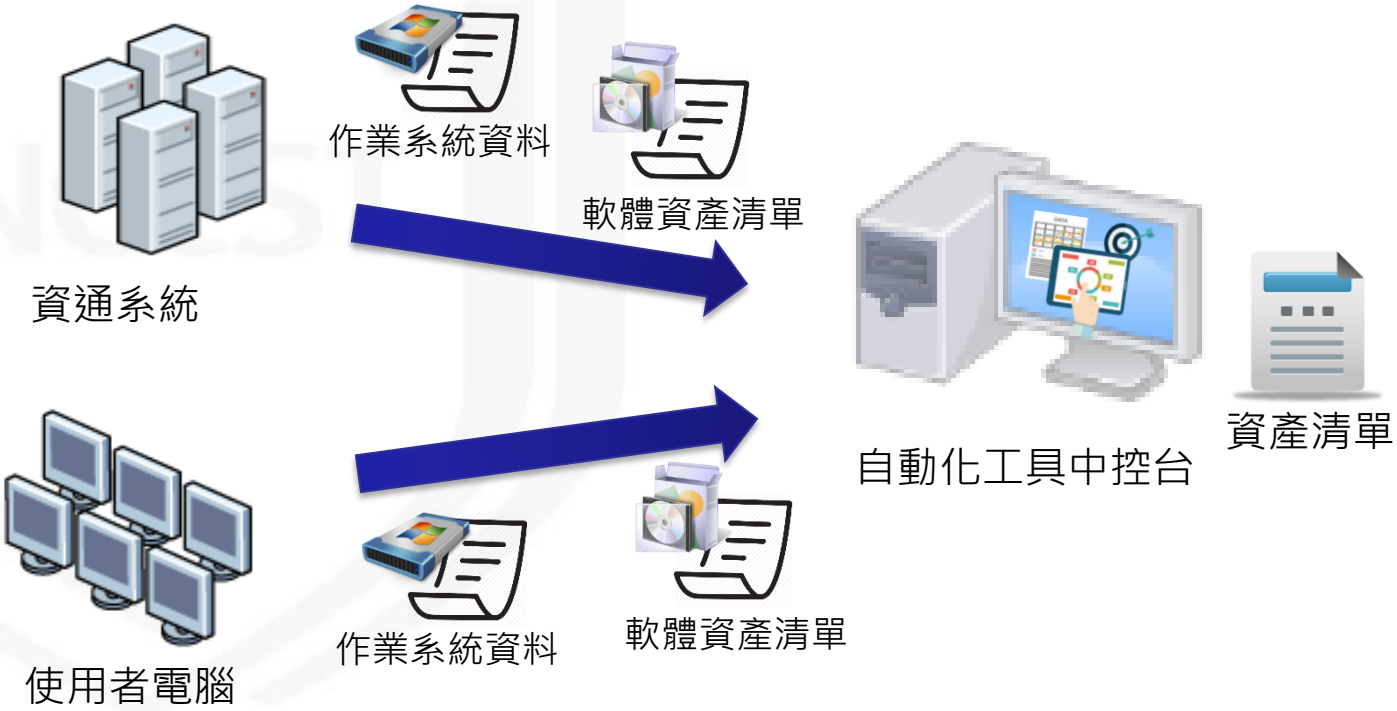
資訊資產正規化作業
(自動化工具)

資訊資產正規化作業流程

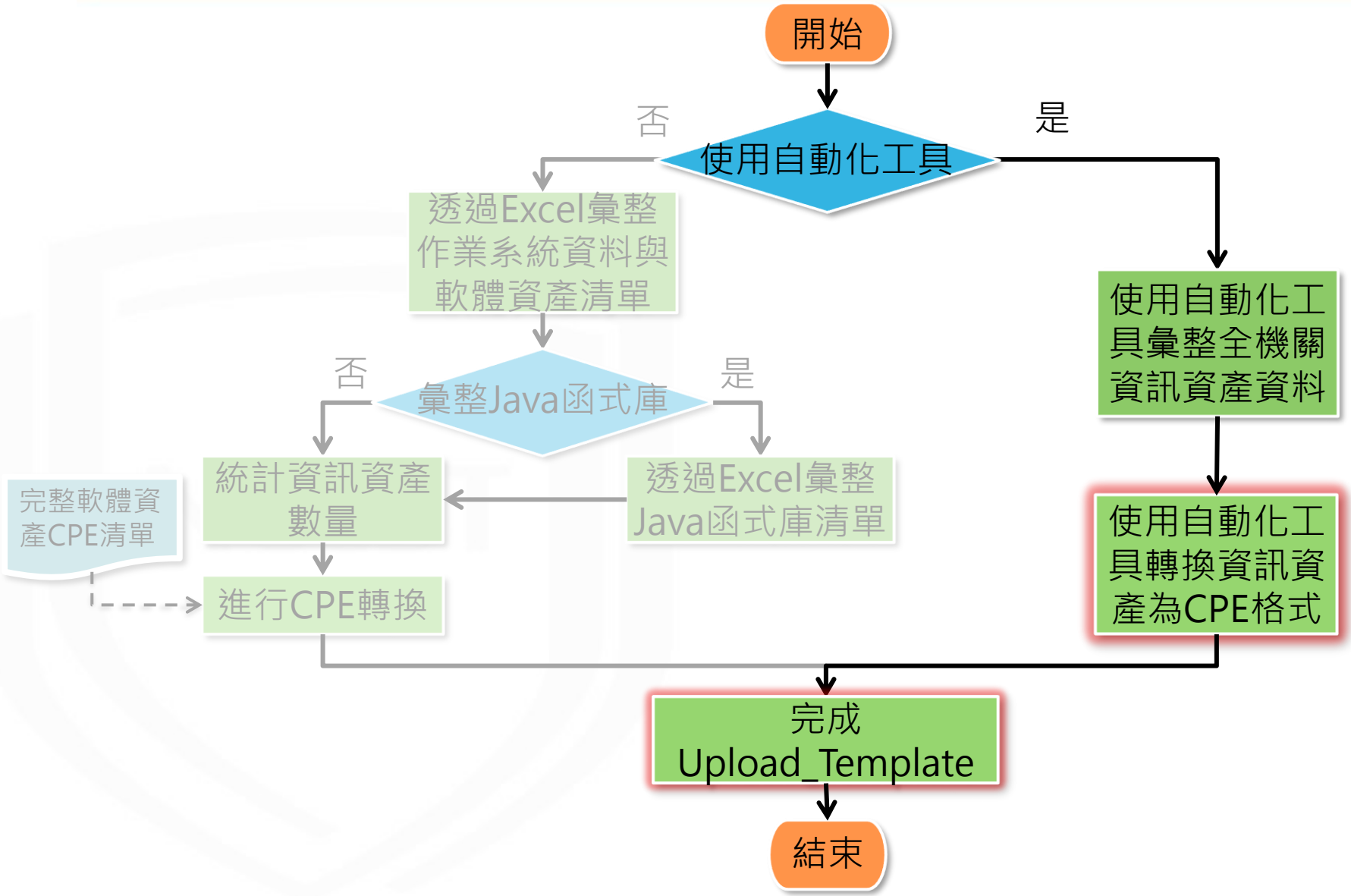


使用自動化工具彙整資訊資產

- 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

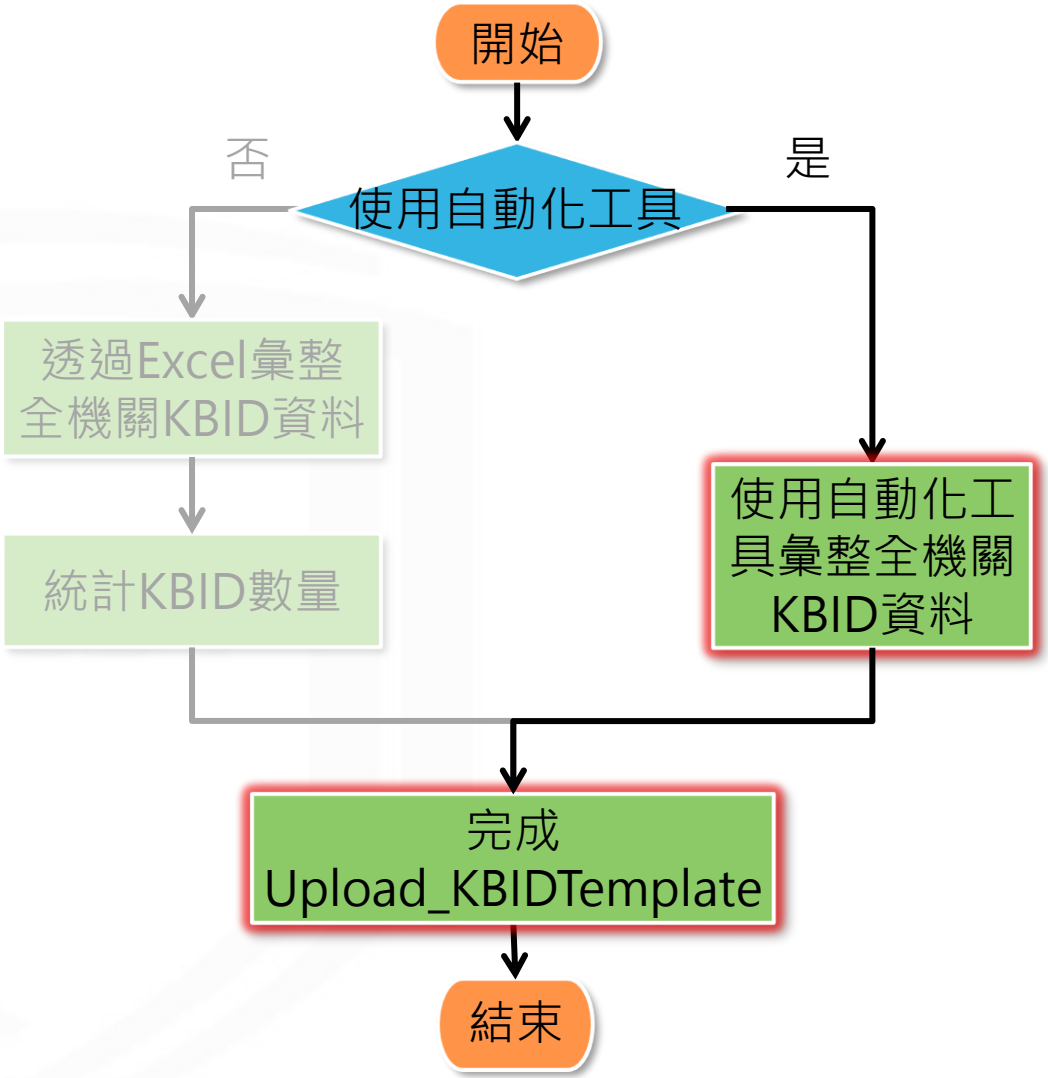


使用自動化工具轉換資訊資產格式

- 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

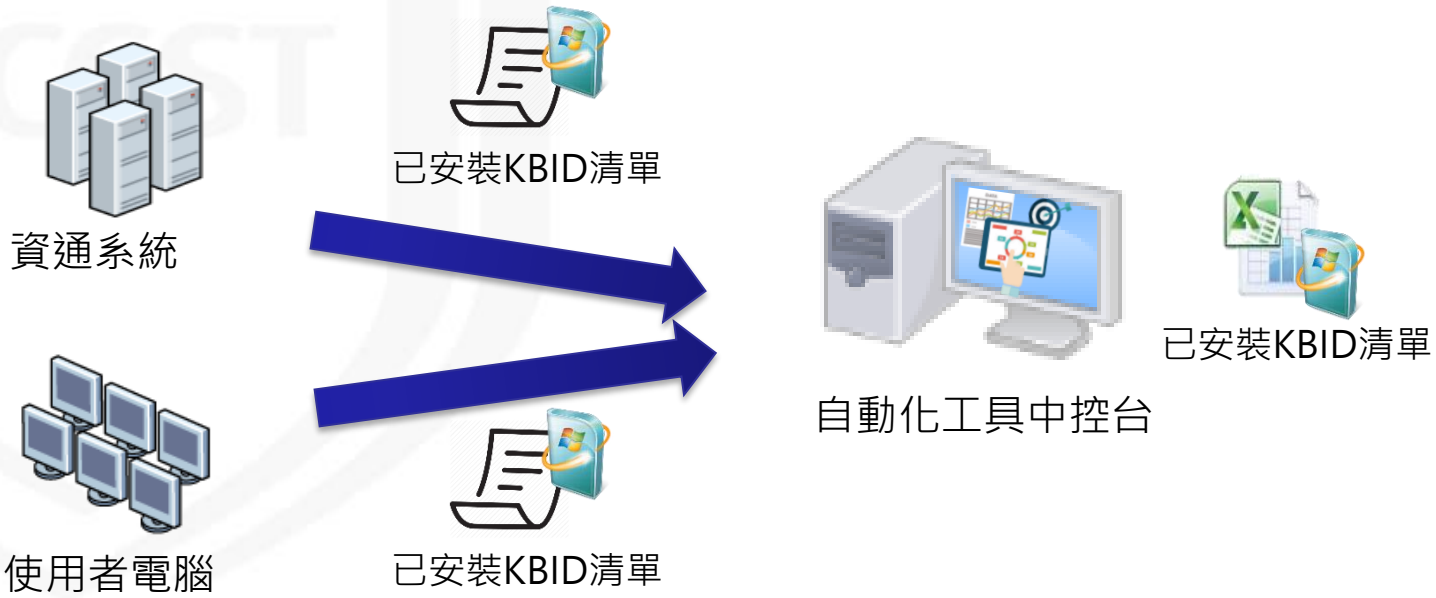
已安裝KBID正規化作業
(自動化工具)

已安裝KBID正規化作業流程



使用自動化工具彙整已安裝KBID

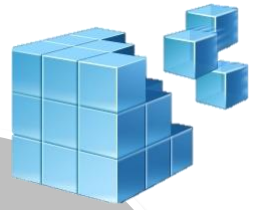
- 自動化蒐集與彙整資通系統與使用者電腦之已安裝KBID
- 透過排程定時回傳盤點結果予自動化工具中控台
- 自動去識別化整併為全機關已安裝KBID清單，並提供反查對照功能，便於機關管理已安裝KBID清單
- 完成已安裝KBID清單



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



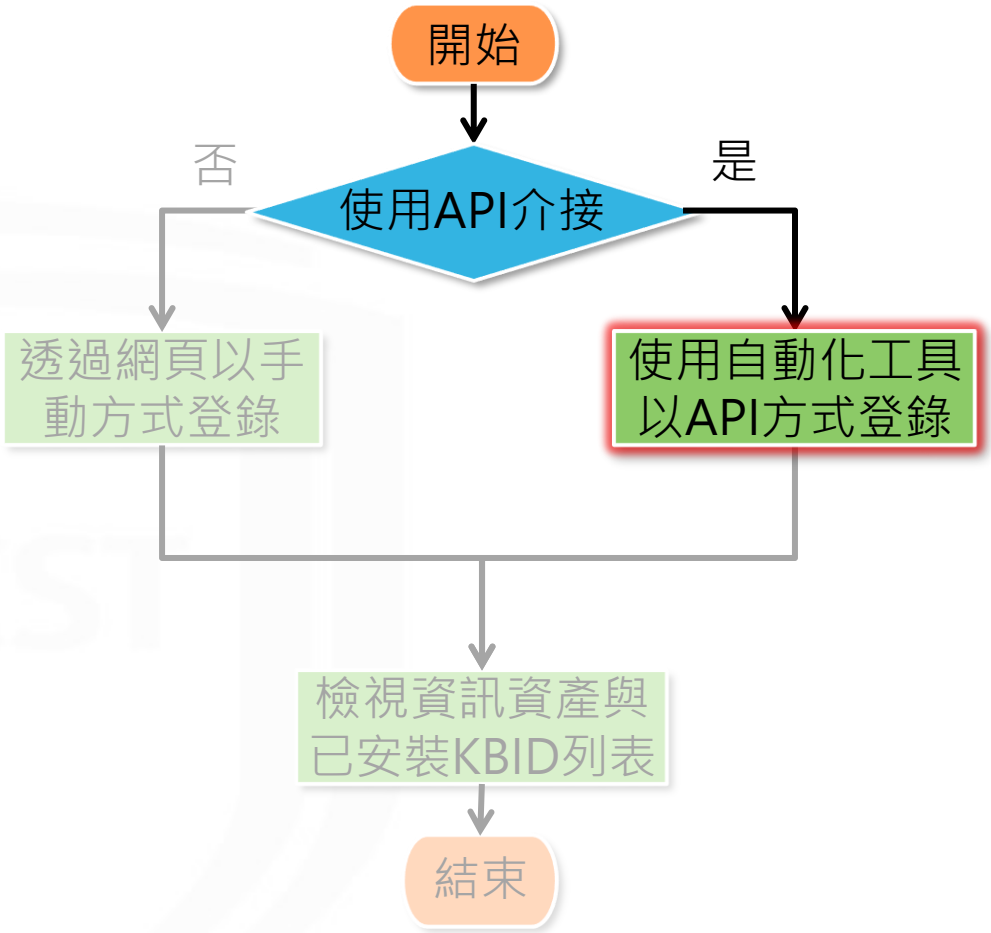
資訊資產與
已安裝KBID
正規化作業

自動化工具

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

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，完成後提供資安處審核(https://www.nccst.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

主旨(U)　【VANS】政府機關資安弱點通報系統API介接申請審核結果通知

附件(T)　VANS_API_Sample.json .json 檔案　VANS API操作說明.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：
資通系統(System)：
https://vans.nccst.nat.gov.tw/[redacted]
使用者電腦(Computer)：
https://vans.nccst.nat.gov.tw/[redacted]

3.VANS API 操作說明與 JSON 範例提供如附檔。

API Key

機關資訊

API傳輸網址

自動化工具

JSON CPE

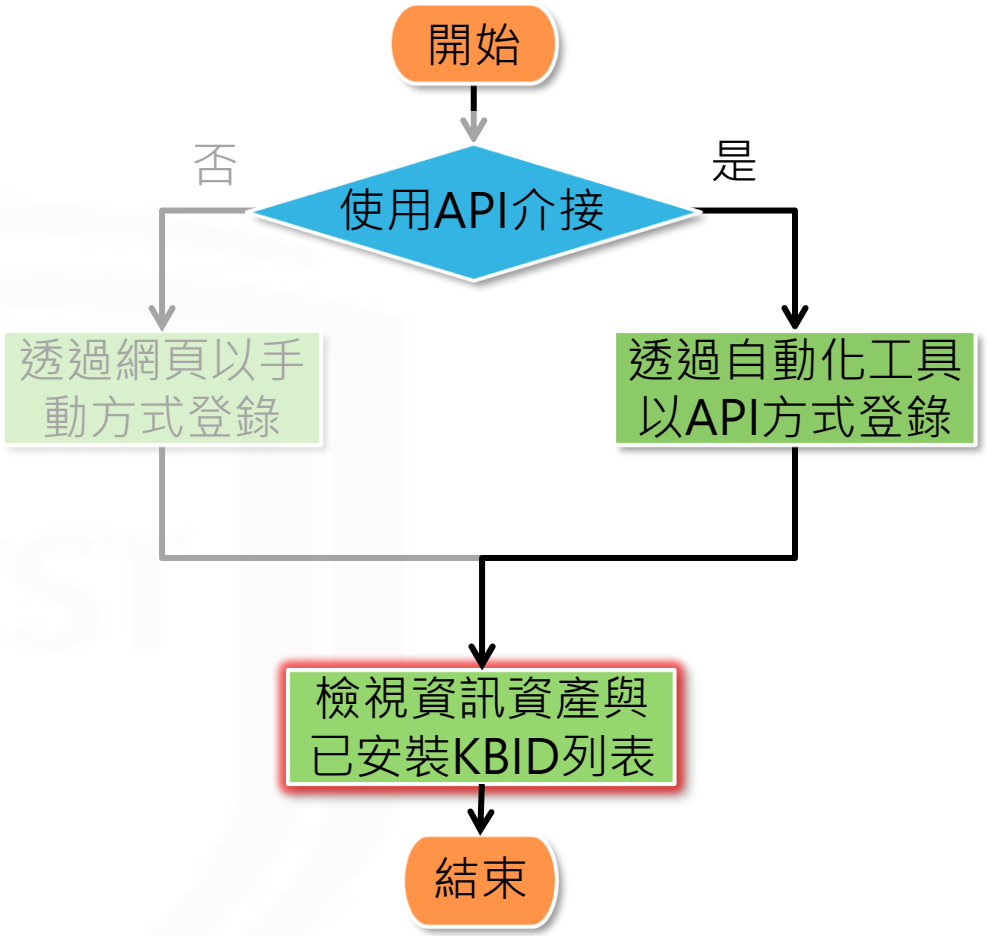
JSON

VANS

NCCST

VANS系統

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
透過自動化工具以API方式登錄
檢視資訊資產與已安裝KBID列表
結束

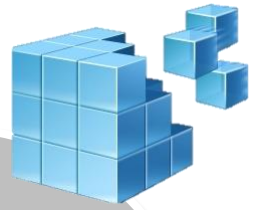
檢視資訊資產與已安裝KBID列表

- 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

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

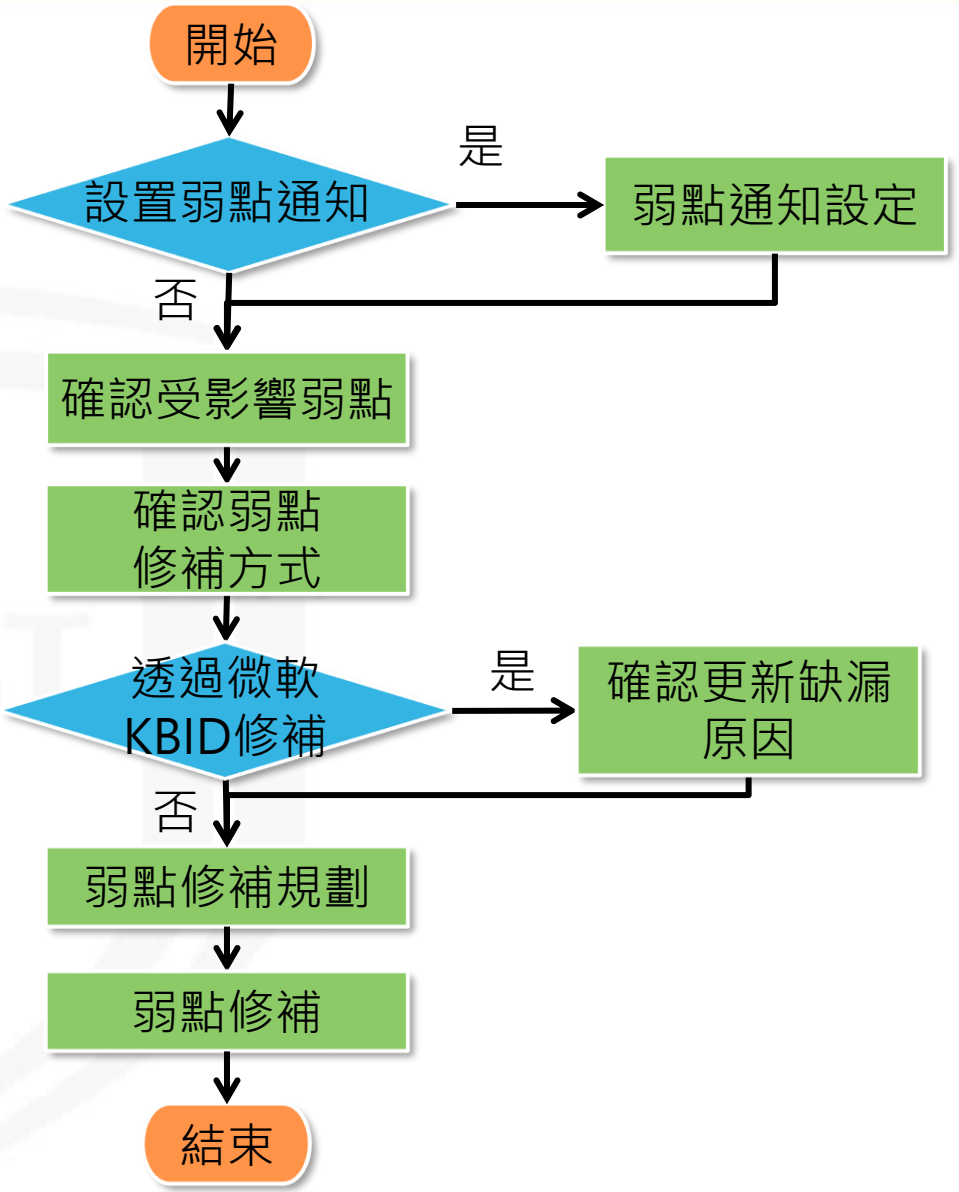


資訊資產與
已安裝KBID
正規化作業

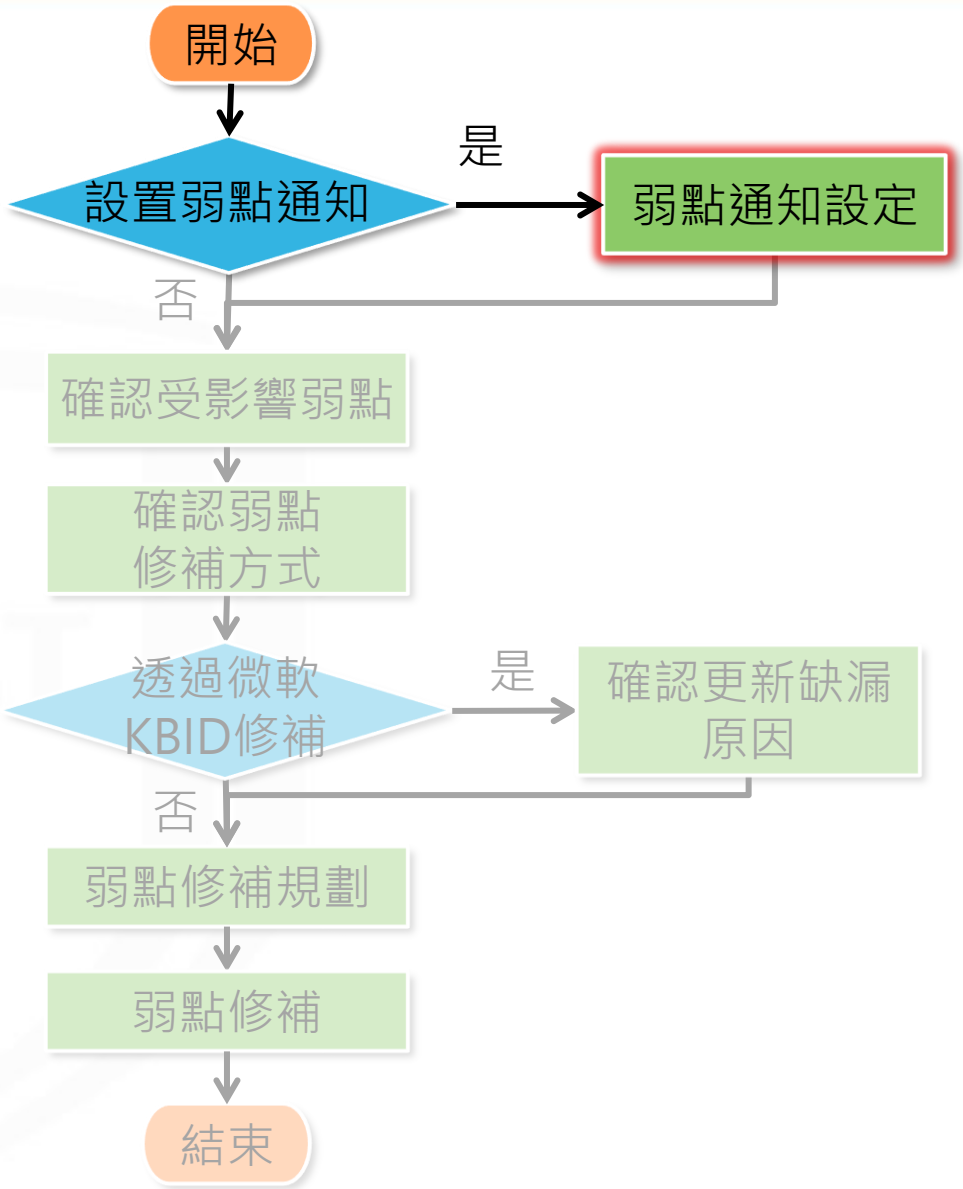
資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

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

敬啟者 您好：
此為「政府機關資安弱點通報系統」之通知郵件。

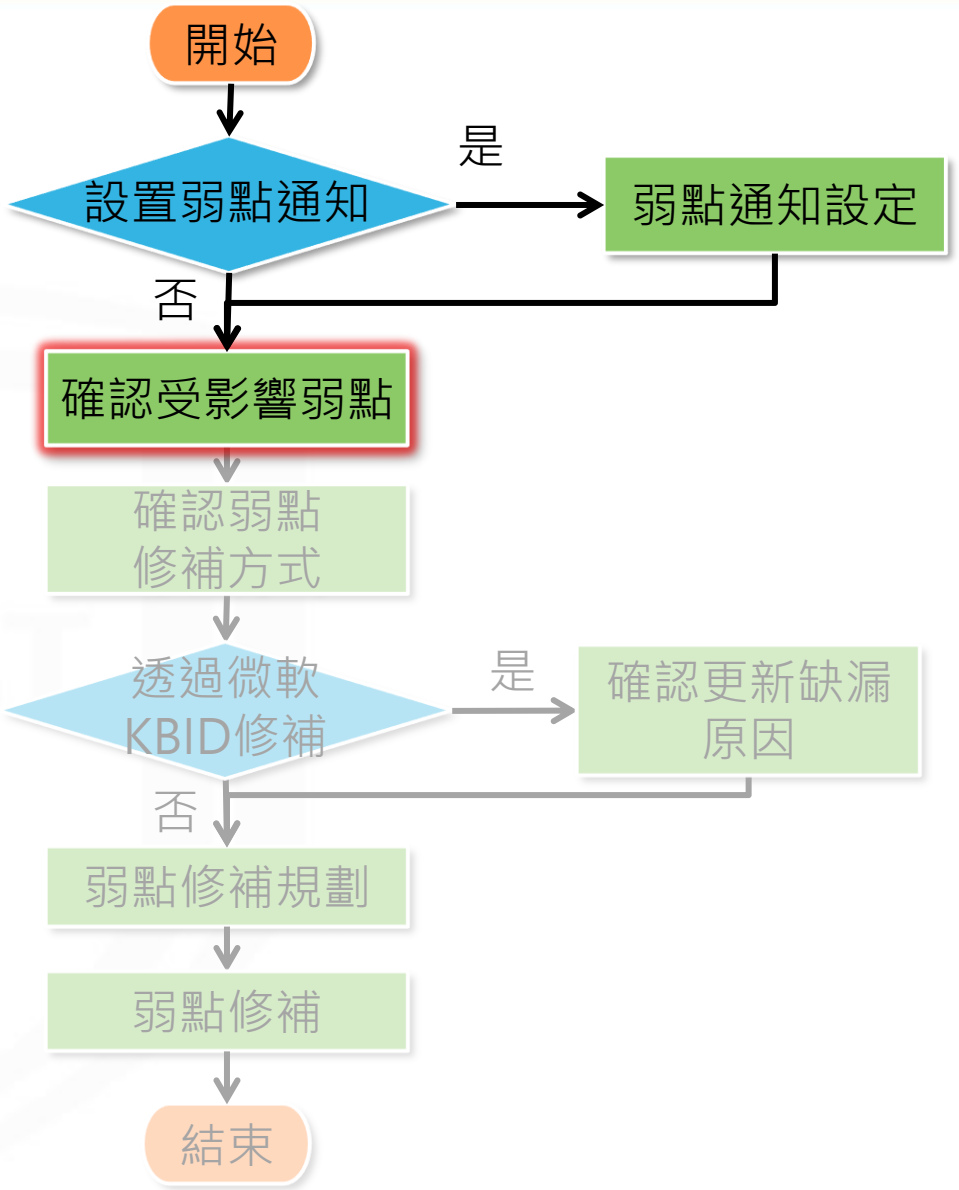
貴機關之所以收到此通知信件，在於貴機關於 VANS 系統所登錄之資訊資產，
經過系統比對弱點資料庫後，發現存有風險項目，建議貴機關對資訊資產風險進行修補，以避免資安風險。
修補作業完成後，再煩請貴機關至 VANS 系統進行資訊更新，以協助本中心掌握修補情況。
謝謝。

VANS 系統網頁連結：
https://vans.nccst.nat.gov.tw/

如有任何疑問，聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

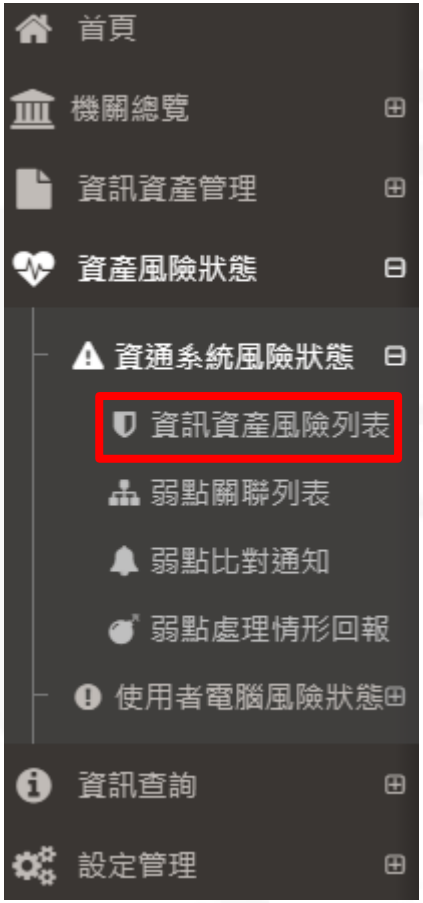
- 同一項資產的同一個弱點只會於首次比對到時進行1次通知，之後不會再出現相同之弱點通知

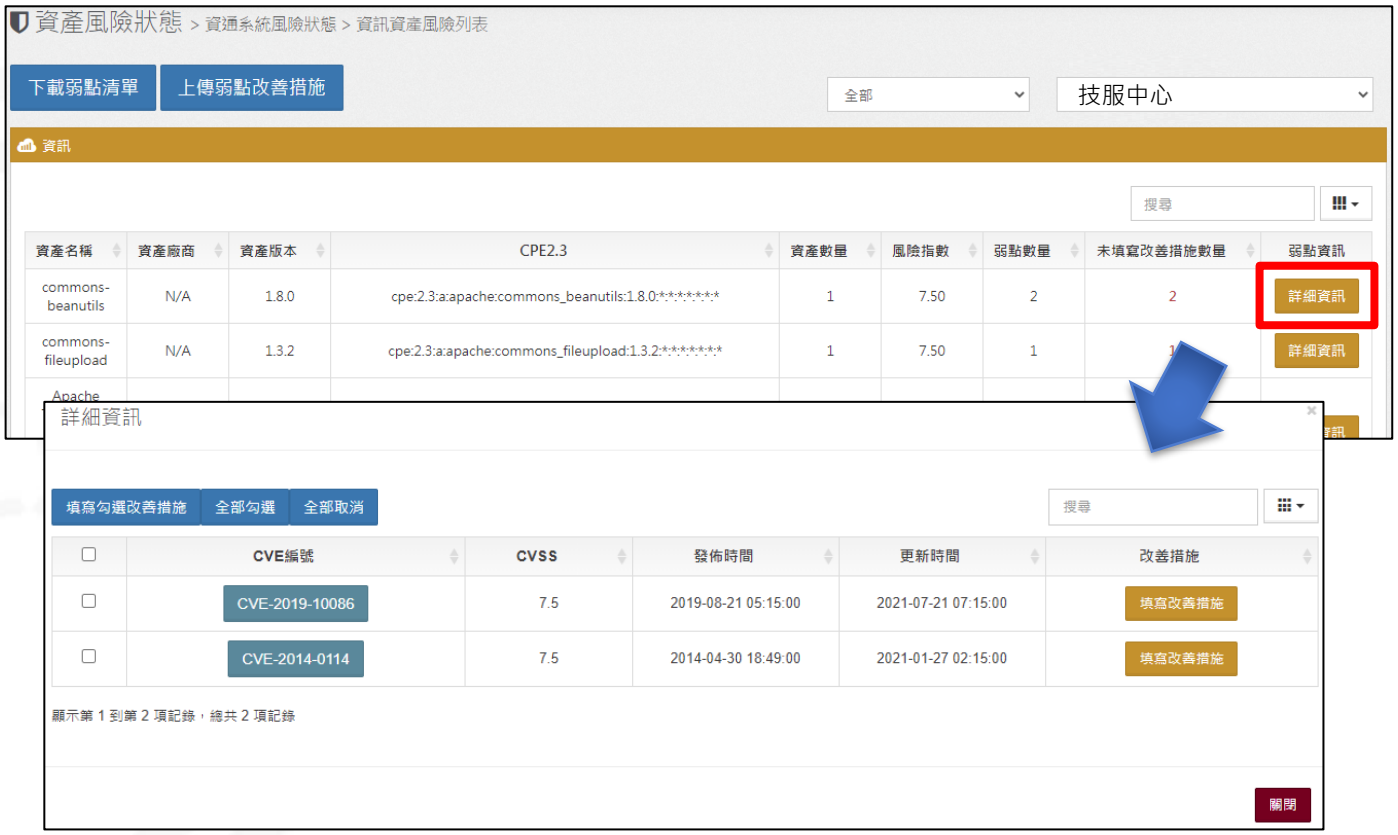
弱點通知與修補規劃作業流程



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

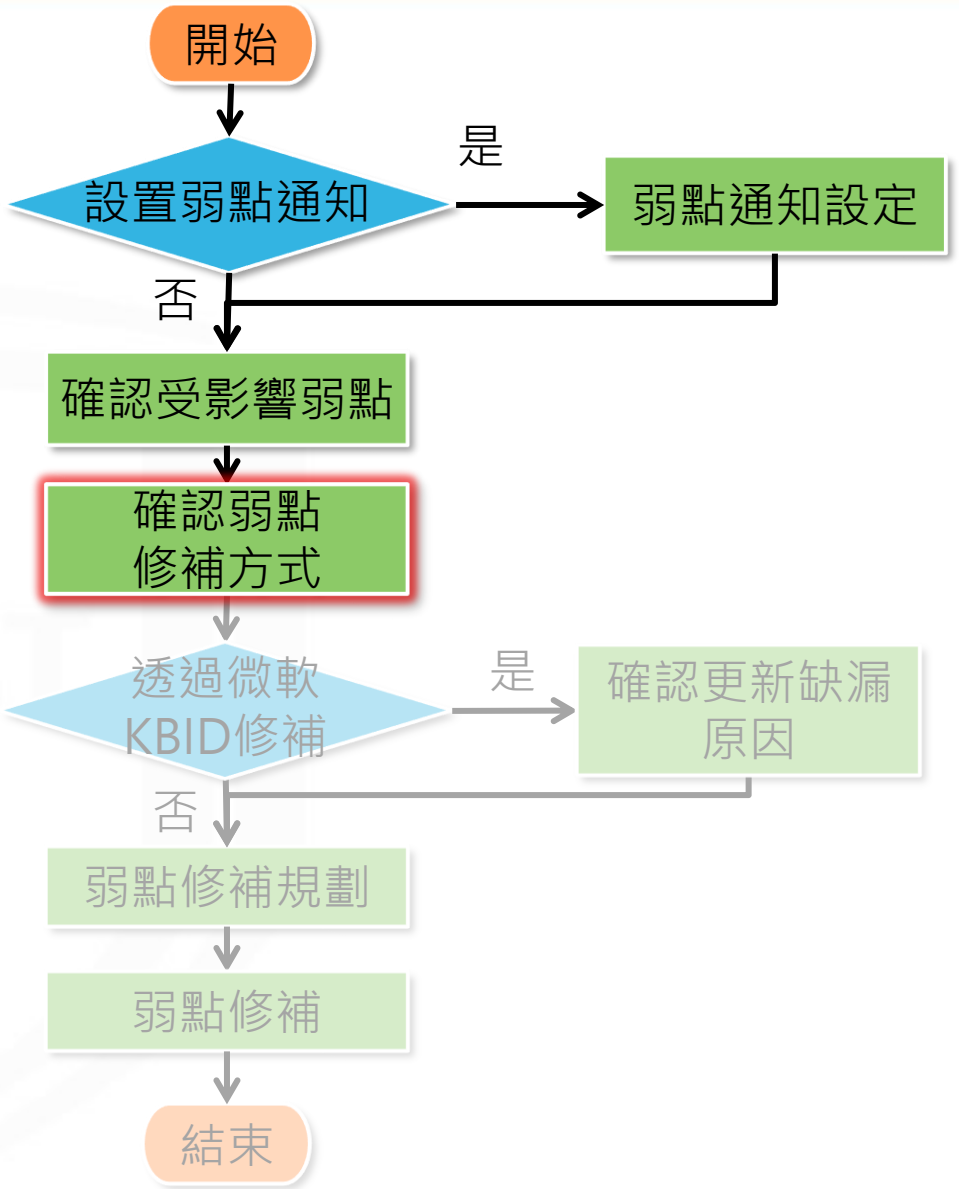




確認受影響弱點–弱點關聯列表

- 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

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

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

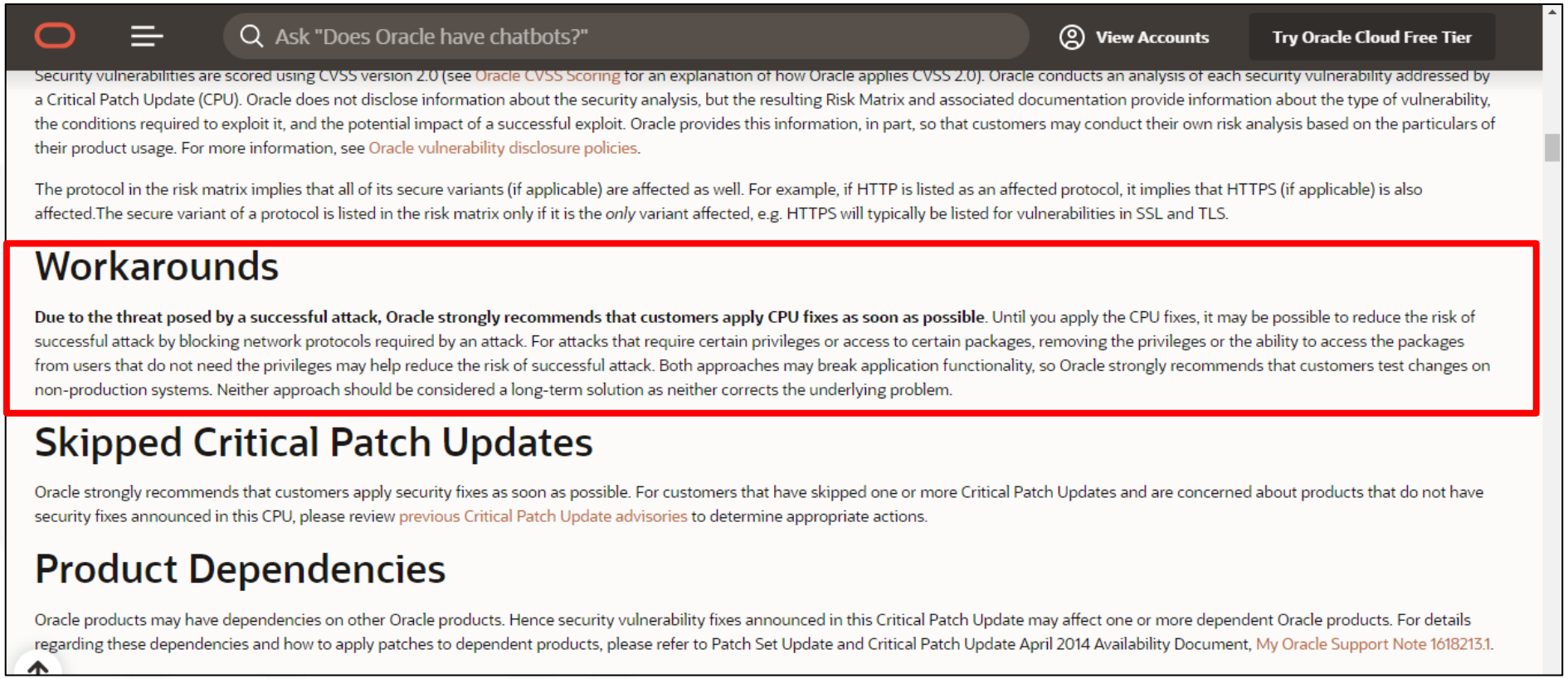
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites 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)

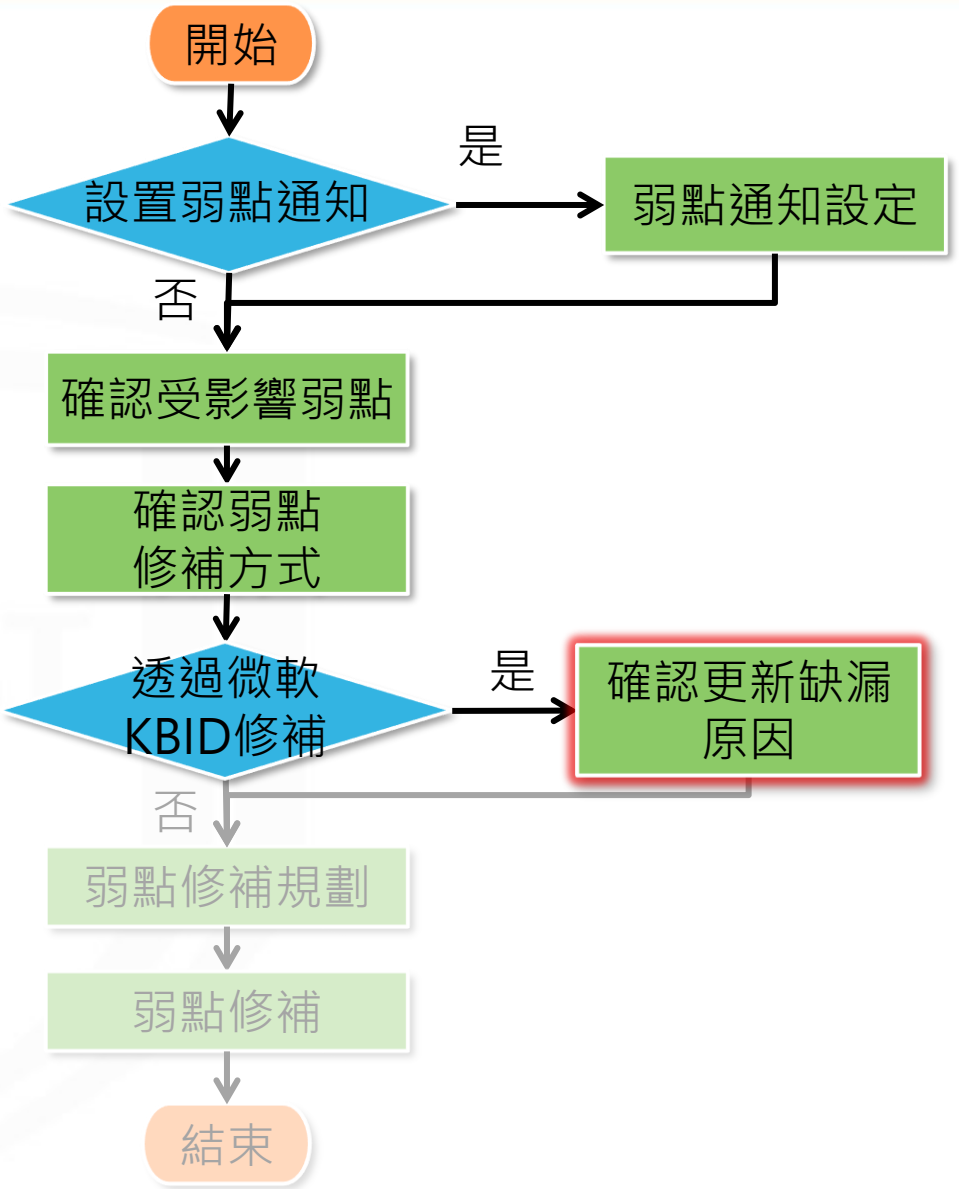
- 透過弱點詳細資訊中的連結，查閱原廠或相關廠商建議弱點修補方式



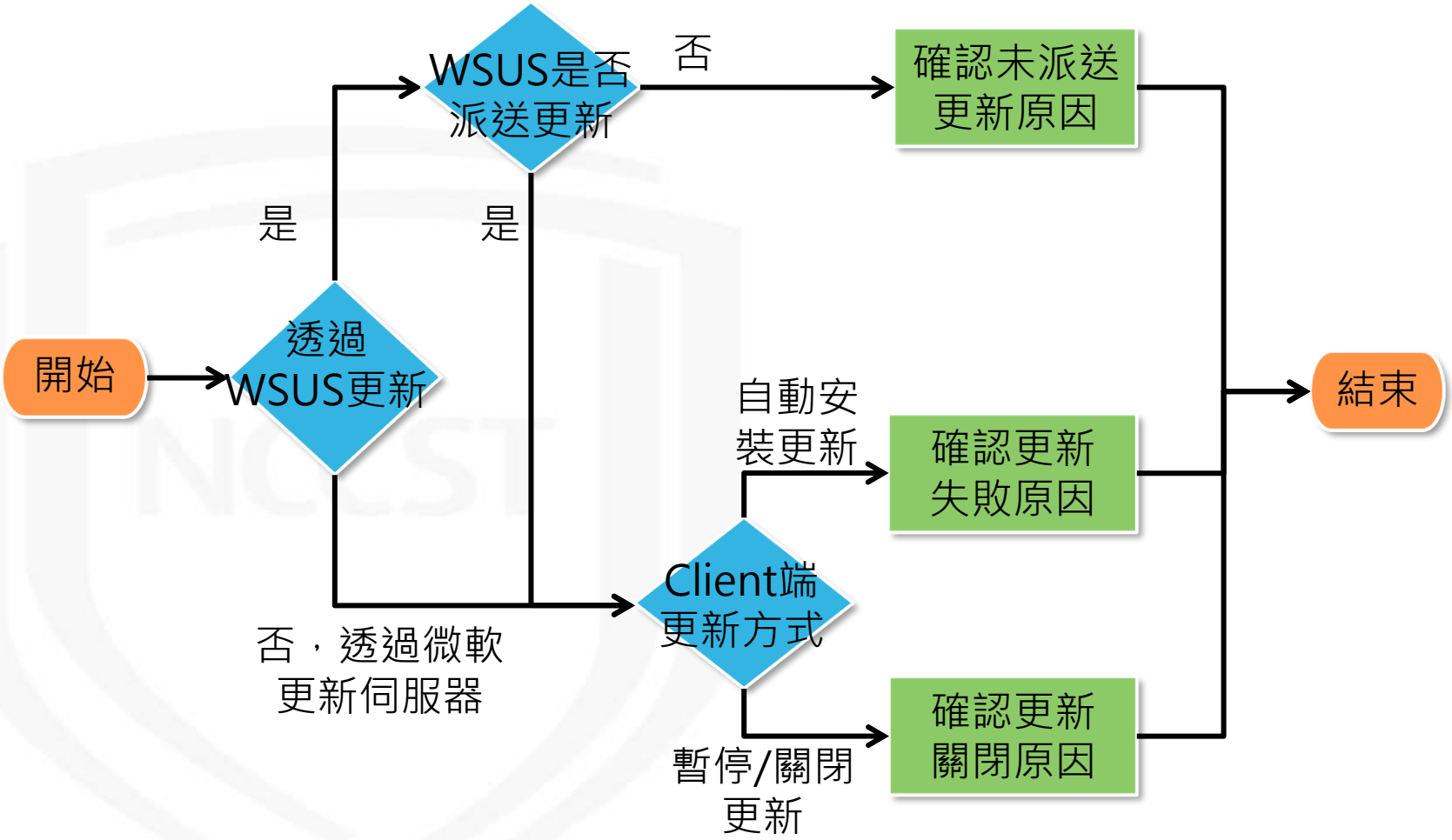
確認弱點修補方式-微軟類

- 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與應安裝KBID數量
  - 紅色為尚有缺漏KBID，綠色為完成安裝KBID
  - 點選檢視可修補該弱點之KBID

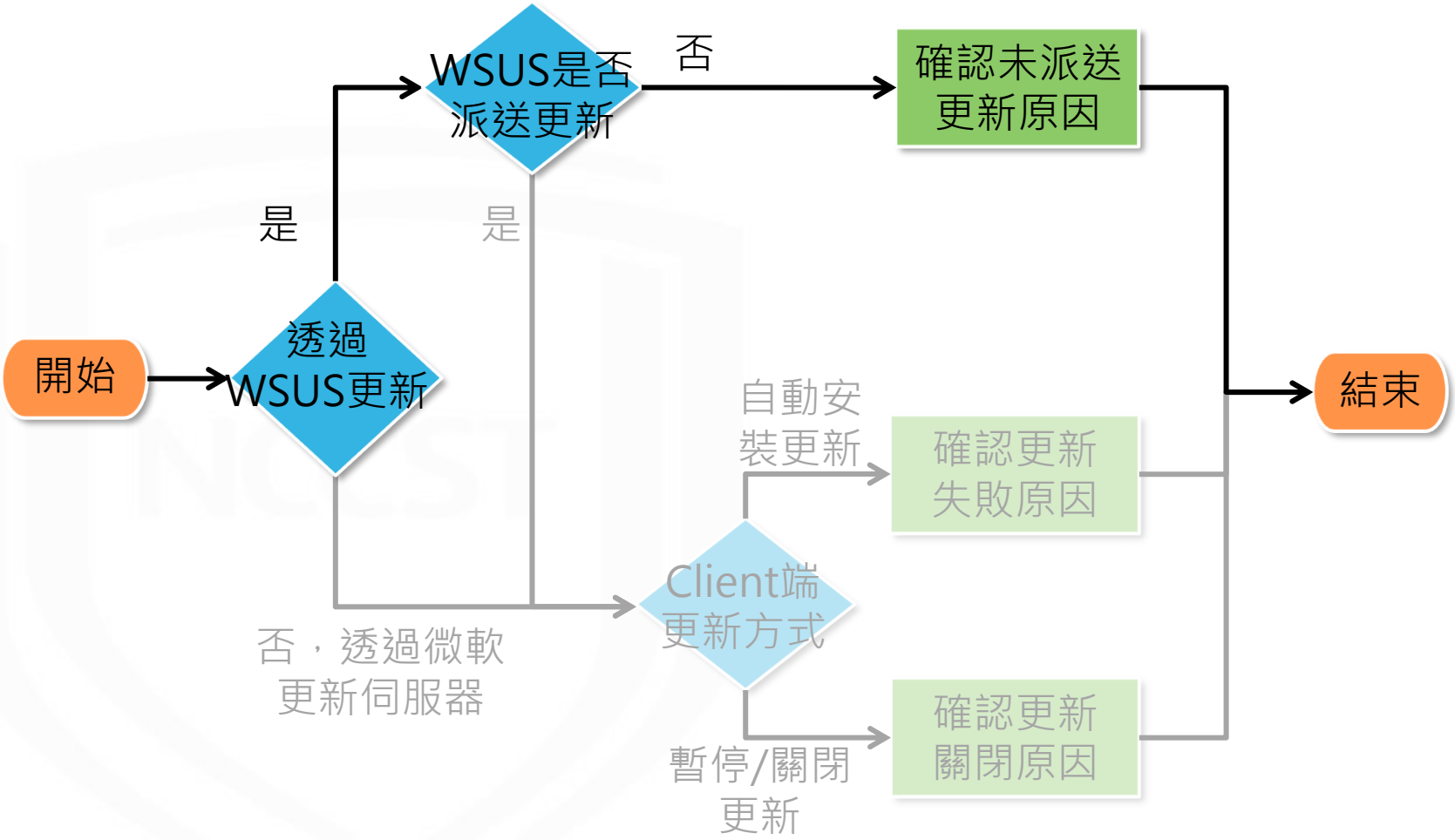
弱點通知與修補規劃作業流程



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

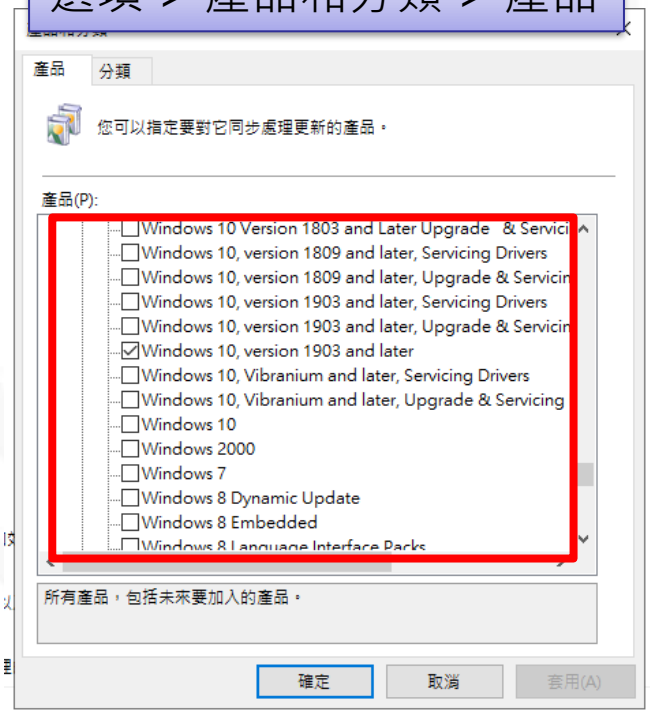
確認更新缺漏原因


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

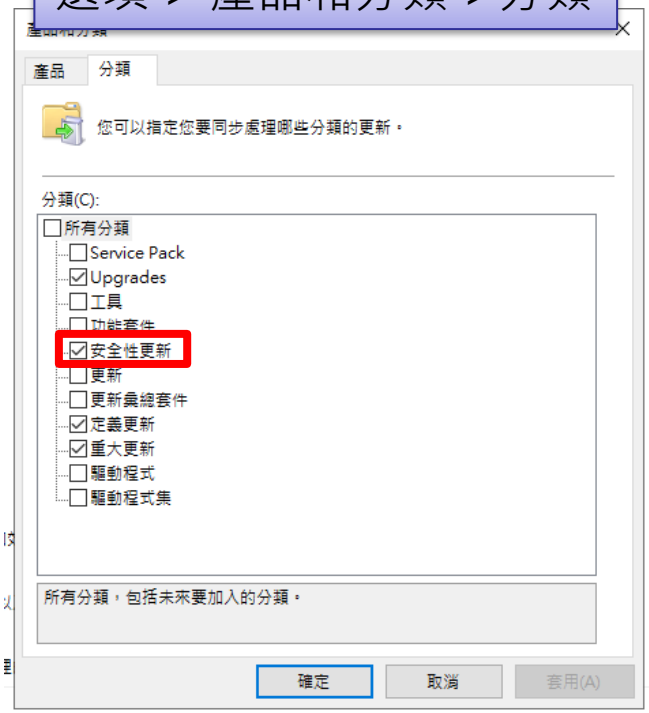
確認WSUS更新派送狀態(1/2)

- 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

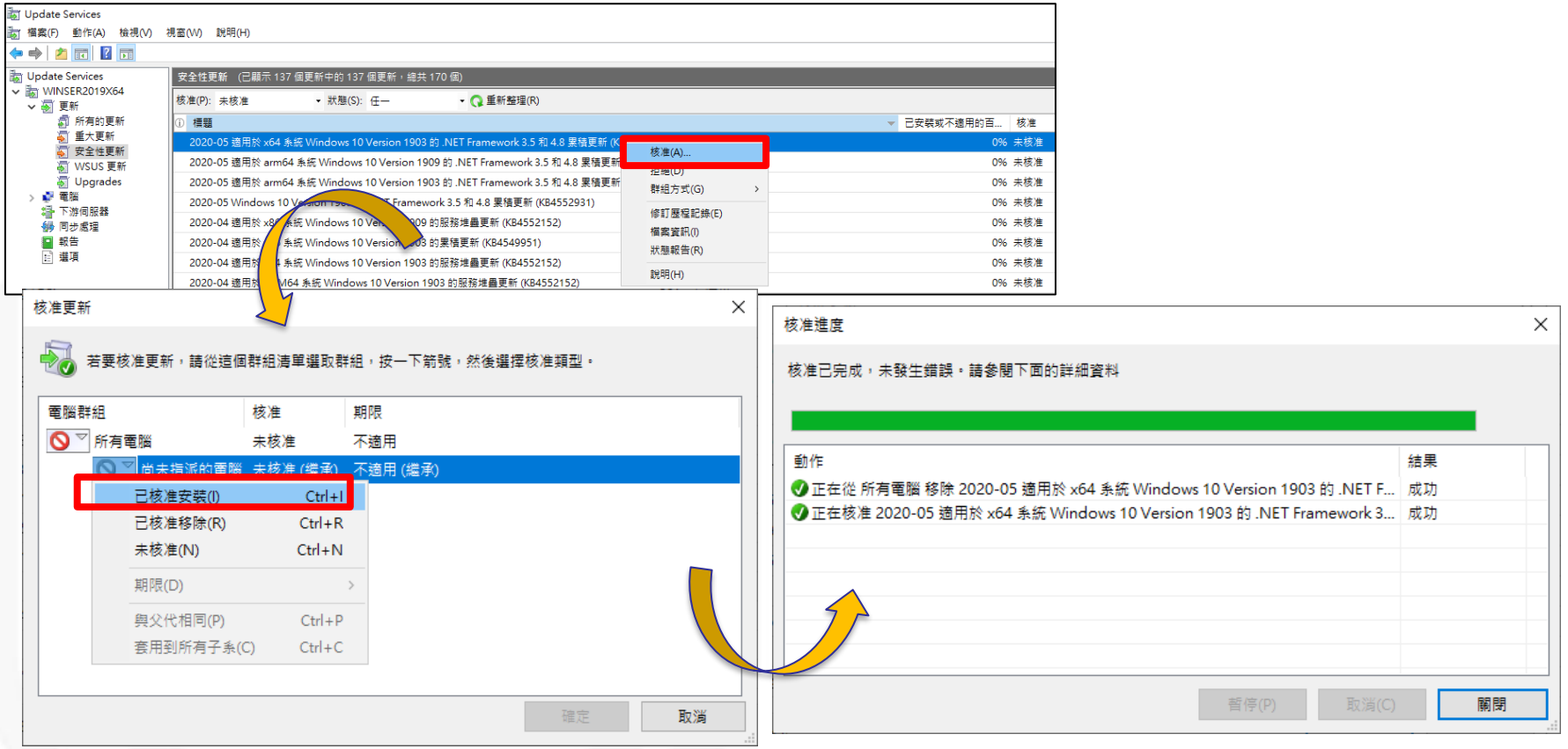


選項 > 產品和分類 >分類



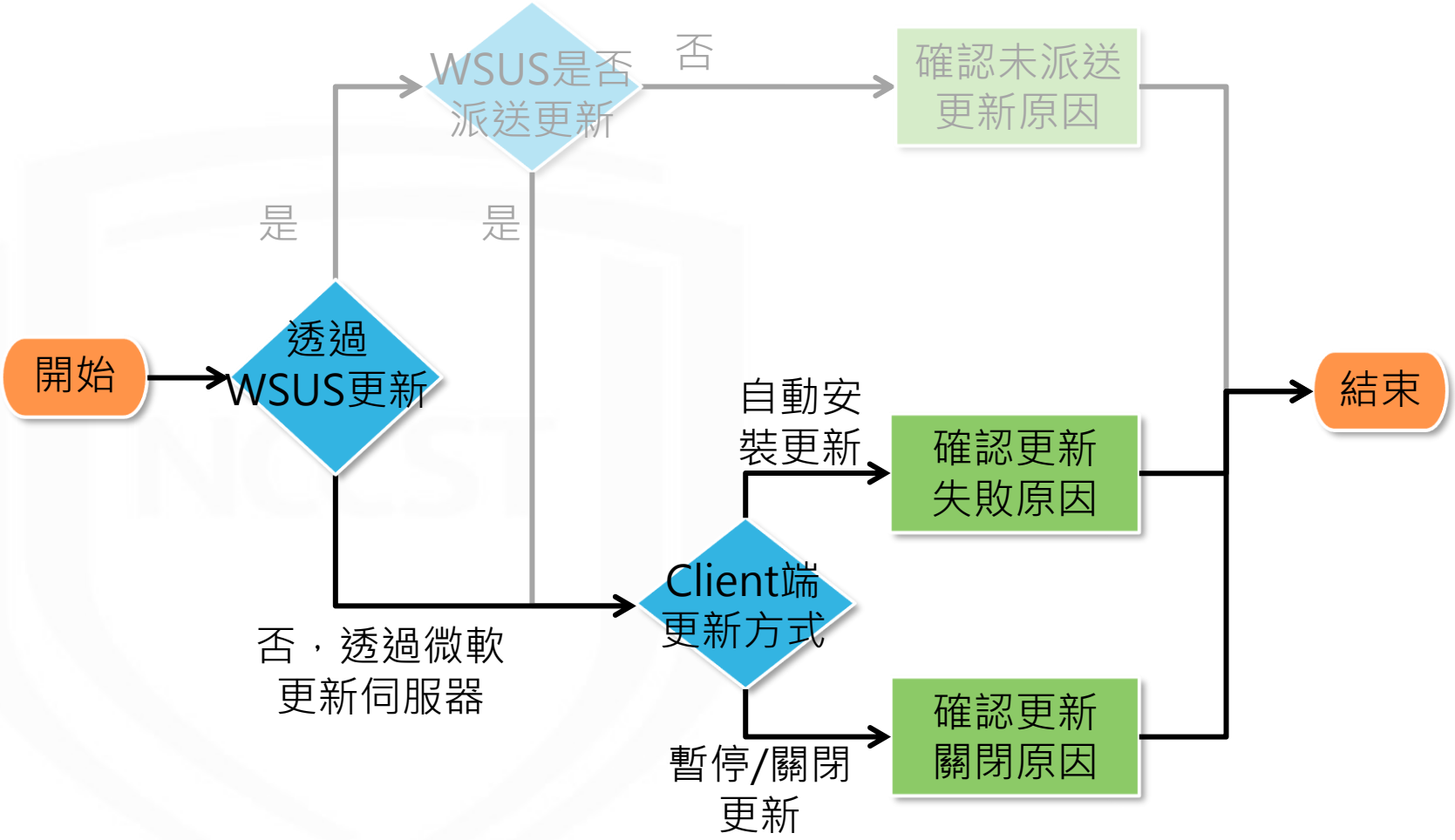
確認WSUS更新派送狀態(2/2)

- 確認缺漏更新是否已於WSUS核准派送



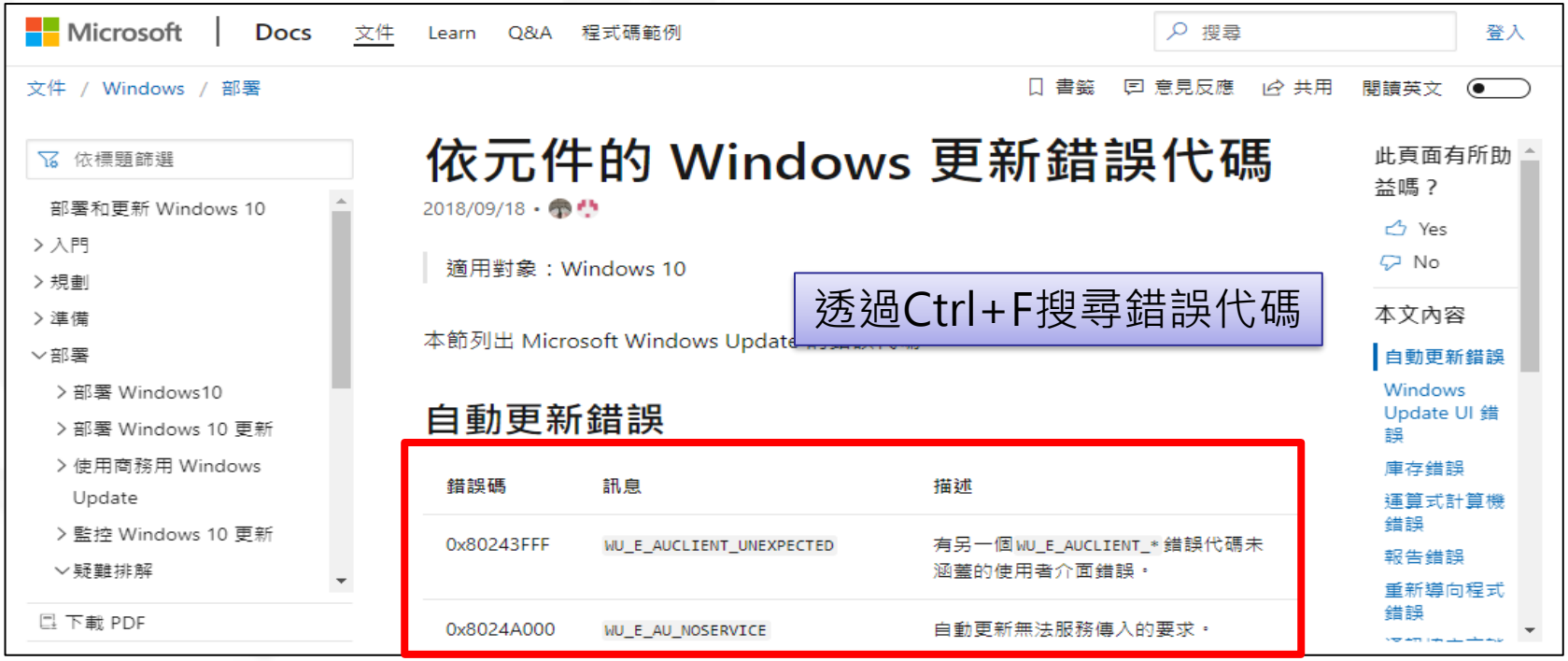
- 若上述確認完畢後，仍有缺漏更新，則需確認是否為Client端問題

確認更新缺漏原因

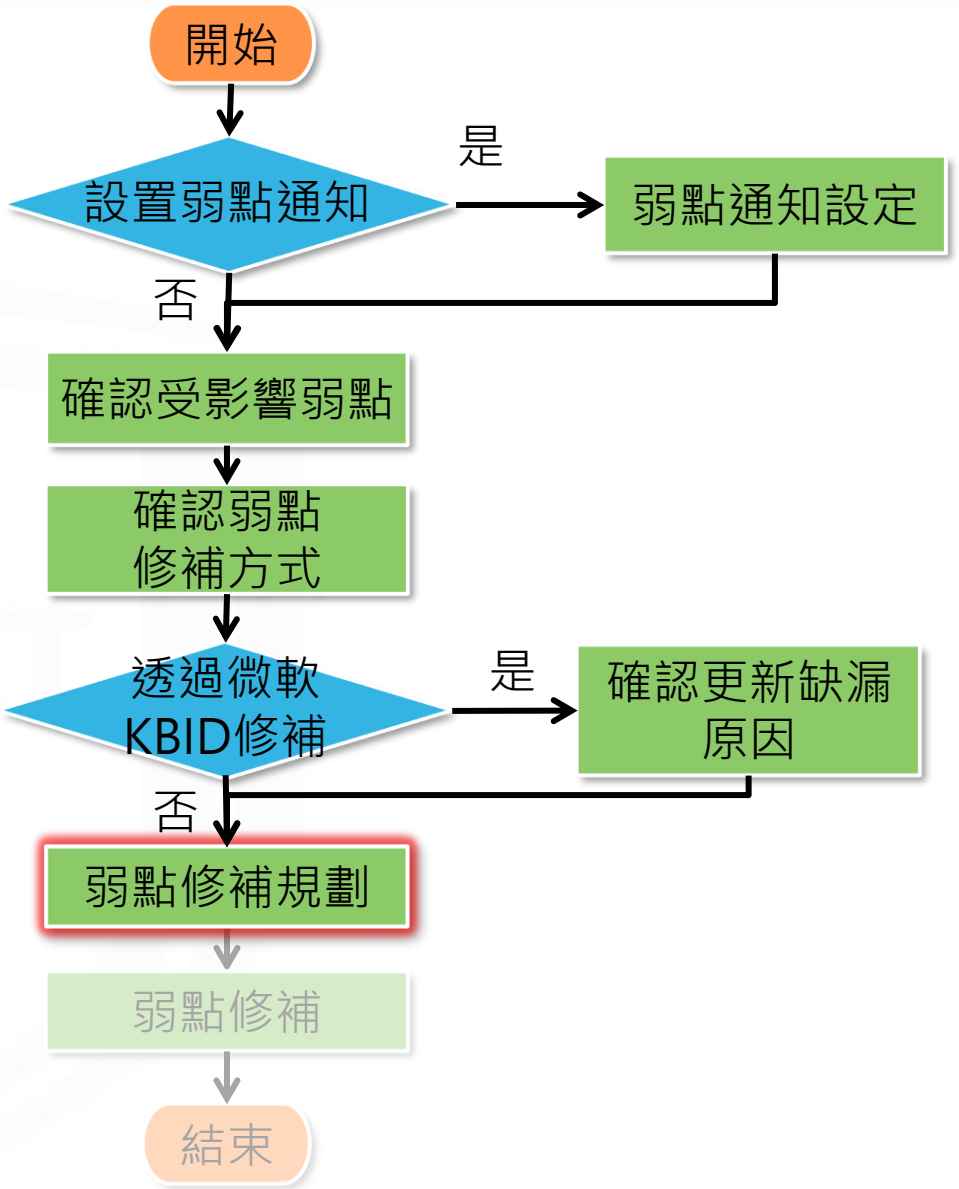

開始
透過WSUS更新
是
WSUS是否派送更新
否
確認未派送更新原因
是
否，透過微軟更新伺服器
Client端更新方式
自動安裝更新
確認更新失敗原因
暫停/關閉更新
確認更新關閉原因
結束

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含意，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

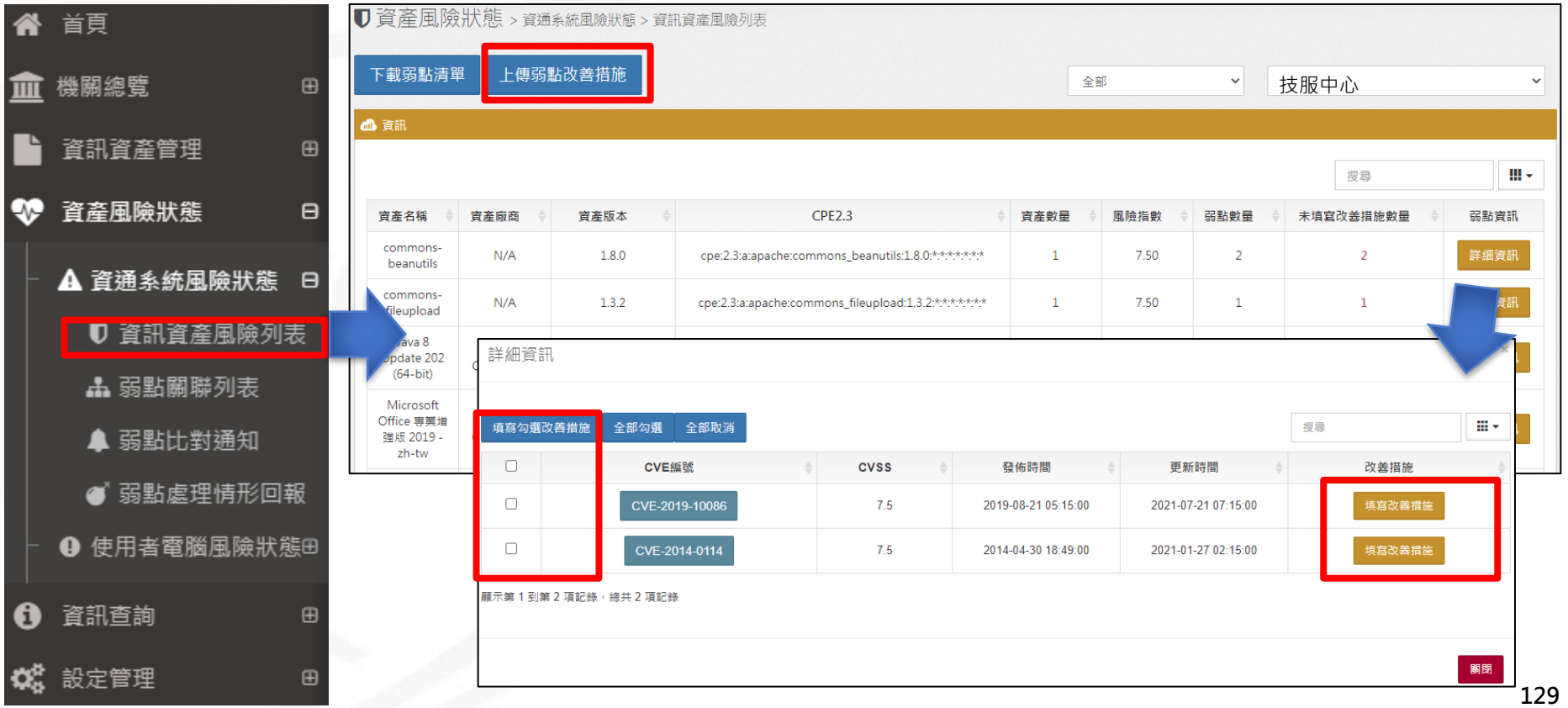


弱點修補規劃(1/6)

- 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)

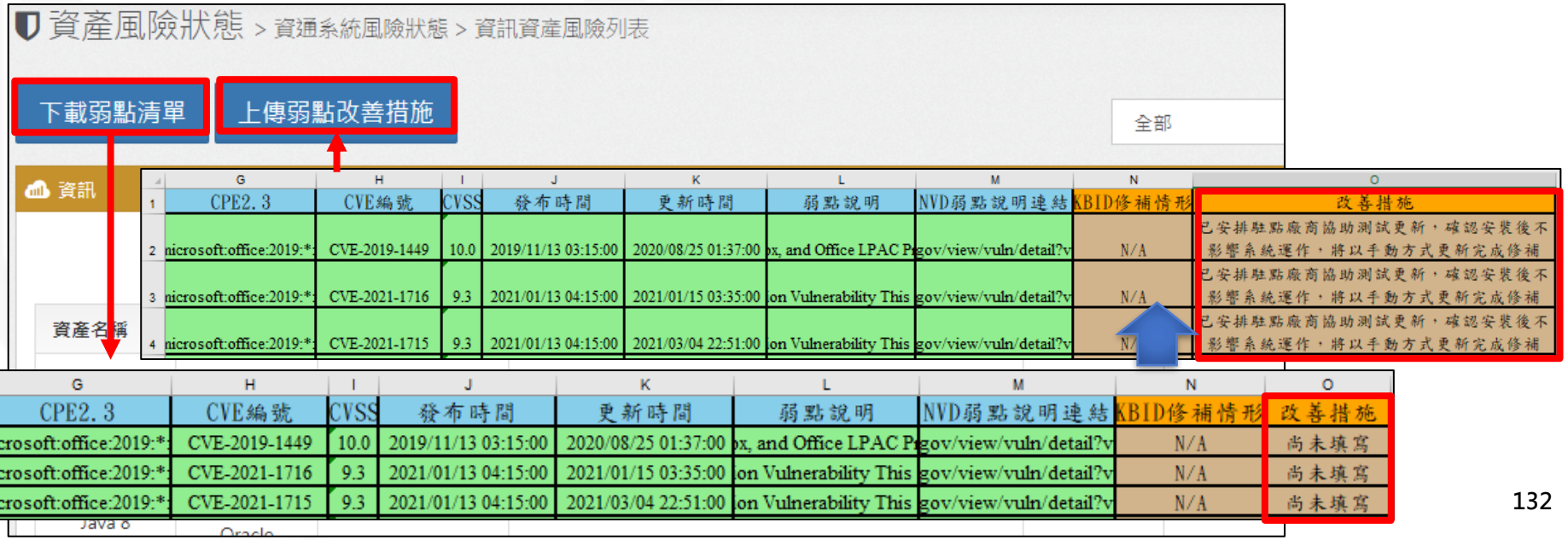
- 單筆填寫：可針對各弱點進行弱點修補規劃
  - STEP1：確認弱點後，點選「填寫改善措施」，針對該弱點進行修補規劃
  - STEP2：點選「送出」即完成填寫改善措施
  - 填寫改善措施請避免使用 >、<、 &、"或'等特殊字元

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，勾選右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)

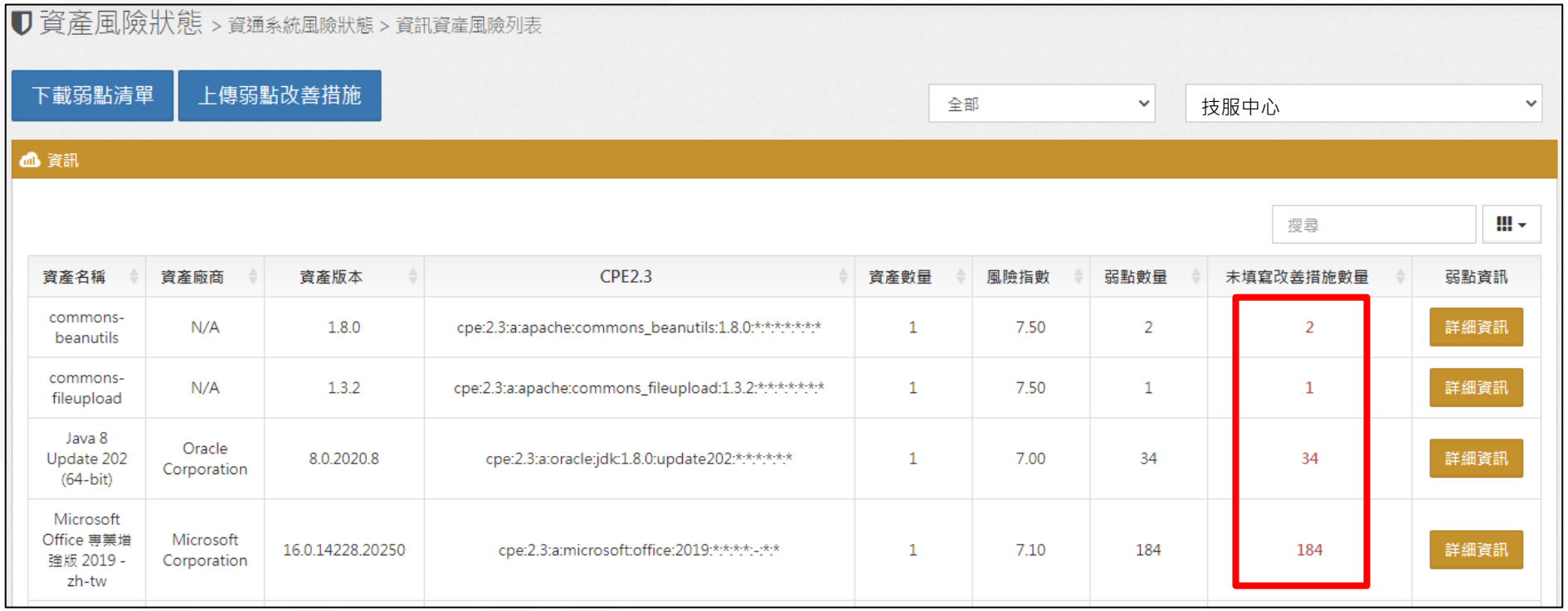
弱點修補規劃(5/6)

- 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
  - 「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



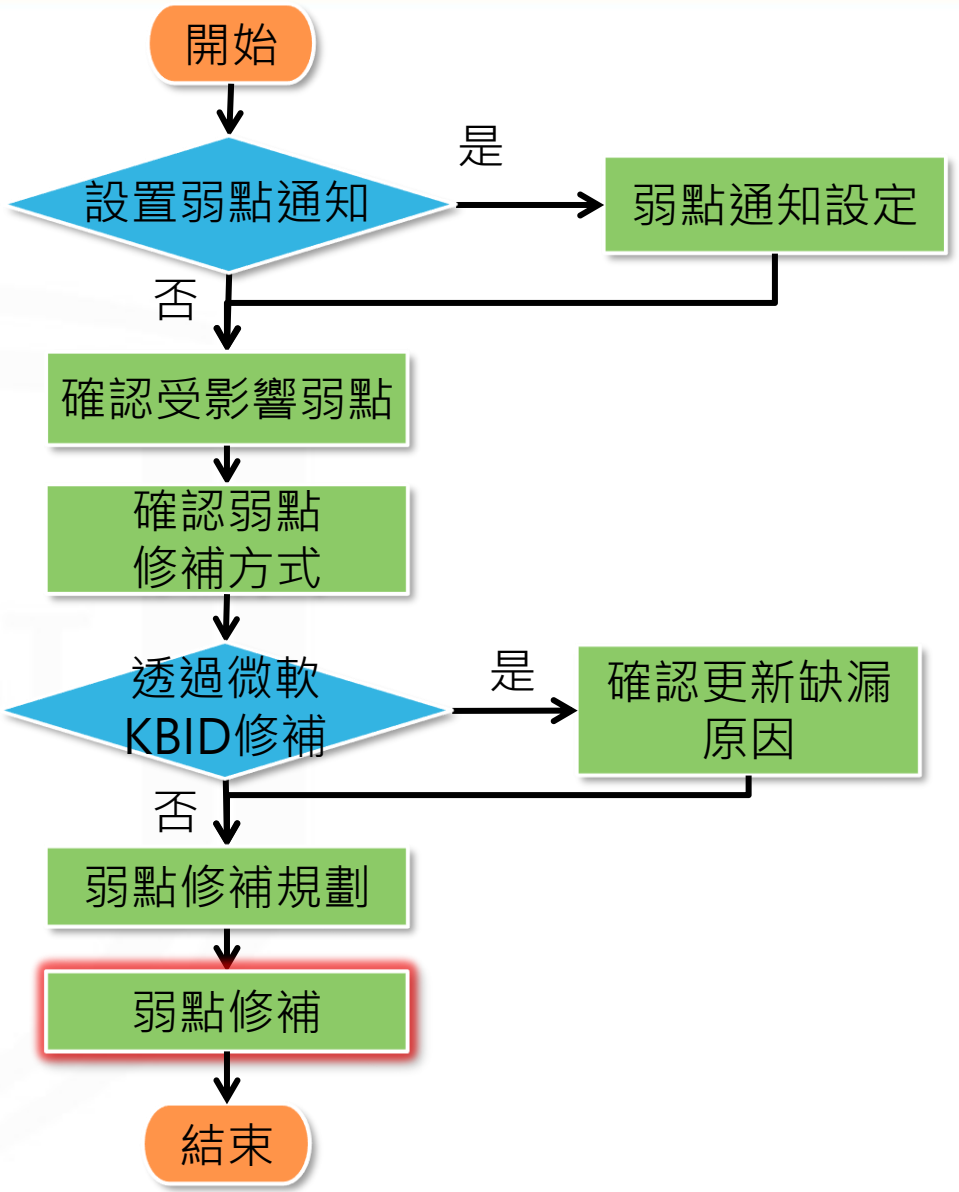
弱點修補規劃(6/6)

- 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修補規劃之弱點數量
  - 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
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

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3

實作練習3

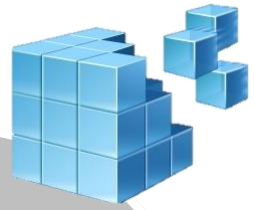
- 檢視弱點通知，並進行弱點修補規劃
- 本項練習時間20分鐘

項次	參考頁數	執行項目	產出項目/執行結果
1	P.109	接收弱點通知	檢視設定接收通知之信箱
2	P.111、P.114~117、P.129	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
3	P.111、P.114~118、P.129	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

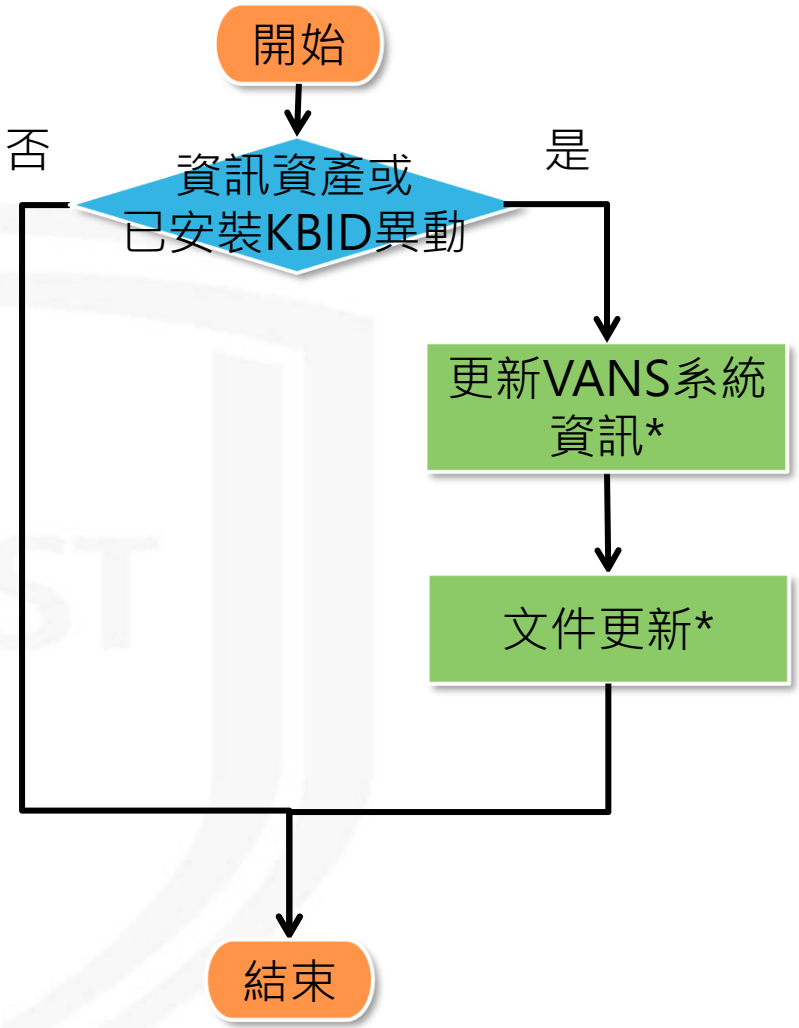


資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

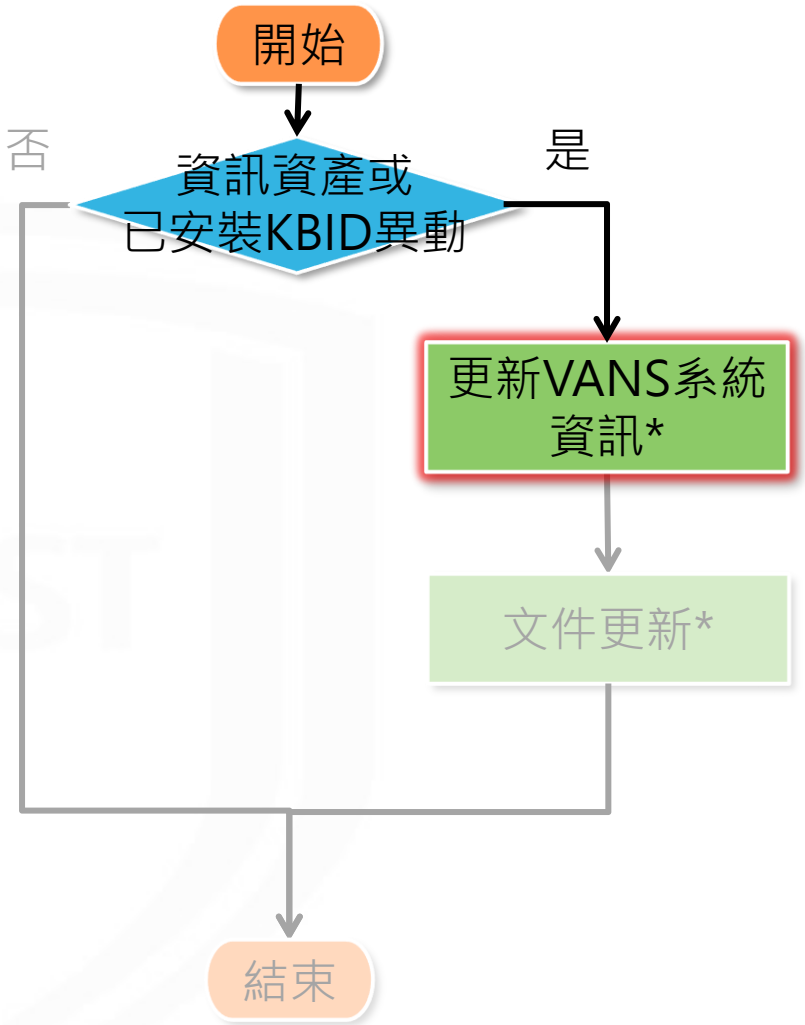
資訊資產與已安裝KBID更新作業流程



*更新VANS系統資訊：
新增、修改及刪除VANS系統資訊

*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

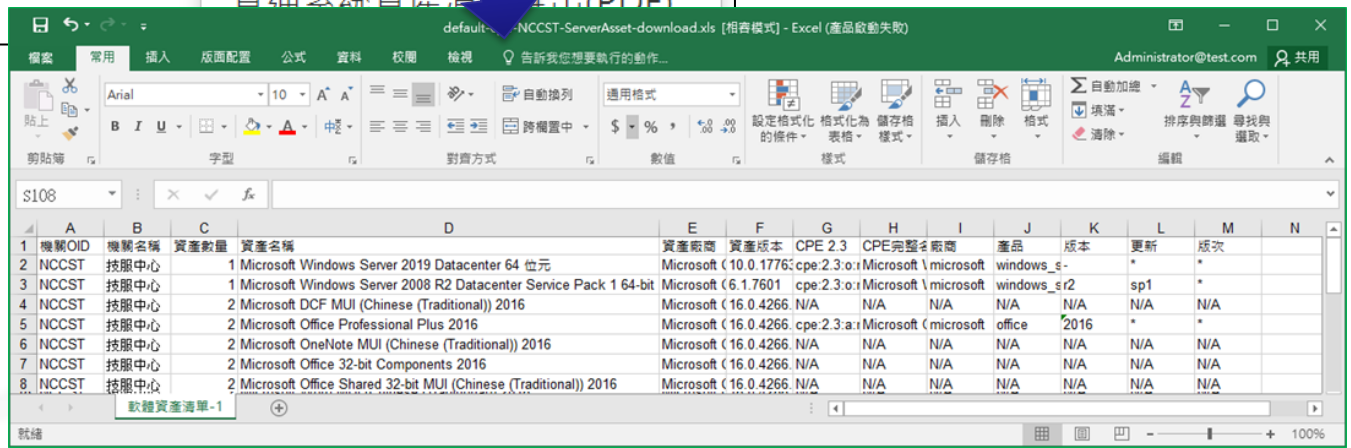


*更新VANS系統資訊：
新增、修改及刪除VANS系統資訊

*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



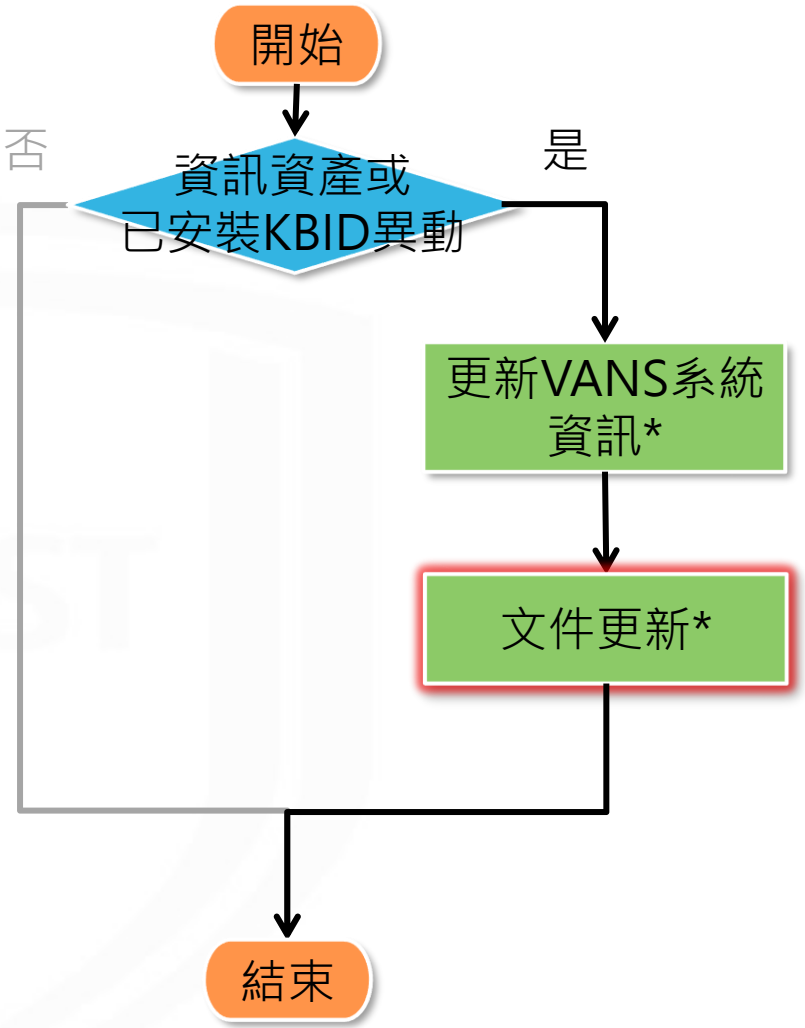
更新VANS系統資訊-單筆更新(1/2)

- 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



*更新VANS系統資訊：
新增、修改及刪除VANS系統資訊

*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	版次
NCCST	技服中心	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	*	*
NCCST	技服中心	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	*	*
NCCST	技服中心	1	commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*:*:*:*:*:*:*	Apache Software Foundation Commons FileUpload 1.3.2	apache	commons_fileupload	1.3.2	*	*
NCCST	技服中心	1	commons-io	N/A	2.2	N/A	N/A	N/A	commons-io	2.2	N/A	N/A
NCCST	技服中心	1	commons-lang	N/A	2.4	N/A	N/A	N/A	commons-lang	2.4	N/A	N/A

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

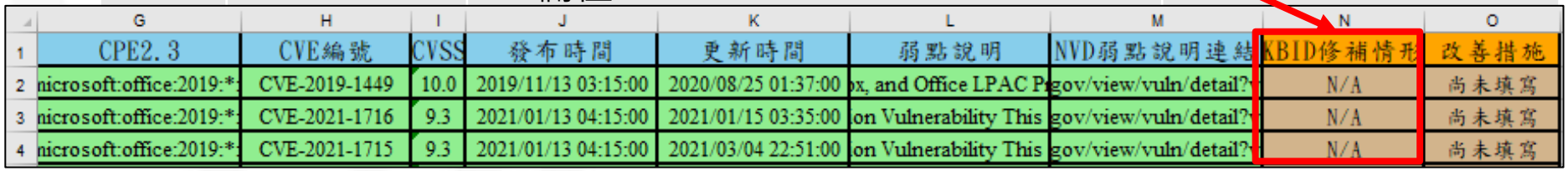
	G	H	I	J	K	L	M	N	O
1	CPE2. 3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
2	nicrosoft:office:2019:*:	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	x, and Office LPAC P	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
3	nicrosoft:office:2019:*:	CVE-2021-1716	9.3	2021/01/13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

實作練習4

- 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	參考頁數	執行項目	產出項目/執行結果
1	P.169~175	參考附件4，將Upload_KBIDTemplate.json登錄至VANS系統	檢視已安裝KBID列表
2	P.131	• 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	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?	N/A	尚未填寫
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?	N/A	尚未填寫
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?	N/A	尚未填寫

常見問答(1/2)

Q1 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

Q2 VANS系統資產更新時，能否只上傳新增的資產項目？

– 透過**上傳清單(Upload_Template.xls)**更新資產時，會以最新**上傳清單**覆蓋既有資產，故須以完整資產內容進行上傳

常見問答(2/2)

Q3 如何得知哪些資產較危險，應立即處理？

- 弱點比對結果會顯示各資產風險指數，計算方式為將各資訊資產比對到的每個弱點CVSS分數加總平均，風險指數較高者建議優先處理

Q4 上傳資產清單時，VANS系統支援哪些格式？

- VANS系統可接受上傳之檔案格式包含Excel活頁簿(*.xlsx)、Excel 97-2003活頁簿(*.xls)及OpenDocument試算表(*.ods)等3種，機關可透過上述格式上傳資產清單

Q5 相同弱點只會通知一次呢？還是會持續寄通知信？

- VANS機制主要提供機關即時掌握弱點、有效修補弱點及做好弱點管理，進而降低資安風險，相同弱點僅會通知一次


Q
&
A

參考資料

參考資料(1/2)

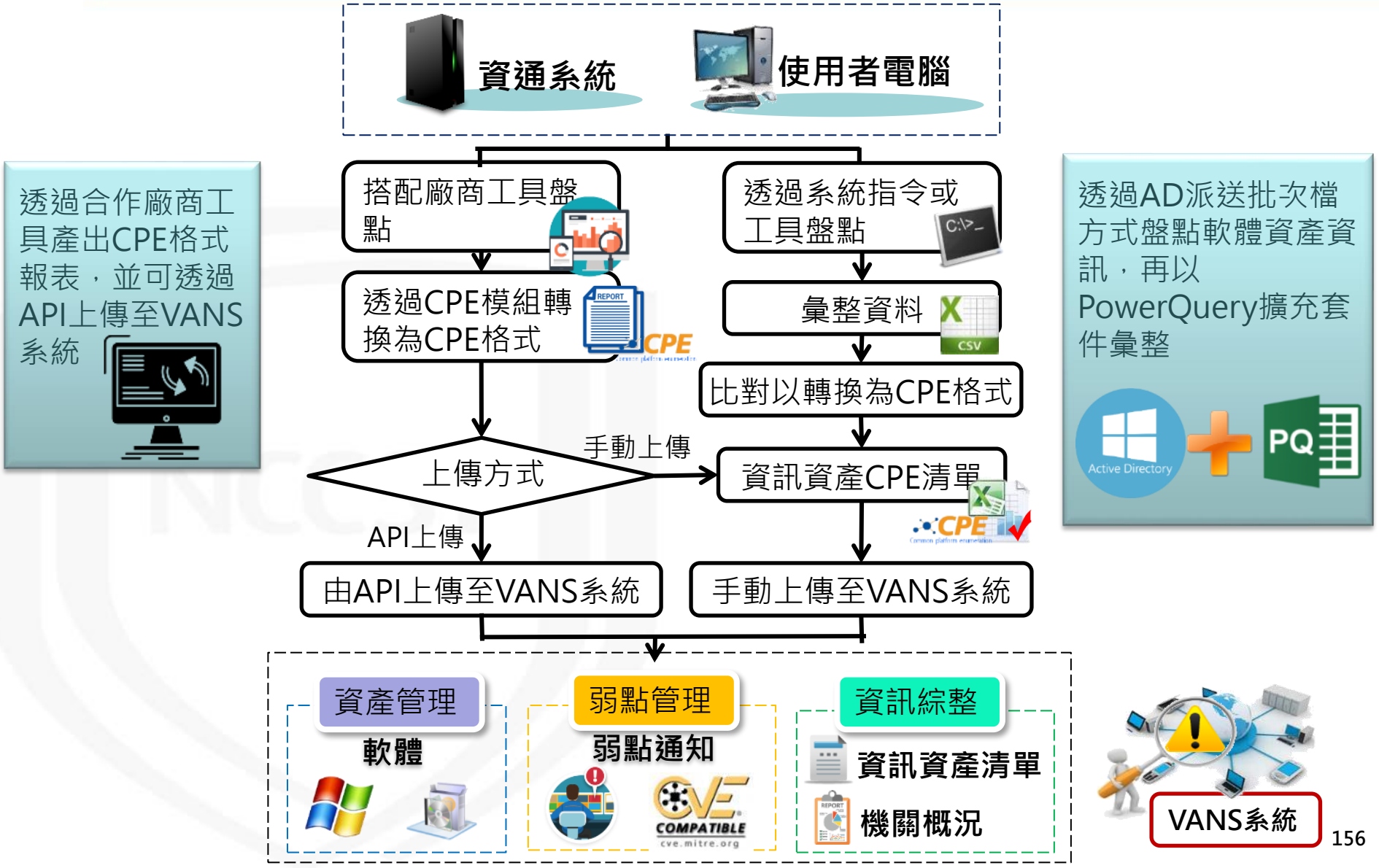
- Windows Management Instrumentation
  - https://docs.microsoft.com/zh-tw/windows/desktop/wmisdk/wmi-start-page
- How to find the Windows version using Registry?
  - https://mivilisnet.wordpress.com/2020/02/04/how-to-find-the-windows-version-using-registry/
- Microsoft Docs - Dir
  - https://docs.microsoft.com/zh-tw/windows-server/administration/windows-commands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

附件1.資訊資產弱點管理總覽



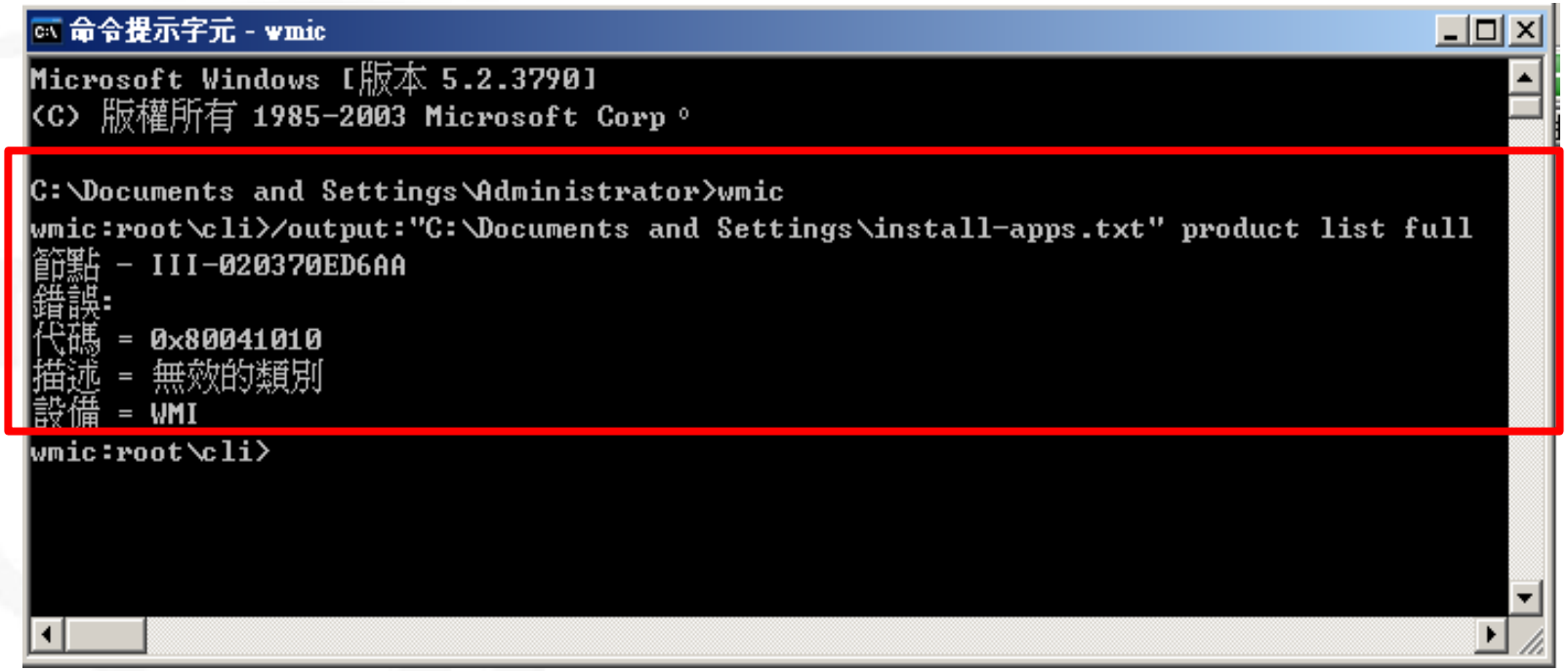
透過合作廠商工具產出CPE格式報表，並可透過API上傳至VANS系統

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

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

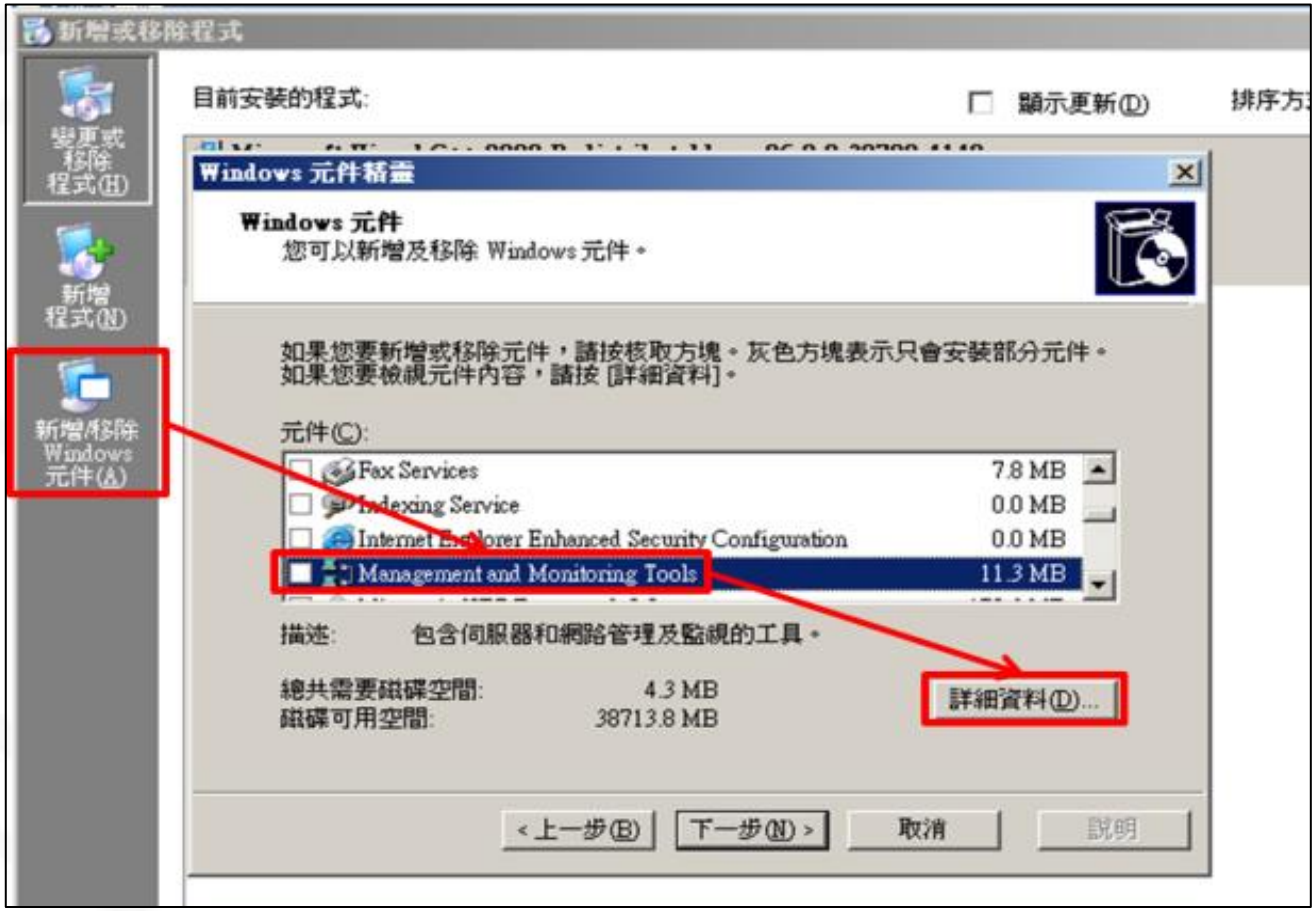


安裝WMI Windows Installer(2/7)

- 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」

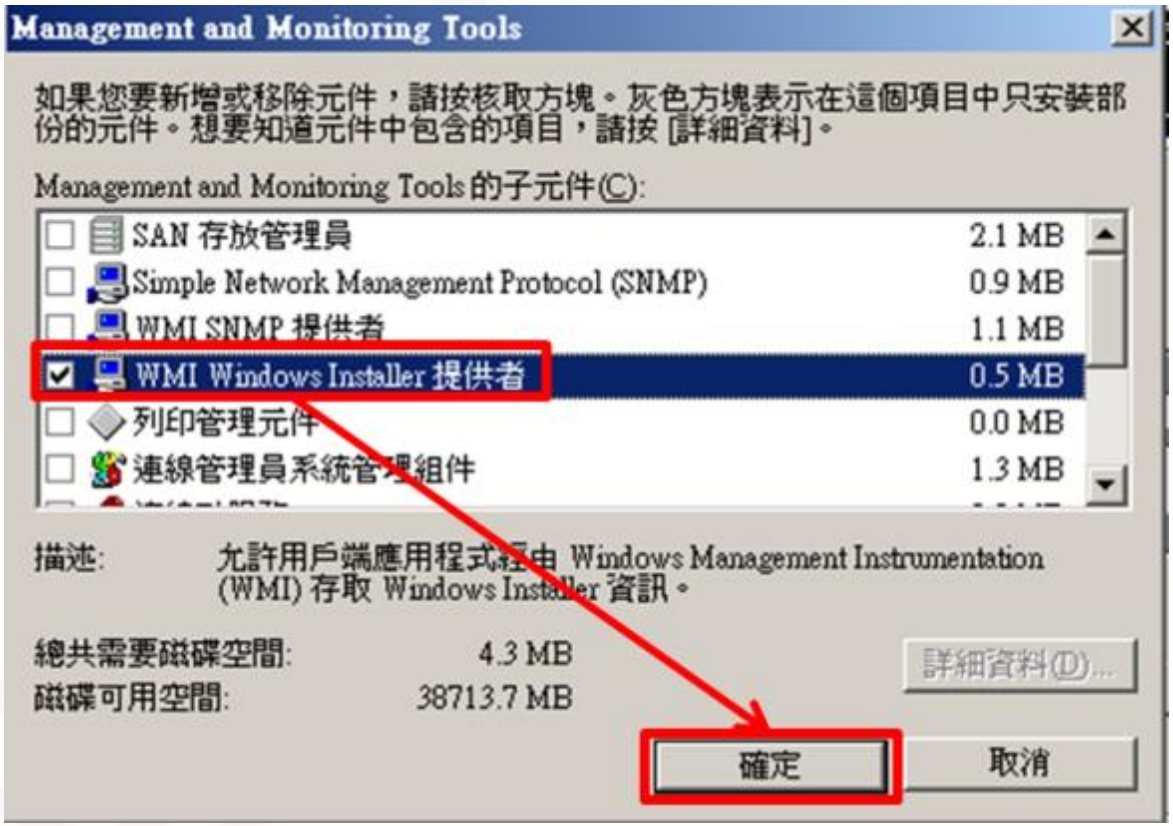
安裝WMI Windows Installer(3/7)

- 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



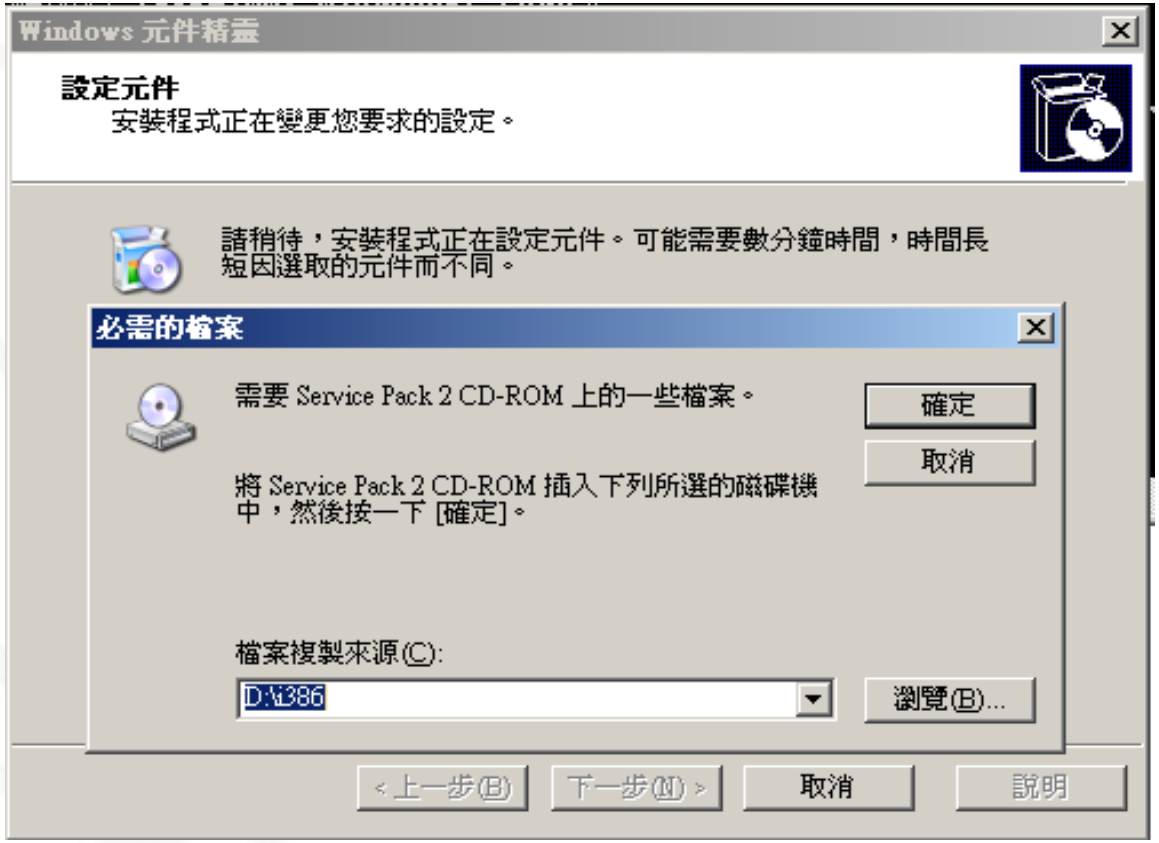
安裝WMI Windows Installer(4/7)

- 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」



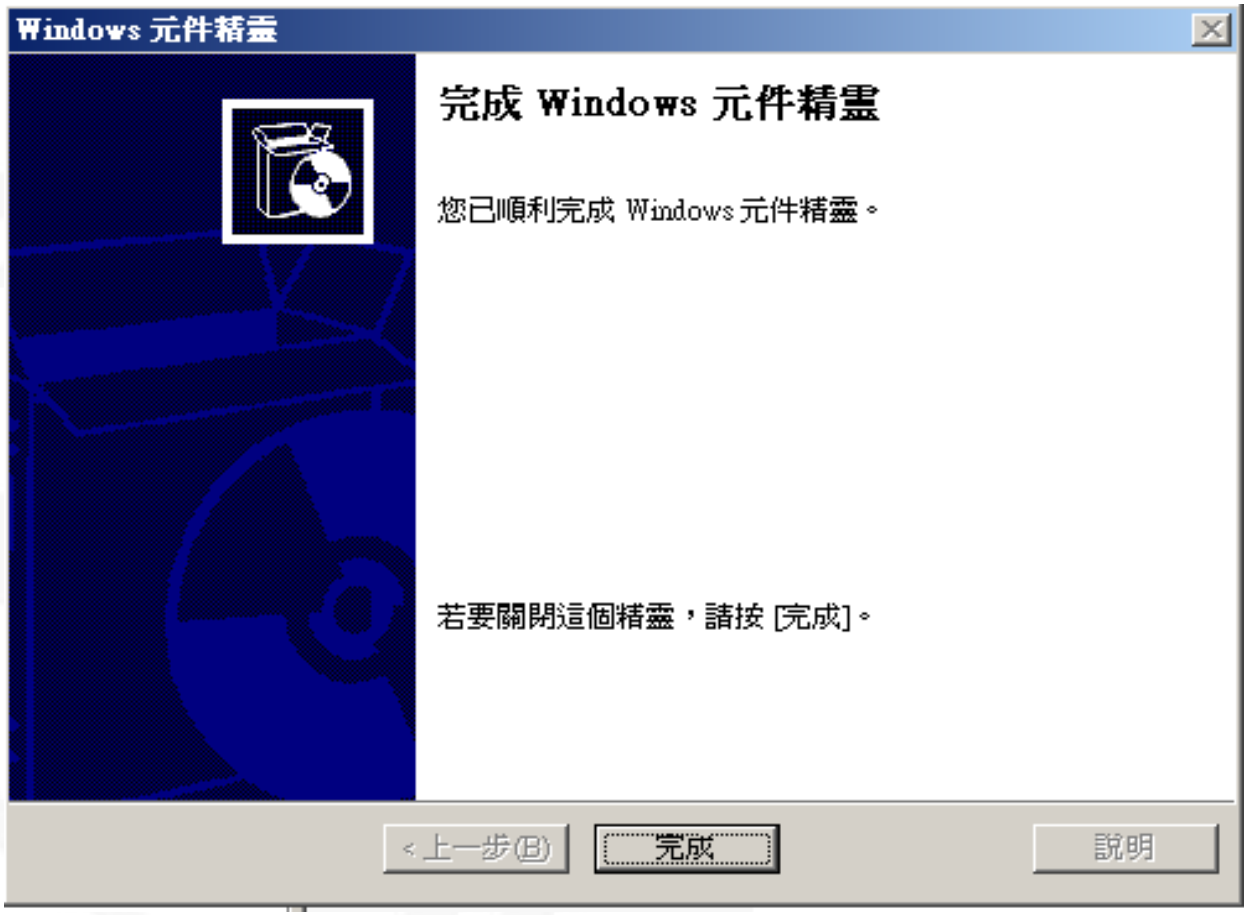
安裝WMI Windows Installer(5/7)

- 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



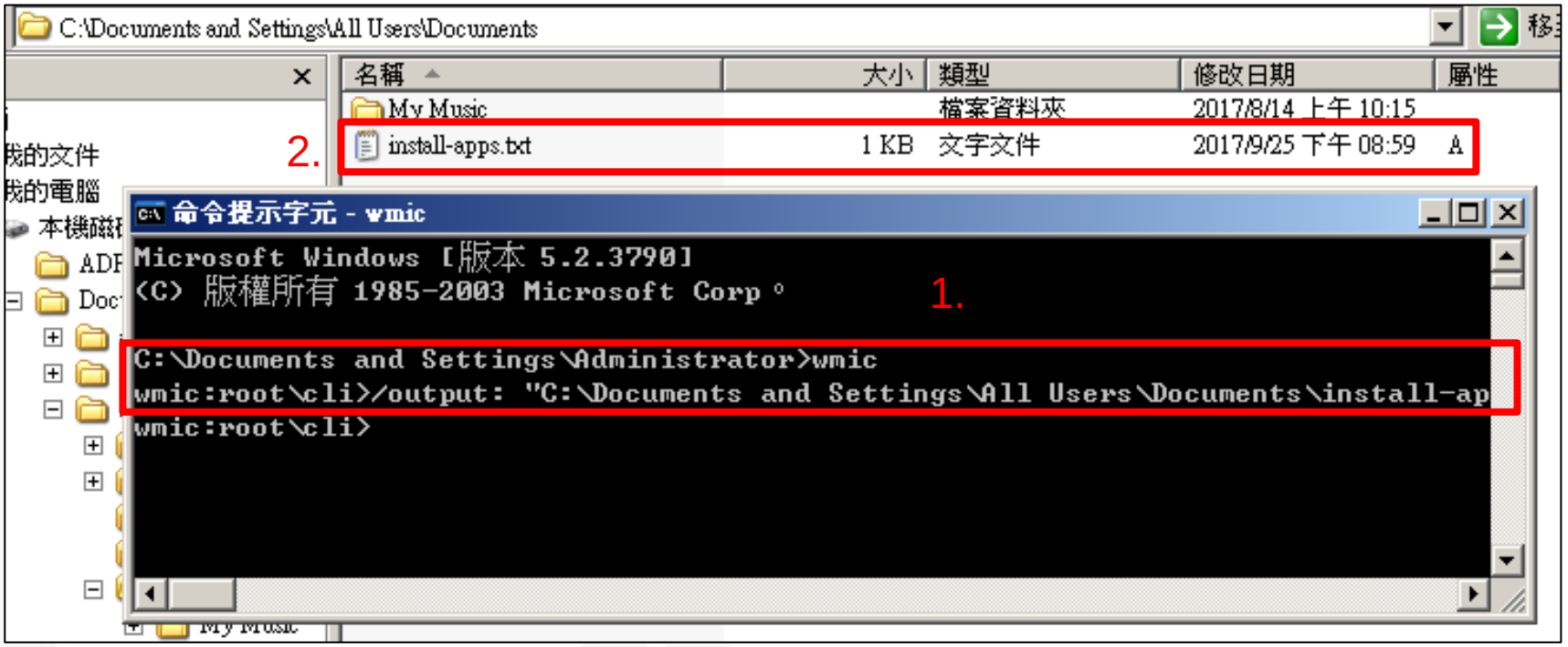
安裝WMI Windows Installer(6/7)

- 步驟五：完成安裝



安裝WMI Windows Installer(7/7)

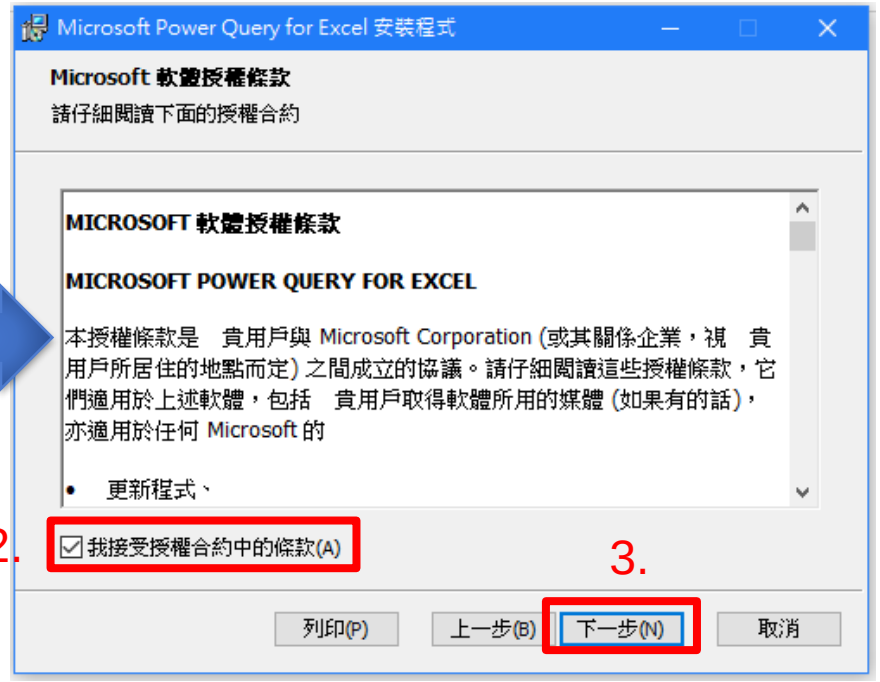
- 步驟六：安裝完成後，即可執行WMIC



附件3
Microsoft Power Query for Excel
安裝步驟

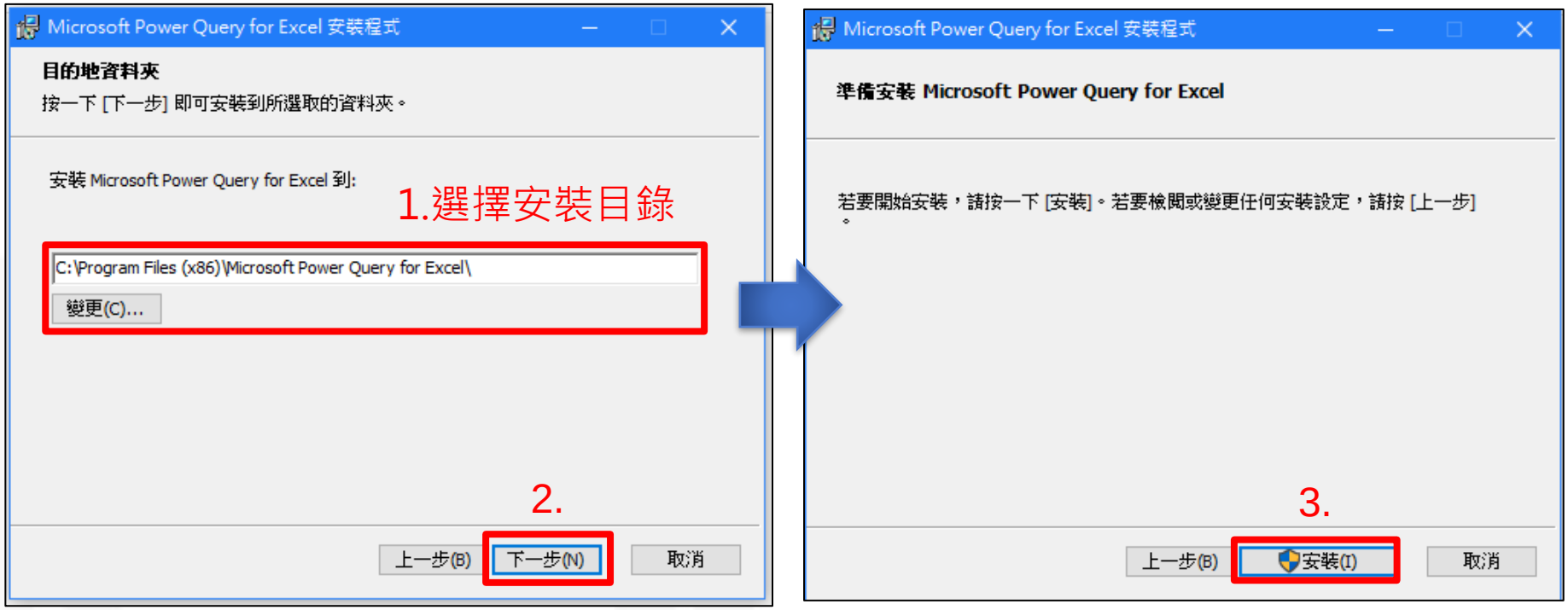
安裝Microsoft Power Query for Excel(1/3)

- 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



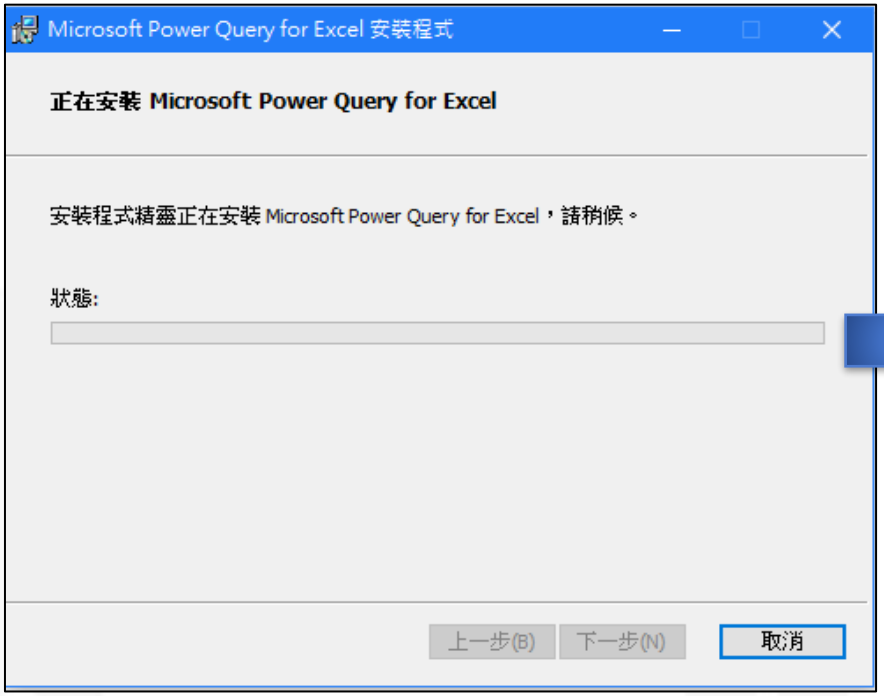
安裝Microsoft Power Query for Excel(2/3)

- 選擇安裝目錄，準備安裝



安裝Microsoft Power Query for Excel(3/3)

- 進行安裝



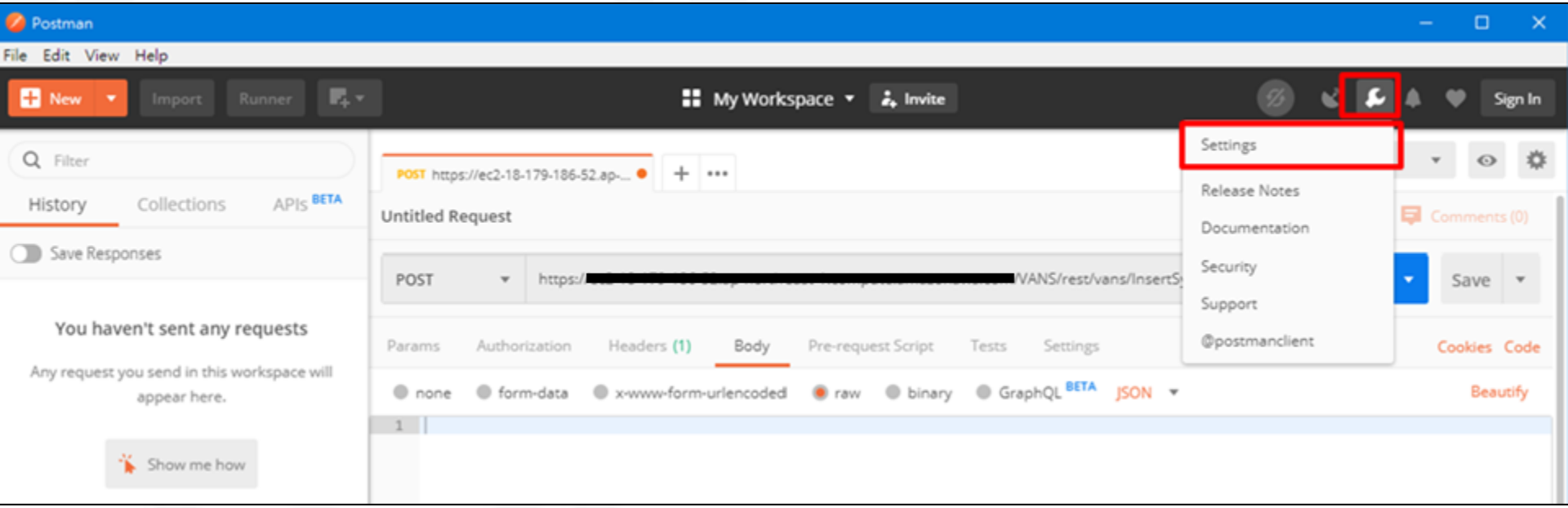
附件4
Postman操作方式

下載與安裝Postman工具

- 至Postman官方網站下載與安裝工具
  - https://www.postman.com/downloads/

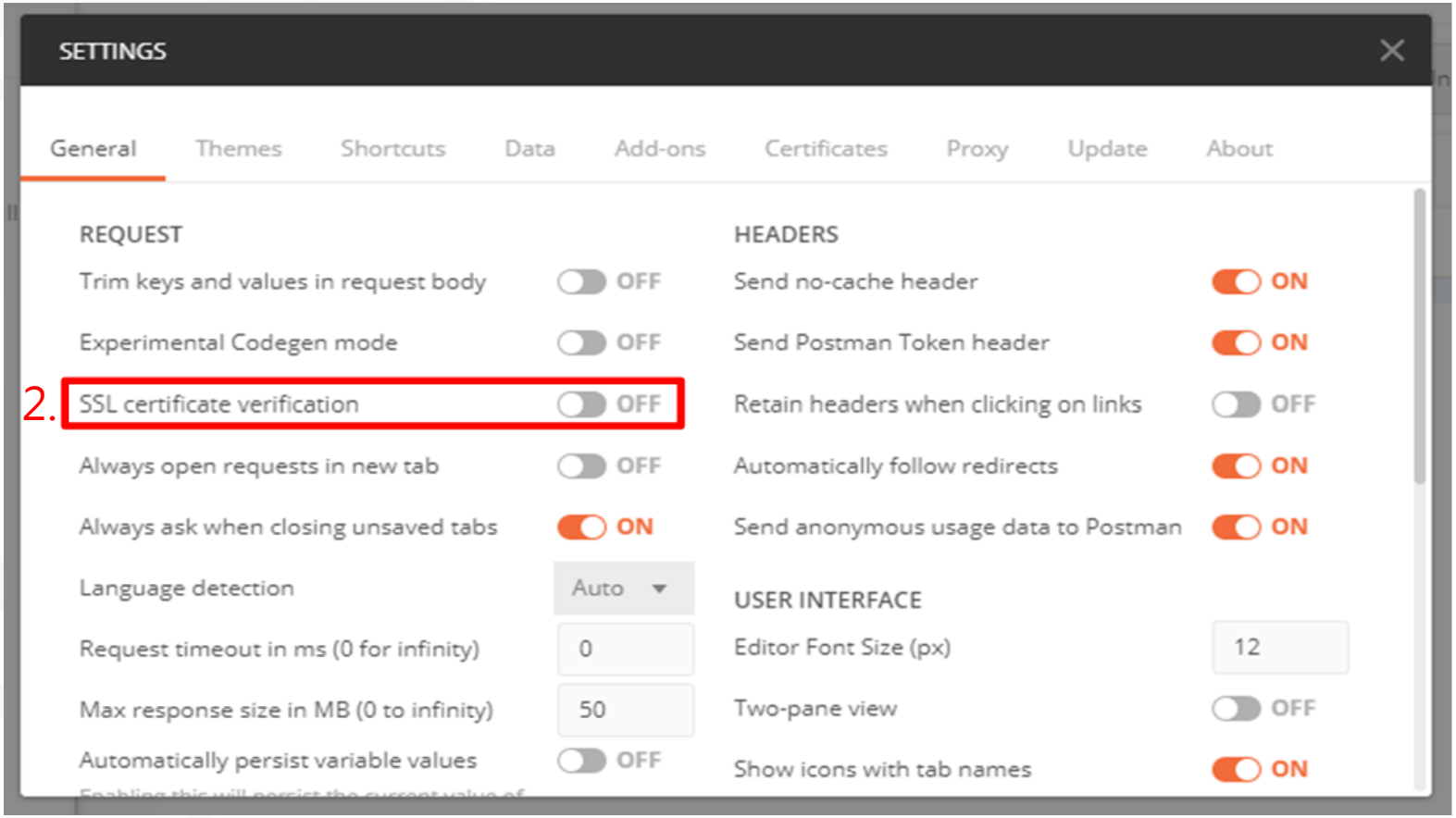
Postman設定(1/4)

- 關閉SSL憑證驗證
  - 因VANS API測試站會有憑證錯誤的問題，故須關閉SSL憑證驗證



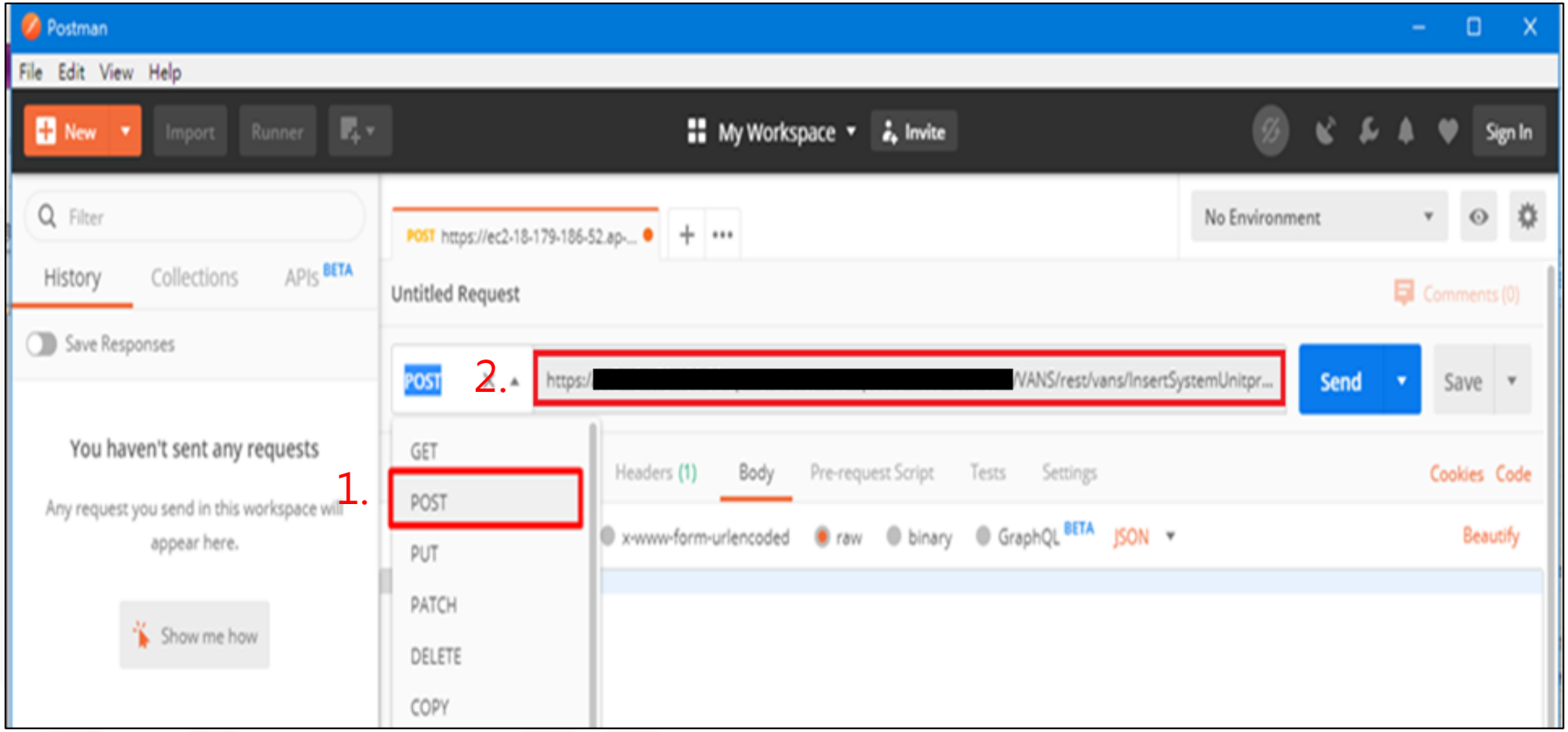
Postman設定(2/4)

- 關閉SSL憑證驗證
  - 因VANS API測試站會有憑證錯誤的問題，故須關閉SSL憑證驗證



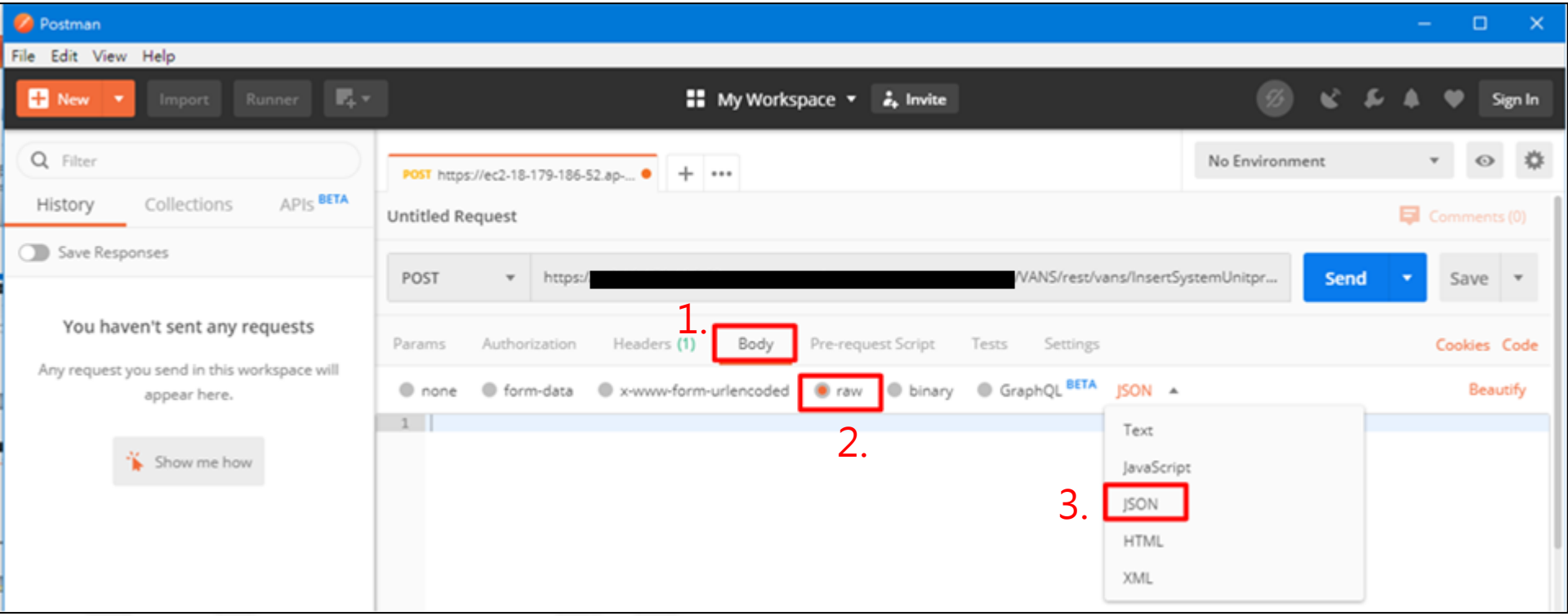
Postman設定(3/4)

- 傳輸方式選擇POST，並貼上實作機API網址



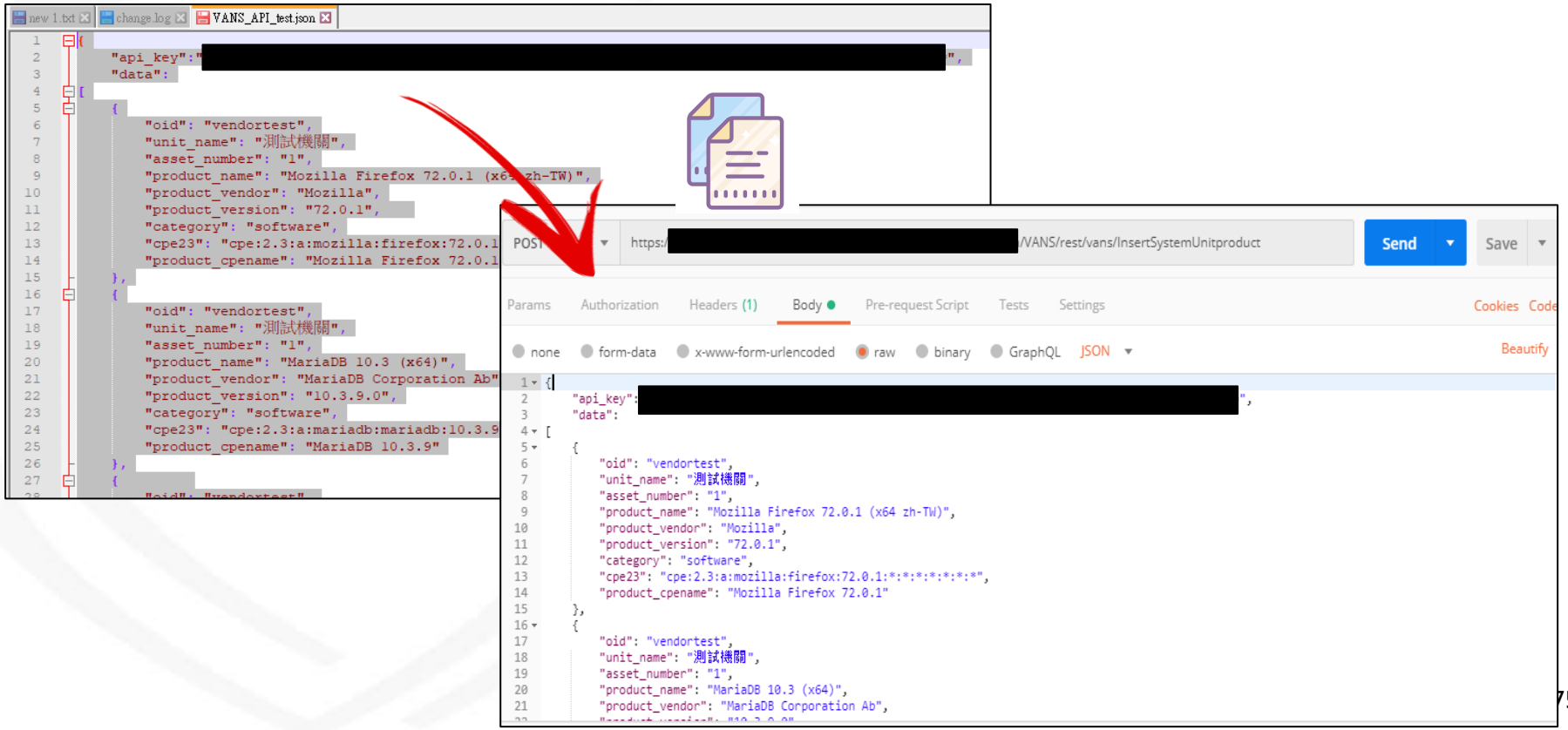
Postman設定(4/4)

- 切換至Body頁籤，選擇raw，右邊格式選擇JSON，即可完成前置設定



執行API登錄(1/2)

- 打開技服中心提供之講師範例JSON檔，並修改其中的API KEY、OID及unitname
- 將調整完的內容複製到postman中



執行API登錄(2/2)

- 按下Send，即可於下方看到測試結果