政府零信任架構身分鑑別與設備鑑別機制導入建議 (V1.0)

國家資通安全研究院

112年12月27日

大綱

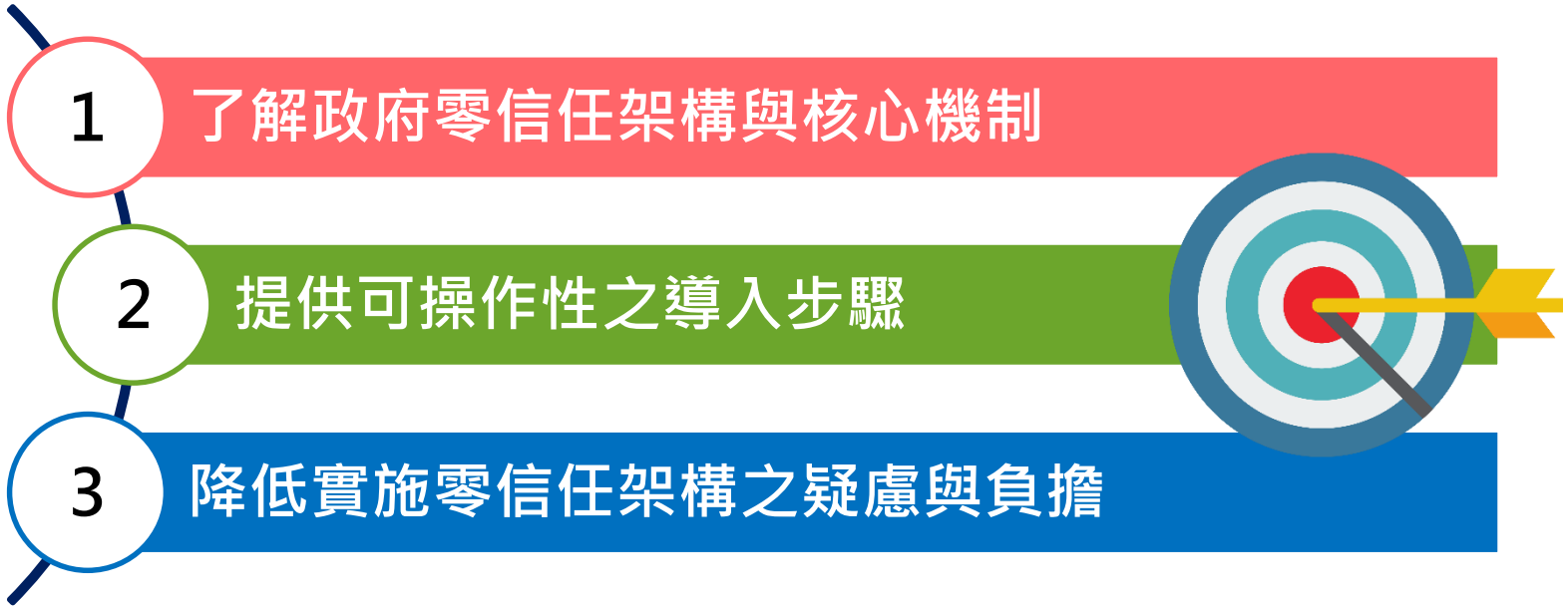
- 發展緣由
- 發展目的
- 政府零信任架構說明
- 政府零信任架構身分鑑別機制導入建議
- 參考資料

發展緣由

- 依據「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任架構資安防護環境，推動政府機關導入零信任架構，以完善政府網際服務網防禦深廣度
- 導入零信任架構是一段逐步成熟之過程，不是一次大規模替換基礎架構與存取流程，而零信任架構身分鑑別為優先導入機制
- 藉由提供導入建議，協助政府機關實施零信任架構，強化資安防護能力

發展目的

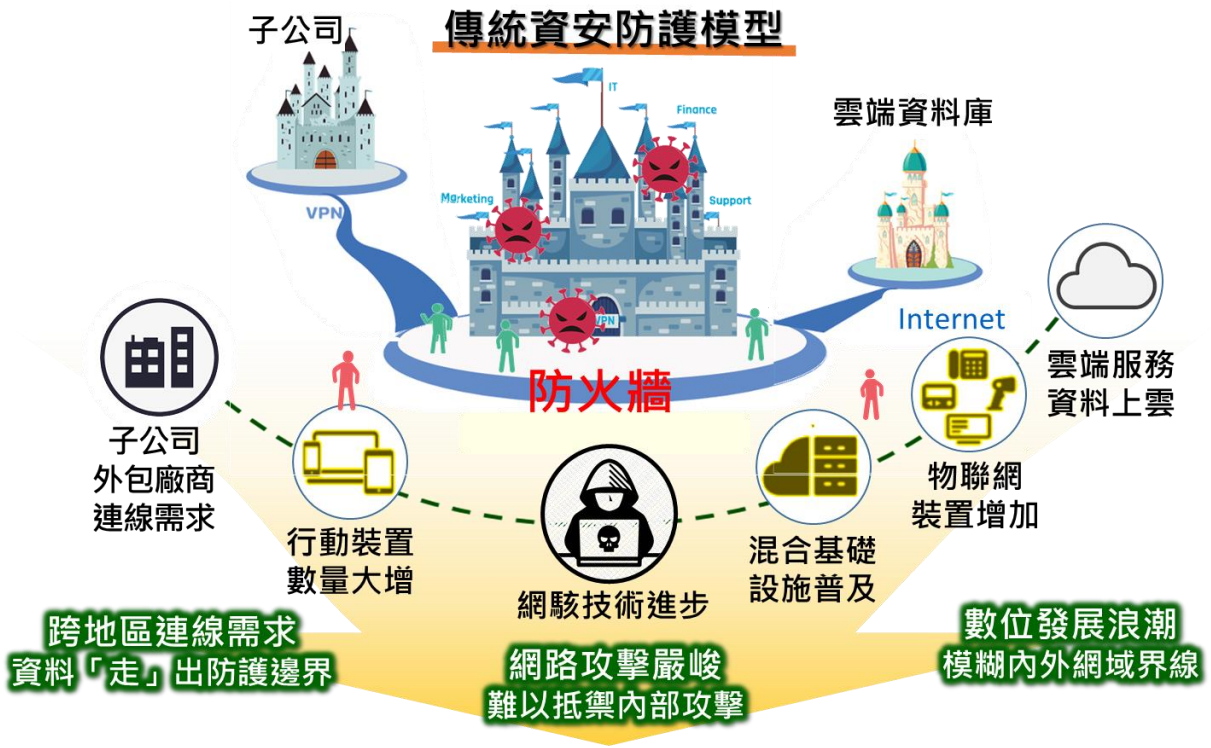
- 發展本導入建議之目的，在於協助機關了解政府零信任架構與核心機制，透過提供可操作性之導入步驟，降低機關實施零信任架構之疑慮與負擔，逐步建立零信任架構資安防護環境



政府零信任架構說明

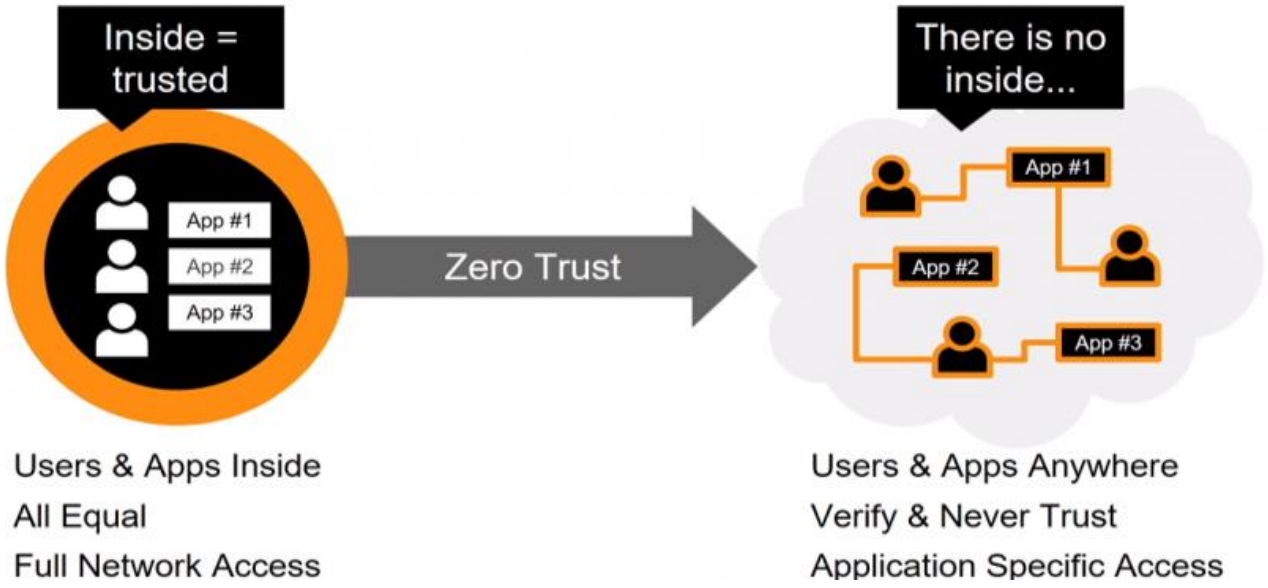
傳統網路模型的資安窘境

- 隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已現資安窘境，難以滿足新形態工作需求



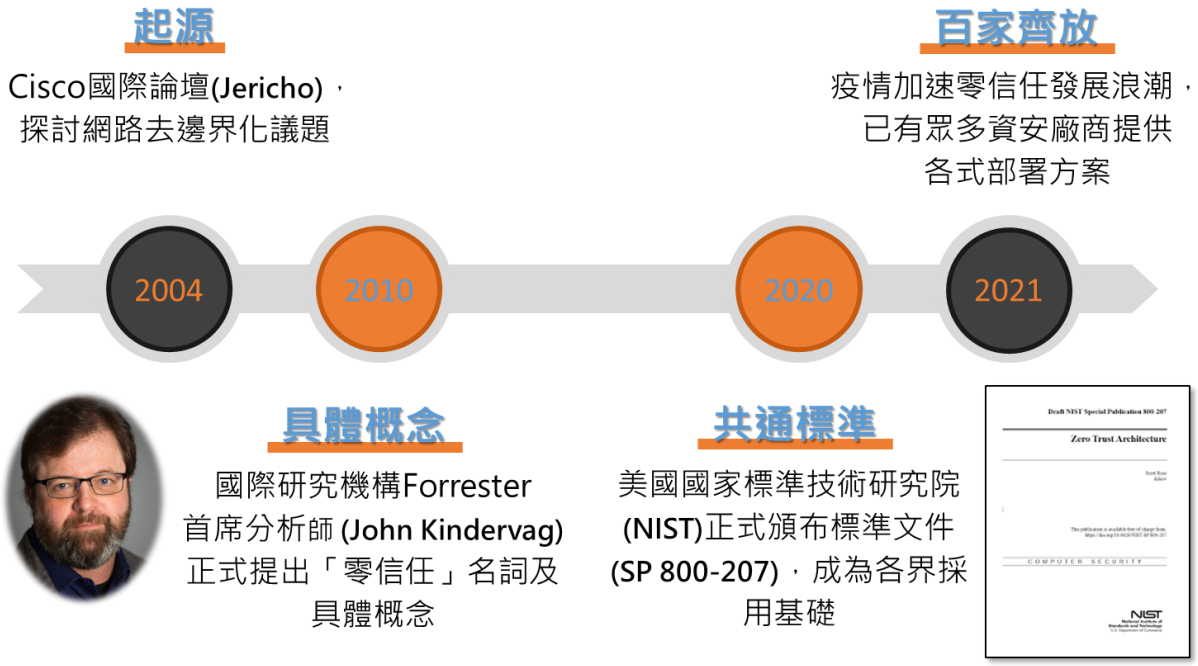
零信任概念

- 零信任希望突破傳統網路模型的資安窘境，並能保護資料存取
  - 不是保護網路存取，而是保護資料/應用存取
  - 無具體邊界，使用者/設備與資料/應用無處不在
  - 任何資料存取永不信任且必須驗證



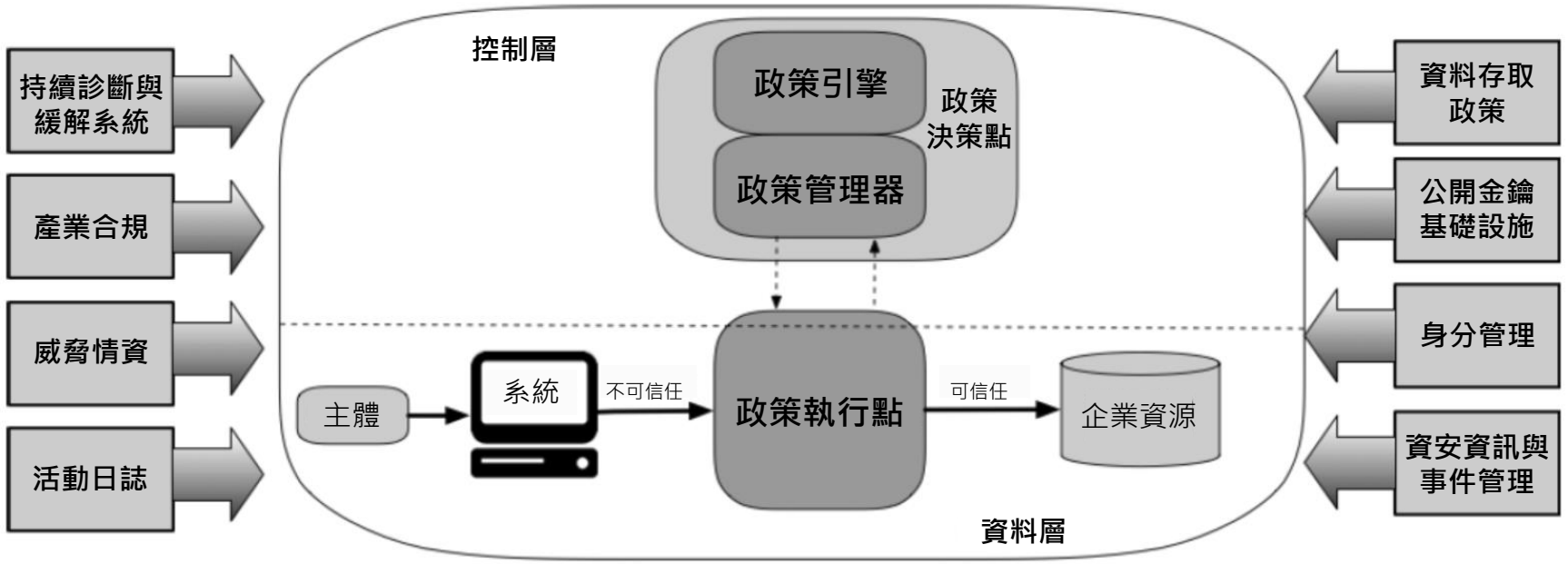
零信任演進

- 零信任概念歷經10幾年發展，2020年美國國家標準技術研究院(NIST)正式頒布標準文件SP 800-207：零信任架構(Zero Trust Architecture, ZTA)，成為各界採用基礎



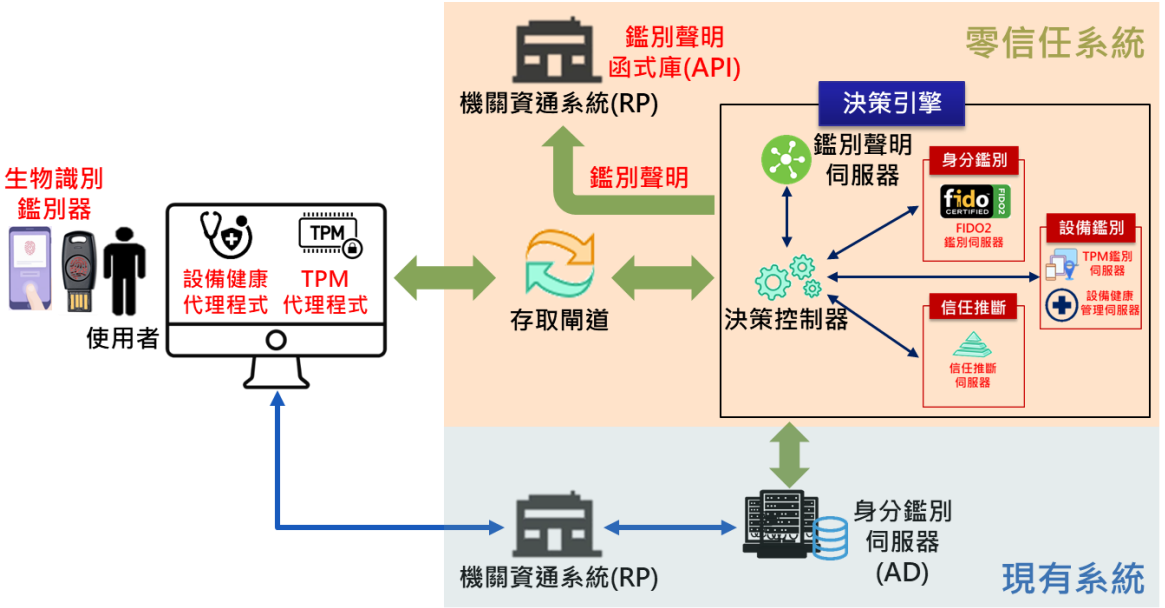
NIST零信任架構

- NIST SP 800-207將零信任架構分成核心組件與支援組件
  - –核心組件：執行鑑別、決定授權及管理連線
  - –支援組件：支援存取決策的資訊與系統



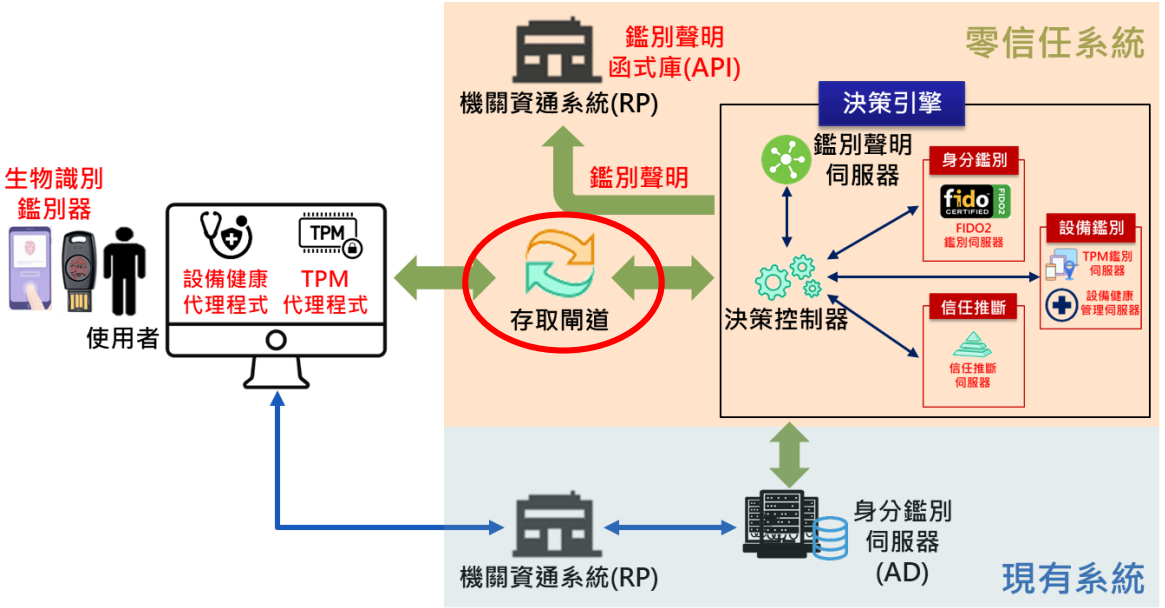
政府零信任架構

- 政府零信任架構係參考NIST SP 800-207零信任架構，同時結合向上集中之防護需求，採取資源門戶之部署方式(Resource Portal-Based Deployment)，包含身分鑑別、設備鑑別及信任推斷3大核心機制
  - 身分鑑別：多因子身分鑑別與身分鑑別聲明
  - 設備鑑別：設備鑑別與設備健康管理
  - 信任推斷：使用者情境信任推斷機制



資源門戶部署方式

- 政府零信任架構採資源門戶之部署方式，存取閘道為機關資通系統之存取門戶，其依據決策引擎之存取決定，負責建立、監控及終止使用者與機關資通系統間之網路連線
  - 不論來自內部或外部網路，均經由存取閘道進行存取
  - 透過反向代理技術，隱藏內部伺服器與機關資通系統之網路路徑
  - 實施負載平衡與防止阻斷服務攻擊之機制



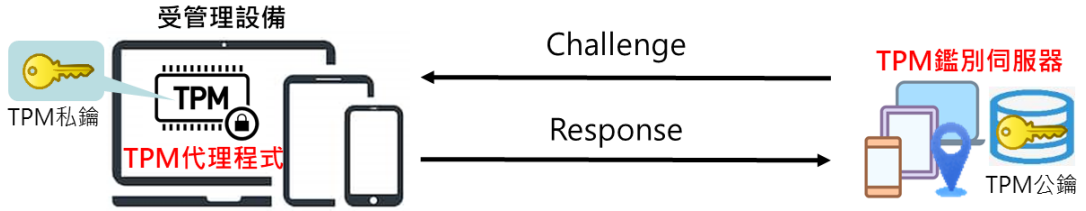
身分鑑別

- 多因子身分鑑別
  - 例如FIDO多因子身分鑑別機制，可使用實體安全金鑰(USB Token)或手機APP進行無密碼登入

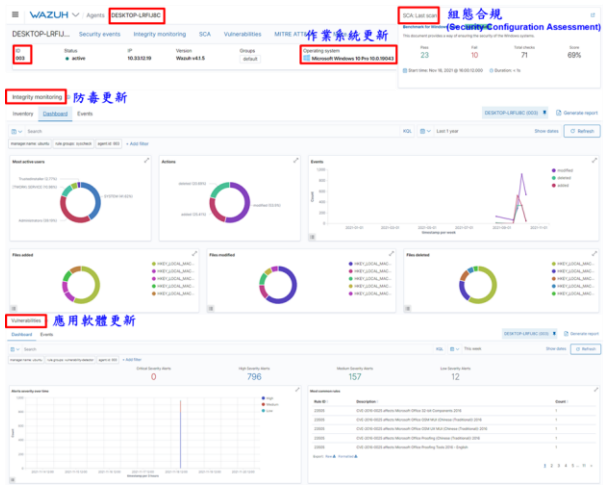
- 簽章與加密之身分鑑別聲明
  - 使用者於獲得存取允許後，由鑑別聲明伺服器發行給使用者之存取授權證明(例如JWT或SAML標準格式)，透過鑑別聲明函式庫(API)，機關資通系統介接時可取得與驗證鑑別聲明

設備鑑別

- 設備鑑別方法
  - 執行基於軟體憑證或信任平台模組(TPM)之公開金鑰密碼系統鑑別協議，以確認使用者端點設備是受機關管理之設備



- 設備健康管理
  - 持續性設備健康狀態監控與管理系統
  - 依設備健康狀態隨時更新設備健康信任等級

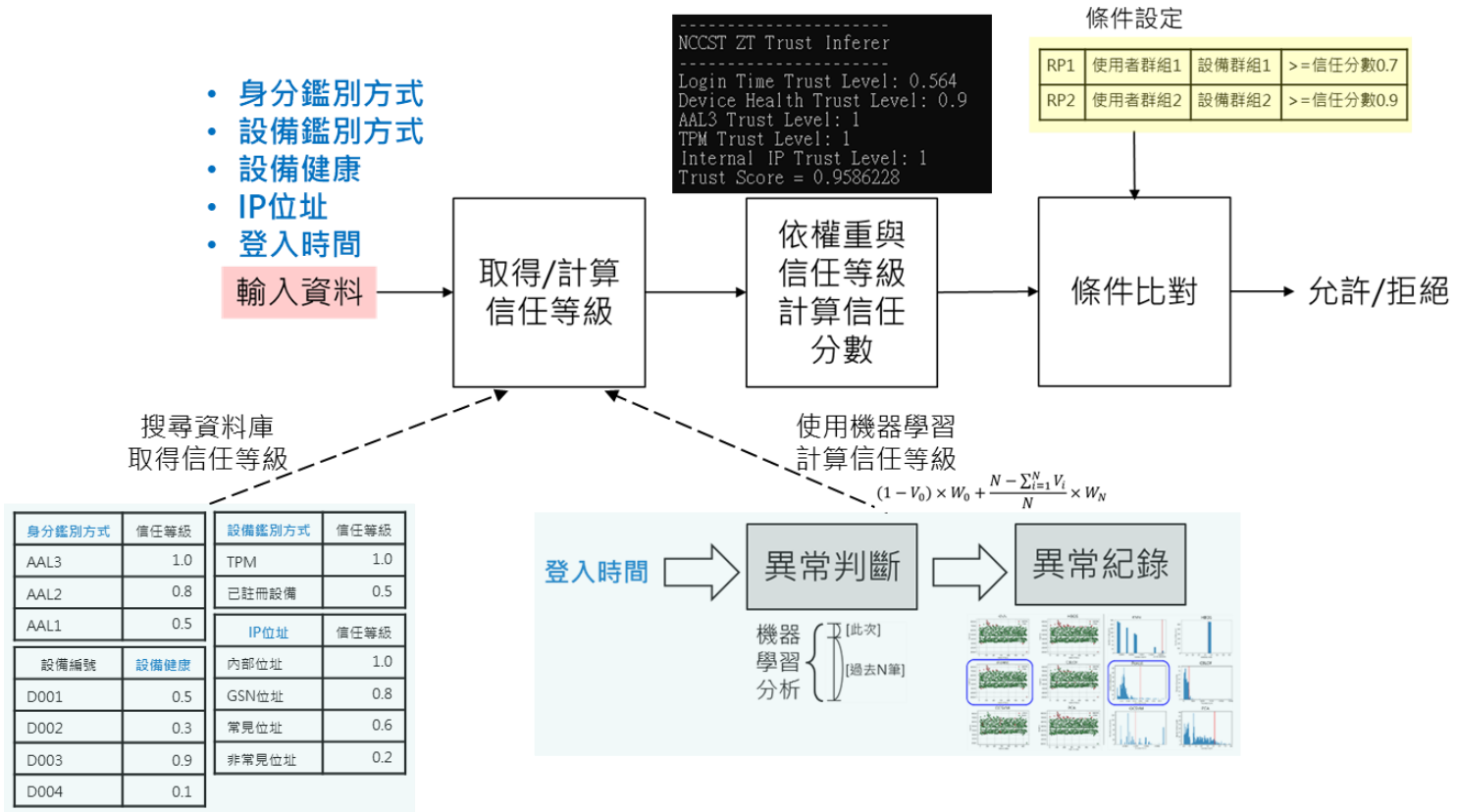


設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

健康狀態/等級分配
(A)作業系統更新：0.4
(B)防毒更新　　：0.3
(C)應用軟體更新：0.2
(D)組態合規　　：0.1

信任推斷

- 信任推斷依各類輸入資料(身分鑑別結果、設備鑑別結果、設備健康信任等級及使用者情境等)，進行(智慧)評估與計算，輸出信任分數以提供存取決策

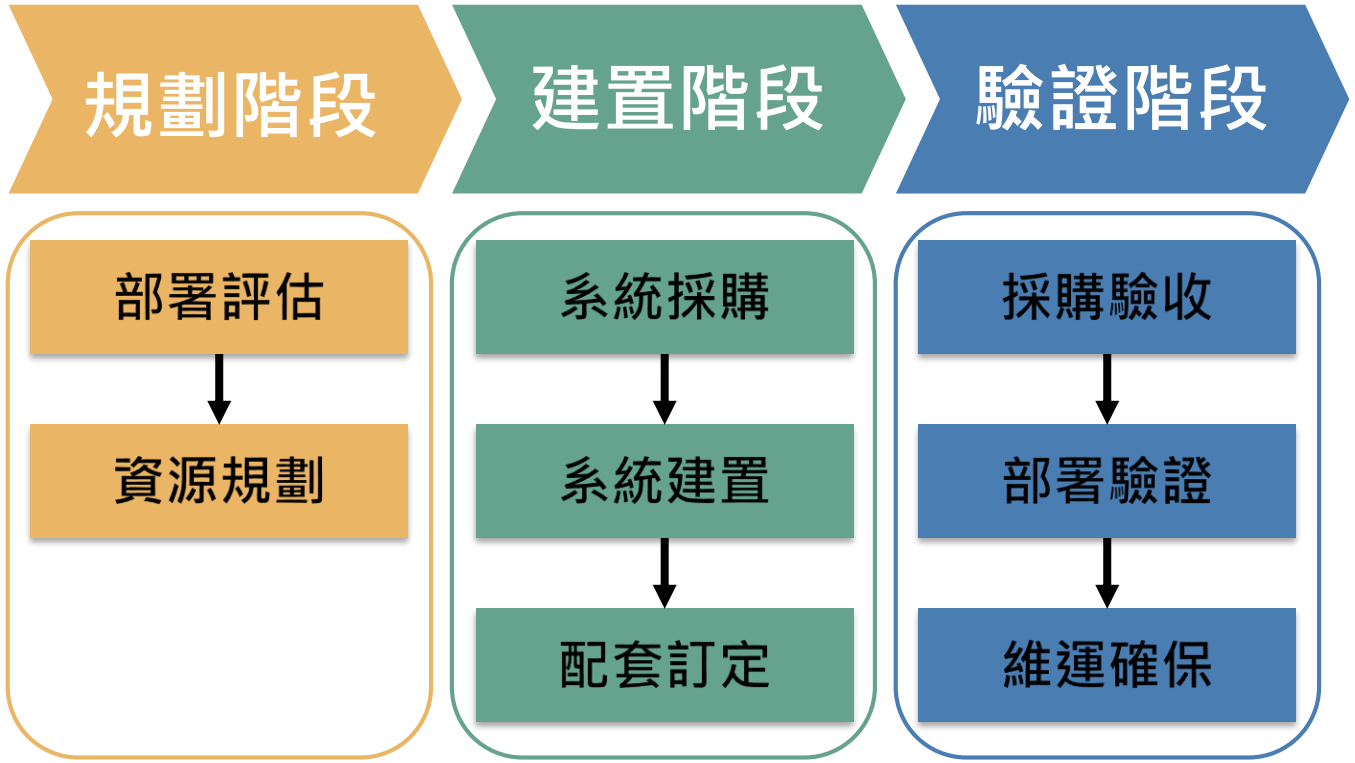


部署原則

- 相關機關試行零信任身分鑑別系統，以介接具個資或高度敏感資料之RP系統為原則，且試行對象以機關所選RP系統之維運人員為主
- 導入零信任架構是一段逐步成熟之過程，不是一次大規模替換基礎架構與存取流程，相關組件之部署須與現有系統同時混合運作
- 零信任架構之導入以資源門戶部署方式為基礎，逐步導入決策引擎之身分鑑別、設備鑑別及信任推斷3大核心機制

政府零信任架構身分鑑別機制導入建議

導入流程



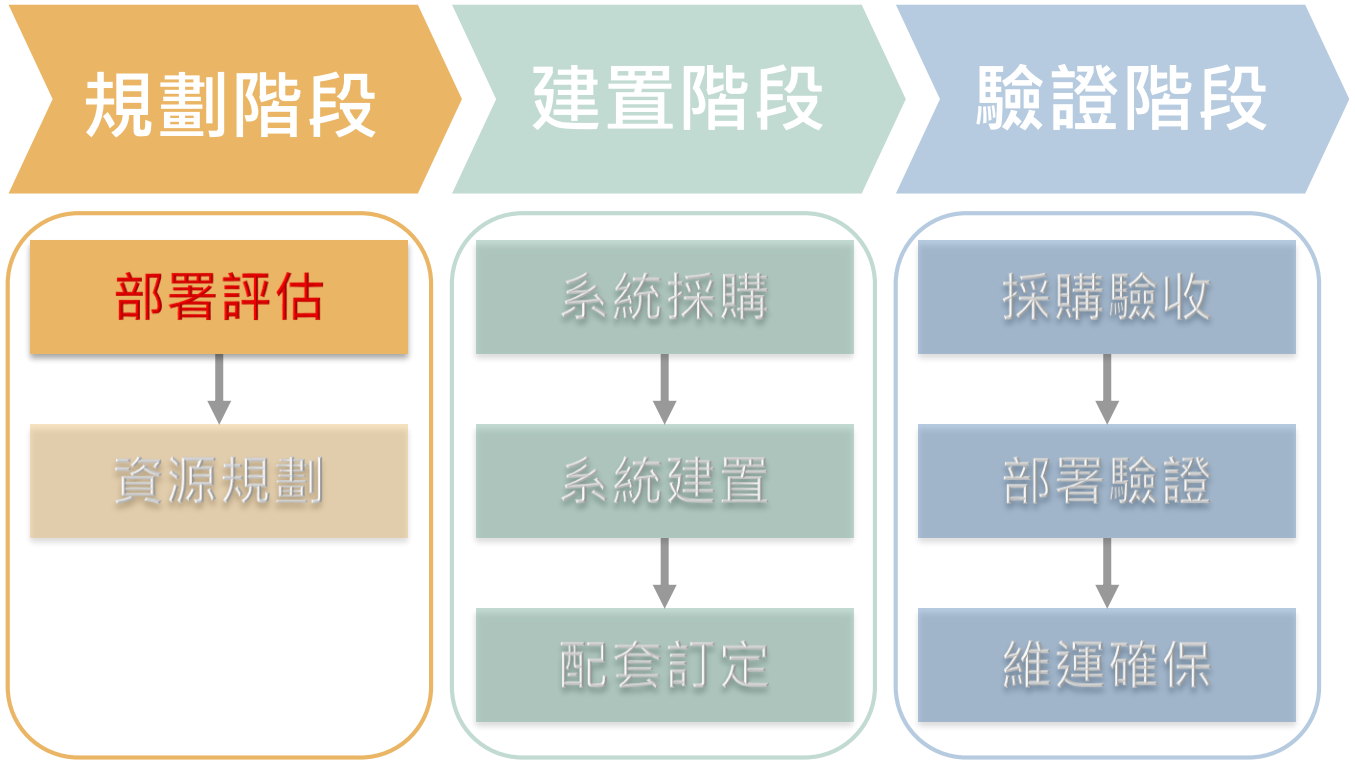
導入檢核清單(1/2)

項次	導入作為	依據	完成
規劃階段			
1	選擇導入之資通系統	表1-1	☐
2	評估身分鑑別與設備鑑別	表2-1、表2-2、表2-3	☐
3	評估使用者帳號與設備是否維持一致	表3-1	☐
4	尋求零信任架構身分鑑別與設備鑑別系統	通過功能符合性驗證廠商清單	☐
5	評估鑑別器採用方案	表5-1	☐
6	評估資通系統介接之工作量	表6-1	☐
7	規劃導入所需軟體	表7-1	☐
8	規劃導入所需硬體	表8-1	☐
9	規劃導入所需經費	表9-1	☐
建置階段			
10	採購導入所需之軟硬體	機關採購作業程序	☐
11	部署零信任架構身分鑑別與設備鑑別系統	表11-1	☐
12	介接現有身分鑑別伺服器	表12-1	☐
13	介接導入之資通系統	零信任架構資通系統連線測試	☐
14	設定網路環境	表14-1、表14-2	☐
15	訂定鑑別器與設備管理作業辦法	機關鑑別器與設備管理作業辦法	☐

導入檢核清單(2/2)

項次	導入作為	依據	完成
驗證階段			
16	驗收採購項目	機關採購驗收作業程序	☐
17	驗證部署符合性	政府零信任架構身分鑑別部署驗證檢核表、政府零信任網路設備鑑別部署驗證檢核表	☐
18	確保具備維運與使用能力	說明文件與教育訓練課程	☐

導入流程



選擇導入之資通系統(1/2)

- 說明
  - 傳統存取方式受限於內網或外網需透過VPN連線，零信任網路的身分鑑別與設備鑑別機制解除了地域限制，使得無論在內外網，都可透過存取閘道存取機關允許的資通系統
  - 存取閘道成為關鍵的存取控制點，透過身分鑑別與設備鑑別機制，有效篩選合法且受信任的使用者和設備，確保僅有授權的存取
  - 零信任網路允許機關實施選擇性存取控制，可依據使用者的身分和設備的信任度，差異化地控制對不同資通系統的存取權限。作法
  - 盤點機關資通系統之
    - 允許存取之身分方式
    - 允許存取之設備
    - 允許存取之網路連線
  - 排定導入優先序
- 建議
  - 由於尚未導入設備鑑別與信任推斷機制，建議優先選擇原本允許透過VPN存取之資通系統
  - 建議優先選擇原本以通行碼為身分鑑別方式之資通系統，以提升鑑別保證等級
  - 建議僅導入1個或少數資通系統，先累積經驗
- 檢核依據
  - 完成表1-1，並依優先序選擇導入之資通系統

選擇導入之資通系統(2/2)

- 表1-1

1-1：盤點機關資通系統並排定導入優先序							
資通系統名稱	身分鑑別方式				網路連線		優先序
	通行碼	SSO	自然人憑證	其他	內網	VPN	
資通系統A	√				√		3
資通系統B		√			√	√	2
資通系統C	√				√	√	1
資通系統D			√		√		4

評估身分鑑別與設備鑑別(1/2)

- 說明
  - 身分鑑別方式之改變將影響使用者登入習慣與管理者相關管理作業
  - 機關之多元環境可能尚無法全面改採多因子身分鑑別方式
- 作法
  - 針對導入之資通系統
    - 條列多因子身分鑑別與設備鑑別之影響事項與程度
    - 條列尚無法改採多因子身分鑑別方式之環境、原因及人數
- 建議
  - 若多因子方式之影響程度為中級以上，建議先階段性新舊鑑別方式併行
  - 若存在無法改採多因子身分鑑別方式之環境，建議先階段性新舊身分鑑別方式併行
  - 機關可以選擇先實施可行的多因子身分鑑別與設備鑑別方式，同時繼續使用現有的身分鑑別方式和設備鑑別方式，直到資源、環境與人員的適應度達到轉換的可行性
- 檢核依據
  - 完成表2-1、2-2與2-3，並參考建議決定是否新舊鑑別方式併行

評估身分鑑別與設備鑑別(2/2)

- 表2-1

2-1：條列多因子身分鑑別方式之影響事項與程度				
資通系統名稱：資通系統C				
多因子方式	影響事項	影響程度		
		低	中	高
實體安全金鑰	• 攜帶與遺失困擾 • 增加資產管理作業		√	
手機APP	• 私有手機公務使用意願		√	
自然人憑證	• 須讀卡機配合使用	√		

- 表2-2

2-2：條列尚無法改採多因子身分鑑別方式之環境、原因及人數		
資通系統名稱：資通系統C		
環境	無法配合原因	人數
偏鄉所屬機構	• 電腦設備老舊 • 手機通訊不穩	200
駐外單位	• 實體安全金鑰配發不易	100

- 表2-3

2-3：條列設備鑑別方式之影響事項與程度						
資通系統名稱：資通系統C						
設備類型	保證等級		影響事項	影響程度		
	硬體保護	軟體保護		低	中	高
桌上型電腦	√		•設備購置、維護和更新的費用			√
筆記型電腦	√		•設備購置、維護和更新的費用		√	
行動裝置		√	•APP擴充的可能性			√
其他	√		•面臨技術整合上的挑戰	√		

評估使用者帳號與設備是否維持一致(1/2)

- 說明
  - 導入零信任架構身分鑑別與設備鑑別機制須在新的多因子身分與設備鑑別伺服器重新註冊使用者帳號與設備資訊，機關須評估重新註冊之帳號是否維持與現有帳號(例如AD帳號)一致，並落實設備盤點，驗證使用者設備是否符合機關所制定的安全要求
- 作法
  - 分析使用者帳號與設備維持一致之優缺點
- 建議
  - 因導入零信任架構之過程現有系統仍須同時運作，且現有系統之使用者帳號管理機制(新增、刪除、鎖定及解鎖等)相對成熟與穩定，若考量導入初期希望減少管理負擔，建議維持使用者帳號與設備一致，對內部員工與主要合作夥伴保持帳號一致，對外部使用者與次要合作單位分開管理，未來再擴展為單一帳號登入體驗
- 檢核依據
  - 完成表3-1，並參考建議決定是否維持使用者帳號一致

評估使用者帳號與設備是否維持一致(2/2)

- 表3-1

3-1：分析使用者帳號與設備維持一致之優缺點	
優點	缺點
• 可確保帳號名稱一致 • 可確保帳號狀態一致 • 可確保設備狀態一致 • 可減少管理負擔 • 其他	• 須提供1組介接之帳號/通行碼，該帳號須具備可查詢使用者帳號狀態之權限 • 失去帳號與設備重新清點的機會 • 難以細緻區隔使用者功能與權限 • 有些特殊情境可能不適用一致性原則，例如業務需求的多樣性或合規性要求的不同。 • 其他

尋求整合零信任網路身分鑑別與設備鑑別系統

- 說明
  - 導入零信任架構身分鑑別與設備鑑別機制須部署存取閘道、決策引擎、多因子身分鑑別及身分鑑別聲明等組件，機關須尋求符合架構與功能需求之技術解決方案
- 作法
  - 尋求已整合須部署組件並符合需求之整體解決方案
- 建議
  - 建議參考資安院零信任架構專區網頁(https://www.nics.nat.gov.tw/ZeroTrustMain.htm?lang=zh)之通過功能符合性驗證廠商清單
- 檢核依據
  - 已參考資安院提供之通過功能符合性驗證廠商清單

評估鑑別器採用方案(1/2)

- 說明
  - 零信任架構身分鑑別機制之使用者須使用鑑別器(Authenticator)以進行多因子身分鑑別，依身分鑑別機制之設計，常用之鑑別器包含：
    - 簡訊手機
    - 一次性密碼(One Time Password, OTP)裝置
    - 自然人憑證
    - FIDO實體安全金鑰(USB Token)或手機APP
  - 針對FIDO身分鑑別機制，通常同時提供實體安全金鑰與手機APP選擇使用，機關須評估採用實體安全金鑰或手機APP或兩者混合
- 作法
  - 針對FIDO實體安全金鑰與手機APP，分析使用優缺點與所需配套措施，並評估使用數量
- 建議
  - 建議以實體安全金鑰與手機APP混合使用，可因應不同環境與經費預算之限制，亦可了解不同之使用體驗意見以做為後續使用參考
- 檢核依據
  - 完成表5-1，並決定鑑別器採用方案

評估鑑別器採用方案(2/2)

- 表5-1

5-1：分析使用不同FIDO鑑別器之優缺點，並評估使用數量			
FIDO鑑別器	優點	缺點	使用數量
實體安全金鑰	免安裝軟體	• 須採購經費 • 有遺失風險 • 有資產管理議題	50
手機APP	• 使用便利 • 不須額外採購	私有手機公務使用意願	200

評估資通系統介接之工作量(1/2)

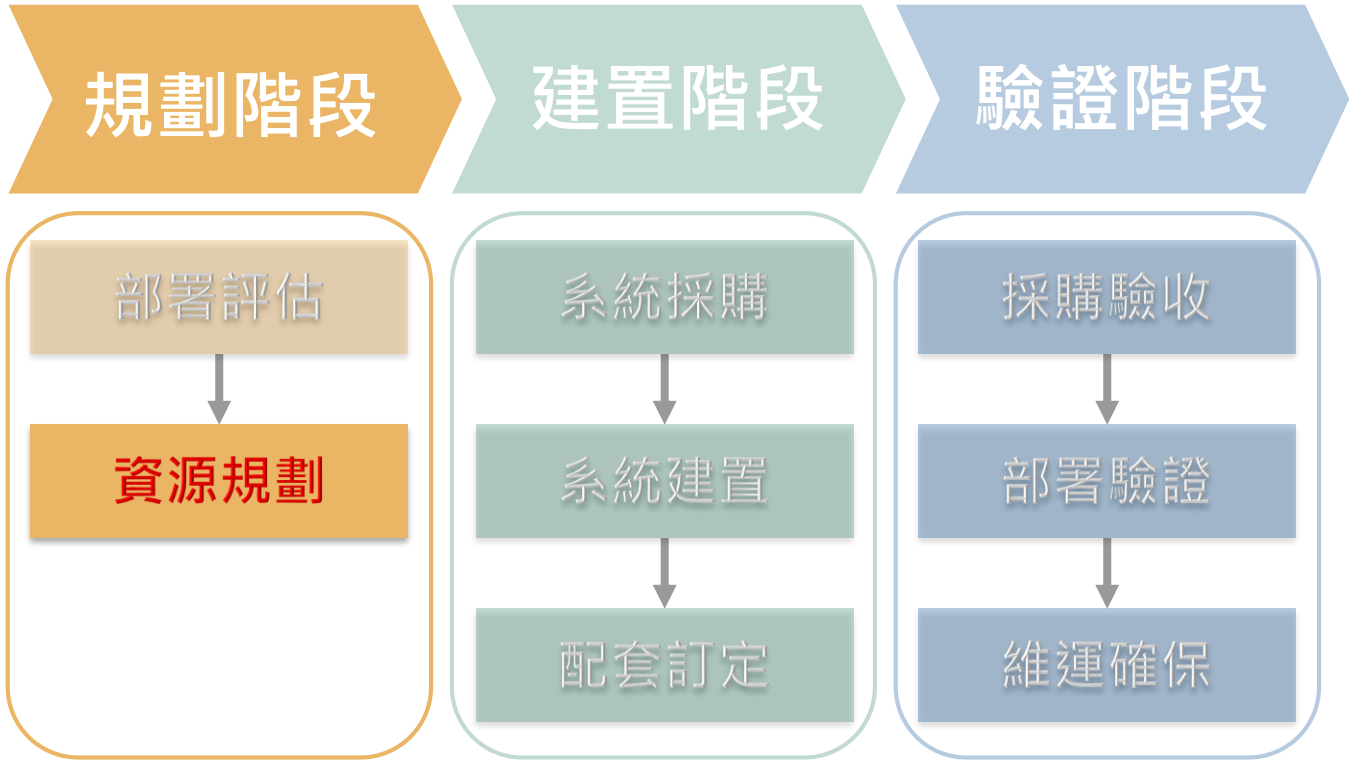
- 說明
  - 導入之資通系統須調整鑑別流程以介接零信任網路，亦即調整決策引擎整合身分鑑別與設備鑑別允許存取之依據，此部分可能須修改資通系統程式呼叫鑑別聲明函式庫API以取得決策引擎驗證鑑別聲明
- 作法
  - 針對導入之資通系統，與開發團隊或廠商討論，評估資通系統介接所需之工作量與時程
- 建議
  - 由於此階段尚未確定零信任架構身分鑑別與設備鑑別系統之提供廠商，因此可請候選廠商或資安院協助提供鑑別聲明函式庫API參考範例與介接經驗，供機關評估參考
- 檢核依據
  - 完成表6-1

評估資通系統介接之工作量(2/2)

- 表6-1

6-1：評估資通系統介接所需之工作量與時程		
資通系統名稱：資通系統C		
介接工作項目	工作量	時程
調整身分鑑別方式	1人日	XXX年XX月
調整設備鑑別方式	1人日	XXX年XX月
調整允許存取依據	3人日	XXX年XX月
介接測試	1人日	XXX年XX月

導入流程



規劃導入所需軟體(1/2)

- 說明
  - 依部署評估結果，規劃需部署之軟體，包含
    - 決策引擎系統軟體，具備多因子身分鑑別功能，能整合設備鑑別與其他安全模組，提供API介接其他資通系統，並考量系統擴充彈性與韌性
    - 終端設備代理程式軟體，可支援各類終端設備平台，提供硬體與軟體保護功能，具備自動化設備註冊與金鑰管理，並能記錄設備完整生命週期
    - 資通系統介接軟體， 負責與決策引擎API溝通，對資通系統原功能最小化影響，提供設備與使用者存取日誌，並支援自動化權限控管作法
- 建議
  - 零信任架構身分鑑別與設備鑑別系統
    - 請提供整體或個別組件解決方案之廠商依所需之使用者註冊授權數提供報價(建置與維護)與規格
    - 評估所需之使用者註冊授權數
  - 資通系統介接
    - 依評估之資通系統介接工作量請開發廠商提供報價
- 檢核依據
  - 完成表7-1

規劃導入所需軟體(2/2)

- 表7-1

7-1：規劃需部署之軟體			
軟體名稱：零信任架構身分鑑別與設備鑑別系統			
使用者註冊授權數	解決方案	建置報價	維護報價
200	甲廠商整體解決方案	XXX萬	建置報價10%
軟體名稱：資通系統介接			
解決方案		建置報價	維護報價
資通系統C開發廠商		XX萬	無

規劃導入所需硬體(1/2)

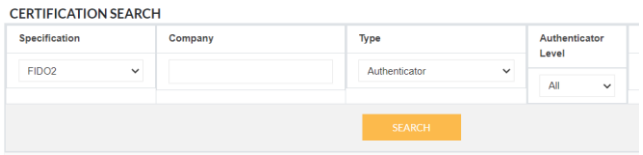
- 說明
  - 依部署評估結果，規劃需部署之硬體，包含
    - 伺服器主機，用於安裝零信任架構身分鑑別與設備鑑別系統之軟體組件
    - 實體安全金鑰
- 作法
  - 伺服器主機
    - 依零信任架構身分鑑別系統廠商提供之規格，評估所需之伺服器主機數量
    - 評估使用實體電腦或虛擬機器
    - 評估使用既有資源或須額外採購
  - 實體安全金鑰
    - 依評估之實體安全金鑰使用數量，請合規廠商提供報價
- 檢核依據
  - 完成表8-1

規劃導入所需硬體(2/2)

- 表8-1

8-1：規劃需部署之硬體		
硬體名稱：伺服器主機		
所需數量	使用類型(規格)	報價
3	實體電腦1台	XX萬
	虛擬機器2台	既有資源
硬體名稱：實體安全金鑰		
所需數量	使用類型(規格)	報價
50	• 指紋識別 • Type-A介面	X萬

通過FIDO聯盟驗證之實體安全金鑰，可至FIDO Certified網頁查詢(https://fidoalliance.org/certification/fido-certified-products/)



規劃導入所需經費(1/2)

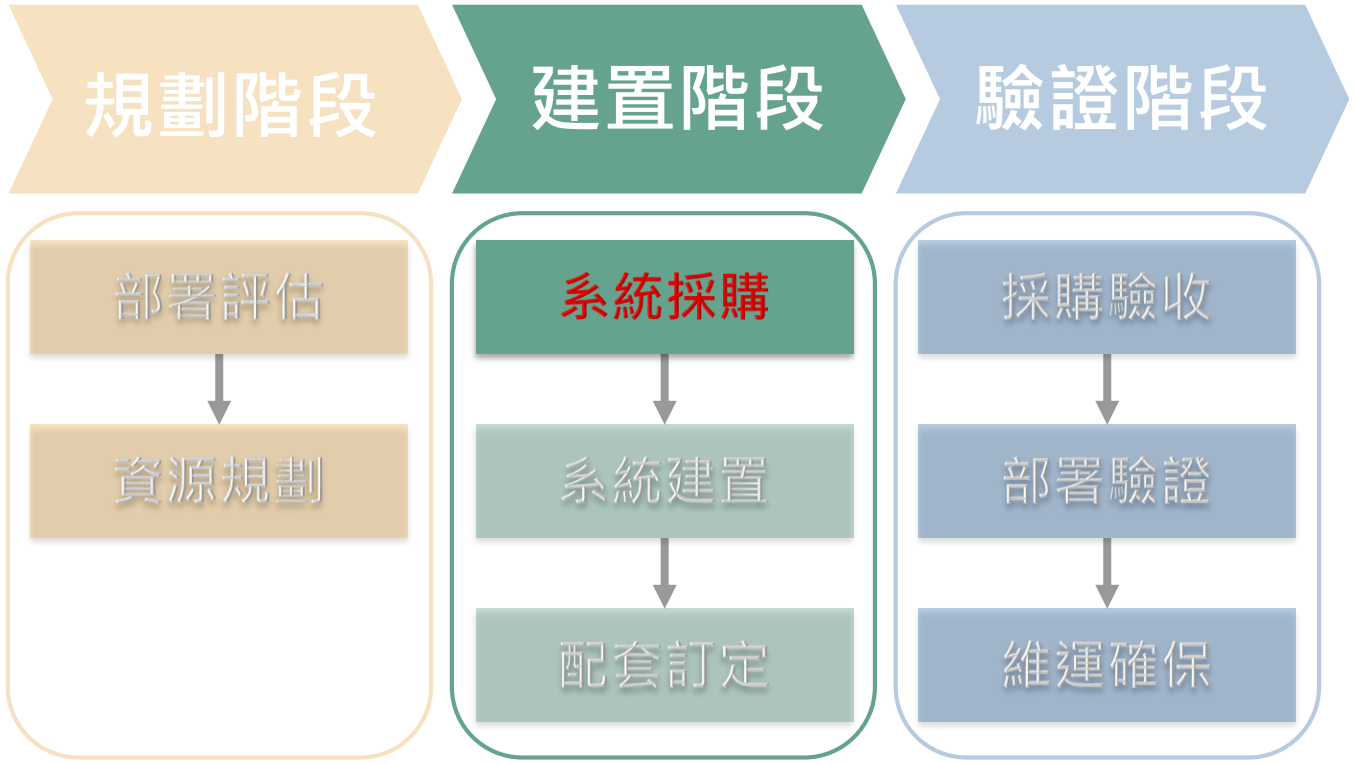
- 說明
  - 計算導入所需全部經費，並規劃經費來源
- 作法
  - 依軟體與硬體規劃之結果
    - 條列需採購項目
    - 規劃經費來源
- 檢核依據
  - 完成表9-1

規劃導入所需經費(2/2)

- 表9-1

9-1：條列需採購項目並規劃經費來源			
採購項目	經費說明	所需經費	經費來源
零信任架構身分鑑別與設備鑑別系統	系統建置	XXX萬	專案補助
	系統維護	XX萬	113年起逐年預算
資通系統介接	介接開發	X萬	113年預算
伺服器主機	實體電腦1台	XX萬	113年預算
實體安全金鑰	50隻	X萬	113年預算

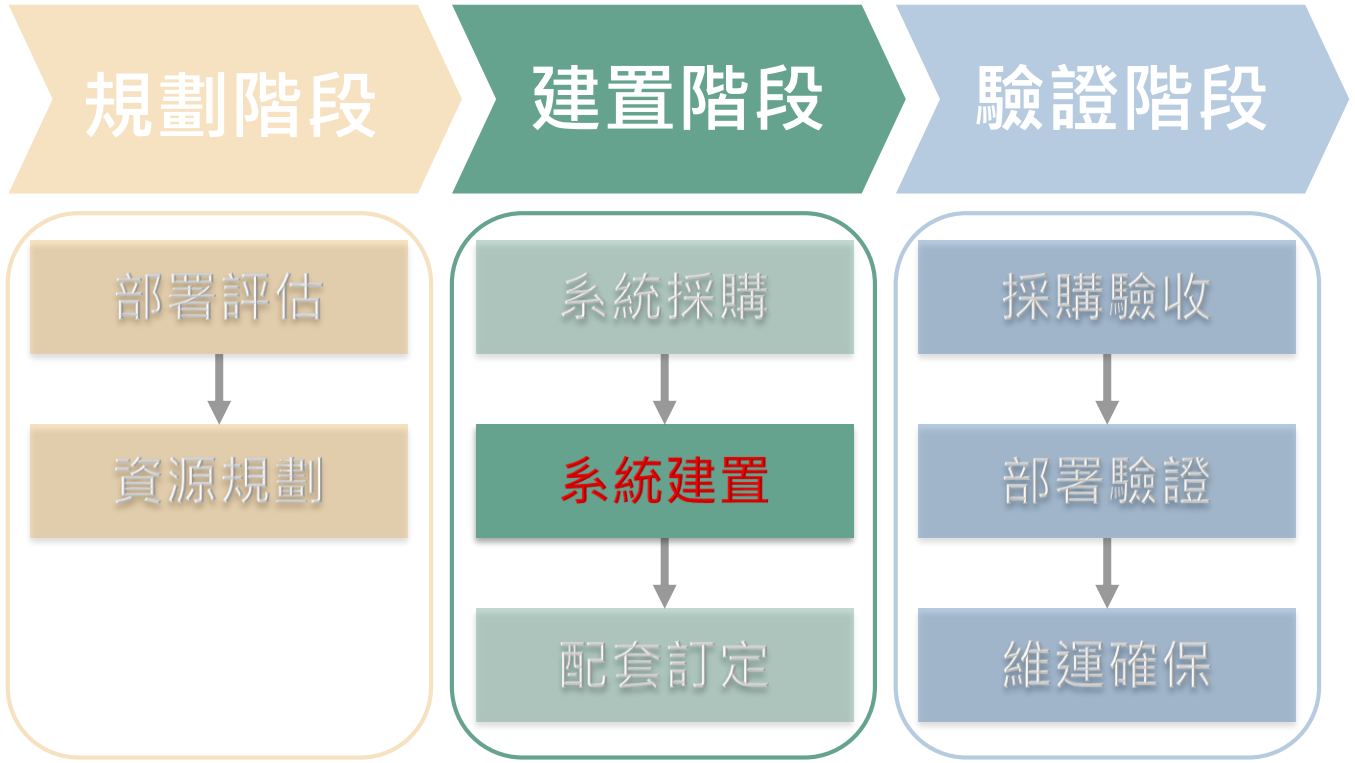
導入流程



採購導入所需之軟硬體

- 說明
  - 進行導入所需之軟硬體採購作業
- 作法
  - 針對規劃之採購項目，依政府採購法與機關採購相關辦法，辦理各項目採購作業
    - 零信任架構身分鑑別與設備鑑別系統
      - 建議採購需求說明書要求得標廠商需依機關需求客製化存取閘道入口網頁
      - 建議採購需求說明書要求得標廠商需協助鑑別聲明函式庫之介接使用
      - 終端設備代理程式套件
    - 資通系統介接
    - 伺服器主機
    - 實體安全金鑰
- 檢核依據
  - 機關採購作業程序

導入流程



部署零信任架構身分鑑別與設備鑑別系統(1/2)

- 說明
  - 針對完成採購之零信任架構身分鑑別與設備鑑別系統，由得標廠商進行系統安裝
- 作法
  - 系統安裝前
    - 機關與得標廠商確認存取閘道入口網頁之客製化需求
    - 機關與得標廠商確認機關應準備之系統組件資源
      - 伺服器主機(實體電腦或虛擬機器)
      - 伺服器IP位址
      - 伺服器網域名稱
      - 伺服器憑證
      - 代理程式套件安裝之終端設備
  - 系統安裝
    - 由得標廠商完成系統與終端安裝
- 檢核依據
  - 完成表11-1之系統安裝與功能測試

部署零信任架構身分鑑別與設備鑑別系統(2/2)

- 表11-1

11-1：系統組件所需資源與功能測試					
組件名稱	伺服器主機	IP位址	網域名稱	憑證	功能測試
存取閘道	實體電腦	192.168.33.101	ag.abc.gov.tw	ag.abc.gov.tw.p12	□
決策引擎	虛擬機器	192.168.33.102	de.abc.gov.tw	de.abc.gov.tw.p12	
身分鑑別聲明					
設備鑑別聲明					
多因子身分鑑別	虛擬機器	192.168.33.103	au.abc.gov.tw	au.abc.gov.tw.p12	
終端設備代理程式套件	終端設備			設備憑證一覽表	□

介接現有身分鑑別伺服器(1/2)

- 說明
  - 依使用者帳號維持一致之評估結果，由零信任架構身分鑑別系統之得標廠商進行與現有身分鑑別伺服器之介接設定
- 作法
  - 介接前
    - 機關與得標廠商確認機關應準備之資源
      - 現有身分鑑別伺服器IP位址
      - 現有身分鑑別伺服器網域名稱
      - 現有身分鑑別伺服器之1組介接用帳號/通行碼，該帳號須具備可查詢使用者帳號狀態之權限
  - 系統介接
    - 由得標廠商完成介接設定
- 檢核依據
  - 完成表12-1之現有身分鑑別伺服器連線與帳號一致性測試

介接現有身分鑑別伺服器(2/2)

- 表12-1

12-1：現有身分鑑別伺服器資源與介接測試			
IP位址	網域名稱	介接用帳號/通行碼	帳號一致性測試
192.168.22.101	ad.abc.gov.tw	ldapquery/xxxxxxxx	☐

介接導入之資通系統

- 說明
  - 依資通系統介接之工作量評估，由資通系統開發廠商調整身分鑑別流程，以介接零信任架構
- 作法
  - 介接前
    - 機關確認鑑別聲明函式庫廠商須提供之資源
      - 鑑別聲明函式庫
      - 鑑別聲明函式庫說明文件
      - 鑑別聲明函式庫範例程式
  - 系統介接
    - 由資通系統開發廠商完成身分鑑別流程之調整，必要時得請鑑別聲明函式庫廠商協助函式庫之介接使用
- 檢核依據
  - 完成零信任架構之資通系統連線測試

設定網路環境(1/2)

- 說明
  - 針對存取閘道與防火牆等進行網路環境設定，以符合零信任架構存取要求
- 作法
  - 存取閘道
    - 參考存取閘道說明文件，設定存取閘道與各伺服器之反向代理規則
  - 防火牆
    - 調整防火牆規則，使得不論來自內部或外部網路對資通系統之存取，皆必須且唯一經由存取閘道
- 檢核依據
  - 完成表14-1與14-2之網路環境設定

設定網路環境(2/2)

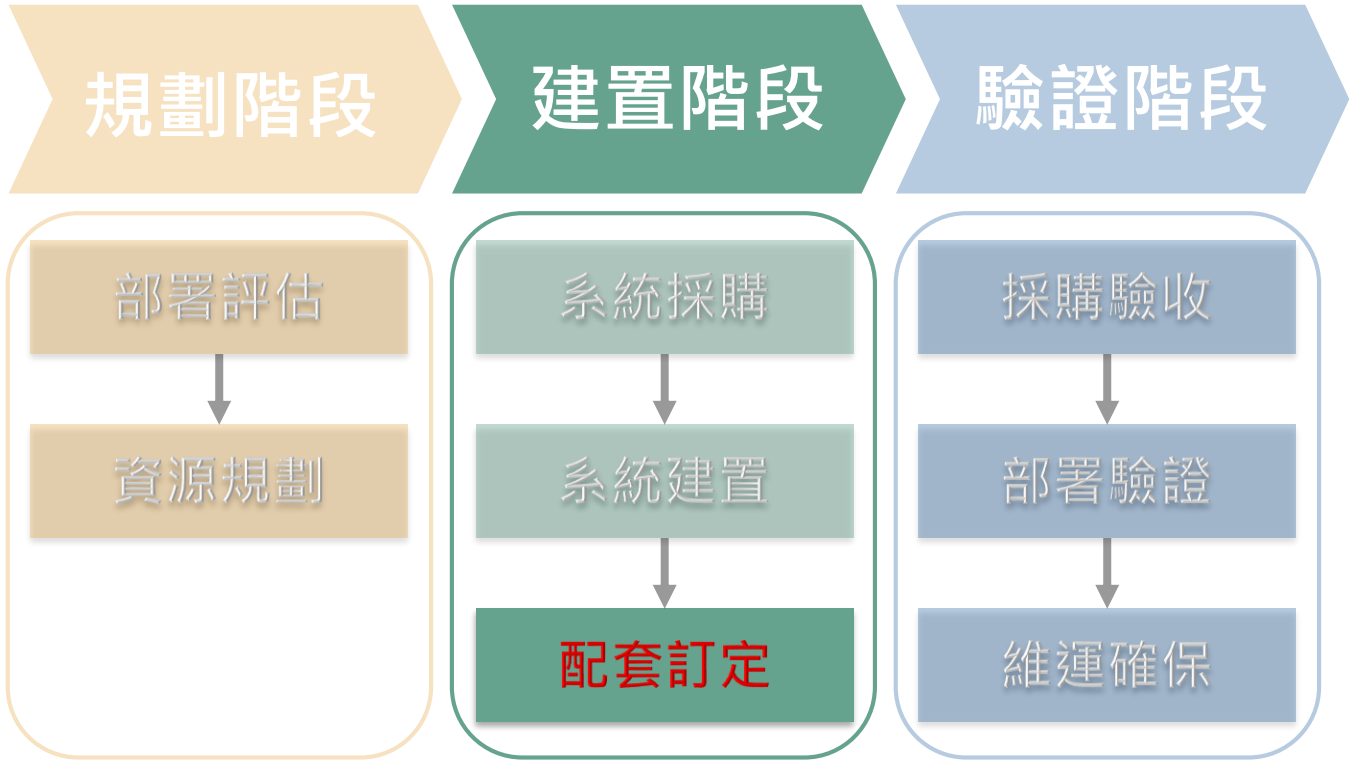
- 表14-1

14-1：存取閘道反向代理規則設定		
代理目標	存取請求	伺服器網址
決策引擎	/path1/	https://de.abc.gov.tw:8001/link1
身分鑑別聲明	/path2/	https://de.abc.gov.tw:8002/link2
多因子身分鑑別	/path3/	https://au.abc.gov.tw:8080/link3
設備鑑別聲明	/path5/	https://de.abc.gov.tw:8002/link2
資通系統	/path4/	https://rp.abc.gov.tw/link4

- 表14-2

14-2：防火牆規則設定	
項目	設定原則
內網/外網存取決策引擎、身分鑑別聲明、多因子身分鑑別、資通系統	拒絕
內網/外網存取存取閘道	允許

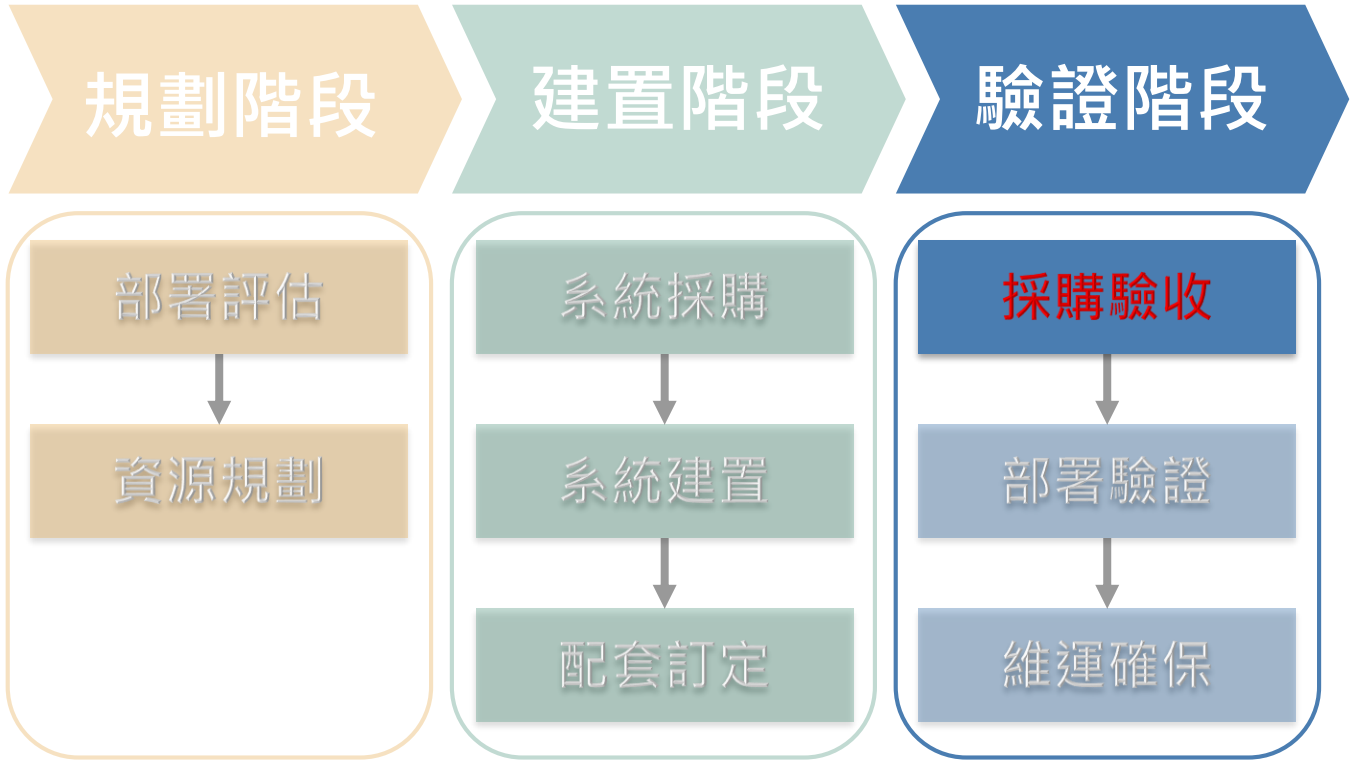
導入流程



訂定鑑別器與設備管理作業辦法

- 說明
  - 針對實體安全金鑰與手機APP等鑑別器，訂定資產管理與使用等相關作業辦法，以管控資產並確保正常運作
- 作法
  - 實體安全金鑰
    - 實體安全金鑰之配發以1人1隻為原則
    - 針對實體安全金鑰之登錄、配發、保管及遺失等訂定相關作業辦法
  - 手機APP
    - 依機關對行動裝置管理之相關資安政策，針對手機APP之安裝、使用、版本更新及解除安裝等訂定相關作業辦法
  - 終端設備
    - 依機關對行動裝置管理之相關資安政策，針對設備授權與註銷機制、更換設備的移轉流程、設備異動與變更的核准程序、設備報廢、遺失的處理原則等訂定相關作業辦法
- 檢核依據
  - 機關鑑別器管理作業辦法

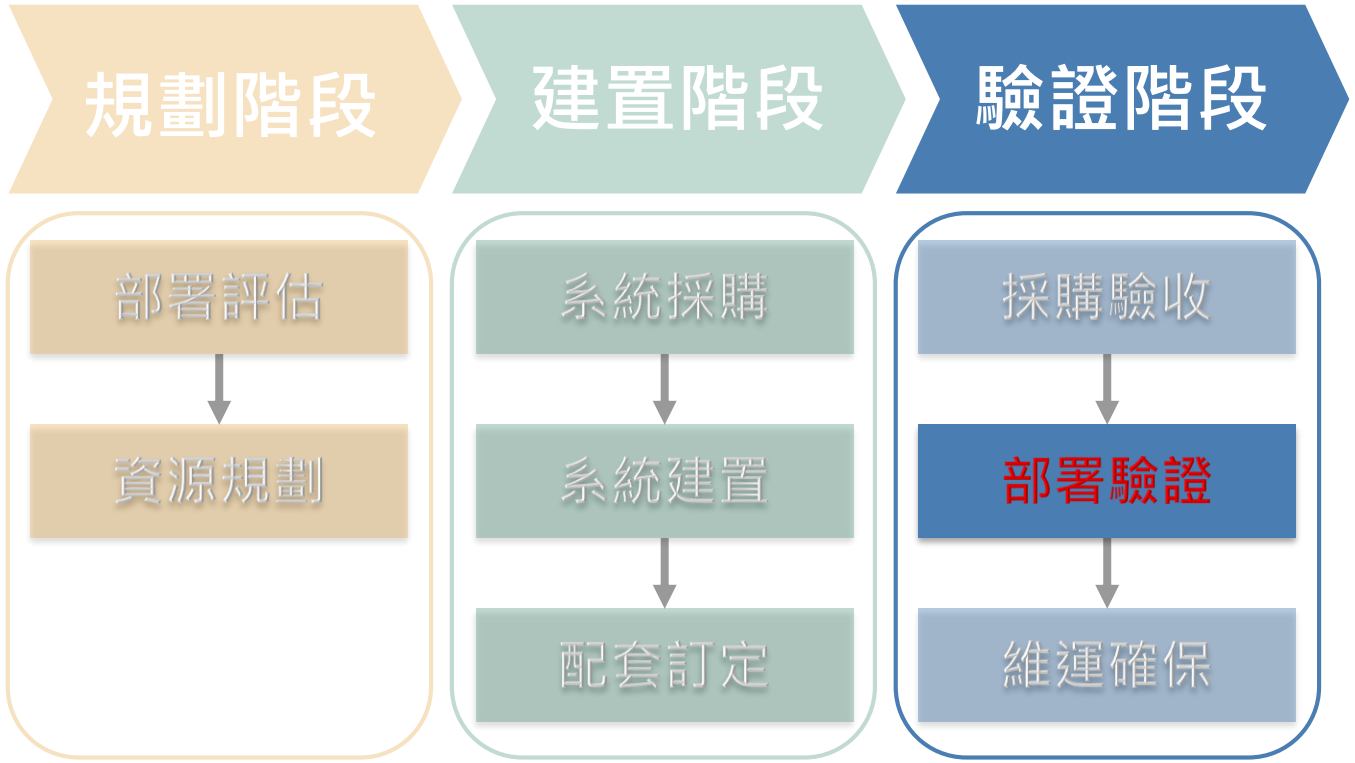
導入流程



驗收採購項目

- 說明
  - 所有採購項目均須依採購需求說明書之驗收規範進行驗收作業
- 作法
  - 針對每項採購項目，由採購承辦人員依機關採購驗收程序完成驗收作業
- 檢核依據
  - 機關採購驗收作業程序

導入流程



驗證部署符合性

- 說明
  - 針對系統建置所完成之組件部署、介接及設定，驗證是否符合政府零信任架構之架構、功能需求及部署原則
- 作法
  - 資安院協助機關依「政府零信任架構身分與設備鑑別部署驗證檢核表」進行部署驗證作業
- 檢核依據
  - 完成並符合「政府零信任架構身分與設備鑑別部署驗證檢核表」之驗證檢核

政府零信任架構身分鑑別部署驗證檢核表

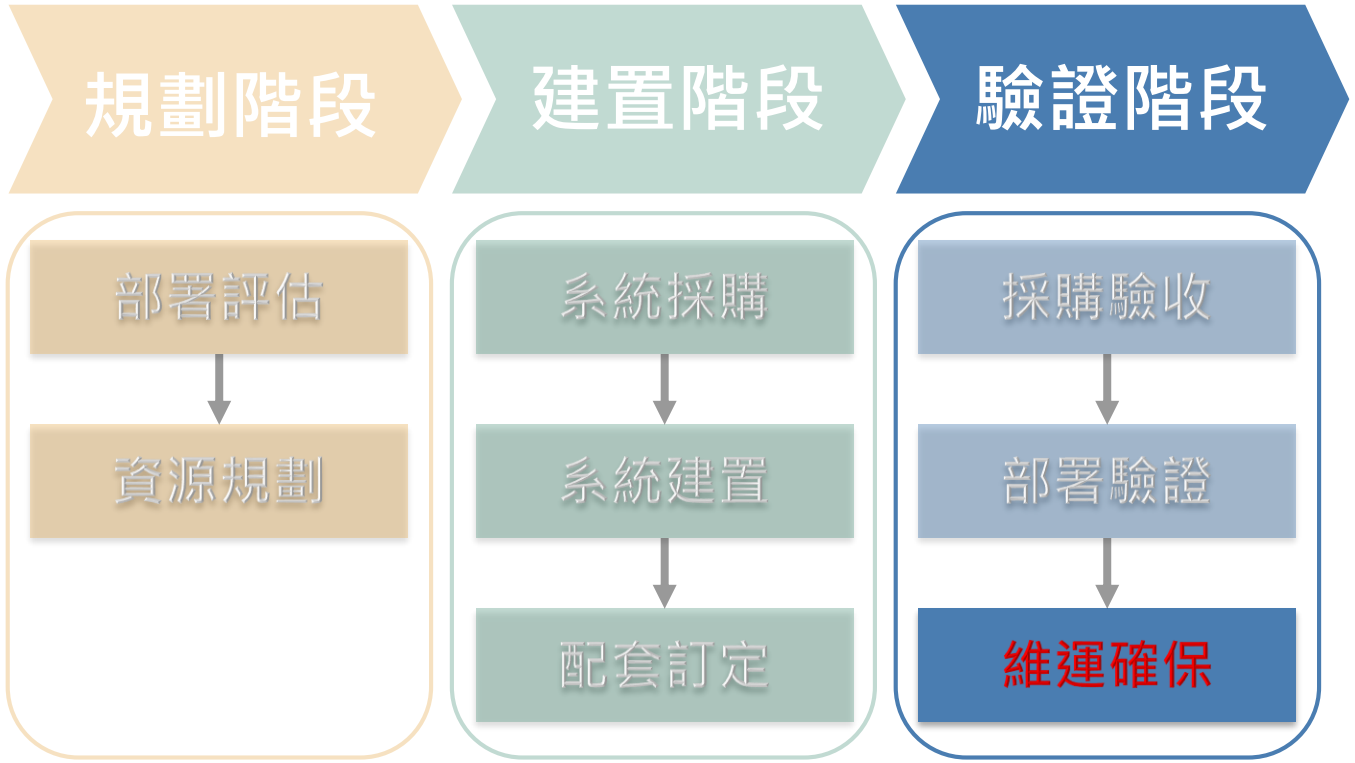
1. 零信任網路架構檢視

架構檢視包含核心組件與部署方式。

●核心組件

類別	零信任網路架構								
編號	名稱	說明	檢核項目			適用性	部署	未部署	組件名稱
ZTA-1	零信任網路核心組件	檢視零信任網路已部署之核心組件	1	已部署之決策引擎組件	身分鑑別	必要			
					設備鑑別	選項			
					信任推斷	選項			
					決策控制	必要			
			2	已部署之存取閘道組件		必要			
			3	已部署之資通系統(RP)		必要			
			4	已部署之使用者端組件		必要			
			5	已部署之其他核心組件		選項			

導入流程



確保具備維運與使用能力

- 說明
  - 針對導入之零信任架構身分鑑別與設備鑑別機制，機關須確保具備維運與使用能力
- 作法
  - 機關依採購需求說明書之交付項目，要求廠商提供維運與使用等相關說明文件
  - 機關依採購需求說明書之教育訓練，要求廠商辦理維運與使用等相關教育訓練課程
- 檢核依據
  - 依採購需求說明書，廠商完成說明文件交付與教育訓練課程辦理

參考資料

- 數位部資安署。「國家資通安全發展方案(110年至113年)」。https://moda.gov.tw/ACS/operations/policies-and-regulations/648
- NIST, "Zero Trust Architecture," NIST Special Publication 800-207, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final
- 行政院資通安全處(111年1月)。「110年數位國家資通安全主動防禦聯防計畫委外辦理案」零信任網路規劃與部署研究報告
- 資安院零信任架構專區，https://www.nics.nat.gov.tw/ZeroTrustMain.htm?lang=zh
- FIDO Alliance, https://fidoalliance.org/

報告完畢
敬請指教