Communications of the CCISA
Vol. 31 No. 1 Feb. 2025

零信任成熟度評估模型 ZTAID 介紹

李逸元[1§]、廖世偉[2]、杜奕鋒[3]、張政權[4]
[1,2]國立臺灣大學資訊工程學系、[3,4]精誠集團
[1] iyylee@ntu.edu.tw、[2] liao@csie.ntu.edu.tw、[3] duncantu@xsolutions.com.tw、
[4] allenchang@xsolutions.com.tw

摘要

本文探討零信任架構 (Zero Trust Architecture，ZTA) 近幾年落實在國內外的動態，包含美國國家標準與技術研究院 NIST 的零信任架構標準(2020)、美國國防部 DoD 零信任策略(2022)涵蓋的技術支柱，以及美國國土安全部零信任成熟度四級架構(2023)，並結合我國 2022 年起對於零信任架構的政策性推動，分享適合我國企業實施零信任成熟度評估的 ZTAID 模型。此模型乃根據我國金管會《零信任架構導入參考指引》(2024)所設計，結合前述的各標準，透過零信任成熟度的現況盤點與評估，藉以找出潛在風險並擬定未來分階段精進改善措施，另輔以網路安全框架 (Cybersecurity Framework，CSF) 五個核心功能，於資安防禦週期管理流程之事前、事中及事後(識別、保護、偵測、回應及復原)進行統合，最後量化歸納呈現組織於零信任框架能力成熟度。最後可以針對評估結果再設計階段性的改善計劃與實施項目，逐步提升其資安防護能力，以達成零信任架構導入與應用的資安防護目標。

關鍵詞：零信任架構 (Zero Trust Architecture, ZTA)、零信任支柱 (Zero Trust Pillars)、零信任成熟度評估 (Zero Trust Maturity Assessment, ZTMA)、零信任成熟度模型 (Zero Trust Maturity Model, ZTMM)、網路安全框架 (Cybersecurity Framework，CSF)、ZTAID 模型 (ZTAID Model)

§ 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol. 31 No. 1 Feb. 2025

Introduction to The ZTAID Model for Zero Trust Maturity Assessment (ZTMA)

Isaac Yi-Yuan Lee[1]、Shih Wei Liao[2]、Duncan Tu[3]、Allen Chang[4]
[1,2] Dept. of CSIE, NTU、[3,4] SYSTEX Corporation
[1] iyylee@ntu.edu.tw、[2] liao@csie.ntu.edu.tw、[3] duncantu@xsolutions.com.tw、
[4] allenchang@xsolutions.com.tw

Abstract

This paper discusses the progress of the implementation of Zero Trust Architecture (ZTA) in recent years, including the Zero Trust Architecture Standard (2020) of the National Institute of Standards and Technology (NIST), the technology pillars covered by the Zero Trust Strategy of the U.S. Department of Defense (2022), and the Zero Trust Maturity 4-Level Architecture of the U.S. Department of Homeland Security (2023). In combination with Taiwan authority's promotion of Zero Trust Architecture starting in 2022, we share the ZTAID model suitable for organizations to implement Zero Trust Maturity Assessment. This model is designed based on the "Reference Guidelines for the Introduction of Zero Trust Architecture" (2024) of the Financial Supervisory Commission of Taiwan. It combines the aforementioned standards and conducts an inventory and assessment of the current status of zero trust maturity to identify potential risks and formulate future phased improvement measures. It is also supplemented by the five core functions of the Cybersecurity Framework (CSF) to integrate the pre-, mid- and post-event (identification, protection, detection, response and recovery) of the information security defense lifecycle management process, and finally quantifies and summarizes the organization's maturity in the zero trust framework. Finally, we can redesign phased improvement plans and implementation projects based on the evaluation results to gradually enhance its information security protection capabilities and achieve the information security protection goals of introducing and applying ZTA.

Keywords: Zero Trust Architecture (ZTA)、Zero Trust Pillars、Zero Trust Maturity Assessment (ZTMA)、Zero Trust Maturity Model (ZTMM)、Cybersecurity Framework (CSF)、ZTAID Model

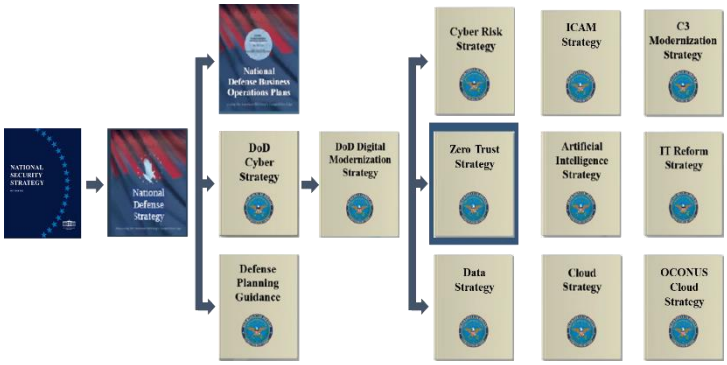
壹、前言

「零信任之父」John Kindervag 在 2010 年提出零信任架構 (Zero Trust Architecture, ZTA) [3]，期望透過對任何網路上的資料存取皆永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證安全性的相關技術。美國國家標準與技術研究院 NIST 經過多年發展於 2020 年提出了零信任架構標準 [5]、兩年後美國國防部 DoD 也提出零信任戰略及參考架構 [2][6]，稍晚美國國土安全部在 2023 年也據此更新了第二版的零信任成熟度四級架構 [1]，我國也從 2022 年起政策性推動對於零信任架構的強化要求 [7][9]，特別是 A 級政府機關與金融相關單位。這幾年來作者陸陸續續以顧問身分參與了非常多的零信任相關專案，都是根據這些政策，制度與相關的規劃而來。國內對於 NIST SP 800-207 的論述已經非常豐富，本文後續將提出對於我國零信任架構實施方向的心得與建議，基於符合金管會【零信任架構導入參考指引】要求的零信任成熟度模型 (ZTMM)評估服務。藉由本方法論協助受評金融機構完成零信任架構成熟度的現況評估時，可針對評估後之結果提供分階段性的改善計劃與實施路徑，藉以逐步提升金融機構之資安防護能力，達成零信任架構的全面導入與應用。

貳、美國零信任架構近期發展

2.1 美軍零信任戰略規劃與要求

2022 年 1 月，美國國防部在資訊長辦公室內設立了國防部零信任組合管理辦公室 (Zero Trust Portfolio Management Office, ZT PfMO) ，以協調國防部零信任戰略中律定的相關工作，並透過多項行動加速零信任的採用。半年後，DoD 在 2022 年夏天提出零信任戰略 (DISA 2022，如圖一)，再三個月後公布了參考架構[6]。ZT PfMO 表示國防部的每一位成員都必須採取零信任思維，無論他們是在技術部門、網路安全部門還是人力資源部門工作。 這種“永不信任，始終驗證”(never trust, always verify) 的心態要求大家對

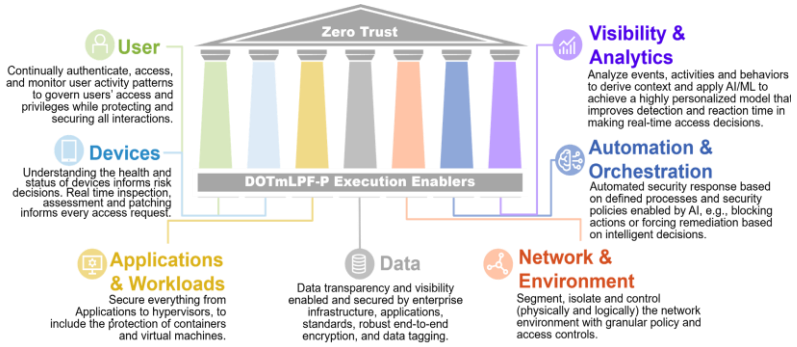


圖一: 美國國家整體戰略規劃藍圖[2]

設備、應用程序、資產和服務的安全負責； 用戶只能在需要時訪問他們需要的數據。

國防部所有人都必須在與對手的戰鬥中發揮作用，無論何時何地出現安全威脅，都必須迅速而正確地採取行動來應對它們。國防部內外的數據洩露暴露的漏洞表明需要一個新的、更強大的網路安全框架，以促進基於風險的明智決策。零信任安全消除了邊界、可信網路、設備、角色的傳統概念 ，或處理並轉變為基於多屬性的信賴等級，從而落實基於最小特權訪問概念的身份驗證和授權策略等概念。

DoD 零信任戰略是國家安全戰略的一部分，由國防部資訊長負全責推動[2]。DoD 戰略還提到了國防部零信任的七個支柱(見圖二)，這是該戰略的零信任能力路線圖、基於能力的執行計劃以及國防部零信任和網路安全參考架構的基礎。DoD 零信任戰略描述了國防部將如何通過提供基礎和方向來幫助協調條令、組織、培訓、物資、領導力和教育、人員、設施和政策 (Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy, DOTmLPF-P) 所有要素實現零信任七支柱。該戰略認識到，零信任的採用將要求不僅在整個部門而且在其組成部分中對 DOTmLPF-P 進行更改，並在其零信任執行計劃中予以解決。



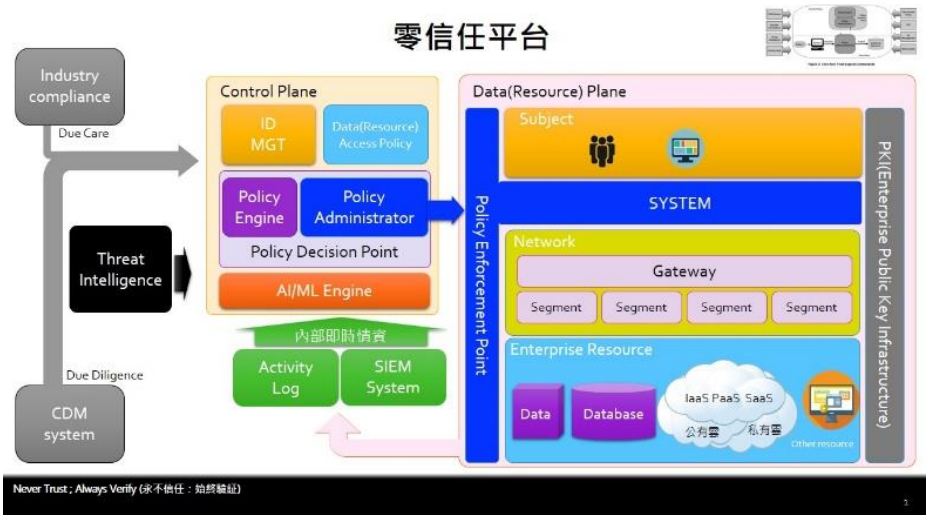
圖二: 零信任架構七大支柱 [2]

針對這七個支柱，DoD 零信任戰略進一步盧列了四十多個重要的資安關鍵技術，來支持與完善七個支柱的內容，稱為零信任能力模型 (DoD Zero Trust Capabilities Model)。

2.2 NIST SP800-207

DoD 七個零信任支柱來自於美國國家標準與技術研究院 (NIST) 特別出版物 (SP) 800-207 [5]描述的零信任七原則，其中包括： 1) 所有資料來源和計算服務被視為資源； 2) 無論網路位置如何，所有通訊都是安全的； 3) 按會話 (session) 授予單一企業資源的存取權限； 4)資源的存取由動態策略決定； 5) 企業監控和衡量所有擁有和相關資產的完整性和安全狀況； 6) 所有資源認證和授權都是動態的，並且在允許存取之前嚴格執行； 7) 企業收集盡可能多的有關資產、網路基礎設施和通訊當前狀態的信息，並利用

這些資訊來改善其安全狀況。圖三為本研究依據 NIST SP800-207 所彙整零信任平台框架所應具備之功能模組，以利未來針對零信任平台之導入提供更簡易清晰呈現之框架呈現:

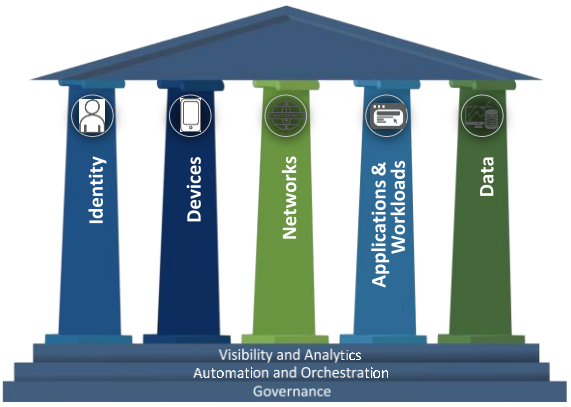


圖三: 依據 NIST SP800-207 彙整零信任平台框架應具備之功能模組

參、國土安全部零信任成熟度建策

國土安全部 (Department of Homeland Security, DHS) 所屬的網路安全和基礎設施安全局 (Cybersecurity and Infrastructure Security Agency, CISA) 的任務是領導國家理解、管理和降低網路安全風險的工作，包括支援聯邦民事行政部門機構發展和實施網路安全計畫和能力。CISA 因此在 2021 年開始提出零信任成熟度模型 (Zero Trust Maturity Model, ZTMM) 來提供一種在快速發展的環境和技術格局中，實現與零信任相關的持續現代化工作的方法，目前的最新版本是 2023 年發布的第二版[1]。

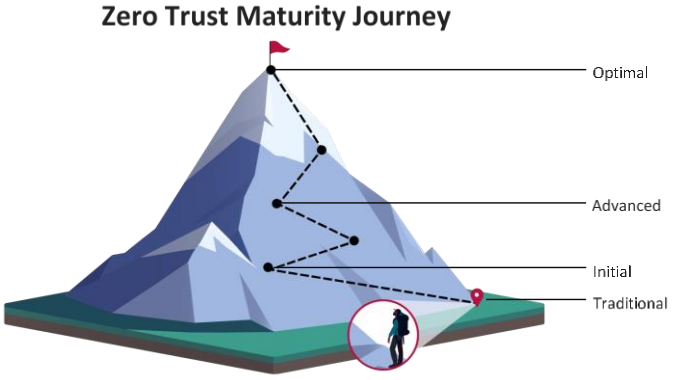
CISA 提出的 ZTMM 降低導入零信任時的障礙；ZTMM 代表了五個不同基礎技術支柱的實施程度，隨著時間的推移，可以在最佳化方面取得持續的進步。如圖四所示，支柱包括身分、設備、網路、應用程式和工作負載以及資料。每個支柱都包含有關以下橫向交互功能的三個支柱：可視性和分析、自動化和協作以及治理。我們可以發現這個架構與 DoD 相比多了治理支柱，這也很自然，軍人強調的是服從與執行，民間單位才會需要考慮的治理議題。



圖四: CISA 零信任架構 [1]

隨著機構向最佳零信任實施過渡，相關解決方案越來越依賴自動化流程和系統，這些流程和系統可以更全面地跨支柱整合並更動態地執行政策決策。每個支柱都可以按照自己的步調取得進展，並且可能比其他支柱進展得更快，直到需要跨支柱協調為止。然而，這種協調只能透過彼此相容以及企業範圍環境的功能和依賴關係來實現。這允許並定義了向零信任的逐步演變，隨著時間的推移分配成本，而不是完全預先分配。

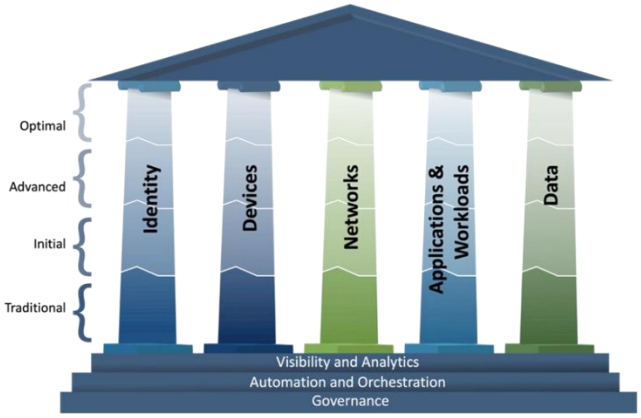
根據 NIST 向零信任過渡的步驟，各機構應在投資零信任能力（包括本模型中概述的支柱和功能）之前評估其當前的企業系統、資源、基礎設施、人員和流程。 此評估可以幫助機構確定現有能力，以支持進一步的零信任成熟度和優先差距。各機構還可以規劃機會來協調跨支柱的能力，以實現精細的、最小權限的存取控制並減輕額外的風險。隨著零信任成熟度在支柱之間和支柱內不斷進步，各機構應該預期所需的努力程度和實現的收益將顯著增加。當各機構規劃其 ZTA 旅程時，他們應該探索提高支柱成熟度的機會，以適應特定的任務需求並支持其他支柱的進一步成長。



圖五: CISA 零信任成熟度模型 [1]

圖六突顯了預期組織隨著時間的推移從傳統企業向未來狀態的演變，該狀態具有更多動

態更新、自動化流程、整合功能以及最佳階段的其他特徵（如成熟度模型中所述）。這些階段是動態的並且呈指數級增長；從一個成熟階段到另一個成熟階段的計劃進展可能會隨著時間的推移而發生範圍和影響的變化。

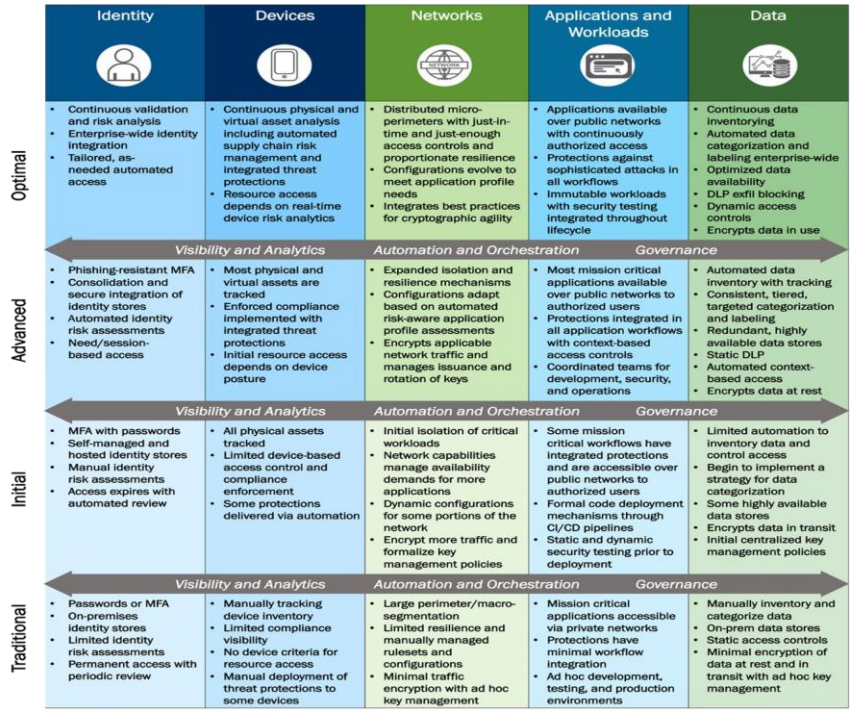


圖六: CISA 零信任架構結合成熟度模型 [1]

各機構應使用以下每個階段的指導標準來確定每個零信任技術支柱的成熟度，並在整個成熟度模型中提供一致性：

1) Traditional/傳統－手動配置生命週期（即從建立到退役）和屬性分配（安全性和日誌記錄）；靜態安全策略和解決方案，一次解決一個支柱，且對外部系統具有離散依賴關係；僅在配置時建立最低特權；孤立的政策執行支柱；手動響應和緩解部署；依賴項、日誌和遙測的相關性有限。
2) Initial/初始－啟動生命週期屬性分配和配置、策略決策和執行的自動化，以及與外部系統整合的初始跨支柱解決方案；配置後對最小權限進行一些響應性更改；以及內部系統的聚合可見性。
3) Advanced/進階－可透過跨支柱協調對生命週期以及配置和策略分配進行自動化控制；集中可見性與身分控制；跨支柱的政策執行；對預先定義的緩解措施的回應；根據風險和態勢評估更改最低特權；並建立企業範圍的意識（包括外部託管的資源）。
4) Optimal/最佳－完全自動化、及時的生命週期以及資產和資源的屬性分配，透過基於自動/觀察到的觸發器的動態策略進行自我報告；對企業範圍內的資產及其各自的依賴項進行動態最小權限存取（恰到好處且在閾值內）；具有持續監控的跨支柱互通性；以及具有全面態勢感知的集中可見性。

圖七提供了 ZTMM 的高階概述，包括每個支柱和每個成熟階段的支柱特定功能的關鍵評估指標，這樣可以有助於使用者評估機構目前或未來的零信任成熟度:



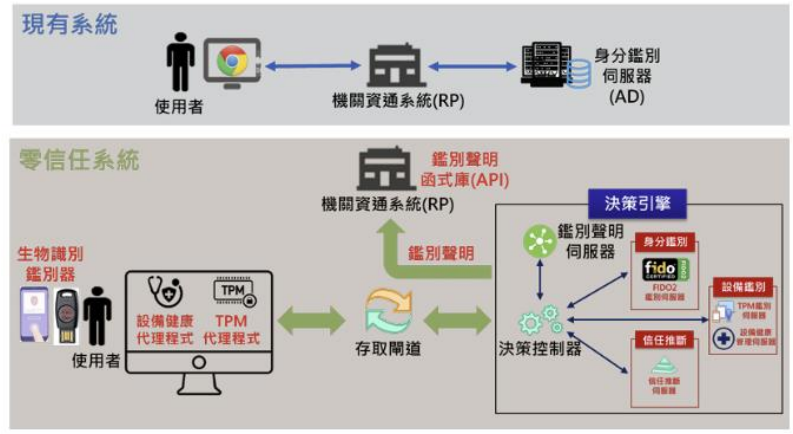
圖七: ZTMM 的高階概述，包括每個支柱和每個成熟階段的支柱特定功能的關鍵評估指標 [1]

這些成熟度階段和與每個支柱相關的詳細資訊使各機構能夠評估、規劃和維護實現 ZTA 所需的投資。在標準中 NIST 也提供了詳細的評估建議，以支持機構在五個不同支柱上過渡到零信任：身份、設備、網路、應用程序和工作負載以及數據。每個支柱還包括有關可視性和分析、自動化和協作以及治理功能的一般詳細信息，以支援與該支柱和跨模型的整合。

在規劃 ZTA 實施時，各機構應根據風險、使命、聯邦要求和營運限制等因素做出決策。雖然該模型通常與聯邦企業的單一管理域或認證邊界保持一致，但各機構也應評估其與外部合作夥伴、利害關係人和服務提供者的互動和依賴如何影響其 ZTA。此 ZTMM 成熟度模型不應被視為一組嚴格的要求，而應被視為幫助機構成功實施 ZTA 並採取整體改進的網路安全態勢的一套指引與工具。

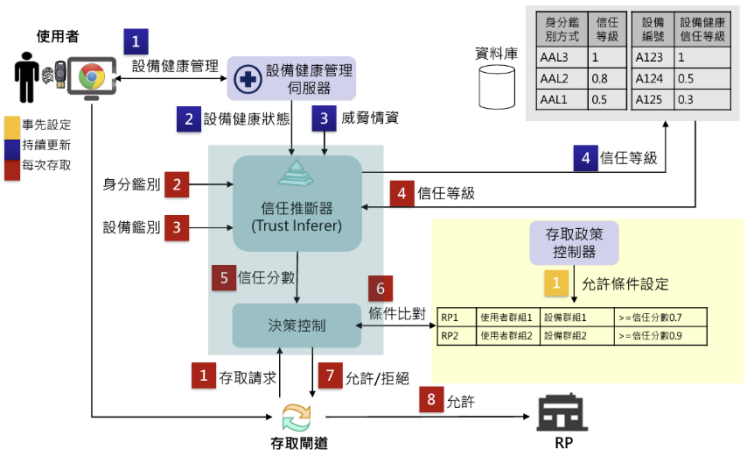
肆、我國政府零信任推動目標

從 2021 年開始，行政院開始依據第六期「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，藉由發展主動式防禦技術，推動政府機關導入零信任架構，完善政府網際服務網防禦深廣度。推動規劃由行政院資通安全會報技服中心與轉型後的數位發展部及資通安全研究院擔責，數發部資通安全署這幾年都規劃投入經費，優先推動 A 級公務機關導入零信任架構[9]。我國的做法號稱根據 NIST 零信任推動建議，零信任架構以決策引擎為核心，採取資源門戶之部署方式 (Resource Portal-Based Deployment)，包含 3 大核心機制：–身分鑑別：多因子身分鑑別與鑑別聲明–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，而且提醒各單位實施零信任會是一段過程，而不是一次大規模替換基礎架構，且與傳統模式會同時混合運作:



圖八: 我國政府零信任架構導入示意圖 [7]

政府規劃的完整登入流程如下:



圖九: 我國政府零信任架構登入流程圖 [7]

原本第六期「國家資通安全發展方案(110 年至 113 年)」規劃的零信任進度視三期分三年完成，也就是 110 年做到身分鑑別，111 年做好設備鑑別，而 112 年完成信任推斷；但由於諸多內外在因素，加上疫情衝擊，特別是零信任的解決方案其實也沒有發展得如此迅速，所以配合金融監督管理委員會(以下稱金管會)在 2022 年底公布的「金融資安行動方案」第 2.0 版，整體時程延後兩年。因此 111 年有十多個機關完成了身分鑑別工作，而在 112 年已經有兩個政府機關率先完成設備鑑別的初步佈建工作。

金管會為確保金融系統營運不中斷，提供民眾安心交易環境，賡續發布「金融資安行動方案」2.0 版，期能強化金融業資安防護能力[7]。金管會表示，為追求安全便利不中斷的金融服務，於 109 年 8 月 6 日發布金融資安行動方案，執行迄今已逾兩年，經與金融周邊單位、金融同業公會與金融機構公私協力積極執行下，主要績效指標(如設置資安長、導入國際資安標準、辦理資安攻防演練與競賽、建立金融資安事件應變體系等項)均已達成，占全計畫 86%，持續辦理項目占比 14%。為因應業務發展與科技進步，持續提升金融機構資安防護能量，金管會再審視近兩年金融科技發展趨勢、國內外資安情勢變化及實務運作情形，並參考國際資安監理政策，滾動檢討研訂金融資安行動方案 2.0 版，作為下一階段執行之準據。金融資安行動方案 2.0 版以擴大適用、落實與深化、鼓勵前瞻為持續精進方向，訂有 40 項措施，其中新增資安措施計 12 項、擴大適用範圍計 5 項、持續性措施計 23 項；其中第六的重點就是鼓勵零信任網路部署，強化連線驗證與授權管控：因應疫情帶動異地/居家辦公模式，及資料與服務雲端化、使用者行動化、存取設備多元化，傳統基於信任邊界之網路模型已難以滿足新形態工作需求，爰規劃鼓勵金融機構逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路 3 大核心機制，搭配網路及資源的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。但目前進度大致落後原規劃一到兩年。

圖十: 我國政府零信任架構導入時程規劃 [7]

隨著數位化轉型的推進與行動工作模式的普及，我國金融機構的業務運作逐漸依賴於雲端技術與多樣化設備，這使得傳統邊界防護的網絡安全架構已無法滿足現今的需求。依據 113 年金管會所正式公布之《零信任架構導入參考指引》其實施之主要目標如下:

(一) 依據 CISA Zero Trust Maturity Model (ZTMM) V2.0 框架，進行金融機構零信任架構的成熟度評估，涵蓋五大資安支柱：身份識別、設備鑑別、網路安全、應用與工作負載、資料保護。

(二) 通過現況評估，識別現有資安架構及管理機制中的風險與不足之處，並根據評估結果提出具體的改善計劃與實施路徑，確保受評金融機構逐步達到符合零信任架構的要求。

ZTAID 模型乃根據我國《參考指引》所設計，結合前文提及的各種標準，透過零信任成熟度的現況盤點與評估，藉此找出潛在風險並制訂未來的精進改善措施，另輔以網路安全框架 (Cybersecurity Framework，CSF) 五個核心功能，以進行統合關聯性量化評估歸納並呈現事前、事中及事後之多維度視角初探 [10]。

伍、零信任成熟度評估 (ZTMA) 流程

5.1 金融機構 ZTMA 要求

金融機構基植於零信任成熟度評估之工作範圍，通常包括但不限於以下內容：

1、 受評機構針對【選定的場域】進行基於 CISA 2.0 Zero Trust Maturity Model (ZTMM) 的成熟度評估，涵蓋五大資安支柱。另依據 ZTMM 模型，透過與相關負責人進行訪談、文件檢視及執行紀錄的比對，全面驗證場域內各項資安措施的實施成效，並確保「說、寫、做」之一致性。此評估將為受評機構提供現有資安體系之詳細分析，並作為後續零信任架構導入與優化計劃之依據。

2、 現況調查與資料蒐集：

針對受評金融機構的現況調查與資料蒐集，調查範圍涵蓋身份識別、設備鑑別、網路安全、應用與工作負載及資料保護等五大資安支柱。依據 CISA V2.0 內容所設計之問項透過內部文件審查、現場訪談等方式，全面了解受評機構的資安現狀及零信任導入的進度，並根據 CISA 2.0 與金管會《零信任架構導入參考指引》進行評估準備工作。針對五大支柱之評估內容可參考以下重點項目

(一) 身份驗證

廠商需針對本機構場域內的身份管理流程進行全面評估，通過與負責人訪談，深入了解現行的身份驗證、角色分離及授權控制機制。廠商需檢視相關的身份管理政策文件，並進行實際操作紀錄的比對與抽查，確認身份管理的政策與實際執行之

間的一致性。

(二) 設備鑑別

廠商需對場域內的設備管理機制進行評估，特別是針對設備鑑別、安全監控及合規性檢查的執行情況。廠商需與設備管理負責人訪談，瞭解設備的安全管理策略，並檢查現有的設備管理文件與實際操作紀錄，確認場域內設備管理與現行規範的一致。

(三) 網路安全

廠商需對本機構場域內的網路安全措施進行評估，重點檢查內外網路的隔離、加密及動態存取控制機制的執行情況。廠商需訪談網路安全負責人，檢查網路安全政策文件，並進行流量監控數據的抽查，驗證網路安全機制的有效性。

(四) 應用與工作負載

廠商需對場域內的關鍵應用程式與工作負載進行評估，特別針對高風險應用的存取控制與防護措施進行檢視。廠商需訪談應用管理部門，檢視應用層的安全策略文件，並抽查應用程式的實際操作紀錄，確認應用程式的安全防護機制已按照零信任原則落實，並保障應用層的操作安全。

(五) 資料保護

廠商需對場域內的資料保護機制進行全面評估，包含資料分類、加密及存取控制的實施情況。廠商需與資料保護負責人訪談，檢查現有的資料保護政策，並進行資料流動與加密紀錄的比對，確認敏感數據在存儲及傳輸過程中的安全性是否得到充分保障並符合資料保護相關的規範要求。

3、 五大支柱成熟度評級：

根據 Zero Trust Maturity Model (ZTMM) 對受評機構的五大資安支柱進行縱向評估。透過資料蒐集、問卷回收及現場訪談，需依 ZTMM 的標準，將五大支柱進行從 Class 1 到 Class 5 的成熟度分級，並針對每一支柱的風險與改善空間提供具體量化報告。此評級將作為後續資安強化的基礎，幫助識別需優先處理的風險區域。

4、 三大構面對比分析：

在完成五大支柱成熟度評級後，需進行橫向的三大構面（維運面、可視面、自動化/治理面）對比分析。該分析需整合受評機構在這三大構面的表現，通過資料彙整及數據分析，提供對應百分比結果。另需具體描述三大構面中資安能力的優勢與不足，並為受評機構未來的資安策略提供具體的數據支持。

5、 零信任架構改善與目標設定：

根據五大支柱成熟度評級及三大構面分析，需協助受評機構設定具體的零信任目標，並進行目標差距分析。另提供詳細的資安機制方案，並根據 NIST CSF 的對應陣列，提出切合實際且具可操作性的零信任架構導入建議。所有改善措施需依據金管會《零信任架構導入參考指引》進行對應，確保符合相關法規要求。

在完成場域內的零信任成熟度評估（現況）後，可參考產業的資安水平、受評機構的業務屬性及客戶高層的自我期許，提供受評機構進行改善目標的設定。針對受評機構的需求，需協助確立適當的資安成熟度目標，並針對各個支柱的對應功能進行適切性評估，逐步建立、改善或補強各項資安機制。此過程中，需列出具體的【機制/方案/工具】，並設計分階段的實施計劃，最終達到零信任能力的預期成熟度。

接下來需針對零信任架構的五大支柱（身份管理、設備鑑別、網路安全、應用與工作負載、資料保護）進行功能適切性評估，針對每一支柱現行的防護機制與運作流程進行深入分析，並評估其是否滿足受評機構的資安需求及改善目標。該評估將作為後續資安機制調整及強化措施的依據。在後續之建立/改善/補強措施之活動應根據功能適切性評估結果，分階段提出具體的行動方案，以確保每個支柱的對應功能達到零信任架構的成熟度要求。這些措施包括：

1.機制：針對每個支柱建立新的資安機制（如加強身份管理或數據加密機制），或改善/擴大現有機制，確保資安控制點覆蓋本專案之風險範疇。

2.方案：設計或採用適合的資安方案，確保在零信任導入過程中，方案能切合本機構業務特性及操作需求，並持續提供有效的資安保護。

3.工具：引入或優化資安工具，輔助管理身份、監控設備、保障網路安全及保護數據的流動性，確保技術工具在資安體系中發揮最大效益。

Pillars		Mechanism	MFA	IAM	PAM	Compliance check	EDR	Micro-Segmentation	Threat Protection	Encry	SSDLC	DLP	Inventory (PII/Cont.)	DAM	Logger	SIEM/SOAR
		Functions / Phase	I	II			I	I		II	II~III		I	II	I	I
Identity	ID-1	Authentication	B	B												
	ID-2	Identity Stores	B	B	B											
	ID-3	Risk Assessment	B	B	B											
	ID-4	Access Management	B	B	B		B									
	ID-5	Visibility and Analytics Capability				C									B	C
	ID-6	Automation and Orchestration Capability				C	C								B	C
	ID-7	Governance Capability				C									B	C
Devices	DE-1	Policy Enforcement & Compliance Monitoring	B	B		B	C	C	C							
	DE-2	Asset & Supply ChainRisk Management		B	B	B			C							
	DE-3	Resource Access		B	B	B	C									
	DE-4	Device Threat Protection			C	C	B	C	B	D						
	DE-5	Visibility and Analytics Capability					C	C			D	C	C	D		
	DE-6	Automation and Orchestration Capability							C	D						
	DE-7	Governance Capability							C							
Networks	NW-1	Network Segmentation		B	B		B	B								B
	NW-2	Network Traffic Management		B	B		C	C	C						C	
	NW-3	Traffic Encryption		C	C		C			C					D	
	NW-4	Network Resilience					D	D						D	D	
	NW-5	Visibility and Analytics Capability						C						C	D	
	NW-6	Automation and Orchestration Capability						D						D	D	
	NW-7	Governance Capability						D						D		D
Applications & Workloads	AP-1	Application Access	B	B												
	AP-2	Application Threat Protections				B	C	B								
	AP-3	Accessible Applications	B	B	B		C	B								
	AP-4	Secure Application Development and Deployment Workflow				B	C		C		B					
	AP-5	Application Security Testing				C	C				C				B	C
	AP-6	Visibility and Analytics Capability				C	C	B							B	C
	AP-7	Automation and Orchestration Capability				D	C		D						C	D
	AP-8	Governance Capability				D	C		D						C	D
Data	DA-1	Data Inventory Management		B		B						B	B			
	DA-2	Data Categorization				B										
	DA-3	Data Availability				B										
	DA-4	Data Access		C		C				C			C	C		
	DA-5	Data Encryption				C				C					B	C
	DA-6	Visibility and Analytics Capability				C									B	C
	DA-7	Automation and Orchestration Capability				D				D					C	D
	DA-8	Governance Capability				D								D	C	D

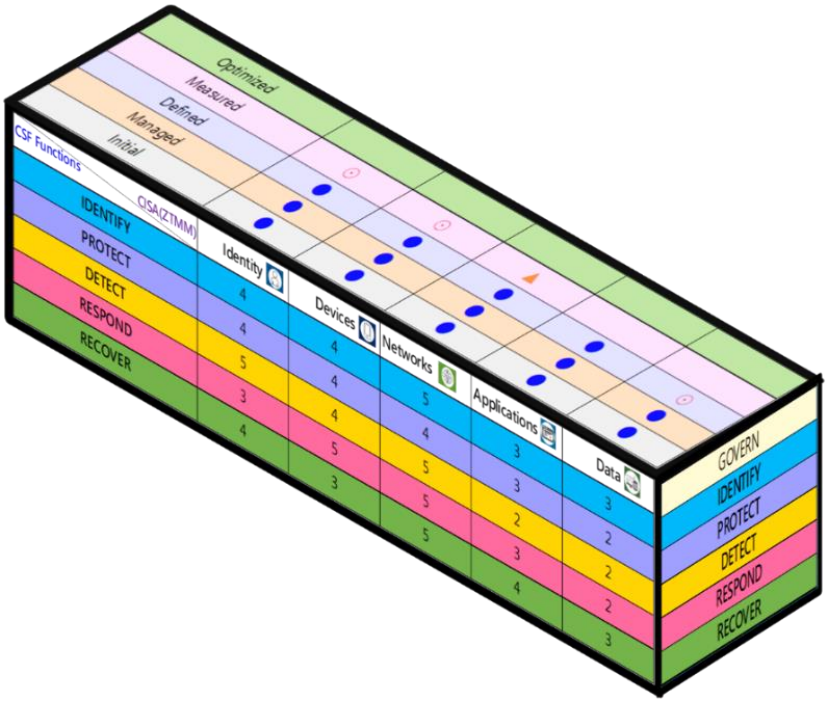
圖十一: 資安機制方案對應矩陣

圖十一乃根據評估場域彙整之分階段性資安機制方案對應矩陣，另參考 NIST

CSF(Cybersecurity Framework) 的階段性指引，為受評機構設計分階段的資安機制方案對應矩陣。該矩陣將依據改善目標，對應每個支柱的資安措施，並按不同成熟度階段明確列出所需實施的機制、方案與工具。

5.2 ZTAID 模型說明

ZTAID 模型參考 113 年金管會公布實施金融單位【零信任架構導入參考指引】要求的零信任成熟度模型 (ZTMM) 評估機制，並且依照該指引進行零信任成熟度的現況盤點與評估，藉此找出潛在風險並制訂組織於未來之精進改善措施。另針對評估結果提供階段性的改善計劃與實施項目，逐步提升其資安防護能力，以達成零信任架構的導入與應用。擬以零信任成熟度評估模型 (ZTMM) 之認知養成、盤點訪查、成熟度顧問評估框架及分階段精進改善規畫四個構面並結合網路安全框架 (Cybersecurity Framework，CSF) 五個核心功能進行事前、事中及事後之統合關聯量化評估之初探，這也就是 ZTAID 模型的整體概念，而下圖是 ZTAID 零信任成熟度評估模型與網路安全框架 (CSF) 多維度統合關聯視角:



圖十二: ZTAID 模型

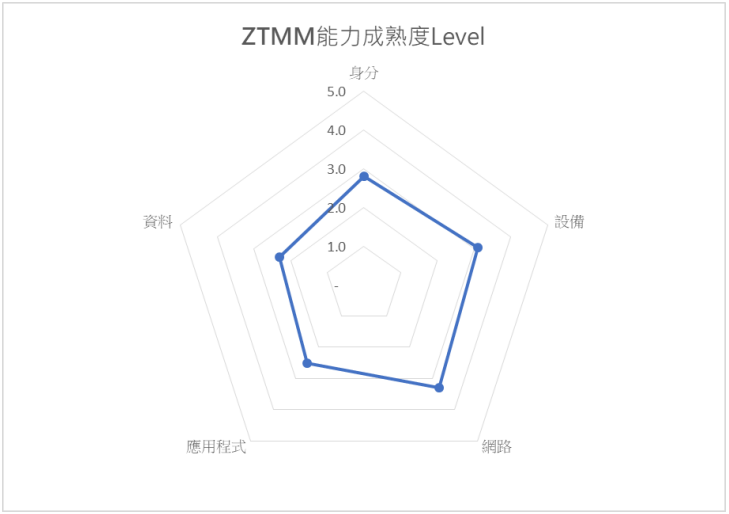
5.3 ZTAID 執行結果說明

我們從 2023 年起即運用 ZTAID 模型在幾個台灣的大型企業中，以下為過往產出之評估報告目錄及部分擷取之量化評估圖表:

目　　錄

圖十三: ZTAID 模型評估報告示意圖

零信任五大支柱之能力成熟度如下圖所示：



五大支柱	能力成熟度Level
身分	2.8
設備	3.1
網路	3.3
應用程式	2.5
資料	2.3
平均能力成熟度值	2.8

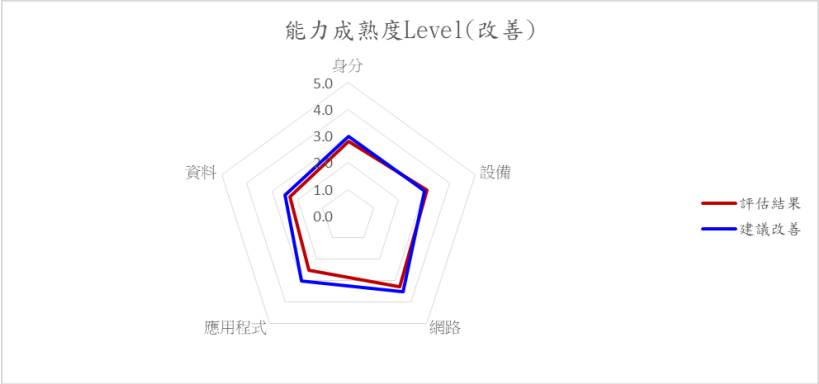
圖十四: ZTAID 模型能力成熟度評估結果圖

針對零信任五大各支柱之評估後，依據零信任自評表之各功能特性再分類為【維運面】、【可視化面】及【自動+治理面】三個零信任能力構面，進行統合分析。參考如下評估總表：

五大支柱	自動+治理	維運	可視化
身份	45%	38%	70%
設備	60%	48%	80%
網路	55%	52%	90%
應用程式	50%	57%	60%
資料	50%	52%	50%

圖十五: ZTAID 模型能力成熟度評估總表示意圖

綜合上述各構面之說明，受評組織現行五大支柱在【維運面】、【可視化面】及【自動化+治理面】之三大零信任能力構面上有不同程度之達成等級，建議於短期落實幾個於資安機制方案對應矩陣所擬定建議實施精進改善之方案。依此擬訂之建議可由此次所評估之能力成熟度結果平均值 SL 2.8 提升至平均值 SL 3.0(含)以上(此部分待未來於其他施作場域再進行更進一步之評估探討)，五大支柱之各別建議改善能力成熟度請參考圖十六：

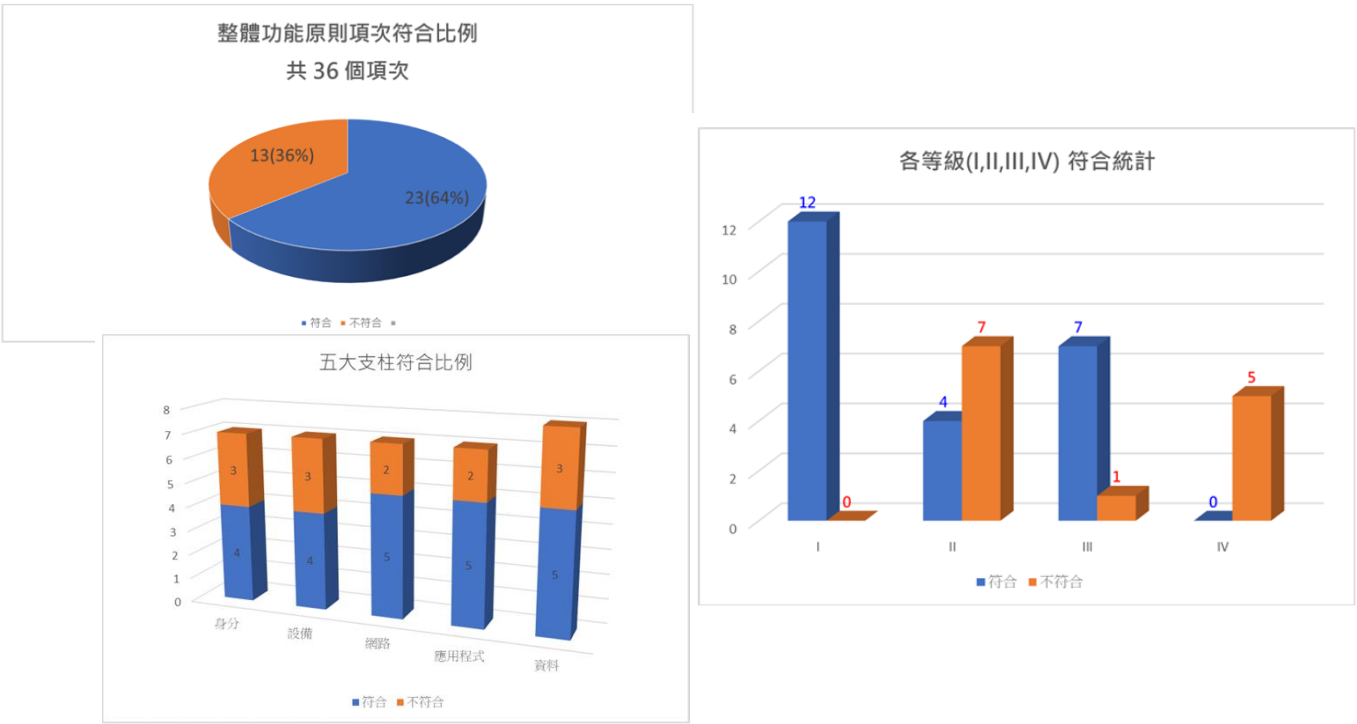


圖十六: ZTAID 模型建議改善能力成熟度示意圖

本研究另提出採用零信任支柱與 NIST CSF 框架之初步探討基礎，以進行詳細之評核後，總結出技術層缺失之矯正目標分析:

圖十七: ZTAID 模型技術層缺失之矯正目標分析示意圖

準此要領，我們也能根據 CISA V2.0 之零信任功能項目與金管會之《零信任架構導入參考指引》進行統合關聯於零信任五大功能支柱之對應，並以資安治理與風險的角度，逐步地來協助組織導入零信任架構，而目前更有些金融機制根據所評估的結論，也推論出金管會版本之零信任架構導入參考指引之合規項目初步結果(請參考圖十八)



圖十八: ZTAID 模型合規項目分析示意圖

本研究依據所設計之資安機制方案對應矩陣於五大支柱及功能項目之成熟度量化評估後，設計出了三年甚至五年的實施計畫，這其實也跟美軍的 ZTA 戰略作法不謀而合，殊途同歸。

陸、結論

零信任是一條無止盡的道路，需要不斷的投入與努力，而如何導入實施則是眾說紛紜。2021 年台灣資安大會上，查士朝教授給出幾個建議[8]，三年後配合筆者的實戰經驗看起來，真的是字字珠璣:

1) 零信任架構與其說是有某一個特殊的「架構」不如說是安全原則
2) 零信任架構並不是一定要立刻替換掉所有的邊緣安全機制
3) 零信任架構導入的幾個關鍵包含盤點使用者與資源，妥善佈署資源，檢視權限並落實存取控制，以及掌握資源與使用者狀態
4) 組織可以考量本身的狀態，引入零信任相關概念，並逐步強化

我國政府的作法對比美國國防部或是國土安全部的建議，屬於比較簡化的一個版本，而且最適合政府公部門對民眾提供服務的單純系統，因此筆者認為是一個非常正確的途徑，既可以提高政府機關對民眾服務的資訊安全水準，降低民眾曝險的概念也很符合 IT 科技風險管理的原則，又可以藉此培養國內廠商，厚植本土資安技術能量，做好資安防護，是很適合的安排。

但話說回來，對於業務繁雜的金融機構，以及眾多的大型科技公司，還有數量龐大的中小型上市公司及股票發行公司，以及擔負各種任務的國營事業，如何安排與規劃 ZTA 架構落實的長遠計畫，也許就不適合用一條鞭的方式要求，反而可以參考美軍的藍圖規畫方式，輔以國土安全部 ZTMM 成熟度評估，量身打造更適合組織的零信任實施規劃，這幾年我們逐步完成了好幾個專案。

我們通常先從資安治理評估開始，依據資安治理成熟度進行整體作業層級與技術管理評估，以強化組織資訊安全成熟度。本研究主要探討一般組織在評估或導入國內資安規範或機制時，除了在產品技術 (Product/Technology) 層面上去做佈署，也應將人員 (People) 及程序 (Process) 這二個層面納入評估，以提供組織更全面性之整體框架治理層級的呈現。另外參考國外學者 Dwayne Phillips [4]指出在軟體專案能成功的關鍵要素在於 3P，也就是人員 (People)、流程 (Process) 以及產品技術 (Product/Technology) 三個層面，一個專案之所以能夠成功，就是人員與流程能與相關產品相呼應，本研究也建議可結合此知識管理理論 (3P 理論)，並以 CISA V2.0 之五大支柱功能問項之導讀建立組織各權責單位認知共識並以文件審查並結合深度訪談之方式，初步發展出「資安機制方案對應矩陣」，並將此歸納出零信任成熟度在產品技術 (Product/Technology)、人員 (People)

以及程序 (Process) 三個主要構面上所需要之分階段精進改善建議，並且於國內幾家金融機構運用此評估流程進行 ZTMM 之相關實務委外服務及初步探討，以便了解該受評組織在現行零信任防禦框架的資安防護程度，並提供組織高階管理者及權責單位人員對零信任防禦框架有更具體之認知思維以及量化評估之參考依據。

參考文獻

[1] Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division, “Zero Trust Maturity Model v2.0,” U.S. Department of Homeland Security, Apr. 2023.

[2] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, “DoD Zero Trust Reference Architecture,” U.S. Department of Defense, Jul. 2022.

[3] J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” 2010, [Online]. Available: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

[4] Dwayne Phillips, “PEOPLE, PROCESS, AND PRODUCT”, Feb. 1995. [Online]. Available: https://dwaynephillips.net/CutterPapers/ppp/ppp.htm

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “NIST SP800-207 Zero Trust Architecture Final,” National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[6] ZT PfMO (DoD Zero Trust Portfolio Management Office, “DoD Zero Trust Strategy,” U.S. Department of Defense, Oct. 2022.

[7] 金融監督管理委員會, “「金融資安行動方案」2.0-2022,” 金融監督管理委員會, Dec. 2022. [Online]. Available: https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202212270001&dtable=News

[8] 查士朝, “淺談零信任架構的迷思與導入策略,” 台灣資安大會(2021), May 2021. [Online]. Available: https://cybersec.ithome.com.tw/2021/session-page/98

[9] 國家資通安全研究院, “政府零信任架構說明-2023,” 國家資通安全研究院, Jun. 2023. [Online]. Available: https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/ZTA/

[10] 張政權, “建構資料外洩防護檢核表之研究-以 ISO/IEC 27001 為基礎”, 華梵大學資訊管理學系碩士論文, Jun. 2010.

[作者簡介] Biography

李逸元博士長期從事IT風險管理 (ITRM) 及網宇資訊安全 (Cyberspace security) 顧問服務，曾服務於資策會，Andersen，Deloitte 與 Dynasafe，在海峽兩岸具有 30 年研發與諮詢服務經驗，工作內容涵蓋資訊技術風險管理、資訊安全管理諮詢、 IT 服務管理諮詢、業務連續性管理諮詢和資訊系統審計/電腦稽核等工作。現在是國際電機電子工程師學會 (IEEE) 會員，國際電腦稽核協會 (ISACA) 會員，及中華民國資訊安全學會 (CCISA) 會員，曾發表資訊安全與風險管理方面學術論文多篇，且曾帶領資策會團隊從 RFC 起研發並實作防火牆與 VPN 協定軟體及韌體。本身擁有台灣專利 5 件，大陸專利 4 件，及美國專利一件。

李博士的服務專長與經驗涵蓋:

- 資訊技術風險管理 (ITRM) 及零信任架構 (ZTA) 規劃及實施
- 資訊安全、AI 及 ESG 整合研究
- Web3 資安，區塊鏈，VASP 虛擬資產服務，RWA 現實世界資產與 FinTech 研究
- 資訊安全意識與電腦輔助教育研究
- 資訊安全管理體系 (ISMS) 規劃建置 (ISO27001/BS7799 認證諮詢)
- IT 服務管理體系 (ITSM/ITIL) 規劃建置 (ISO20000/BS15000 認證諮詢)
- 業務連續性管理體系 (BCP) 規劃建置 (ISO22301/BS25999 認證諮詢)
- 密碼學/資訊系統強化/Internet 安全/大型機房與網路系統規劃管理/滲透測試/入侵預防及偵測/資訊安全事件響應諮詢/紫隊駭客攻防演練場域與培訓規畫及實施
- IPO 上市顧問與電腦審計諮詢
- 大陸金融業分支機構開業規劃顧問與電腦審計諮詢/大陸金融業 IT 風險管理規諮詢
- 經濟部標準檢驗局資訊安全標準委員
- 銀行公會金融最高憑證管理機構 (FPKI-PMA) 工作小組成員
- 中華民國電腦稽核協會 CAA (Computer Audit Association) 專業發展委員會委員