組態安全管理的溫故知新

~ NIST SP 800-128 如何因應新興科技環境及國際標準

May 2024

講者簡介

|經歷|

資誠聯合會計師事務所 風險管理及內部控制服務部 副總經理
資誠聯合會計師事務所 風險管理及內部控制服務部 協理/經理/顧問
曾任 星展(台灣)商業銀行股份有限公司 資訊安全服務部 協理暨資安長
曾任 中華民國銀行商業同業公會全國聯合會 金融業務電子化委員會 技術分組 委員
國際資訊安全系統專家(CISSP)、國際電腦稽核師(CISA)
資訊管理系統主導稽核員(ISO 27001:2022 LA)
國際道德駭客認證(CEH) 、國際滲透測試專家(LPT)
國際資安分析專家(ECSA) 、國際數位鑑識專家(CHFI)
國際加密貨幣專家(CCE)

|學歷|

英國華威大學資訊管理碩士
交通大學管理科學系(輔修資訊工程、電腦軟體、半導體製程、財務工程)

|服務專長|

資安風險與資安維運評估與諮詢 / 資安治理與縱深防禦輔導與諮詢
資訊安全檢測與評估服務與諮詢 / 資安事件系統導入與規劃諮詢
資料庫活動管理系統導入與規劃諮詢 / 資訊安全管理制度(ISMS)輔導諮詢
個人資訊管理系統(PIMS)輔導諮詢 / 資訊系統專案管理輔導與諮詢
區塊練應用分析與諮詢 / 加密貨幣發行 / 證券型代幣發行
資訊系統一般控制、應用系統及企業流程之稽核或診斷諮詢
內部控制及作業流程優化 / 企業流程再造及數位轉型

唐雍為　執行董事
資誠 / 風險及控制服務
(02) 2729 6093
yung-wei.w.tang@pwc.com

Agenda

Let’s get started

1. NIST SP800-128 簡介
2. 強化NIST SP 800-53的組態管理(CM)成為安全導向的組態管理(SecCM)
3. ISO 27001:2022的組態管理需要NIST SP800-53及NIST SP800-128
4. 安全導向的組態管理(SecCM)將與零信任(ZTA)相輔相成

1

NIST SP 800-128 簡介

這一篇指引是資訊系統組態安全作業流程的實作指南，指引中交代了組織內部應該安排的角色與組織，亦交代了組態安全應該涵蓋的範疇。

NIST SP 800-128 簡介

資訊系統是由許多軟硬體元件所組成，透過多種安排或是連線，以滿足各類型的業務、任務或安全需求。資訊系統通常處於不斷變化的狀態，以回應新興的、強化的、糾正的或更新的軟硬體功能，而這些回應手法正是組態調整，會確保隨著變化而更動的組態不會對資訊系統或機構組織形成不利的影響，機構組織需要一個被明確定義的組態管理流程。

其實NIST SP 800-53已經提供了組態管理基本設計的框架，透過建立基準以及追蹤、控制和管理業務開發和營運的許多方面（例如產品、服務、製造、業務流程和資訊技術）。而一個穩健的組態管理更需要考量資訊安全這一個黑天鵝因素，而NIST SP 800-128的重點是 組態管理資訊安全方面的實現，因此術語「以安全為中心的組態管理」(SecCM) 用於強調對資訊安全的關注。SecCM 被定義為對系統配置的管理和控制，以實現安全性並促進資訊安全風險的管理。

NIST SP 800-128 簡介(續)
觀念一：建立組態管理小組

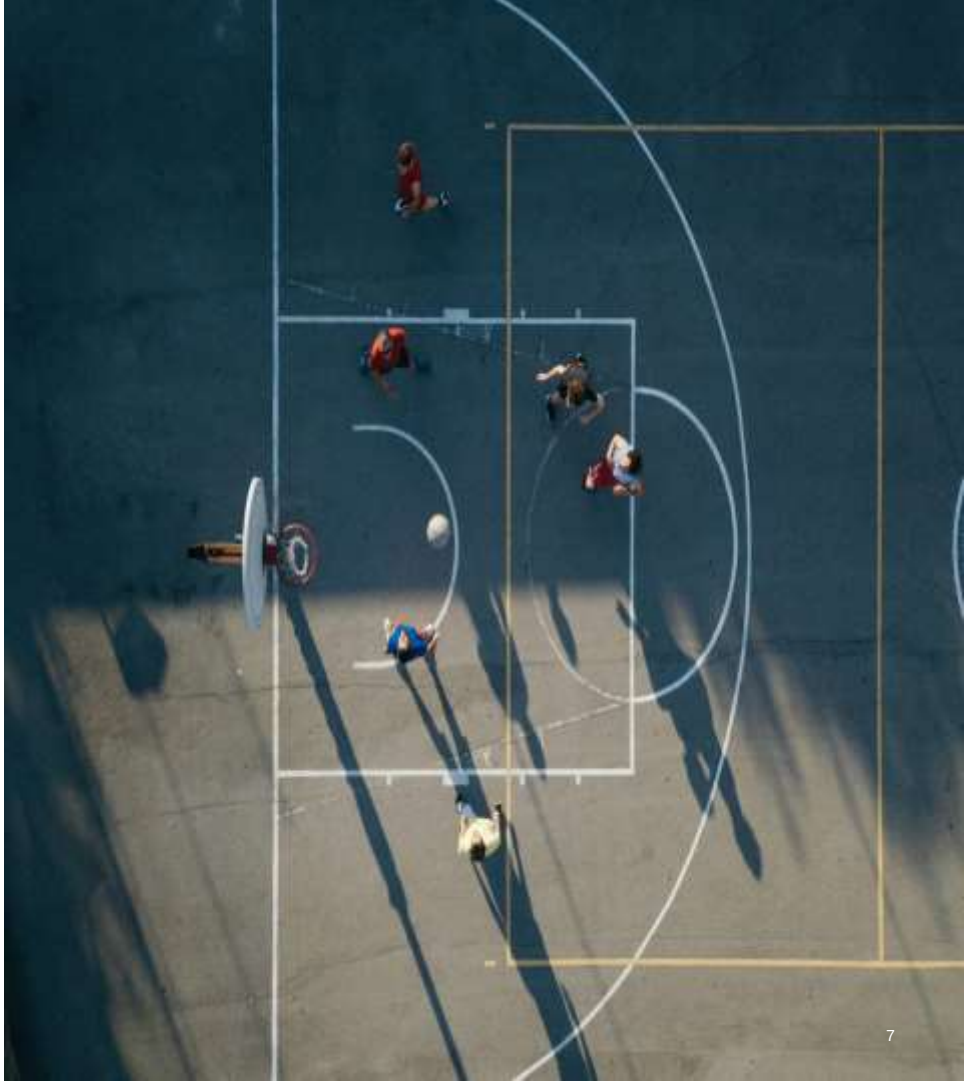
組態管理小組（Configuration Control Board, CCB）是一個通常由兩個或兩個以上個人組成的小組，在設備種類繁多的組織，有些時候會分類別設置（例如：網路設備組態管理小組或作業系統組態管理小組），降低其工作量及提升及審閱品質。

就設計而言，組態管理小組具有審查和批准資訊系統組態變更的集體責任和權力。 該小組代表組織內部的不同觀點，被選中來評估和批准對系統的變更。 組態管理小組是對組態變更活動的檢查和平衡，確保變更在實施之前符合組織定義的標準（例如範圍、成本、對安全性的影響）。 對於在組織使命背景下規模、範圍和重要性有限的系統，組態管理小組可能不太正式。在已經有成熟變更管理流程的組織，該小組將會是定期（或不定期）變更會議的必要參加成員，相關管理作業也將併同變更會議一併進行。

NIST SP 800-128 簡介(續)
觀念二：建立預先核准清單

許多在資訊安全方面較為成熟的組織會建立了一份經批准的硬體和軟體產品清單（例如：物聯網設備白名單、網路設白名單或軟體白名單）以供整個組織於採購時考量或使用。

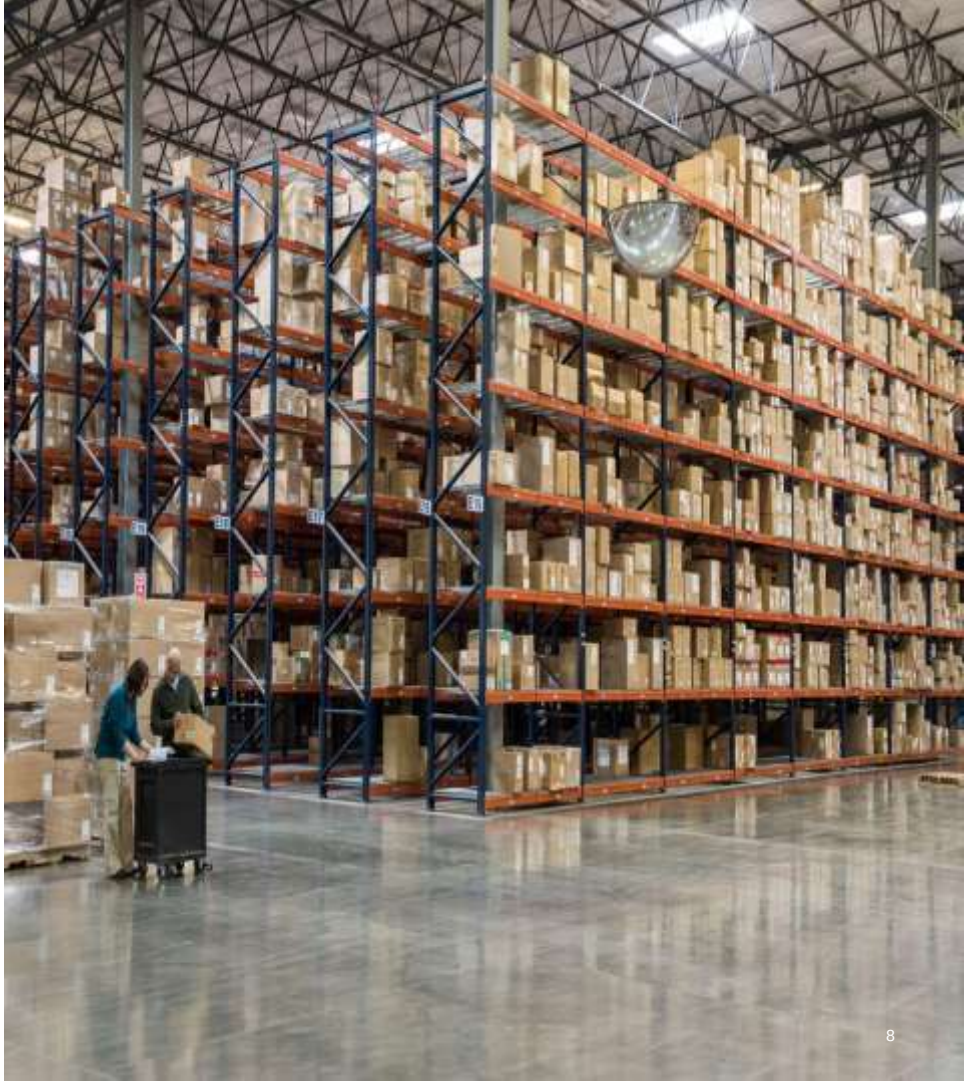
系統擁有者在沒有特殊情形的採購程序中，必須批准清單中選擇和使用產品，但因為預先核准之故，相關核准程序也將較為單純。在建立預先核准清單的時候，組織將針對該硬體或軟體的各元件進行評估，最終由組態變更小組進行審閱與核准，方得以列入清單中。在大多數硬體或軟體都採用預先核准清單的前提下，後續管理的資源耗損將可以大幅下降。



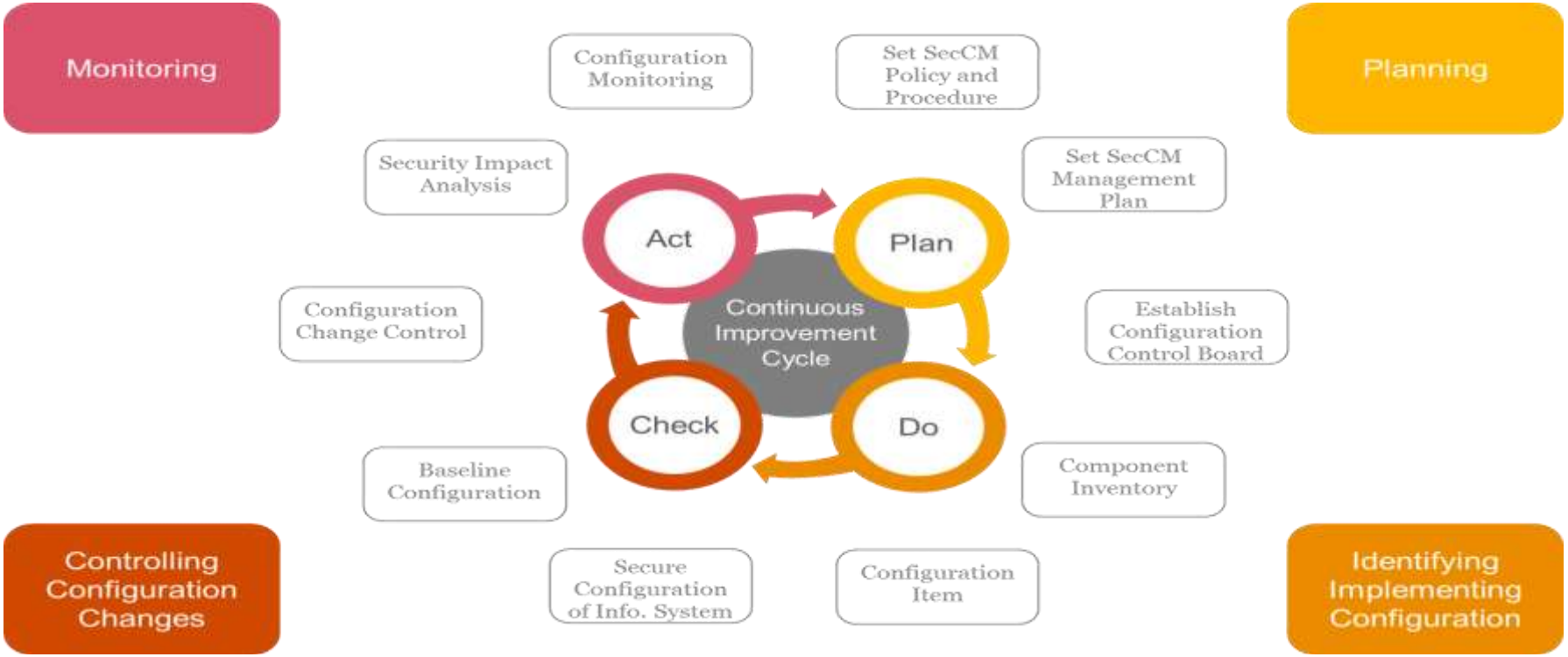
NIST SP 800-128 簡介(續)
觀念三：組態管理包羅萬象

在組織開發和部署系統時，都必須要關注組態管理的議題，這包含系統及其組成元件相關的安全性配置。這些安全配置可能包括：

- **作業系統和應用程式功能**（根據特定功能啟用或停用、設定特定參數等）
- **服務和連接埠**（前者如自動更新後者如Port 53之DNS）
- **網路協定和網路介面**（前者如 NetBIOS、IPv6；後者如藍牙、IEEE 802.11）
- **遠端存取方法**（例如 SSL、VPN、SSH、IPSEC）
- **存取控制**（例如，控制檔案、目錄、登錄項目的權限）
- **識別碼/帳戶的管理**（例如，更改預設帳戶名稱）
- **身份驗證控制**（例如，密碼長度與複雜、密碼最短期限）
- **日誌設定**（例如，擷取關鍵事件，如失敗、登入、權限變更）
- **系統設定**（例如，連線逾時、遠端連線數、連線鎖定）
- **密碼學**（例如，特定強度密碼協定或演算法來保護傳輸中的資料）



NIST SP 800-128 簡介(續)
觀念四：良好的組態管理PDCA

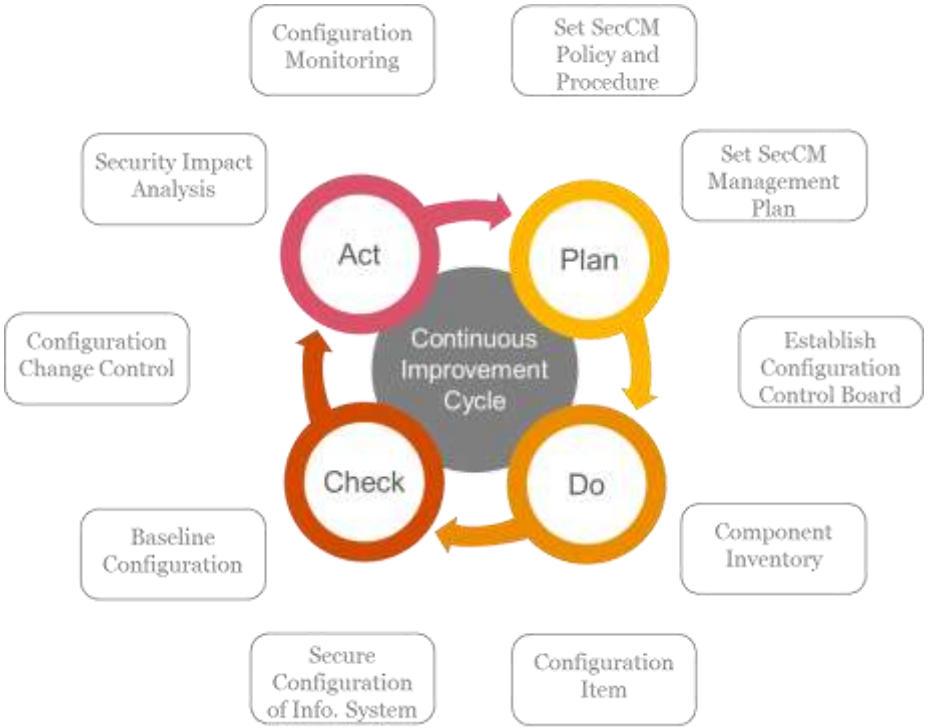


2

強化NIST SP 800-53的組態管理成為安全導向的組態管理

NIST SP 800-128可以提供NIST SP 800-53更多的補充，也將如何實施組態管理的具體指南或是範本，充分將NIST SP 800-53中的CM1至CM9如何妥善落地管理具體敘述。

NIST SP 800-53與SP 800-128的對應關係



NIST SP-800-53 Configuration Management (CM)		
CM1	Policy and Procedure	1 / 2
CM2	Baseline Configuration	7
CM3	Configuration Change Control	3 / 5 / 8
CM4	Impact Analysis	9
CM5	Access Restriction for Change	8
CM6	Configuration Setting	6
CM7	Least Functionality	6
CM8	System Component Inventory	4
CM9	Configuration Management Plan	2
CM10	Software Usage Restrictions	N/A
CM11	User-installed Software	N/A
CM12	Information Location	N/A
CM13	Data Action Mapping	N/A
CM14	Signed Components	N/A

NIST SP 800-53與SP 800-128的對應關係(續)

觀察重點：

- SP 800-53規劃的控制點與SP 800-128的實作流程建議順序不相同但是可以準確對應。
- Configuration Change Control是維繫組態安全的重要流程，SP 800-128有三個步驟都是針對此控制點的強化。
- 在權限管理中授權最小化原則可以映射至組態管理的功能最小化原則。
- 透過SP 800-53更完整的控制點設計，更可以理解若沒有預先核准清單的狀況下，妥善管理組態將會是一大挑戰。
- 權限控管其實不只是組態管理中有所提及，但是也是組態管理的一部分，在組態管理中主要著重在預設及初始之權限。
- Configuration Monitoring雖然沒有對應到SP 800-53，但是Configuration Monitoring涉及確定系統是否按照議定之組態配置，將發會讓整個PDCA循環承上啟下的重要功能。

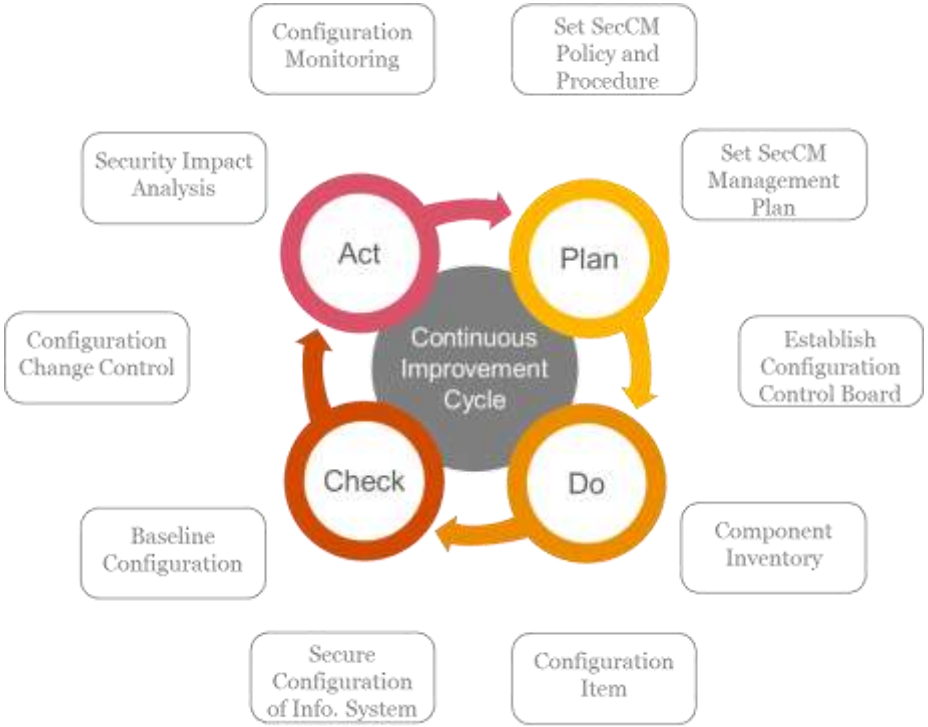
NIST SP-800-53 Configuration Management (CM)		
CM1	Policy and Procedure	1 / 2
CM2	Baseline Configuration	7
CM3	Configuration Change Control	3 / 5 / 8
CM4	Impact Analysis	9
CM5	Access Restriction for Change	8
CM6	Configuration Setting	6
CM7	Least Functionality	6
CM8	System Component Inventory	4
CM9	Configuration Management Plan	2
CM10	Software Usage Restrictions	N/A
CM11	User-installed Software	N/A
CM12	Information Location	N/A
CM13	Data Action Mapping	N/A
CM14	Signed Components	N/A

3

ISO 27001:2022組態管理需要NIST SP800-53/128

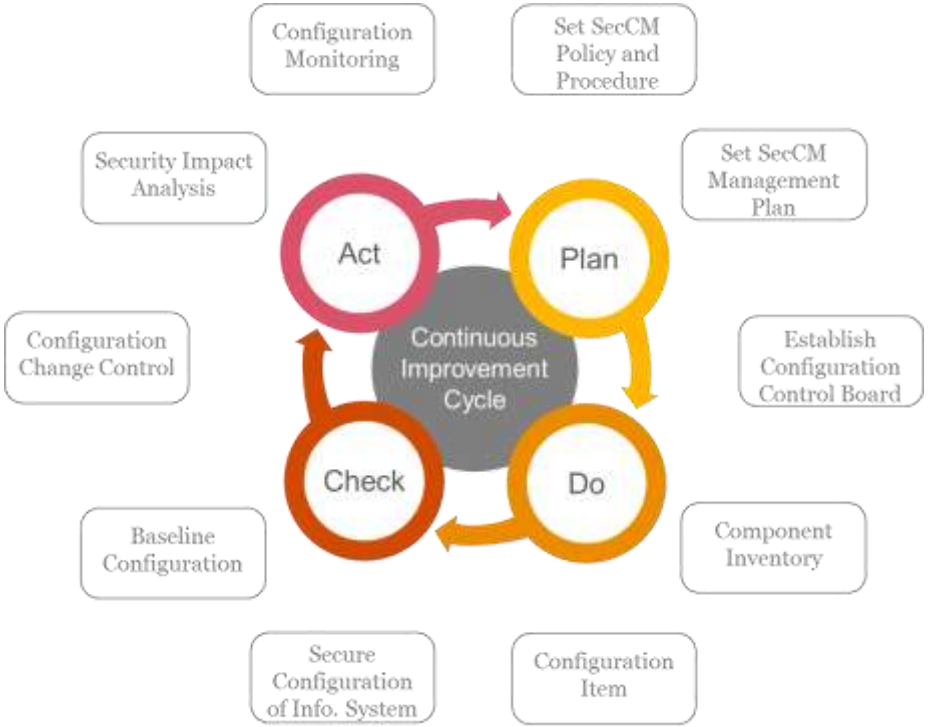
ISO27001是國際資訊安全標準，適用大部分產業；NIST-SP800-128則是美國聯邦的資訊安全標準，此指引對於新版ISO27001要求的變更管理、惡意軟體防範、技術脆弱性管理、組態管理及監視活動都有所裨益。

NIST SP 800-128與 ISO 27001:2022的附錄A 8.9 組態管理



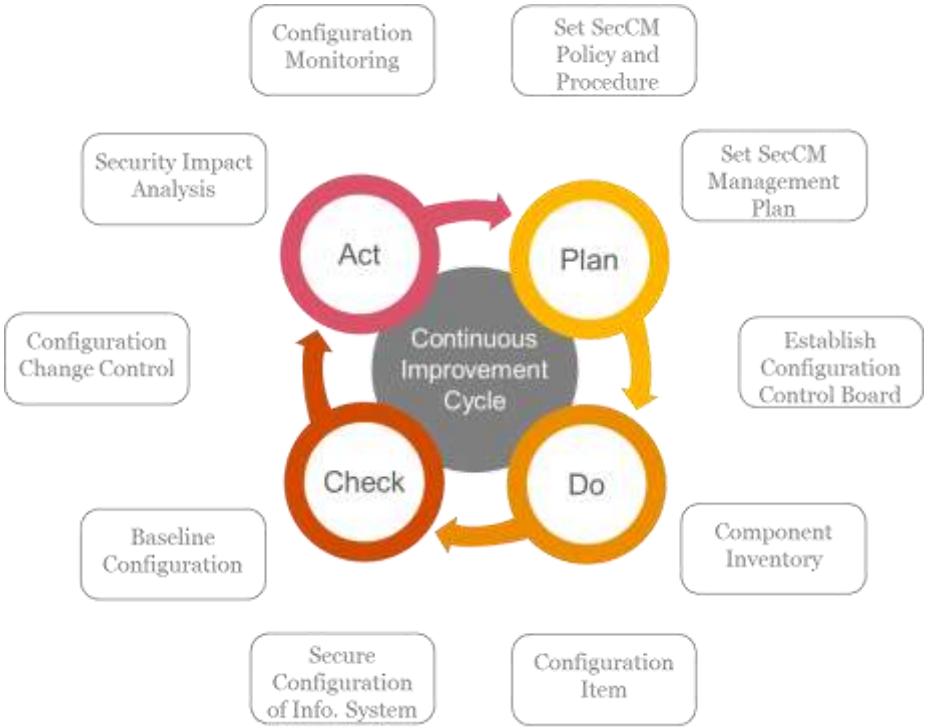
ISO 27001:2022的附錄A		
5.1	資訊安全政策	1 / 2
建立組態管理政策是基本（整併或單獨）		
5.2	資訊安全之角色管理與責任	1 / 2 / 3
在組態管理政策中規定既有角色的新責任及新的虛擬組織		
5.7	威脅情資	5 / 6 / 7
情資可能引領新的組態基準（例：因應WannaCry關閉SMB）		
5.9	資訊與其他關聯資產之清冊	4 / 5
有效盤點軟硬體軟硬體、服務及網路才可得知組態套用範疇		
5.10	資訊與其他關聯資產之可接受用途	5 / 6 / 7
系統或應用的組態將可以限制使用者僅能操作可接受用途（例：無法使用Powershell）		

NIST SP 800-128與 ISO 27001:2022的附錄A 8.9 組態管理(續)



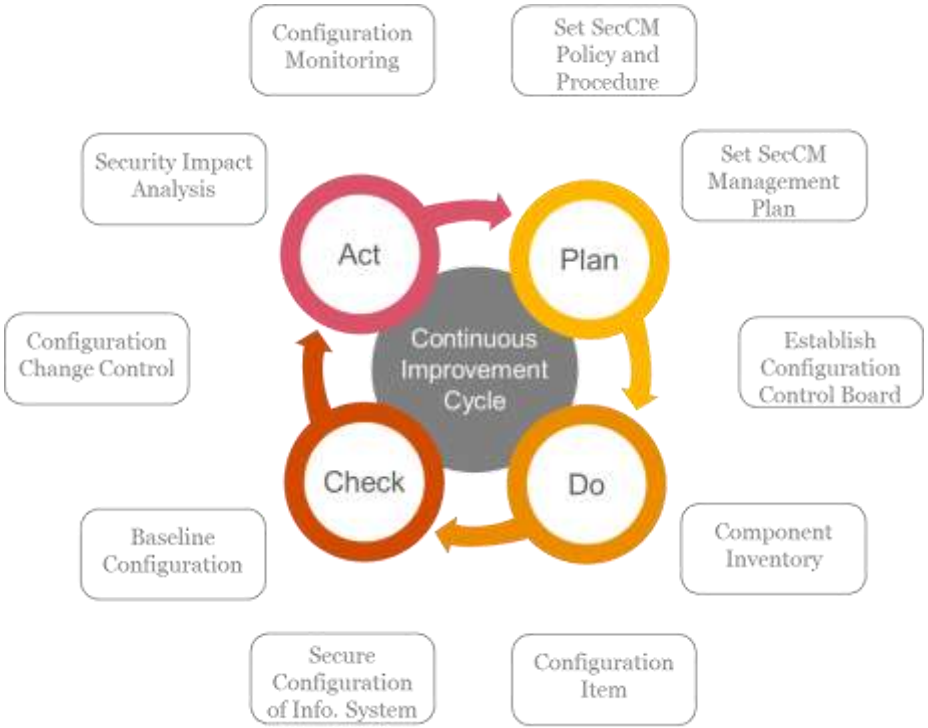
ISO 27001:2022的附錄A		
5.15	存取控制	5 / 6 / 7
以組態進行存取自動控制 (例：停用Guest帳號)		
5.17	存取權限	5 / 6 / 7
以組態進行權限自動控制 (例：停用everyone權限套用至匿名使用者)		
5.22	供應者服務之監視、審查及變更	5 / 6 / 7 / 8 / 10
供應商的服務及設定不在公司內部，必須建立不同的組態基準		
5.23	使用雲端服務之資訊安全	5 / 6 / 7 / 8 / 10
雲端的服務及設定不同於地端，必須建立不同的組態基準		
5.35	資訊安全之獨立審查	3 / 8
CCB對於基準的審查及在變更管理中對於上線的審查皆屬於此		

NIST SP 800-128與 ISO 27001:2022的附錄A 8.9 組態管理(續)



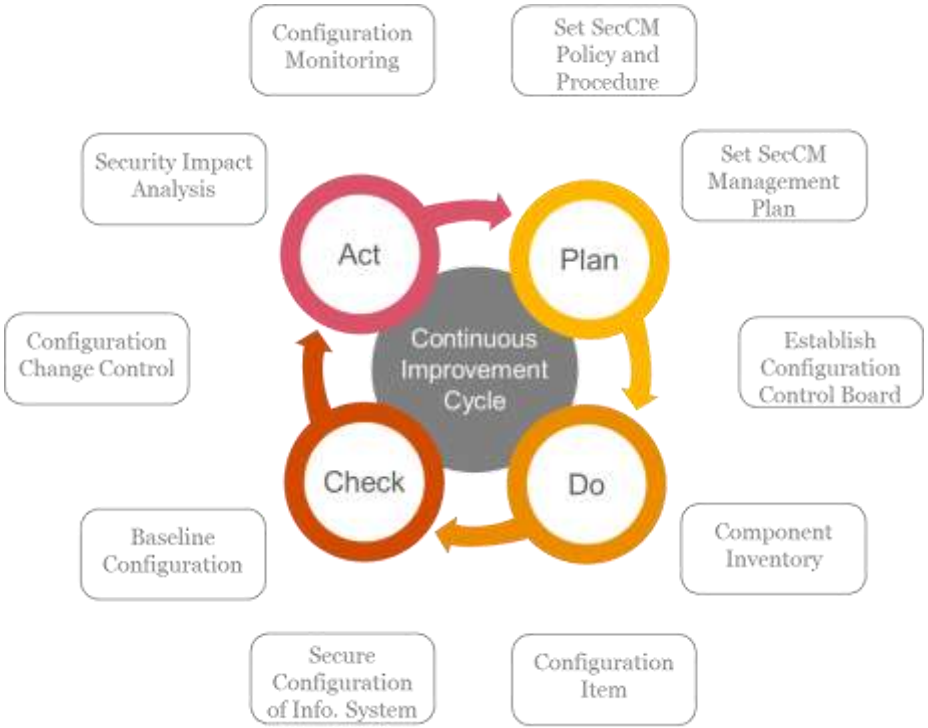
ISO 27001:2022的附錄A		
6.7	遠距辦公	5 / 6 / 7
以組態限制可以遠距辦公的渠道為自動控制（例：關閉Talnet）		
8.1	使用者端點裝置	5 / 6 / 7
以組態限制使用者端設備之資料存取（例：開啟BitLocker）		
8.2	特殊存取權限	5 / 6 / 7
以組態限制特權帳號存取（例：更改預設帳戶名稱）		
8.3	資訊存取限制	5 / 6 / 7
以組態限制特定資料存取（例：限制使用者存取控制台部分功能）		
8.8	技術脆弱性管理	5 / 6 / 7
調整預設組態提升防護（例：透過設定改動密碼Hash演算法）		

NIST SP 800-128與 ISO 27001:2022的附錄A 8.9 組態管理(續)



ISO 27001:2022的附錄A		
8.9	組態管理	ALL
應建立、紀錄、實作、監視及審查軟硬體、服務及網路之組態		
8.15	存錄	10
組態的活動、異常及錯誤也是需要以日誌紀載 (例：Audit Log)		
8.16	監視活動	10
網路、系統及應用之組態可評估資安事件 (例：Logging Disable)		
8.20	網路安全	5 / 6 / 7
以組態自動控制網路與網路裝置 (例：關閉藍芽資料傳輸)		
8.21	網路服務安全	5 / 6 / 7
透過組態自動控制網路服務 (例：關閉預設的FTP服務)		

NIST SP 800-128與
ISO 27001:2022的附錄A 8.9 組態管理(續)



ISO 27001:2022的附錄A		
8.25	安全開發生命週期	5 / 6 / 7 / 8 / 9
在開發過程中就必須考量組態基準的套用，而非上線前再嘗試		
8.29	開發及驗收中之安全測試	5 / 6 / 7 / 8
除了在開發過程中考量組態基準的套用，也必須確保以基準上線		
8.32	變更管理	5 / 6 / 7
傳統變更管理主要針對程式碼，現在組態也需要納入變更管理		

4

安全導向的組態管理將與零信任相輔相成

零信任中信任推斷此一環節，若搭配安全導向組態管理的概念，安全組態保護零信任關鍵元件的安全性，零信任亦可以保護組態之安全運作。

安全導向的組態管理可作為實踐零信任架構的好夥伴

使用安全導向的組態管理流程將可以更有效的保護零信任架構中的關鍵元件，如：政策管理及政策引擎的存取與設定透過組態管理的監控機制確保運作穩定，安全導向組態管理其實更完整的說明了零信任元件的保護如何實作，套用安全組態管理至零信任架構之關鍵為：

- 識別和保護零信任架構關鍵組態項，例如存取控制策略、網路規則和身分驗證設定。（Planning + Identifying Implementing Configuration）
- 實施流程來控制對零信任架構組態項的變更。（Controlling Configuration Change）
- 監控零信任架構組態項以確保它們符合基線組態。（Monitoring）

零信任架構亦是安全導向組態管理的穩定運作保障

零信任架構可以提供一種更安全的方法來實施安全導向的組態管理流程。例：作業系統的組態基線必須透過零信任架構中所驗證的人員及設備，方得以在有足夠信任推論的前提下進行調整，如此將可以提供更高規格的Configuration Change Control；零信任架構中的信任推論，也可以將組態基線作為參考元素之一，如：未啟用作業系統日誌之使用者端點不能存取核心系統，以降低組態異常之資訊安全事件風險。套用零信任架構至安全組態管理的關鍵為：

- 使用零信任架構的原則和技術來驗證使用者、裝置和應用程式，並在授予存取權限之前對其進行授權。
- 使用零信任架構的持續監控和威脅偵測功能來識別和響應安全威脅（將組態異動也視為風險）。

Thank you

pwc.com

© 2024 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.