解讀 NIST Cybersecurity Framework: Identify

登豐數位科技
技術總監 黃建笙

MVP CISSP ISSMP LPT MASTER

本次改版與識別一節有關的變更

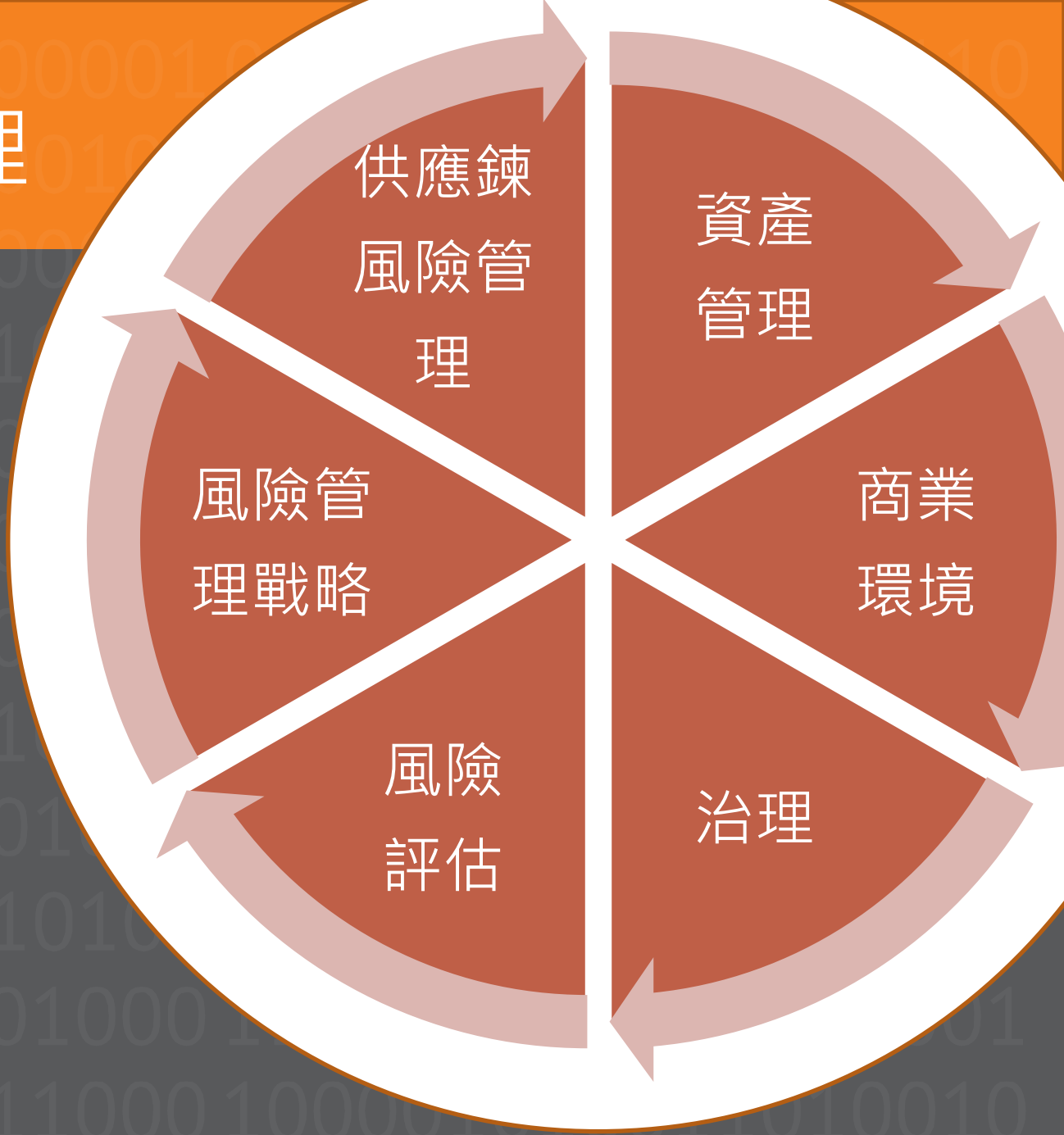
大大的延展了CyberSecurity Framework在利害關系人溝通網路要求，更有助於使用者更好的去理解網路供應鏈風險管理(SCRM)，新增的3.4節購買決策，則強調於使用框架來理解與商業現成產品與服務相關的風險。而其它Cyber SCRM標準已經附加入實施層，最後，供應鍊風險管理類別亦皆加至框架的核心中。

識別功能

組織去了解及發展以管理系統、人員、資產、資料和功能的網路安全風險的能力。

識別功能不只是資產管理

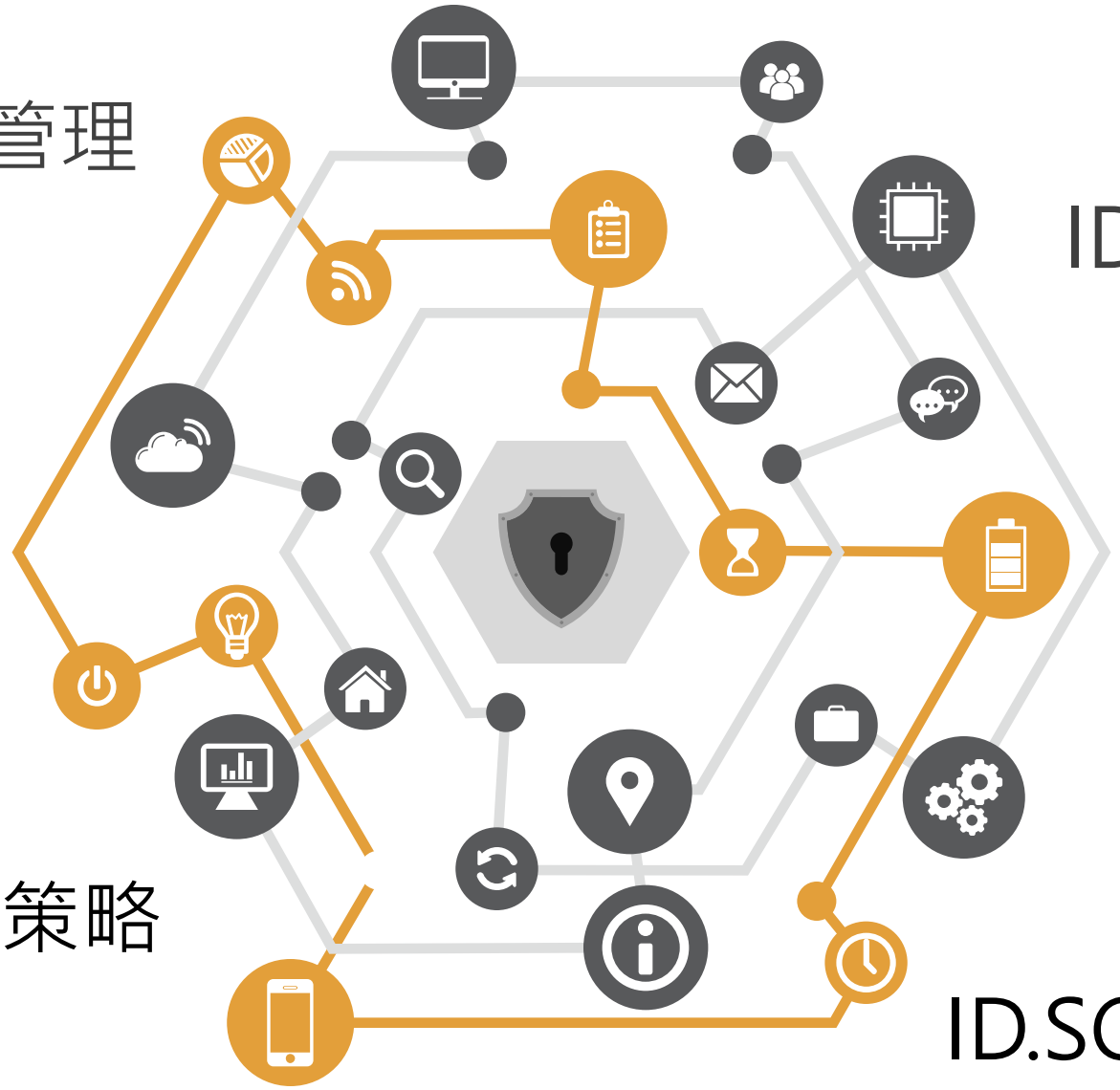
識別功能中的活動是有效使用框架的基礎。
了解業務環境，支持關鍵功能的資源以及相關的網路安全風險，使組織能夠根據其風險管理策略和業務需求，集中精力並確定其工作的優先等級。
此功能中的結果類別分類包括：資產管理; 商業環境;治理; 風險評估; 和風險管理策略。



識別功能下有那些類別該做的?

ID.AM資產管理

ID.GV 治理

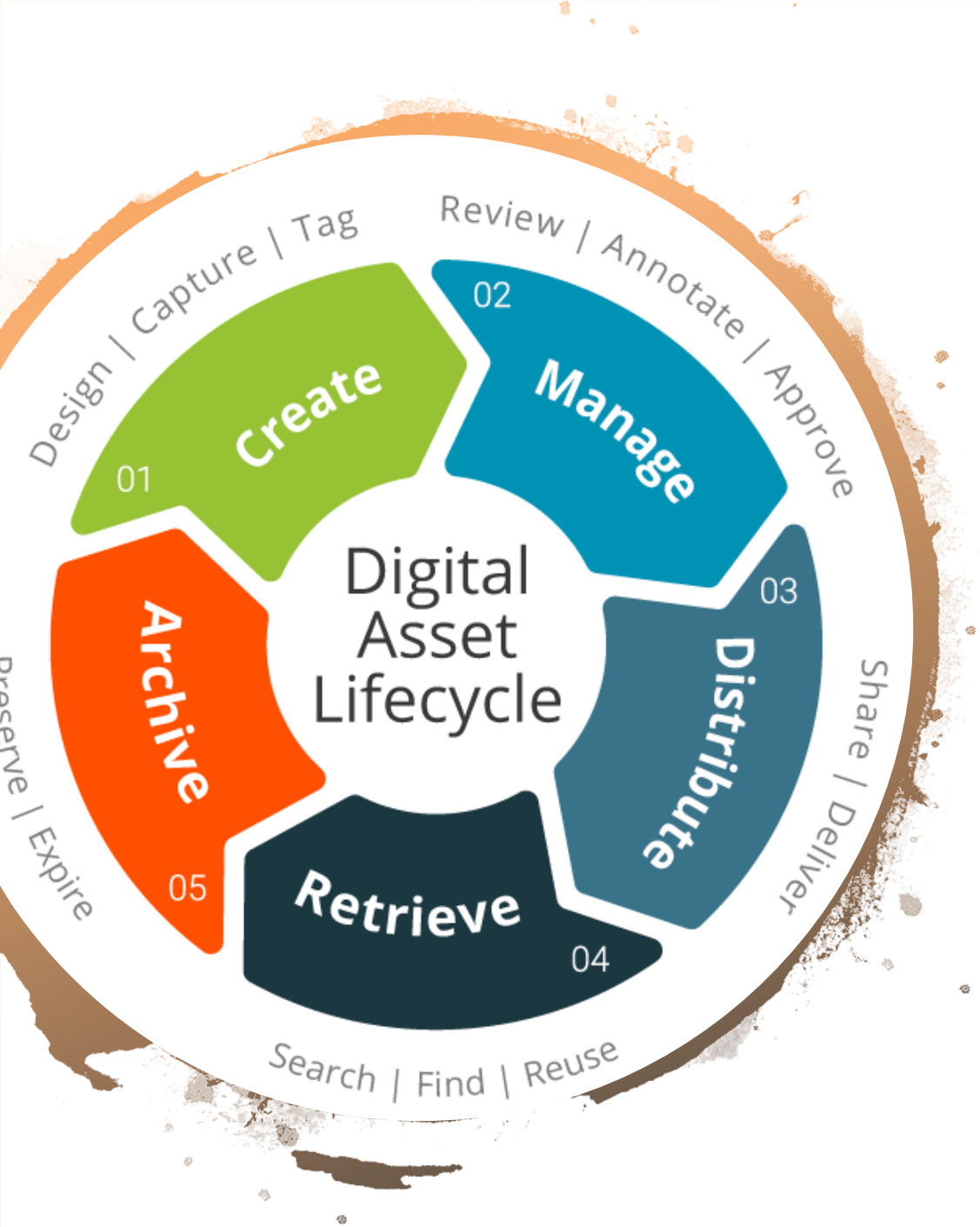


ID.BE商務環境

ID.RA風險評估

ID.RM風險管理策略

ID.SC供應鍊風險管理



ID.AM: 資產管理

根據組織對組織目標和組織風險策略的相對重要性，識別和管理使組織實現業務目的的數據，人員，設備，系統和設施。

ID.AM-1	組織內的實體設備和系統已列入清單
ID.AM-2	組織內的軟體平台和應用程式已列入清單
ID.AM-3	對映組織通信和資料流程
ID.AM-4	對外部資訊系統進行分類
ID.AM-5	資源（例如，硬體，設備，數據，時間，人員和軟件）根據其分類，關鍵性和業務價值劃分優先級
ID.AM-6	建立整個勞動力和第三方利益相關者（例如供應商，客戶，合作夥伴）的網路安全角色和責任

ID.BE 商業環境

了解並優先考慮組織的使命，目標，利益相關者和活動; 此資訊用於告知網路安全角色，職責和風險管理決策。

ID.BE-1	• 確定並傳達組織在供應鏈中的作用
ID.BE-2	• 確定並傳達組織在關鍵基礎設施及其工業部門中的位置
ID.BE-3	• 建立和傳達組織使命，目標和活動的優先事項
ID.BE-4	• 建立了關鍵服務交付的依賴關係和關鍵功能
ID.BE-5	• 為所有運行狀態（例如在脅迫/攻擊，恢復期間，正常運行期間）建立了支持關鍵服務交付的恢復能力要求

ID.GV治理：

管理和監控組織的法規，法律，風險，環境和運營要求的政策，程序和流程得到了解，並為管理層提供網路安全風險。

ID.GV-1	• 建立並傳達組織網路安全政策
ID.GV-2	• 網路安全角色和職責與內部角色和外部合作夥伴協調一致
ID.GV-3	• 了解和管理有關網路安全的法律和監管要求，包括隱私和公民自由義務
ID.GV-4	• 治理和風險管理流程解決網路安全風險

ID.RA 風險評估

組織了解組織運營（包括任務，職能，形像或聲譽），組織資產和個人的網路安全風險。

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

ID.RA-1

- 識別並記錄資產漏洞

ID.RA-2

- 從信息共享論壇和來源收到網路威脅情報

ID.RA-3

- 識別並記錄內部和外部威脅

ID.RA-4

- 確定潛在的業務影響和可能性

ID.RA-5

- 威脅，脆弱性，可能性和影響用於確定風險

ID.RA-6

- 確定風險響應並確定優先順序

ID.RM 風險管理策略

建立組織的優先級，約束，風險容忍度和假設，並用於支持操作風險決策。

ID.RM-1

- 風險管理流程由組織利益相關者建立，管理和同意

ID.RM-2

- 確定並明確表達組織風險承受能力

ID.RM-3

- 組織對風險承受能力的確定取決於其在關鍵基礎設施和行業特定風險分析中的作用

ID.SC供應鏈風險管理

建立組織的優先級，約束，風險容忍度和假設，並用於支持與管理供應鏈風險相關的風險決策。 該組織已建立並實施了識別，評估和管理供應鏈風險的流程。

ID.SC-1

組織利益相關者確定，建立，評估，管理和同意網路供應鏈風險管理流程

ID.SC-2

使用網路供應鏈風險評估流程識別，確定優先級並評估信息系統，組件和服務的供應商和第三方合作夥伴

ID.SC-3

與供應商和第三方合作夥伴簽訂的合約用於實施旨在實現組織網路安全計劃和網路供應鏈風險管理計劃目標的適當措施。

ID.SC-4

供應商和第三方合作夥伴通過稽核，測試結果或其他形式的評估進行例行評估，以確認他們是否履行了合約義務。

識別需要實力，但也需要運氣

Digital Technology