財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

重要數位資料治理暨管理制度規範(EDGS)

Essential Data Governance and Management System

（2021 年 1 版）

資訊工業策進會科技法律研究所

2021.7

目錄

圖目錄

表目錄

0. 前言

0.1 概述

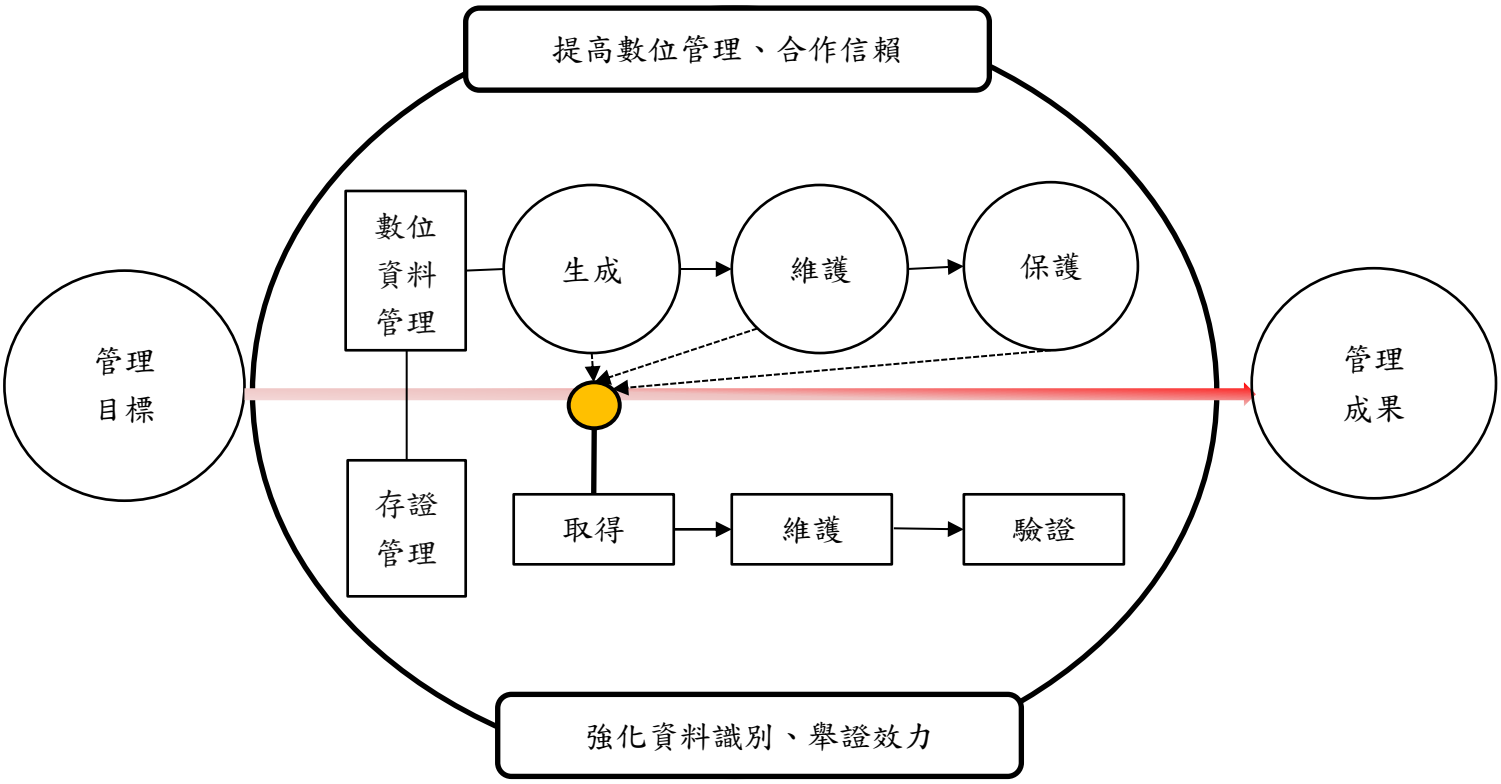
隨著組織面對新興科技發展所帶來之產業、社會與經濟層面之數位轉型趨勢，或面臨災難或緊急事變(例如嚴重特殊傳染性肺炎)發生等情事，驅動組織數位化治理及管理轉型需求提升，包含董事會及最高管理階層之決策、監督至內稽、內控等，需階段性建立與執行內容或流程數位化管理措施，強化資料真實性、完整性、以及資訊充分揭露，提升組織決策、執行、監督與管理效益。

組織進行數位化過程雖帶來便利與效率，但同時亦伴隨著風險。數位資料具有易於竄改、易於散播等特性，往往造成原始版本所有人難以證明其為源頭生成者，進而影響其權利保障。此外，組織在與其他對象合作時，可能提供其他對象、或接收其他對象之重要數位資料，當發生資料外洩或爭議事件，需有輔助識別或證明資料來源之措施，方能釐清責任，以提高各方合作信賴。

重要數位資料治理暨管理制度規範（以下簡稱「本規範」）是一個由組織自主決定是否導入之管理模式，期能漸進推升組織數位化治理暨管理程度，從源頭端完善數位資料歷程保護起步，強化組織重要數位資料之長期保存效力，以確保後端發生訴訟糾紛或相關監管單位調查時，具有證據能力並強化其證據力。

0.2 制度標的

本規範之要求係以組織重要數位資料治理暨管理制度流程為核心標的(如下圖一所示)。所謂組織重要數位資料治理暨管理制度流程，係指組織依其所訂定之管理政策，設定管理目標，從數位資料之生成、保護、維護，至數位資料存證資訊之取得、維護、驗證。



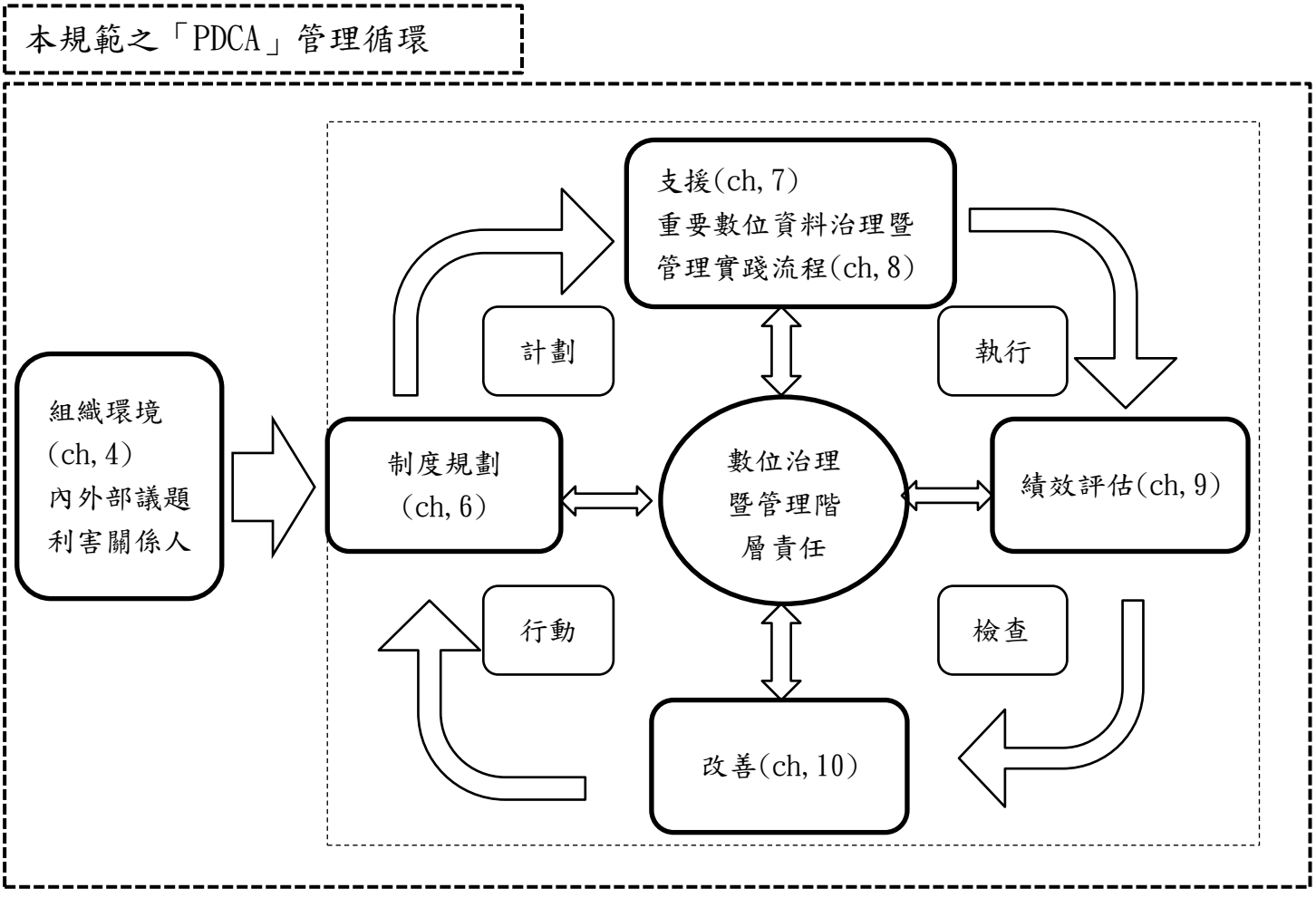
圖一：組織重要數位資料治理暨管理制度流程概念

0.3 流程管理

本規範鼓勵組織連結與強化既有「流程管理」之方法來發展、實施及改善組織重要數位資料治理暨管理制度。

0.4 管理循環

本規範鼓勵組織連結與強化既有「PDCA 管理」循環(如下圖二所示)。



圖二：本規範之 PDCA 管理循環架構

0.5 訂定目的

0.5.1 宗旨

本規範旨在促使組織重要數位資料治理暨管理制度達到下列效益：

(a) 提高組織內控、內稽或監督之數位化治理暨管理程度；

(b) 提高組織間合作信賴與數位轉型機會；

(c) 強化組織識別與管理自行生成、提供或接收外部之數位資料；

(d) 強化組織訴訟舉證或監管單位調查證明之效力。

0.5.2 用途

本規範係為引導組織：

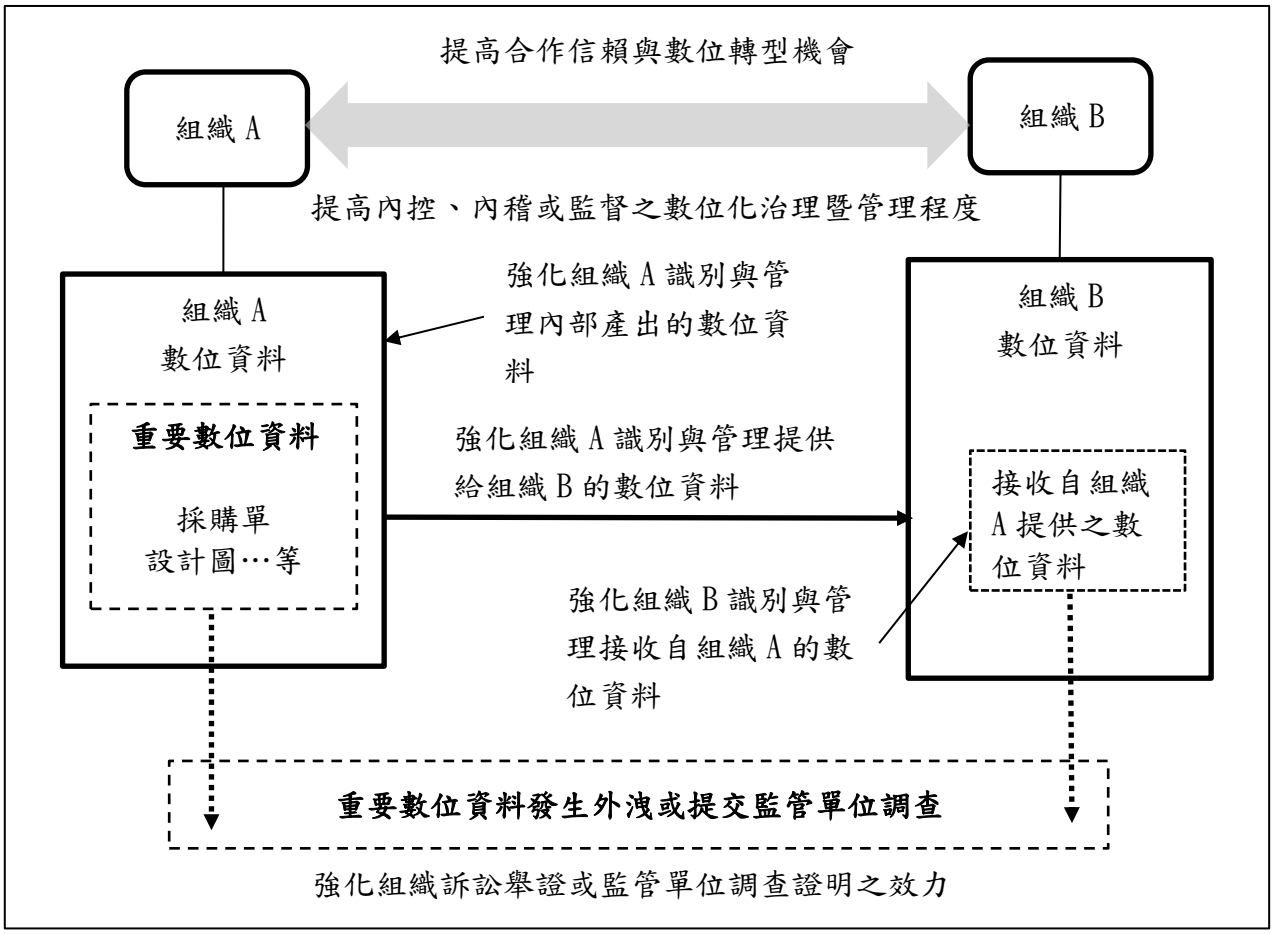
(a) 確保其制度符合組織明訂之重要數位資料治理暨管理政策與目標；

(b) 建立符合本規範之組織重要數位資料治理暨管理制度；

(c) 實施、維持與持續改善組織重要數位資料治理暨管理制度。

0.6 與其他管理系統之相容性

本規範旨在使組織能與內稽、內控、或其他既有管理流程進行整合與調適，以建立符合本規範所要求之組織重要數位資料治理暨管理制度。



圖三：本規範訂定之目的

1. 適用範圍

本規範旨在適用所有組織，不論型態、規模及所提供的產品或服務。

本規範第 0 至 4 單元為系統架構、適用範圍、名詞定義及考量因素之說明；第 5 至 10 單元為管理要項。

表一：本規範目錄架構

導入制度各階段	單元名稱	
導入前	第 4 單元	4.1 評估內外部議題

	組織環境	4.2 關注利害關係人需求
	第 5 單元 數位治理 暨管理階層責任	5.1 管理階層展現領導與承諾
		5.2 擬定政策
		5.3 設定目標
		5.4 確認權責與溝通
	第 6 單元 制度規劃	6.1 應規劃之基本事項
		6.2 應考量之風險與機會
		6.3 變更規劃流程
導入中	第 7 單元 支援	7.1 資源
		7.2 人員
		7.3 設備或系統環境
		7.4 溝通管道
	第 8 單元 重要數位資料 治理暨管理實踐流程	8.1 數位資料之生成、保護、維護
		8.2 存證資訊之取得、維護、驗證
導入後	第 9 單元 績效評估	9.1 基本要求
		9.2 資料分析
		9.3 內部稽核

		9.4 管理審查
	第 10 單元 改善	採取必要矯正措施

2. 版本標示

組織引用本規範，應註明所引用版本年度及版次，例如 2021 年 1 版。

3. 名詞與定義

本規範相關名詞，定義如下。

3.1 組織(organization)

指為達成特定目標所組成之團體。一個機關或機構中的單位或專案團隊，亦可被界定為本規範所謂之組織。

3.2 數位資料(digital record)

指一種透過數位電腦進行操作、傳輸或處理的資料，舉凡電子郵件、影音數位化檔案等皆屬之。

3.3 身份辨識技術(identification technology)

指為確認持有、確認來源或接觸控管之技術手段，包括但不限於數位簽章、生物辨識技術、雙/多因子認證…等。

3.3.1 數位簽章(digital signature)

指將數位資料以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並讓他人得以該把私密金鑰相對應之公開金鑰加以驗證。

3.3.2 生物辨識技術（biometric authentication technologies）

指以人類生理特徵作為辨識依據，舉凡顏面、指/掌紋、靜脈、瞳孔/視網膜、語音等。

3.3.3 雙/多因子認證（two/multi-factor authentication）

一種認證方法，使用複數不同的信物，可包含認知(如密碼)、特徵(如語音)、位置(如 IP 位址)等，合併在一起，用途為加強確認使用者身份。

3.4 後設資料(metadata)

指描述數位資料本體的資料，用於協助對數位資料的辨識、描述、與指示其位置的任何資料，此資料一般不存在於原數位資料本體。

3.5 雜湊函數(hash Function)

指能將任意大小的訊息，濃縮為一定長度的訊息摘要(message digest)之函數，具備單向(one-way)以及抗碰撞(collision resistance)之特性。所謂單向是指不能由訊息摘要反推出訊息原文；抗碰撞則是一個好的雜湊函數具備的特性，亦即不同大小的檔案，其訊息摘要皆不同。

3.6 雜湊值(hash value)

指經雜湊函數運算過後之訊息摘要值，亦稱為訊息指紋，可當作檔案的識別資訊，用於確保資料的完整性。

3.7 時戳(time-stamp)

即數位化之郵戳，證明數位資料或其對應之雜湊值在某一時間點即存在，且自該時間點後內容未被竄改，用於確保資料的不可否認性(non-repudiation)。

4. 組織環境

4.1 內外部議題

組織應關注與組織目標相關之內部和外部議題，並評估這些議題對達成組織重要數位資料治理暨管理制度預期結果之影響。

4.2 利害關係人

組織應決定和組織重要數位資料治理暨管理制度有關的利害關係人，並關注與評估利害關係人對組織重要數位資料治理暨管理制度之要求或期待。

5. 數位治理暨管理階層責任

5.1 管理階層承諾

董事會及最高管理階層應展現對重要數位資料治理暨管理制度之領導、決策、監督與資訊充分掌握，評估與引導調適組織內稽、內控或其他既有管理制度；最高管理階層需確保其承諾在組織中被了解、擬定規劃(參照 6)、提供適切支援（參照 7)、實踐流程(參照 8)、達成預期績效（參照 9)、強化持續改善（參照 10)，並定期向董事會提出重要數位資料之治理政策、目標、制度、執行、績效、改善之報告，董事亦應就涉及公司經營之項目負監督之義務。

5.2 管理政策

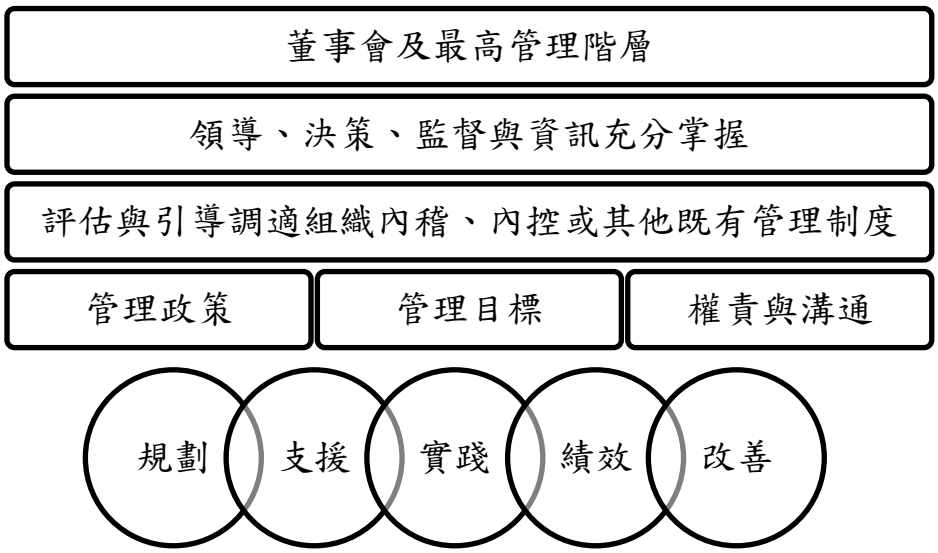
最高管理階層應考量內外部議題和利害關係人(參照 4)，於既有營運管理政策中，建立、實施、維持重要數位資料治理暨管理制度政策。政策中應呈現管理之流程與要求，於組織內進行溝通、了解並被應用，並於適當時可被利害關係人取得。

5.3 管理目標規劃

最高管理階層應設定重要數位資料治理暨管理制度目標，所設定之目標應符合上述管理政策，且該目標應具有能被評估是否達成、受到監督、及適時予以更新之特性。

5.4 管理權責與溝通

最高管理階層應明確界定重要數位資料治理暨管理制度之管理權責，對內部溝通需確保被組織成員周知，自行或指派高階人員負責確保制度流程的建立、實施、維持，以及定期或不定期向最高管理階層報告管理制度的績效（參照 9）及改善需求（參照 10），以確保管理制度的完整性與一致性；對外溝通需符合國外或國內法規要求或經溝通對象同意，採用國外或國內認可之身份辨識技術，或其他提高溝通效率、降低溝通成本之技術做法。



圖四：數位治理暨管理階層責任

6. 制度規劃

6.1 基本要求

組織應依其規模、型態，以及考量國內或國外相關法令、規範、標準或指南，自行或引進外部專家團隊建立、實施、與維持組織重要數位資料治理暨管理制度，並持續改善其有效性。為達成本項要求，組織應至少進行下列事項：

(a) 確保最高管理階層訂定重要數位資料治理暨管理政策與目標，並自行或指派權責人員，依目標建立、實施、維持所需之計畫，統籌、規劃、推行重要數位資料治理暨管理事項，並追蹤成效；

(b) 應取得經國內官方認可核發、或符合具公信力之國外組織規範之身份辨識技術，以利識別組織或特定標的之身分或來源；

(c) 應決定須納入管理制度適用範圍之重要數位資料；

(d) 應規劃並執行數位資料之生成、保護、維護，以及重要資料之存證資訊取得、維護、驗證所需流程；

(e) 應確保支援適切，使得組織重要數位資料治理暨管理制度有效運作；

(f) 應依據內、外部議題、或利害關係人需求變動，規劃與實行適當之變更措施；

(g) 應對違反重要數位資料治理暨管理制度規定，與協助組織保護重

要數位資料(例如通報違規案例)者，分別訂定懲戒與獎勵規則；

(h) 應建立重要數位資料爭議處理機制，當發現重要數位資料受侵害或有受侵害的疑慮時，組織應蒐集、保全相關證據，並依據相關法令規定採取必要救濟措施；

(i) 應定期或不定期向最高管理階層報告或審查重要數位資料治理暨管理制度之執行績效；

(j) 應定期或不定期進行上述事項之檢討與改善。

6.2 風險與機會因應

規劃組織重要數位資料治理暨管理制度時，應決定須被處理之風險和機會，以預防或減少非預期之影響。

6.3 變更規劃

6.3.1 組織應決定組織重要數位資料治理暨管理制度之變更需求，其變更應以有計畫、有系統之措施進行。

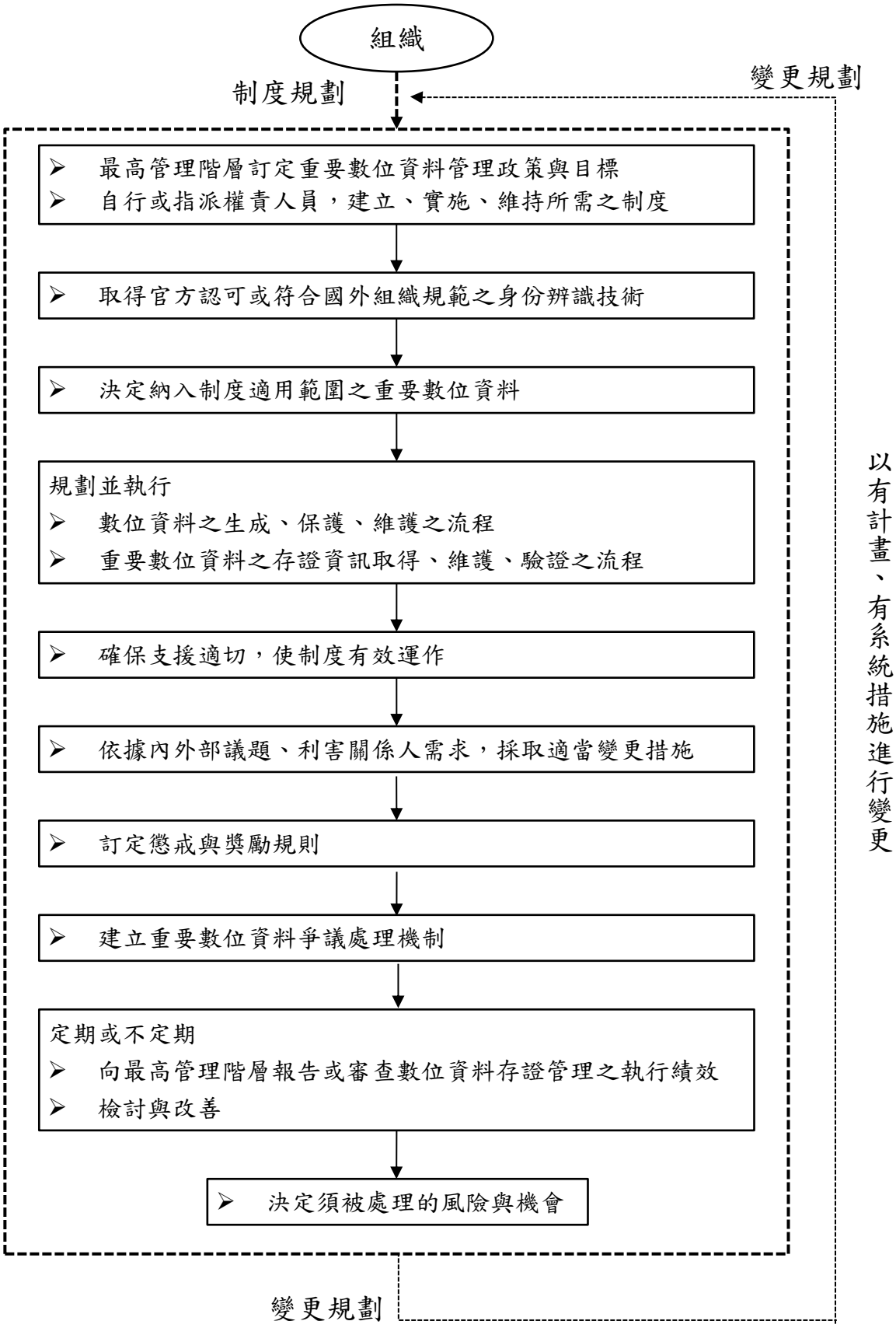
6.3.2 組織應考量：

(a) 變更目的和其潛在影響；

(b) 組織重要數位資料治理暨管理制度之完整性；

(c) 支援適切性(參照 7)；

(d) 職責與權限之分配或重新分配。


組織
制度規劃
變更規劃
最高管理階層訂定重要數位資料管理政策與目標
自行或指派權責人員，建立、實施、維持所需之制度
取得官方認可或符合國外組織規範之身份辨識技術
決定納入制度適用範圍之重要數位資料
規劃並執行
數位資料之生成、保護、維護之流程
重要數位資料之存證資訊取得、維護、驗證之流程
確保支援適切，使制度有效運作
依據內外部議題、利害關係人需求，採取適當變更措施
訂定懲戒與獎勵規則
建立重要數位資料爭議處理機制
定期或不定期
向最高管理階層報告或審查數位資料存證管理之執行績效
檢討與改善
決定須被處理的風險與機會
變更規劃
以有計畫、有系統措施進行變更

圖五：制度規劃

7. 支援

7.1 資源

7.1.1 基本要求

組織應決定及提供所需之資源，以實施和維持組織重要數位資料治理暨管理制度，並持續改善其有效性。

7.1.2 人員

為確保組織可達成重要數位資料治理暨管理目標要求，組織應進行人員管理、選定與教育訓練必要之人員、選用適當之第三方資訊服務提供者，以確保組織重要數位資料治理暨管理制度之有效運作(參照7.2)。

7.1.3 基礎設施與服務

組織應決定、管理、維持及持續改善其重要數位資料治理暨管理流程中所需之設備與系統(參照7.3)。

7.1.4 組織知識

組織應決定與保存組織重要數位資料治理暨管理制度運作所需知識，並在需要時便於取用。

7.2 人員

7.2.1 人員管理

7.2.1.1 保密約定

組織應對人員、離職者、關係企業或第三方約定，明定重要數位資料歸屬與保密要求，並應界定保密範圍、保密義務內容以及保密期間。

7.2.1.2 現職人員

組織對現職人員，須明示有關重要數位資料的相關規定，並針對下列情形分別簽定相關約定：

(a) 就職；

(b) 在職；

(c) 競業禁止。

7.2.1.3 離職者

組織對離職者，應進行下列事項：

(a) 離職面談；

(b) 離職前監控；

(c) 離職後追蹤。

7.2.2 人員能力

7.2.2.1 基本教育訓練及宣導

組織應針對一般人員，自行或委由外部專家團隊，定期或不定期辦理基本教育訓練，其內容應包含：

(a) 國內或國外相關法令、標準、規範或指南之介紹；

(b) 組織制定之重要數位資料治理暨管理政策、目標及制度流程；

(c) 重要數位資料外洩之因應處理程序。

7.2.2.2　進階教育訓練

組織應決定重要數位資料治理暨管理權責人員之必要能力與教育訓練需求，自行或委由外部專家團隊，定期或不定期辦理進階教育訓練，除一般人員適用之基本教育訓練內容之外，應包含：

(a) 數位資料管理及存證相關支援工具操作說明；

(b) 進行有效性評估並保存相關紀錄。

7.2.3 第三方資訊服務提供者之選用

組織應評估第三方資訊服務提供者，符合下列事項；

(a) 取得國內或國外認可之身份辨識技術，以利向組織證明其身分或特定標的來源；

(b) 提供之資訊服務符合國內或國外相關規範；

(c) 持續進行組織內部稽核；

(d) 通過國內官方或國外組織審查或稽核。

7.3 設備或系統環境

7.3.1 資安環境管理

7.3.1.1　區域管制

組織對保管、處理重要數位資料的空間，應進行下列管理：

(a) 明定管制區域，與一般區域明確劃分；

(b) 限制可進入管制區域的人員，並記錄進出人員、時間等事項；

(c) 針對外來人士(包含關係企業或第三方及其人員)出入組織，訂定出入管制程序，避免其任意進出管制區域甚至接觸重要數位資料。

7.3.1.2 監視設備

於管制區域及相關重要設施中裝設監視設備。

7.3.1.3 設備管制

組織應針對含有重要數位資料的紀錄媒體、資訊設備進行攜出入管制，包含以下事項：

(a) 偵測安裝、更改組織資訊設備或紀錄媒體之情形；

(b) 建立資訊設備或紀錄媒體之遺失、防盜管理機制；

(c) 針對重要設施、含有重要數位資料資訊設備、紀錄媒體之維護，記錄更改資訊及權責人員；

(d) 建立資訊設備、紀錄媒體的遠端使用管理機制。

7.3.1.4 網路相關管制

組織應針對電腦、組織作業系統、電子信箱及安裝的軟體進行管理，並設立相關隔絕機制以維護內部網路及資訊設備的安全。

7.3.2 產製資料系統管理

7.3.2.1組織應確保產製數位資料之相關系統，符合下列事項：

(a) 具國內或國際認可之時間校正機制；

(b) 依身份辨識技術進行文件存取之權限控管機制；

(c) 具定期與不定期安全性更新機制；

(d) 具編輯紀錄或版本管理機制。

7.3.3 存放資料系統管理

7.3.3.1 組織應確保存放數位資料之相關系統，符合下列事項：

(a) 具檔案存放安控機制；

(b) 具本地備份或異地備援機制，且備份或備援資料應視同原本進行管理，必要時，得運用相關技術確保備份或備援資料的不可竄改性與真實性。

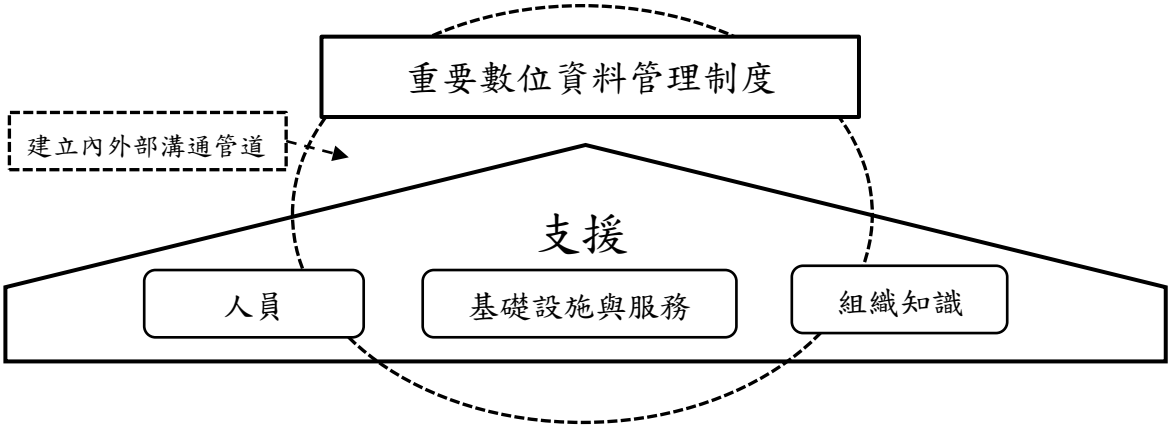
(c) 必要時，應確保存放環境符合國內或國外技術標準要求。

7.3.4 資料系統更新管理

7.3.4.1 組織應自行或委由外部專家團隊，因應數位資料相關環境安全變動，調整工具設備與技術選項。

7.4 溝通管道

7.4.1 組織應建立重要數位資料治理暨管理制度之內、外部溝通管道，並留存溝通資訊紀錄。



人員	人員管理	➢保密約定 ➢現職人員：就職、在職、競業禁止 ➢離職者：面談、監控、追蹤
	人員能力	➢基本教育訓練及宣導：一般人員 ➢進階教育訓練：權責人員
	第三方 資訊服務提供者	➢取得國內或國外認可之身份辨識技術 ➢提供之服務符合國內外規範 ➢持續內部稽核 ➢通過官方或國外組織的審查或稽核
基礎設施 與服務	資安環境管理	➢區域管制 ➢監視設備 ➢設備管制 ➢網路相關管制
	產製資料系統管理	➢具時間校正機制 ➢具權限控管機制 ➢具安全性更新機制 ➢具編輯紀錄或版本管理機制
	存放資料系統管理	➢具檔案存放安控機制 ➢具備份備援機制 ➢必要時需符合國內或國外標準
	資料系統更新管理	因應環境變動，調整工具設備與技術
組織知識		決定與保存制度運作所需知識，並適時取用

圖六：支援

8. 重要數位資料治理暨管理制度實踐流程

8.1 數位資料之生成、保護、與維護

8.1.1 數位資料生成或更新時，組織應確保適當的：

(a) 文件描述；

(b) 權屬確認；

(c) 生成通報及登錄；

(d) 審查和核准，並建立數位資料管理清單。

8.1.2 組織應確保數位資料有受到必要的保存與保護：

(a) 自行管理、提供合作對象、接收合作對象或其他涉及法律效力之重要數位資料，應進行識別與來源區分；

(b) 予以分級和標示，並建立重要數位資料管理清單；

(c) 依據分級設定不同使用權限，實施相應程度的保密措施，至少達到基本效力之維持；

(d) 組織應就存有數位資料的資訊設備、系統等儲存空間，設定所須的帳號與密碼，並定期變更密碼；

(e) 有定期或不定期留存修改版本及最終版本；

(f) 使用紀錄及預警；

(g) 廣宣管制。

8.1.3 組織應確保數位資料有進行維護：

(a) 組織應定期盤點分類數位資料，並定期更新且維持其紀錄；

(b) 組織應定期評估數位資料保存期限；

(c) 組織應訂定銷毀流程，並將相關作業紀錄留存。

8.1.4 組織與關係企業或第三方共有，或向其提供重要數位資料時，應確保符合下列事項：

(a) 依照本規範要求相關對象；

(b) 應明定重要數位資料使用範圍或方式；

(c) 應明定返還或銷毀事由、執行與通報流程，並留存相關作業紀錄。

8.2 數位資料存證資訊之取得、維護、驗證

8.2.1 數位資料存證資訊，應至少包含下列事項：

(a) 數位資料最終版本；

(b) 連結前述(a)之必要後設資料；

(c) 連結前述(a)之雜湊值；

(d) 連結前述(a)之時戳；

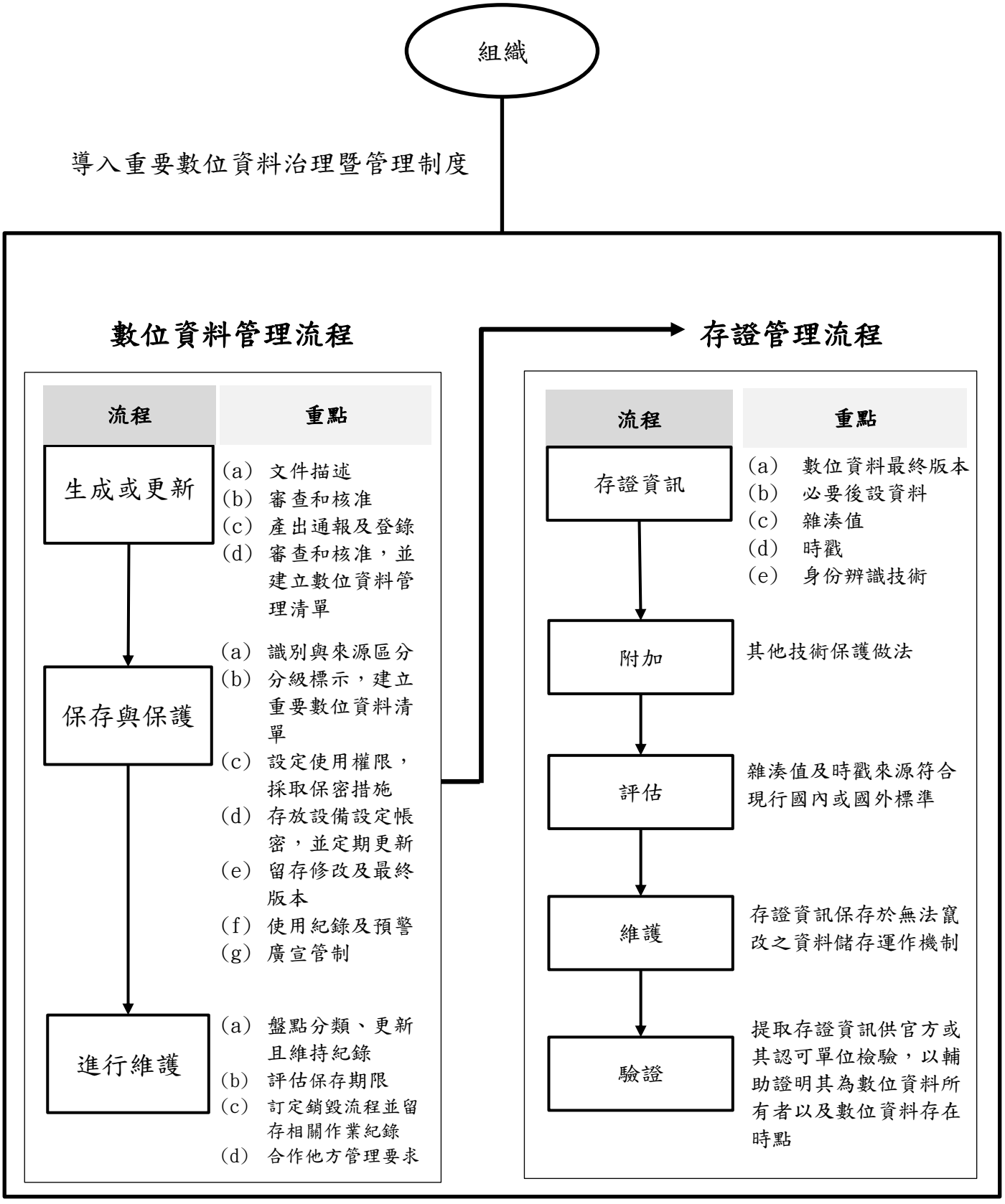
(e) 連結前述(a)之身份辨識技術。

8.2.2 組織宜視需求，於數位資料原本附加其他技術保護做法。

8.2.3 組織應評估存證資訊之雜湊值及時戳來源，符合現行國內或國外標準。

8.2.4 組織應評估存證資訊之維護，保存於無法竄改之資料儲存運作機制。

8.2.5 組織應視驗證需求，提取數位資料存證資訊供官方或其認可單位檢驗，以輔助證明其為數位資料所有者以及數位資料存在時點。



圖七：組織重要數位資料治理暨管理制度流程圖

9. 績效評估

9.1 基本要求

組織應定期檢驗組織重要數位資料治理暨管理制度之執行現況，規劃及實施所需之資料分析、內部稽核及管理審查，必要時得經由第三方驗證稽核，以確保組織重要數位資料治理暨管理制度的運作符合組織預期結果。

9.2 資料分析

組織應決定、蒐集並分析組織重要數位資料治理暨管理制度運作所生成之相關資料，以了解組織重要數位資料治理暨管理制度之適用性、有效性，並藉以評估可持續改善之處。

9.3 內部稽核

組織應在所規劃之期間執行內部稽核，以了解組織重要數位資料治理暨管理制度是否符合下列各項要求：

(a) 符合國內或國外相關法令、規範、標準或指南之要求；

(b) 符合組織所設定之重要數位資料治理暨管理政策與目標；

(c) 有效的實施及維持。

9.4 管理審查

最高管理階層應定期審查組織重要數位資料治理暨管理制度，以確保其持續合適、完備、有效（參照 5）。管理審查應被規劃和執行，並考

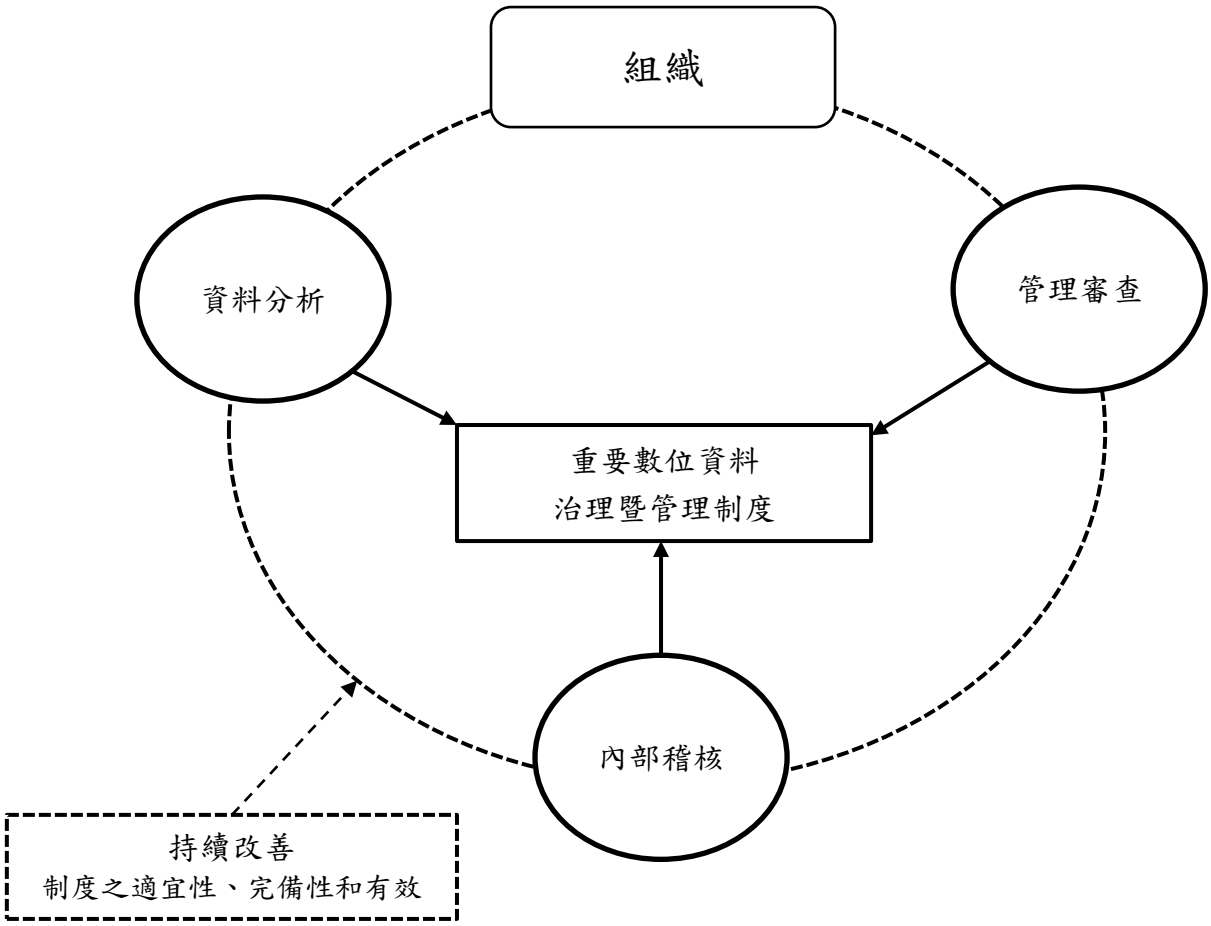
慮：

(a) 管理制度之規劃變更，包括重要數位資料治理暨管理政策與目標設定、內外部議題變化等；

(b) 管理制度之執行結果，包括組織擁有重要數位資料管理狀態、內部稽核結果、重大矯正措施執行情況等；

10. 改善

組織應藉由適當工具和方法(參照 9)，確認組織重要數位資料治理暨管理制度是否有任何績效不佳而應被持續改善部分，採取必要矯正措施，以持續改善組織重要數位資料治理暨管理制度之適宜性、完備性和有效性。



圖八：績效評估與改善