ISO 27701:2025
改版簡介

講師：杜貴忠

本PPT由資安資訊製作

01 改版差異

02 新版條文簡介

03 實務做法

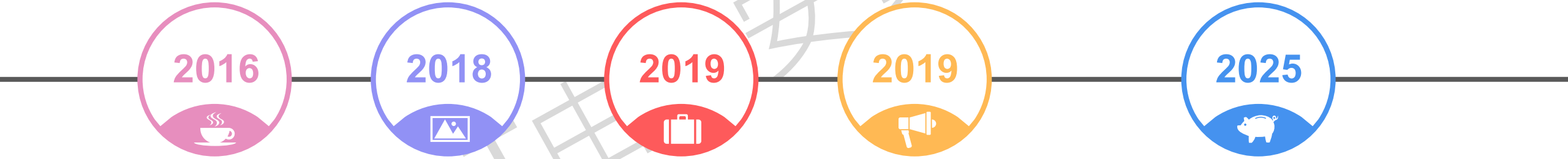
04 結論

本PPT由咨安資訊製作

改版差異

本PPT由台安資訊製作

沿革



2016
JTC 1/SC 27/WG 5 ISO/IEC 27552

2018
GDPR

2019
ISO/IEC 27552 FDIS

2019
ISO/IEC 27552 Management System "type A ISO/IEC 27701:2019

2025
ISO/IEC 27701:2025

本PPT由安資訊製作

改版要素

獨立標準
法規遵循
整合資安
建立問責
夥伴互信

電資安資訊製作

獨立標準

2019

- 必須先建置ISO 27001資訊安全管理系統（ISMS）
- PIMS（隱私資訊管理系統）的範圍必須與ISMS範圍相同或在其內
- 必須先通過ISO 27001認證才能申請ISO 27701認證

2025

- 獨立實施PIMS，無需先建置完整的ISMS
- 降低中小企業採用的門檻和成本
- 簡化資料隱私認證的流程
- 各種規模的企業都能取得資料隱私認證

本PPT由AI製作

名稱

ISO 27701:2019

"Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines"
（安全技術 — ISO/IEC 27001 和 ISO/IEC 27002 的隱私資訊管理延伸 — 要求與指引）

ISO 27701:2025

"Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance"
（資訊安全、網路安全與隱私保護 — 隱私資訊管理系統 — 要求與指引）

本PPT由資訊製作

架構

ISO 27701:2019

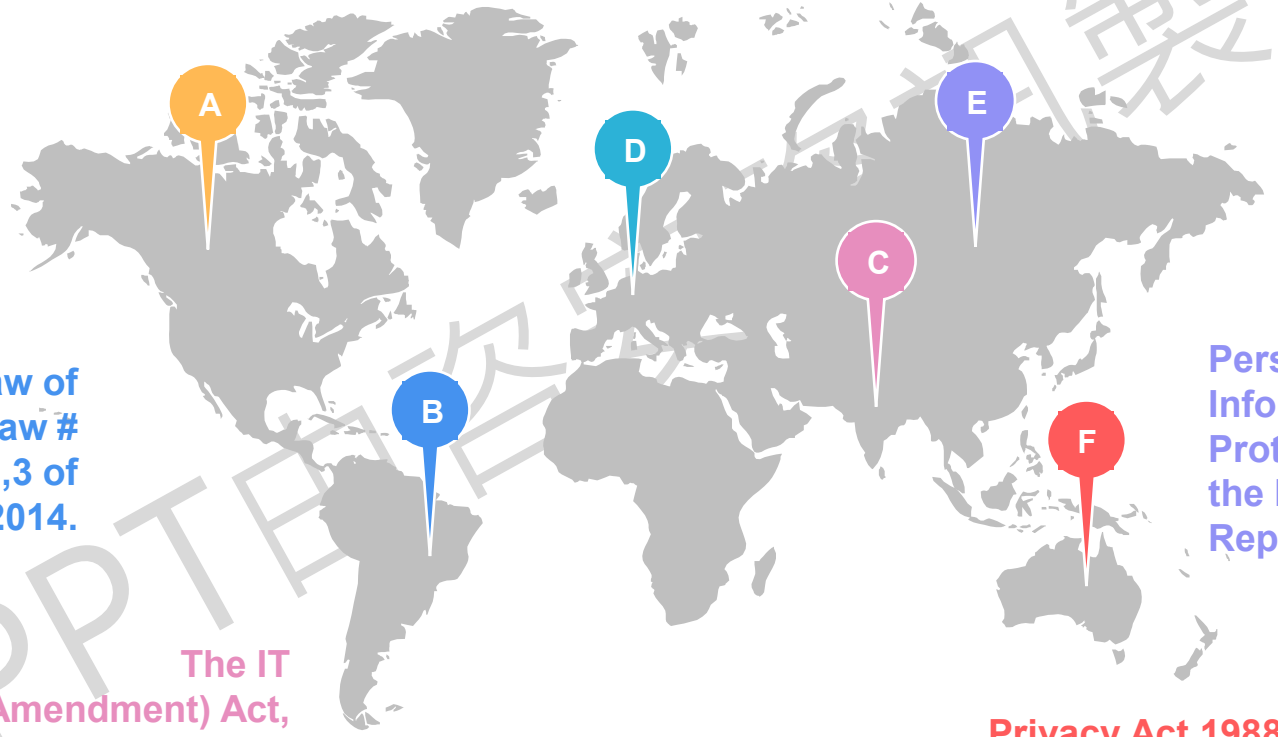
第5章延伸ISO27001要求(PIMS)
第6章延伸ISO27002要求實施指引
第7章控制者控制措施實施指引
第8章處理者者控制措施實施指引

ISO 27701:2025

採用 ISO 制定的高階結構（High Level Structure），提高與其他ISO 管理系統標準的一致性
新版結構（第4至10章）
附錄A：控制措施(控制者、處理者及資訊安全)
附錄B：控制措施實施指引

本PPT由資訊製作

法規遵循



Gramm-Leach-Bliley Act (GLBA) The Fair Credit Reporting Act (FCRA)…

Brazil's Civil Law of the Internet, Law # 12.695, of April 2,3 of 2014.

The IT (Amendment) Act, 2008 (ITAA 2008):

EU General Data Protection Regulation (GDPR)

Personal Information Protection Law of the People's Republic of China

Privacy Act 1988, Act No. 119 of 1988 (13)

本PPT由资产行动制作

ISO/IEC JTC 1/SC 27/WG 5
SC 27 committee document 502
Privacy References List

法規

ISO 27701:2019

主要參考 GDPR

ISO 27701:2025

因應全球隱私法律的多元化，提供適切的管理框架，組織根據其運營所在的司法管轄區訂定合宜之管理系統。

本PPT由[illegible]資訊製作

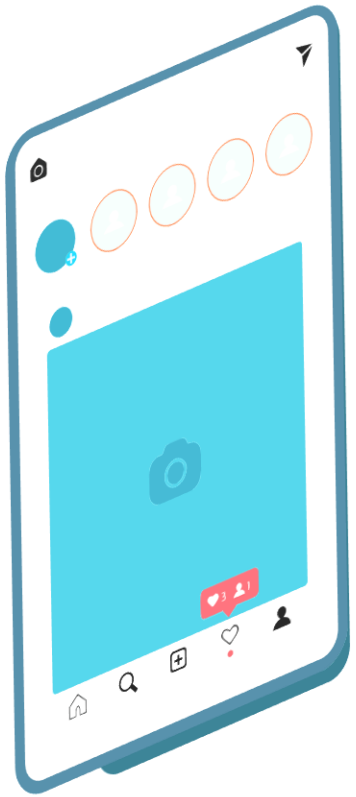
整合資安

以獨立標準的精神，從風險評估及處理過程中識別紀錄所需之資訊安全控制措施，發展資訊安全計畫管理資訊安全作業整合隱私權管理。

資訊安全計畫要素(15項)包含ISO27001及ISO27002

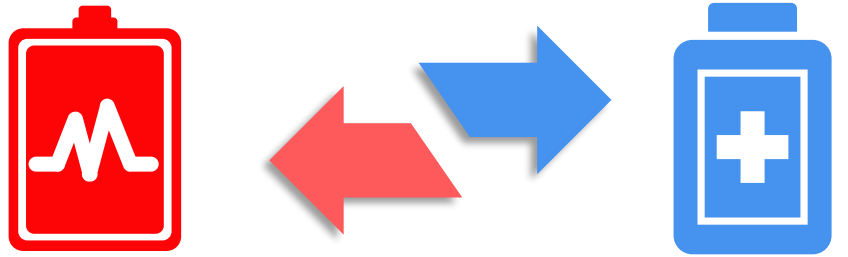
資訊安全控制措施：附錄A.3計有29項適用於PII控制者和PII 處理者的資訊安全控制措施。

本標準使組織能夠將其隱私資訊管理系統 (PIMS) 與其他管理系統標準的要求（特別是 ISO/IEC 27001 中規定的資訊安全管理系統）相協調或整合。



27701:2019

27701:2025



本PPT僅供資安資訊製作

資訊安全計畫

ISO 27701:2019

無

ISO 27701:2025

6.1.3 C)
資訊安全風險管理；資訊安全政策；資訊安全組織；人力資源安全；資產管理；存取控制；營運安全；網路安全管理；開發安全；供應商管理；事件管理；資訊安全連續性；資訊安全審查；密碼學；實體和環境安全

本PPT由資訊製作

資訊安全控制措施

ISO 27701:2019

延伸ISO / IEC 27002:2013控制措施
14個領域中13個延伸控制做法

ISO 27701:2025

表 A.3 安全控制措施
- 資訊安全政策
- 資訊安全角色與責任
- 資訊分類與標記
- 身分管理與存取權限
- 供應商管理
- 資訊安全事件管理
- 法律法規遵循
- 加密技術使用
- 安全開發生命週期等 29項

整合ISO27002:2022控制措施

本PPT由資訊製作

建立問責

獨立標準促進問責和基於證據的隱私資訊管理機制，藉由主條文4-10章建立管理制度，以PDCA循環達成持續改善之目標。
透過遵守本標準中的要求，組織將產生其如何處理 PII 的證據，此類證據可用於促進與業務合作夥伴達成 PII 處理相關的協議，並有助於與其他相關方建立關係，可以為此類證據提供獨立驗證。

本PPT由資安資訊製作

問責及基於證據(主條文一)

章節	ISO 27701:2019	ISO 27701:2025
4 全景	範圍是ISMS的延伸	獨立定義範圍，將 PII 主體識別為 利害關係人
5 領導	領導力繼承自ISMS	獨立隱私政策及治理，確保承諾
6 規劃	風險評估是ISMS的延伸	進行獨立的隱私風險評估，整合資訊安全設定隱私目標
7 支援	與ISMS共享支援	為 PIMS 分配專門的資源、能力和文件化資訊

問責及基於證據(主條文二)

章節	ISO 27701:2019	ISO 27701:2025
8 運作	運作控制是現有ISMS流程的延伸	規劃和控制 PIMS 特定的運作流程和風險處理
9 績效評估	績效評估整合到 ISMS 的審查週期中	進行專門的 PIMS 內部稽核和管理審查
10 改善	改善藉由ISMS的流程執行	管理 PIMS 不符合事項並實施矯正措施以持續改進

夥伴互信

與合作夥伴、客戶和監管機構建立信任機制，達成整體隱私安全的整體管理及互信，專注於資料隱私保護而無需完整的資訊安全框架，提供國際通用的隱私管理框架， 適用於各國資料保護法規的遵循，協助跨國組織建立一致的隱私保護標準

本PPT由各大資訊製作

夥伴互信(PII 控制者的控制措施及指引)31 項

領域	ISO 27701:2019	ISO 27701:2025
蒐集及處理條件	附錄A.7.2(7.2)	附表A.1.2(附錄B.1.2)
對PII當事人之義務	附錄A.7.3(7.3)	附表A.1.3(附錄B.1.3)
於設計即保護隱私及預設保護隱私	附錄A.7.4(7.4)	附表A.1.4(附錄B.1.4)
PII共享、揭露及傳輸	附錄A.7.5(7.5)	附表A.1.5(附錄B.1.5)

夥伴互信(PII 處理者的控制措施及指引)18項

領域	ISO 27701:2019	ISO 27701:2025
蒐集及處理條件	附錄B.8.2(8.2)	附表A.2.2(附錄B.2.2)
遵守PII當事人之義務	附錄B.8.3(8.3)	附表A.2.3(附錄B.2.3)
於設計即保護隱私及預設保護隱私	附錄A.8.4(8.4)	附表A.2.4(附錄B.2.4)
PII共享、揭露及傳輸	附錄A.8.5(8.5)	附表A.2.5(附錄B.2.5)

夥伴互信(PII 控制者及處理者控制措施及指引)29項

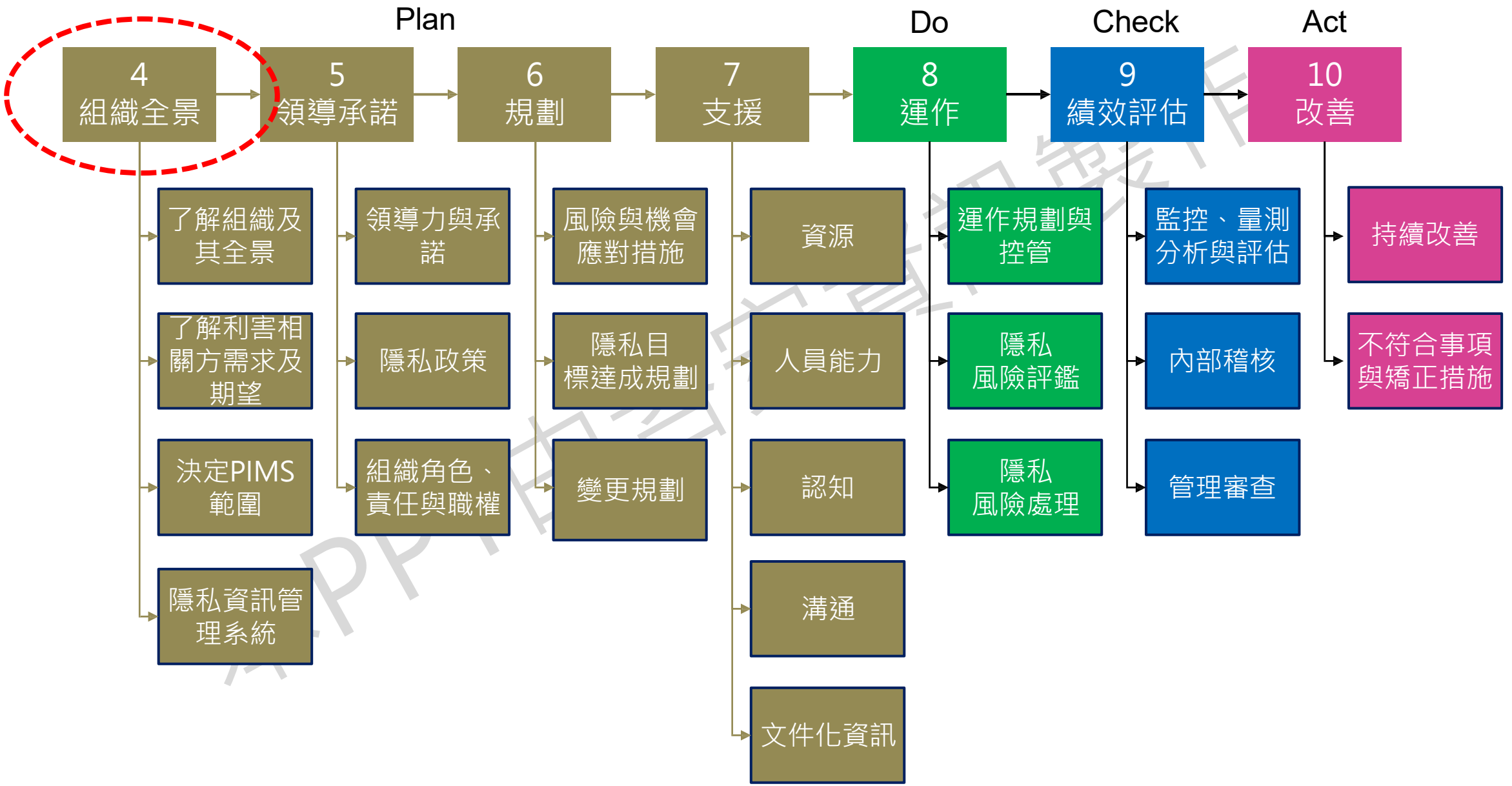
說明	ISO 27701:2019	ISO 27701:2025
確認處理過程中的安全性	第六章(ISO 27002:2013延伸)	附表A.3表 列出了針對 PII 控制者和 PII 處理者的非僅有資訊安全之控制措施。

本PPT由台

新版條文簡介

本PPT由台灣資安資訊製作

ISO 27701：2025 主條文架構



第4章 全景分析

4.1了解組織及其全景-差異：

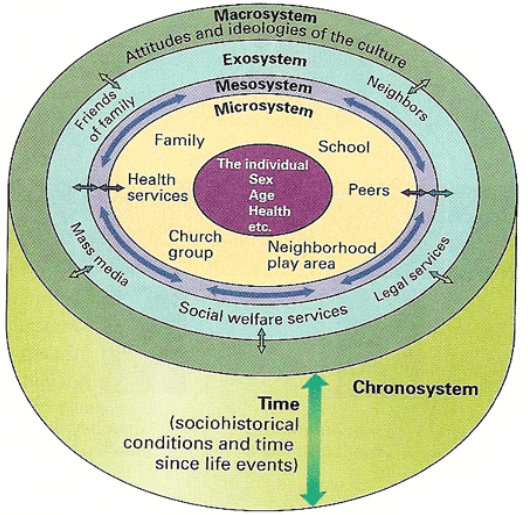
組織應確定其是否為 PII 控制者（包括聯合 PII 控制者）或 PII 處理者。

當組織同時扮演兩種角色（即 PII 控制者和 PII 處理者）時，應確定單獨的角色，每個角色都是一組單獨控制措施。

備註：組織在處理 PII 的每個實例中扮演的角色可能不同，因為這取決於誰決定處理的目的和方法。

■外部和內部問題包括但不限於：

- ➢適用的隱私權立法
- ➢適用的法規
- ➢適用的司法判決
- ➢適用的組織背景、治理、政策和程序
- ➢適用的行政決定
- ➢適用的合約要求



Bronfenbrenner's Ecological Model describing the environmental influences

本PPT由咨安

第4章 全景分析

4.2了解利害相關方需求及期望-差異：

組織應將那些與 PII 處理相關的利害關係人納入其利害關係人之列，其中包括 PII 當事人。

根據組織的角色，「客戶」可以理解為：

a) 與 PII 控制者簽訂合約的組織（例如，PII 控制者的客戶）；註 3：可以是作為聯合 PII 控制者的組織。

b) 與 PII 處理者簽訂合約的 PII 控制者（例如，PII 處理者的客戶）；

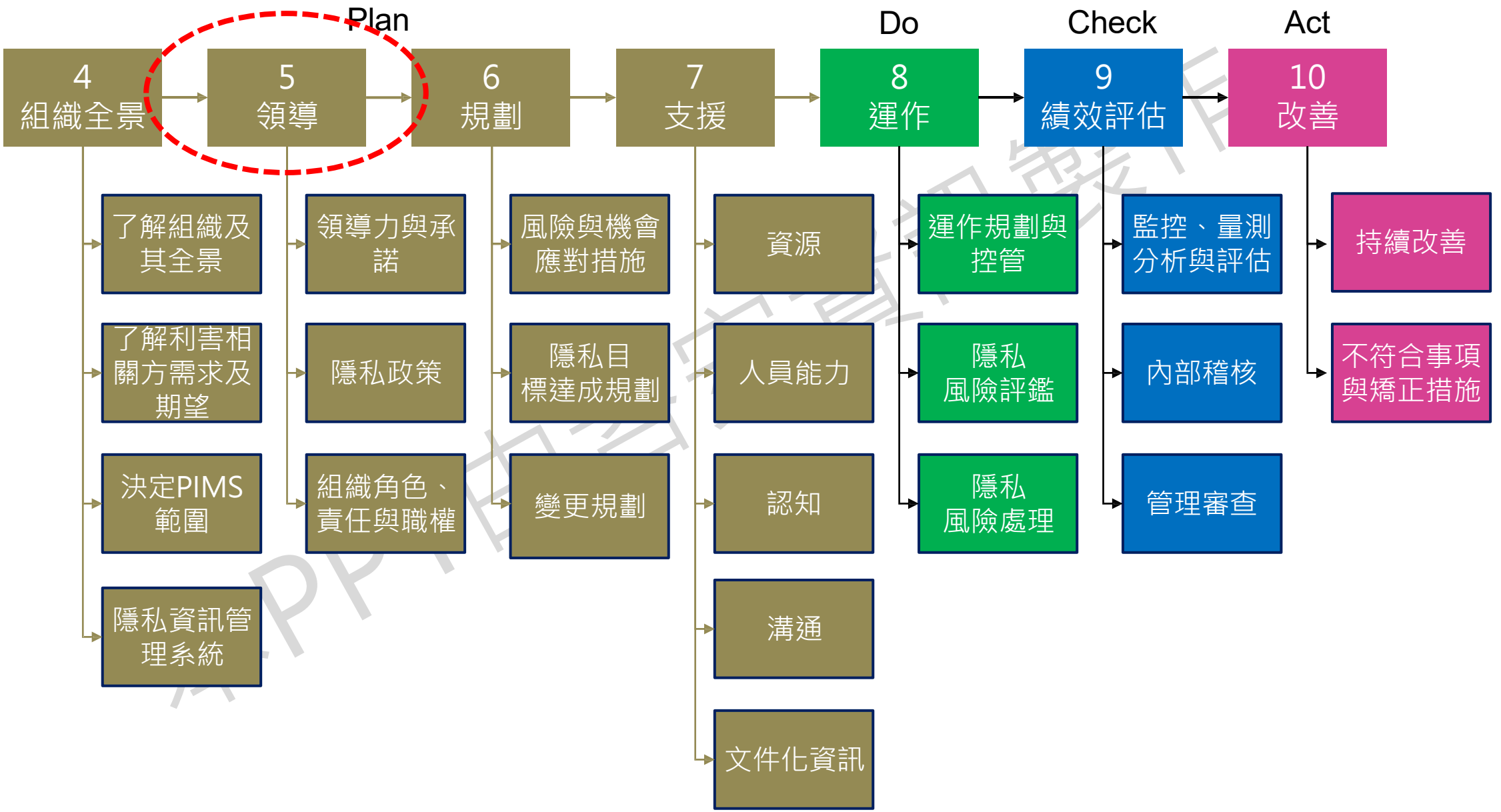
c) 與 PII 處理分包商簽訂合約的 PII 處理者（例如，分包 PII 處理者的客戶）。

備註：

2)其他相關方可以包括客戶、監管機構、其他 PII 控制者、PII 處理者及其分包商。

4)與 PII 處理相關的要求可以由法律法規要求、合約義務以及組織本身設定的目標決定。 ISO/IEC 29100 中規定的隱私原則提供了有關 PII 處理的指導。

ISO 27701：2025 主條文架構



第5章 領導

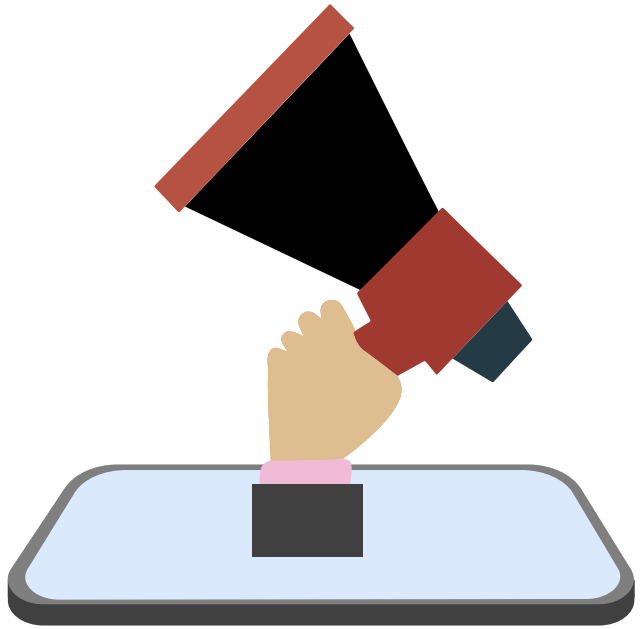
5.1 領導及承諾

5.2 隱私政策

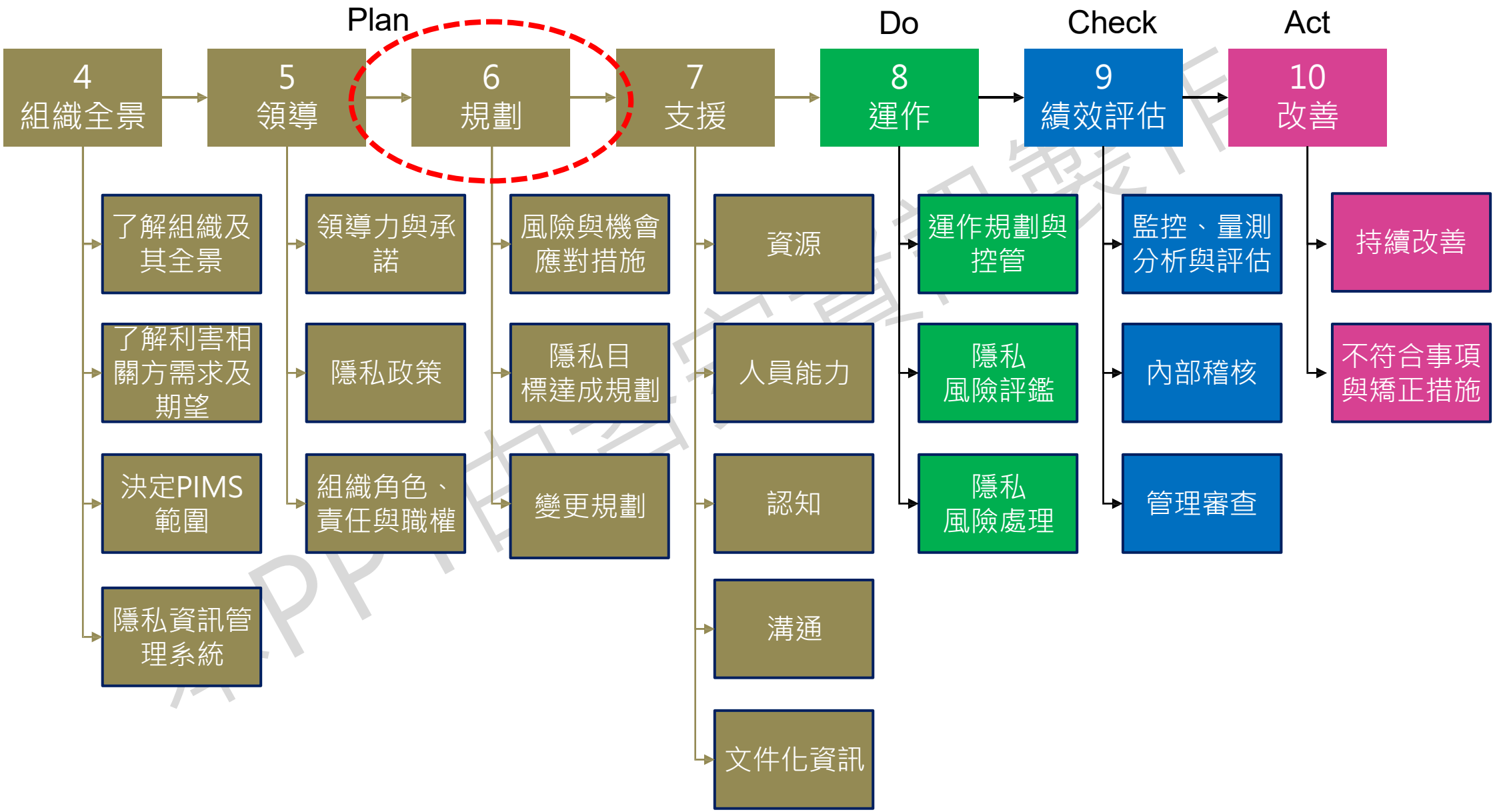
5.3 組織角色、責任及權責

無差異

本PPT由咨安資訊製作



ISO 27701：2025 主條文架構



第6章 規劃

6.1風險與機會應對措施-差異

6.1.2 c) 辨識下列隱私風險：

1) 與隱私資訊管理系統範圍內的隱私保護和資訊安全風險相關的隱私風險；以及

d) 分析隱私風險：1) 評估如果 c) 1) 中確定的風險成為現實，可能對組織和 PII 當事人造成的後果；

備註：有關隱私風險評估流程的更多資訊，請參閱 ISO/IEC 27557。

6.1.3 組織應定義並應用隱私風險處理流程，以處理與 PII 處理相關的風險，包括 PII 當事人風險以及 PII 安全風險，具體方式如下：

c) 辨識並記錄組織實施的資訊安全計畫，包括適當的安全控制措施；資訊安全計畫至少應涵蓋以下內容：

備註5：在考慮 PII 處理的安全性時，組織可以以綜合的方式解決資訊安全和隱私問題，例如結合資訊安全和隱私風險評估，或作為具有重疊領域的獨立實體。

第6章 規劃

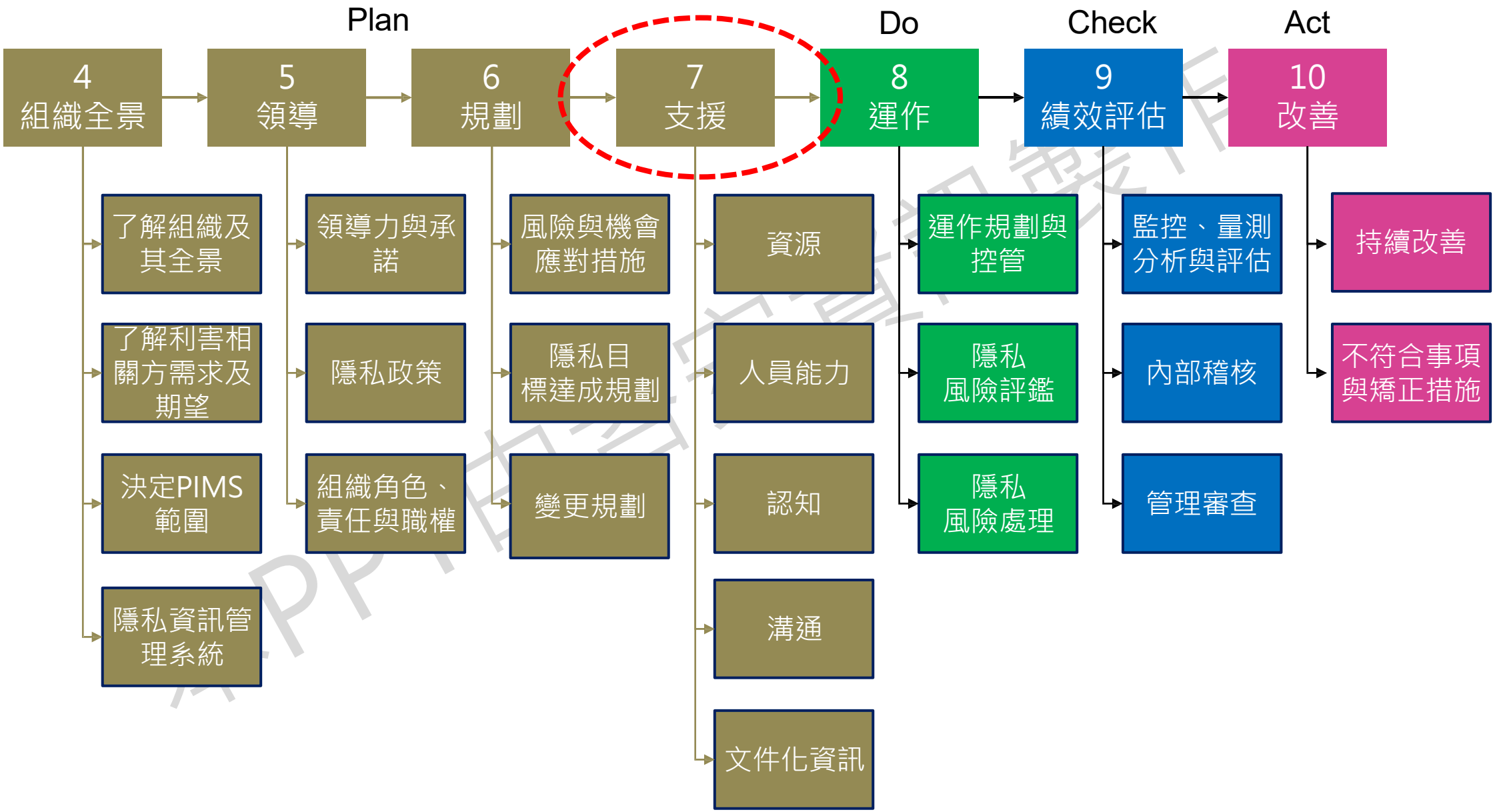
評估項目(構面)	嚴重性衝擊等級表(I)		
	輕微(1)	嚴重(2)	非常嚴重(3)
可識別性	個人資料查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	僅可以間接識別特定當事人者(需要與其他資料進行對照、組合、連結等，始能識別該特定的個人)	可以直接識別特定當事人者(不需要與其他資料進行對照、組合、連結等，就能識別該特定的個人)
個資數量	一般個資1000筆以下 特種個資10筆以下	一般個資1001~10,000筆 特種個資101~1,000筆	一般個資10,001筆以上 特種個資1,001筆以上
敏感程度(符合個資法)	僅有識別資料 (未含其他個人活動、兒童資料、財務金融或特種個人資料)	除識別資料外，還含有個人活動資料、財務金融資料、兒童資料	含有特種個人資料 (病歷、醫療、基因、性生活、健康檢查、犯罪前科)
蒐集處理利用	無外部利用情形	無償委任關係外部蒐集處理利用(例：公務部門)	有償委任關係外部蒐集處理利用(例：廠商)
當事人衝擊程度	對當事人權利(或身心、物質)影響輕微	影響當事人權利運作，或經醫師鑑定已對當事人身心(或物質)造成輕度影響	嚴重影響當事人權利運作，或經醫師鑑定，已對當事人身心(或物質)造成中度(含)以上影響
組織衝擊程度	對組織影響輕微(無造成物質、聲譽損失)	影響組織運作、或聲譽(或20萬元內損失)	嚴重影響組織營運、聲譽(或20萬元以上損失)

6.2 隱私目標達成規劃施

6.3 變更規劃

無差異

ISO 27701：2025 主條文架構



第7章 支援

7.1 資源

7.2 人員能力

7.3 認知

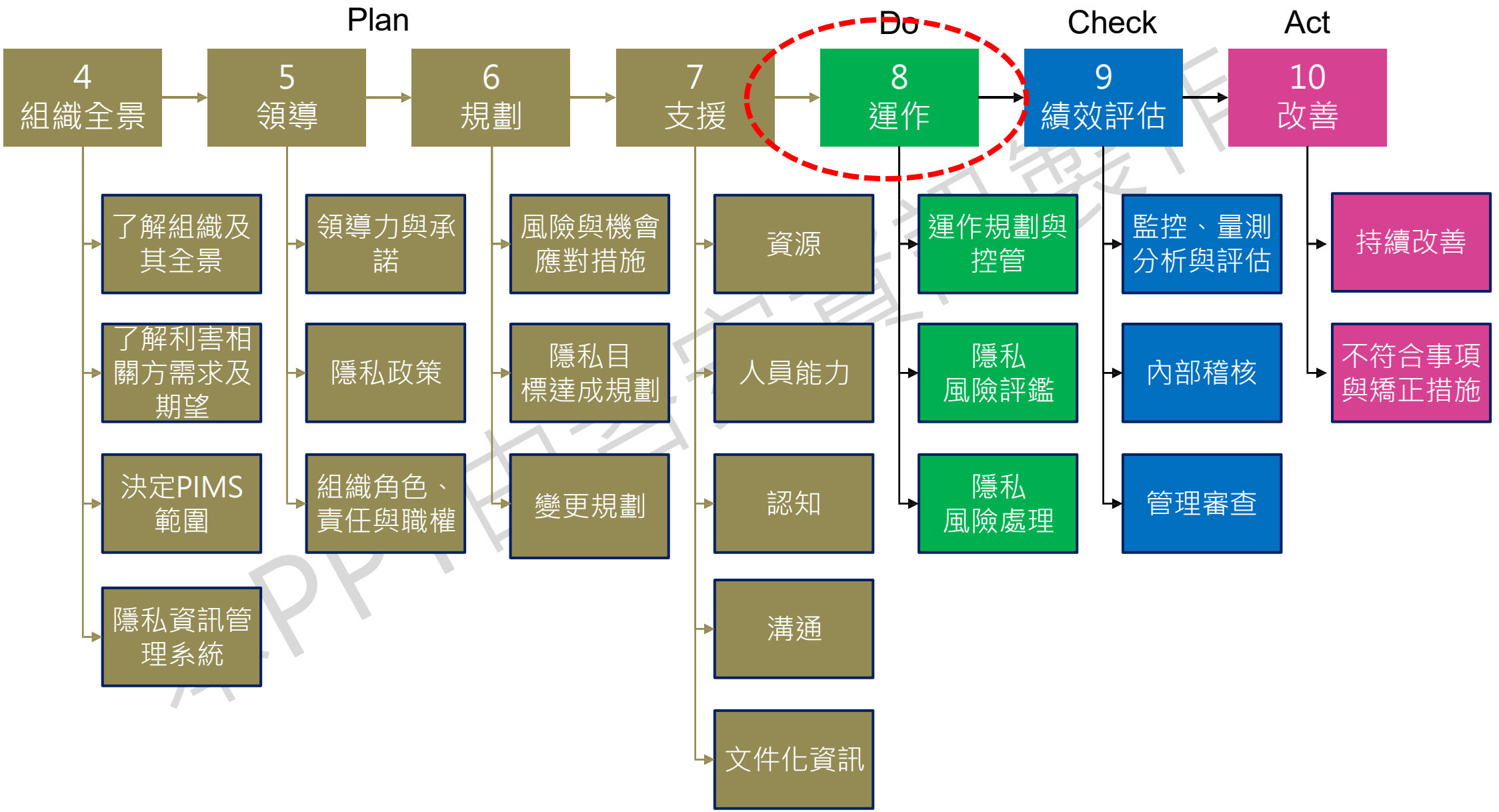
7.4 溝通

7.5 文件化資訊

無差異

本PPT由管家製作

ISO 27701：2025 主條文架構



第8章 運作

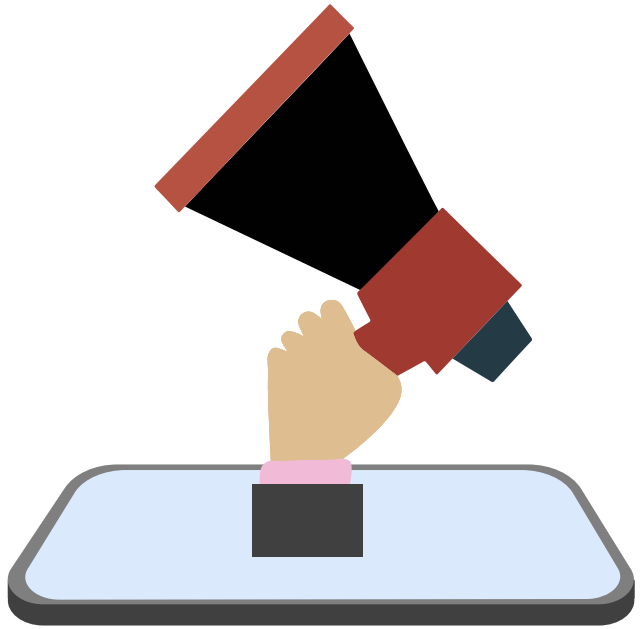
8.1 運作及規劃

8.2 隱私風險評鑑

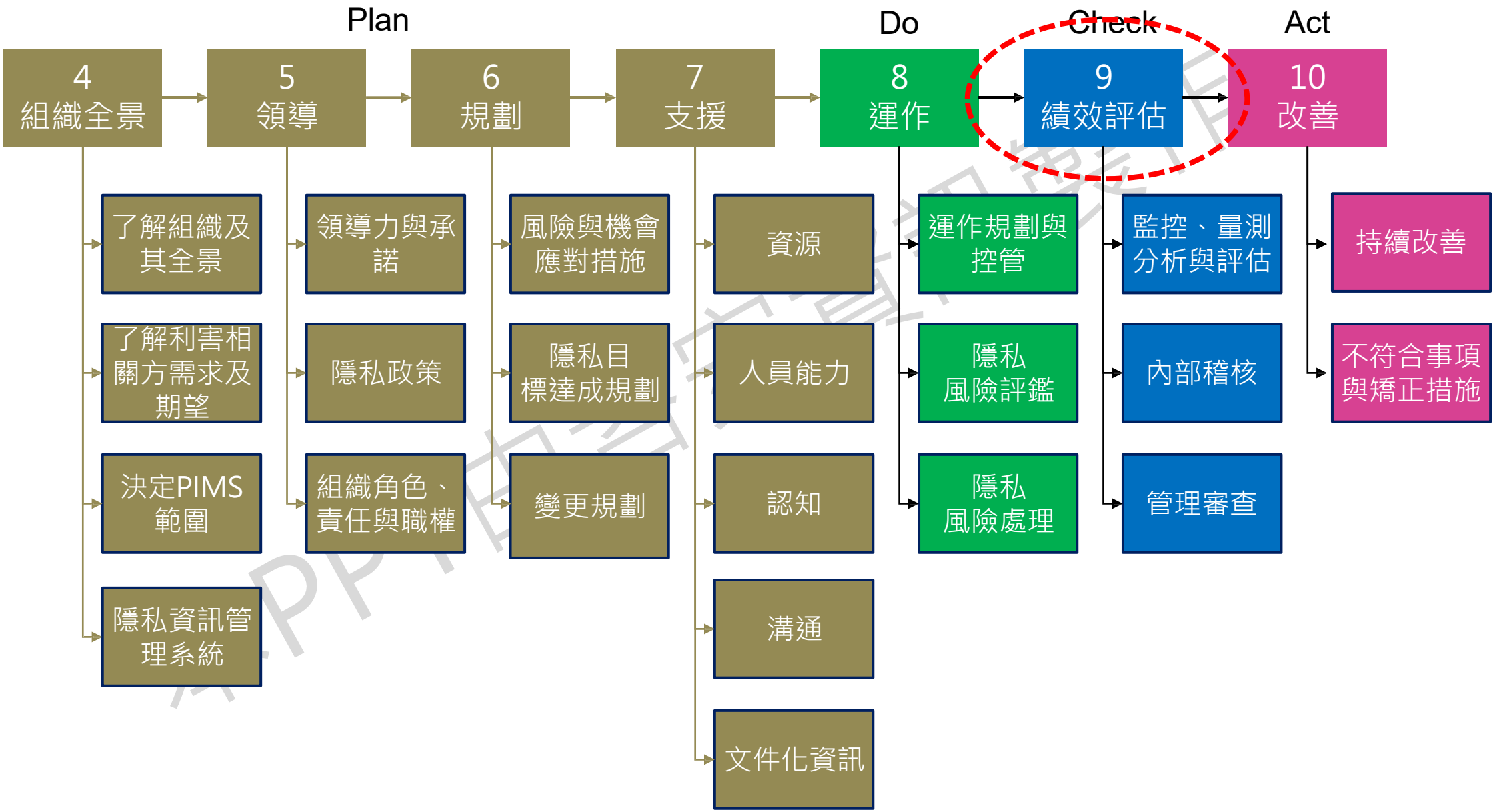
8.3 隱私風險處理

無差異

本PPT由咨安資訊製作



ISO 27701：2025 主條文架構



第9章 績效評估

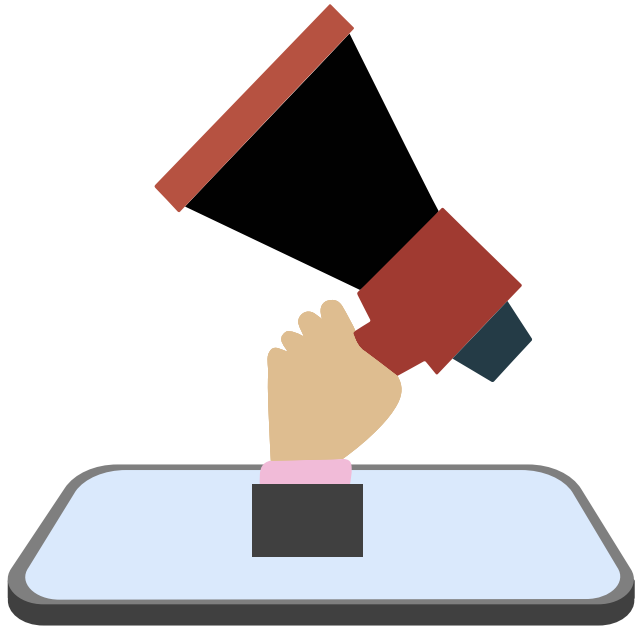
9.1 監控、量測 分析與評估

9.2 內部稽核

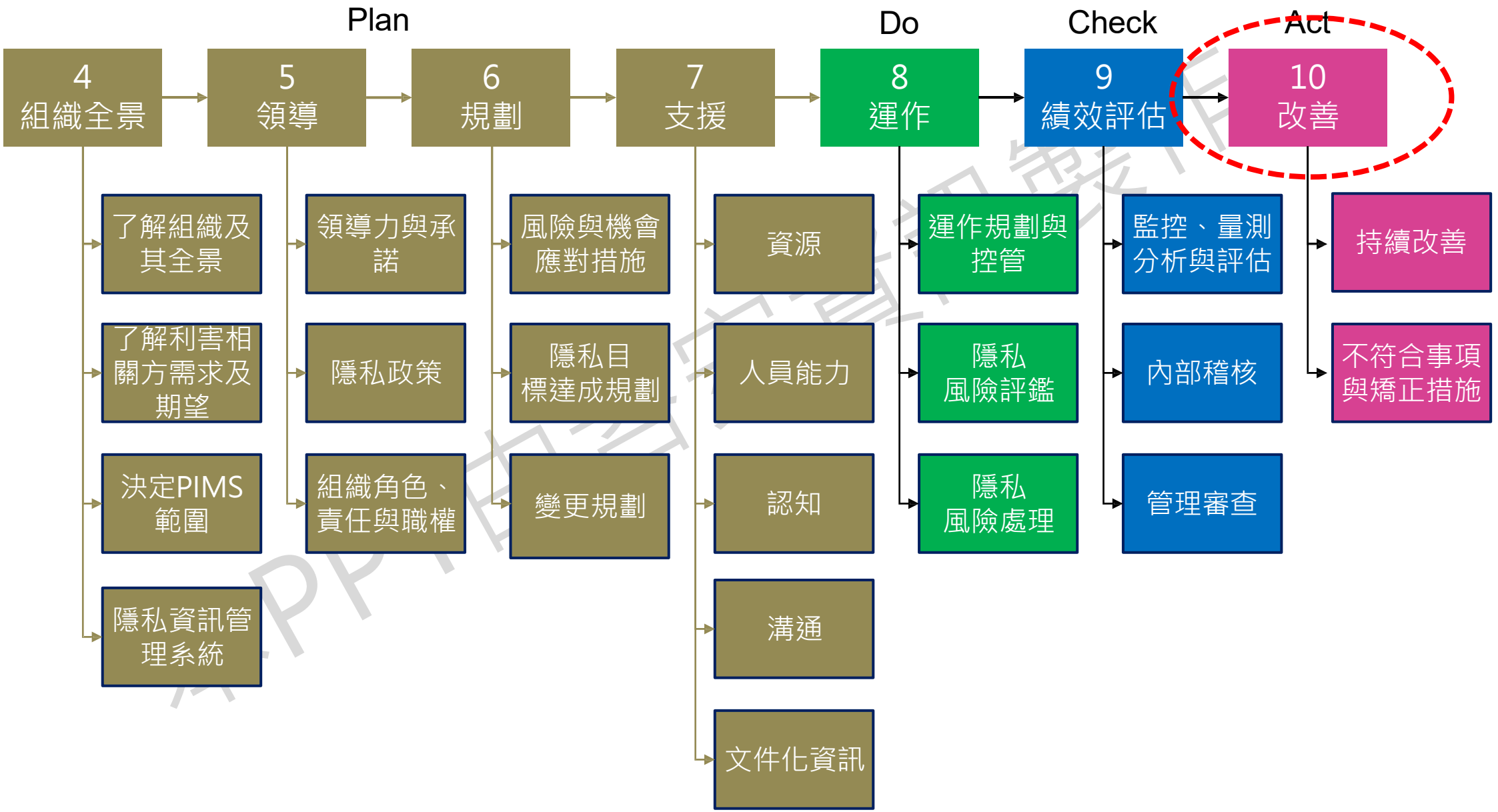
9.3 管理審查

無差異

本PPT由咨安資訊製作



ISO 27701：2025 主條文架構



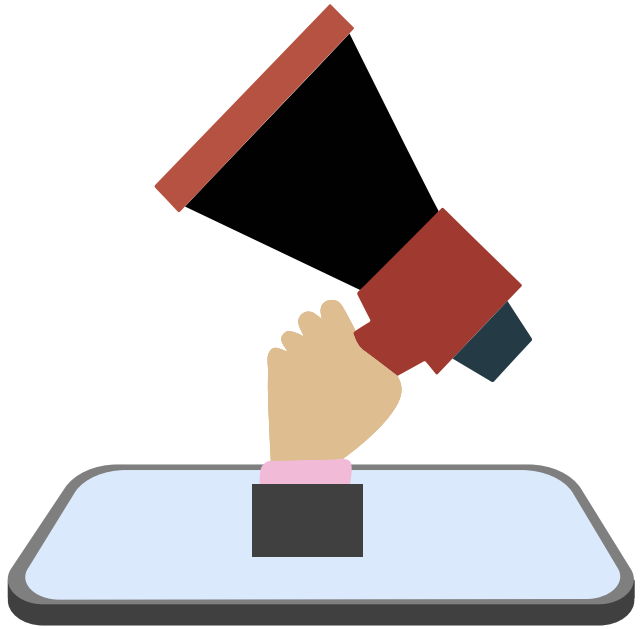
第10章 改善

10.1 持續改善

10.2 不符合事項 與矯正措施

無差異

本PPT由咨安資訊製作



附錄

A PIMS 參考控制目標以及 PII 控制者和 PII 處理者的控制措施

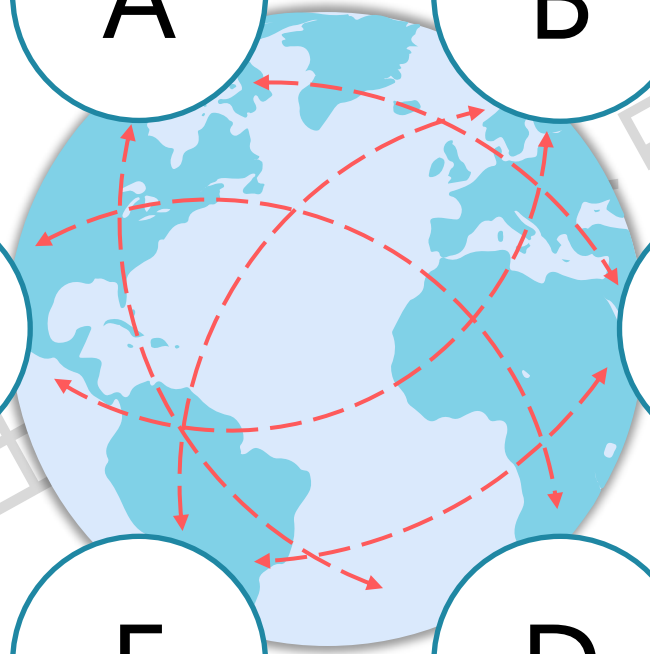
B PII 控制者和 PII 處理者的實施指南

C ISO/IEC 29100對照

D GDPR 對照

E ISO/IEC 27018、ISO/IEC 29151對照

F ISO/IEC 27701:2019 的對應關係



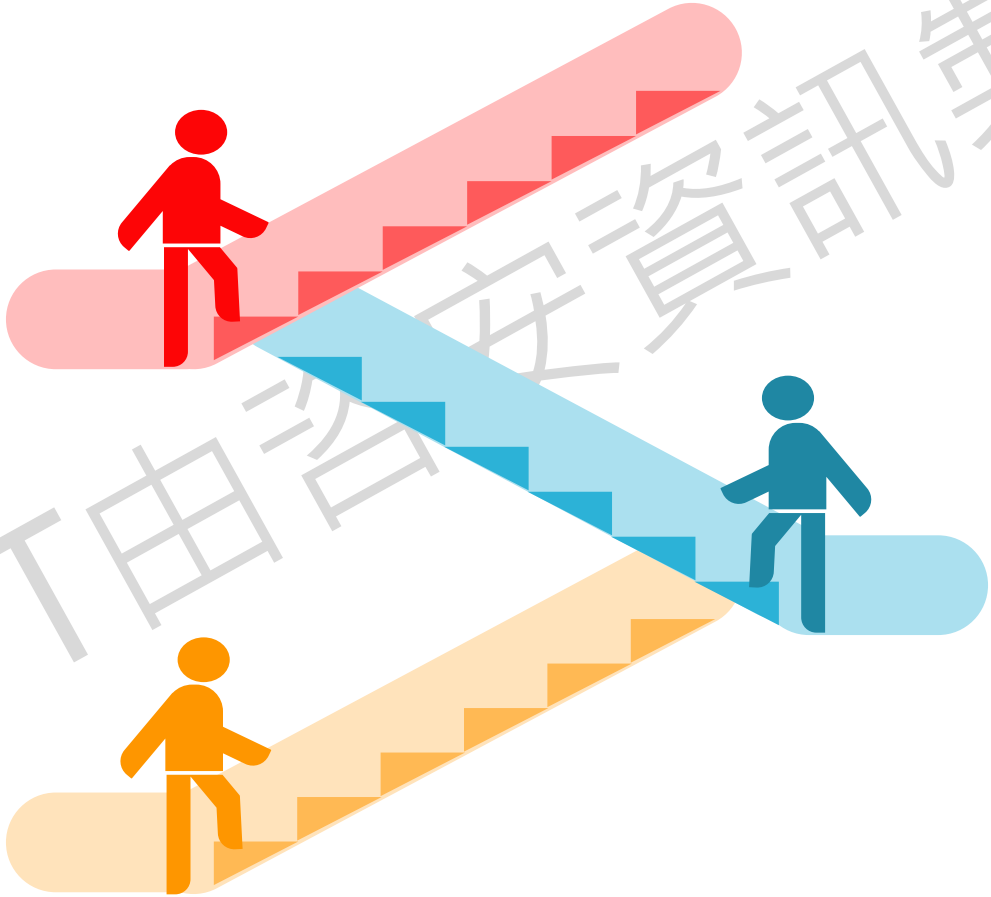
本PPT由資訊製作

實務做法

本PPT由安資部製作

組織現況

27001(已導入)
27701(已導入)

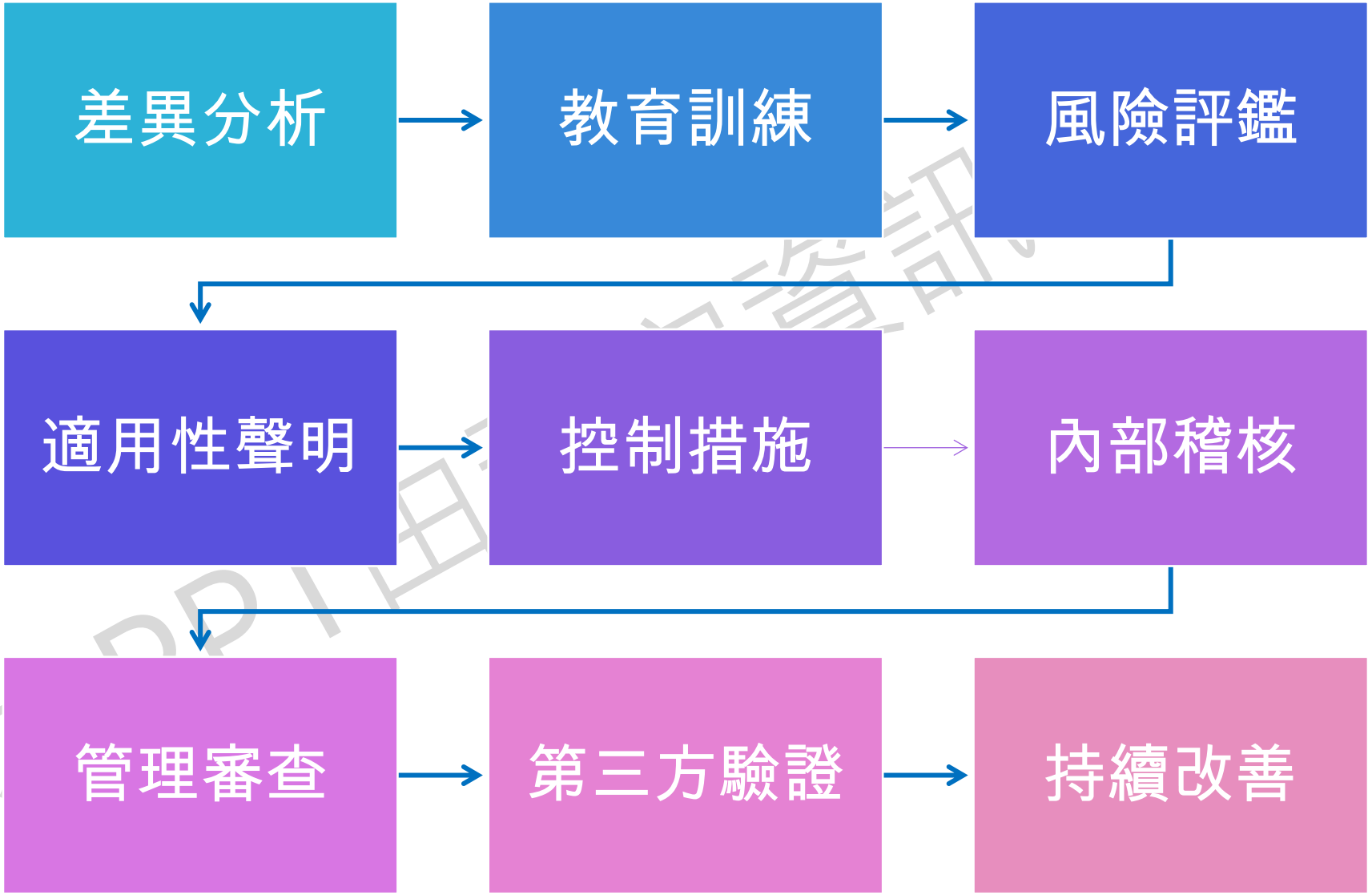


27001(已導入)
27701(未導入)

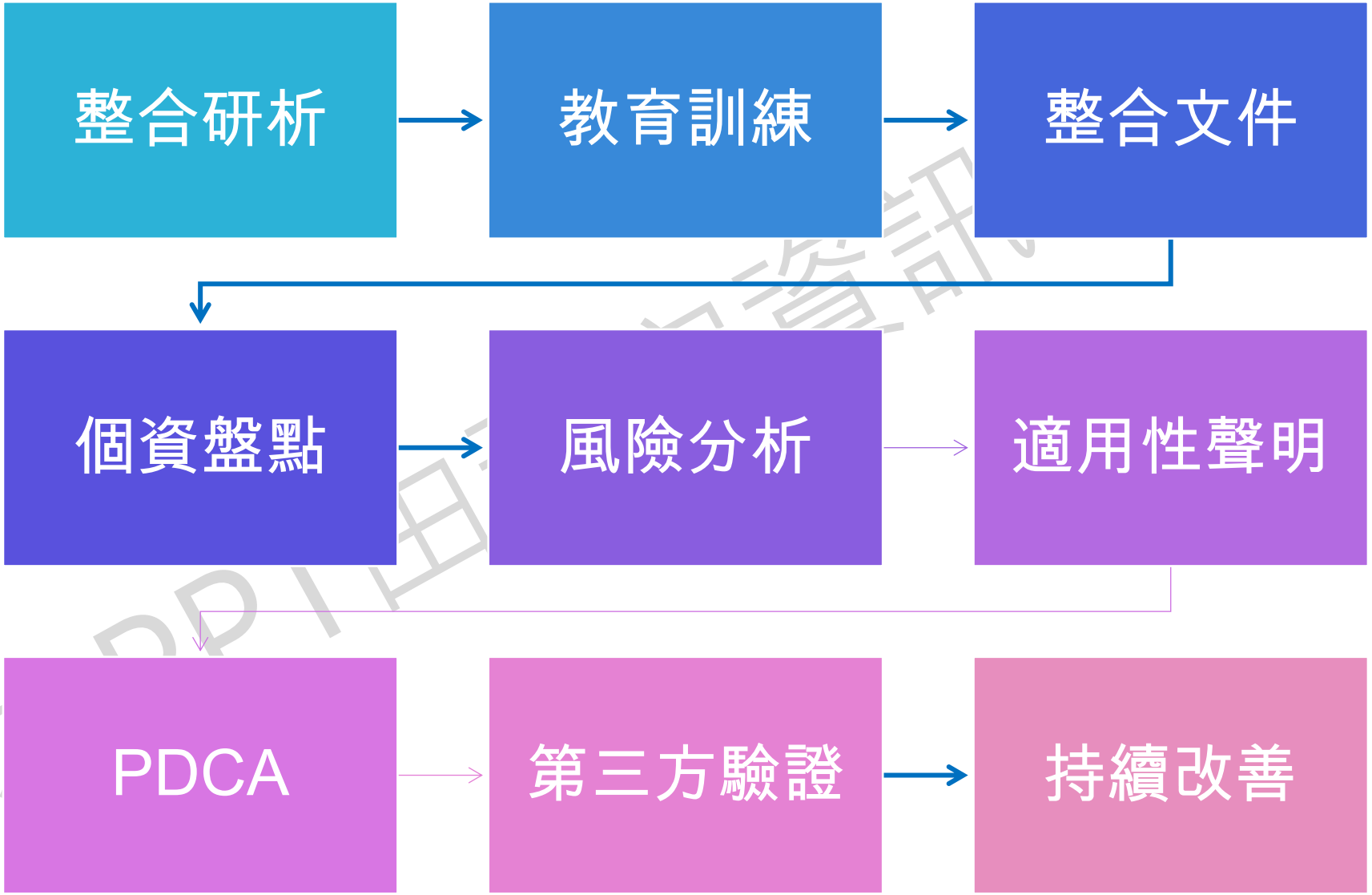
27001(未導入)
27701(未導入)

本PPT由溶安資訊製作

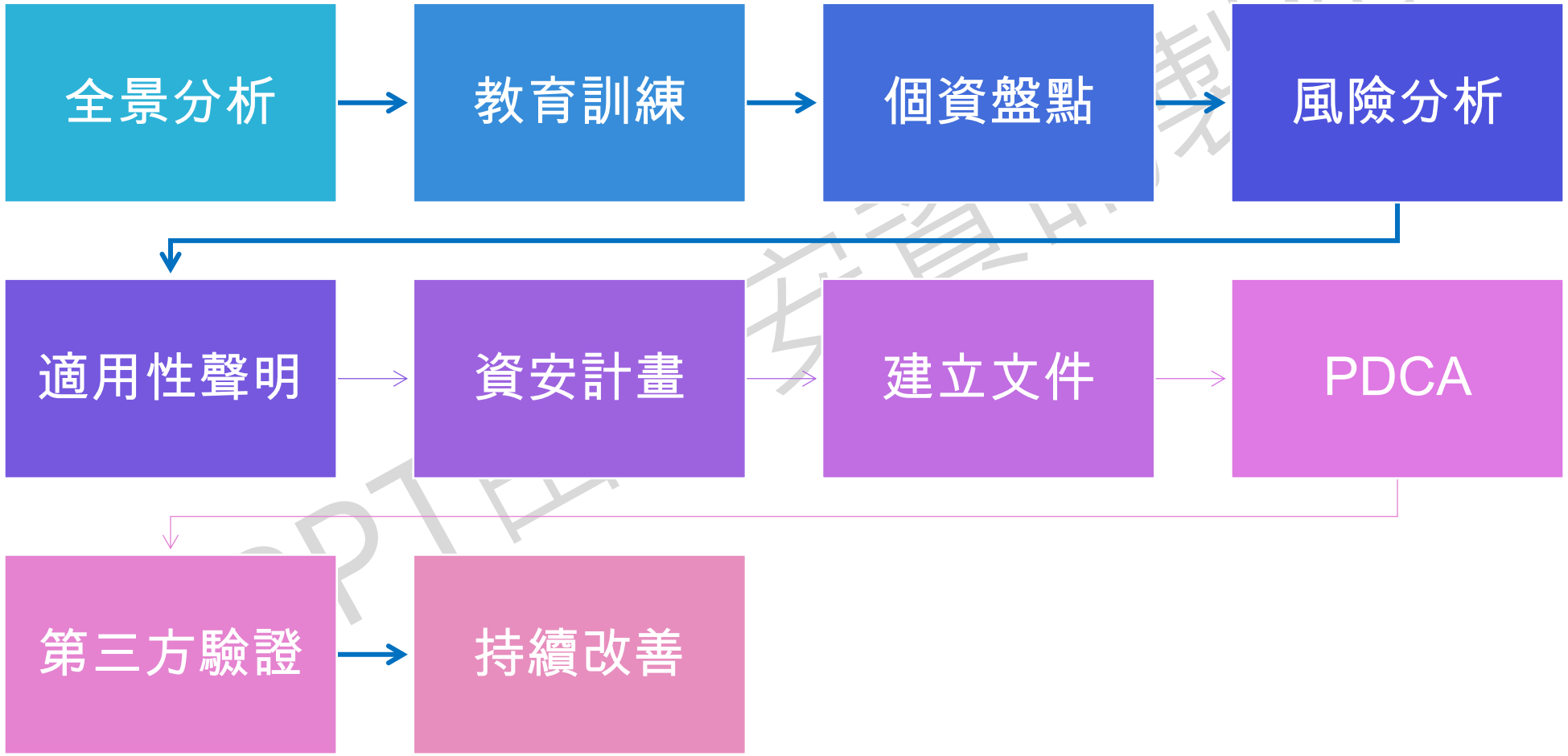
27001(已導入)27701(已導入)轉版



27001(已導入)27701(未導入)轉版



27001(未導入)27701(未導入)轉版

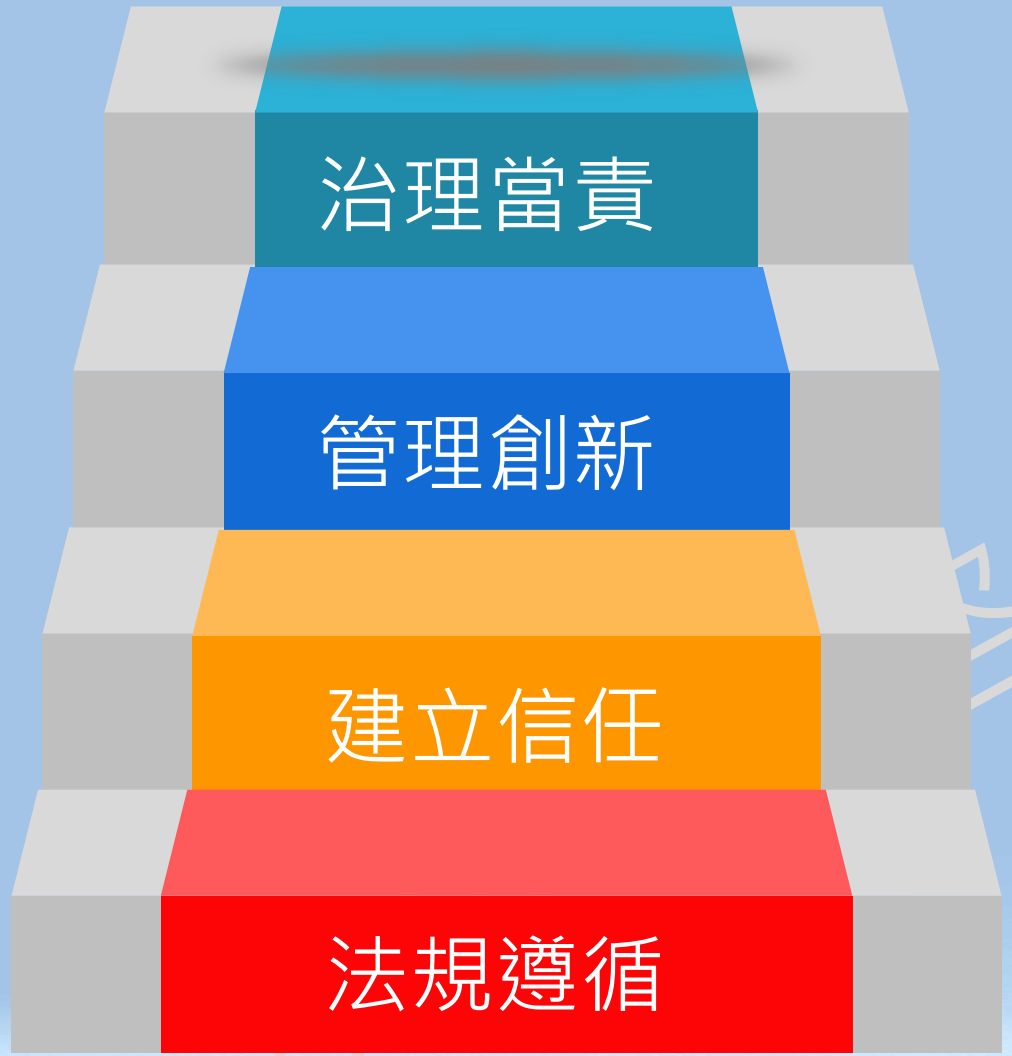


結論

本PPT由安資訊製作

隱私權管理

資安資訊製作



驗證範圍 ISO 27706

「隱私資訊管理系統」

組織在各項活動、產品或服務中所扮演的角色（例如，組織是個人資料控制者、處理者或兩者兼具）；

各項活動、產品或服務中正在處理其個人識別資料主體（例如，員工、顧客）；

組織隱私權資訊管理系統適用性聲明 (SoA) 的版本。

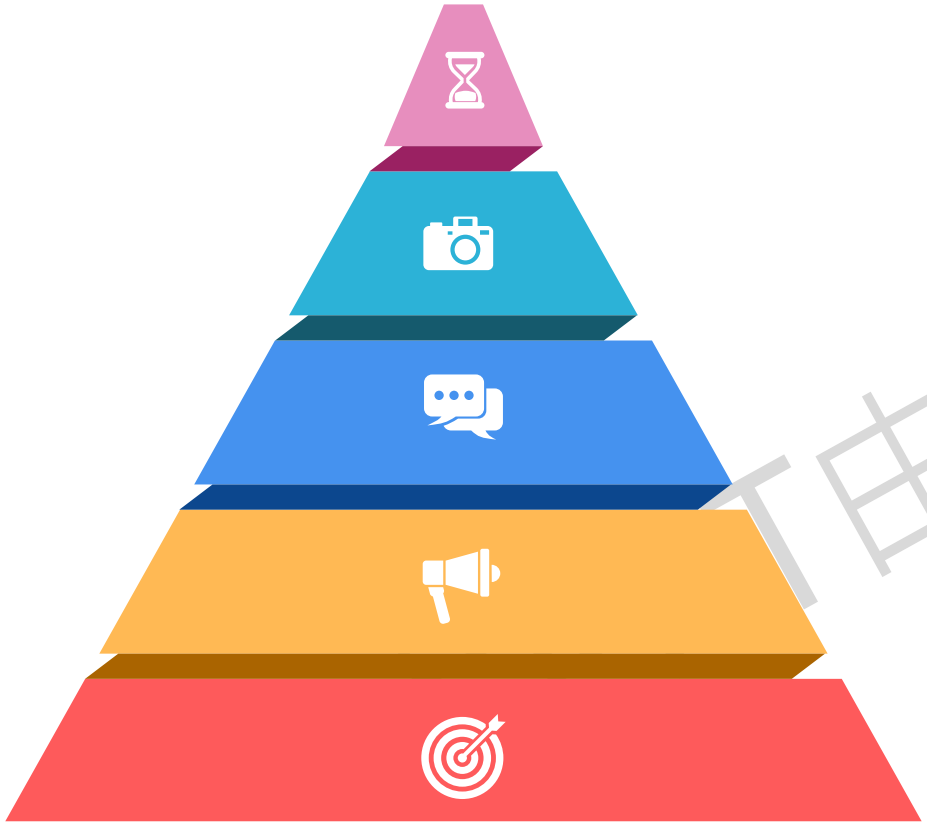
如果組織在認證範圍內的任何活動均未在指定的實體地點進行，則應說明組織的所有活動均以遠端方式進行。

本PPT由資安資訊製作

Table A.1 — Audit time chart

Number of persons doing work under the organization's control involving the handling or processing of PII, or with access to such data		**PII-controllers audit time for initial audit** (auditor days)	**PII-processors audit time for initial audit** (auditor days)	**PII-processor + controller audit time for initial audit** (auditor days)	**Additive and subtractive factors**	**Total audit time**
1–10		4	3,5	6,5	See A.3.5	
11–15		4	3,5	6,5	See A.3.5	
16–25		5	4	6,5	See A.3.5	
26–45		5	4	7	See A.3.5	
46–65		6	4,5	8	See A.3.5	
66–85		6	4,5	9	See A.3.5	
86–125		7	5	10	See A.3.5	
126–175		7	5	11	See A.3.5	
176–275		8	5,5	12	See A.3.5	
276–425		8	6	12	See A.3.5	
426–625		9	6	14	See A.3.5	
626–875		10	7	15	See A.3.5	
876–1 175		11	7	16	See A.3.5	
1 176–1 550		12	8	17	See A.3.5	
1 551–2 025		13	8	19	See A.3.5	
2 026–2 675		13	9	20	See A.3.5	

人天計算因子



- 個人資訊 (PII) 處理活動的複雜性
- 已實施的控制措施數量，包括但不限於 ISO/IEC 27701:2025 附件 A 和附件 B 中的控制措施
- PII 處理活動的數量
- 正在處理的 PII 的分類/類別
- 組織運作的地點/地理區域/司法管轄區的數量
- PII 的傳輸範圍
- 處理或有權存取 PII 的人員數量
- PII 的數量
- 處理 PII 主要資料的平台數量

由資訊製作

人數

01

從事活動且實施嚴格資訊揭露限制的人員，例如，禁止將個人物品和設備帶入工作場所的措施

02

僅擁有資訊唯讀權限以履行職責的人員

03

在PIMS範圍內無權存取組織資訊處理設施的人員

04

在PIMS範圍內擁有對公司資訊處理設施特定且可證明受限存取權限的人員

本PPT由資安資訊製作

從事該活動的人員數量；活動或流程的類型

立法院三讀通過「個人資料保護法」部分條文修正草案

行政院於114年3月27日送請立法院審議之「個人資料保護法」（下稱個資法）部分條文修正草案，業經立法院院會第11屆第4會期第5次會議今（17）日三讀通過。個人資料保護委員會籌備處（下稱個資會籌備處）對立法委員與各界之支持，及各委員於審查時所提供之寶貴意見，表示感謝。今日通過之個資法新法，將賦予個人資料保護委員會（下稱個資會）必要執法權限，惟個資會之正式成立，仍須俟組織法立法通過後始有法源依據；目前組織法草案業經立法院「司法及法制委員會」初審完竣，尚待進一步完成立法程序。未來行政院將配合組織法在立法院之審議進度，並審酌相關行政準備作業時間後，另行指定個資法本次個資法部分條文修正要點如下：

一、賦予個資會必要監管職能：增訂個資事故的通報義務，日後將由個資會統一受理個資外洩等事故通報，以利掌握相關事態，事故機關亦應即時採取應變措施並留存相關紀錄。又為了強化各類公務機關、非公務機關的個資法令遵循及安全控管，個資會也將訂定共通基礎版的安全維護管理辦法，作為日後執法的基準。（個資法修正草案第12條、第18條、第20條之1）

二、強化公部門個資監督管理：本次個資法修正增訂公務機關應置個資保護長，由機關首長指派適當人員兼任，以統籌規劃的角色，由上而下、深化落實公部門的個資保護文化。同時增訂公部門內、外部監管機制，由上級機關督導所屬，搭配個資會的外部稽核及行政檢查，內外並行加強個資保護。（個資法修正草案第18條、第21條之1至第21條之4）

三、對私部門另設過渡期間：考量個資會成立初期的監管資源尚未齊備，故設計過渡機制，由個資會直接監管目前沒有明確目的事業主管機關的業者，已有明確目的事業主管機關的業者，則在個資會成立後6年內，依行政院公告範圍，繼續由目的事業主管機關監管，並每2年檢討減列，逐步完成監理事權劃一。（個資法修正草案第51條之1）

THANK YOU