ISO27001：2013轉版

課程大綱

- ISO27001架構
- 本文架構
- 附錄架構
- 4.組織環境
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.
- 附錄A
- 條文A.5~A.18

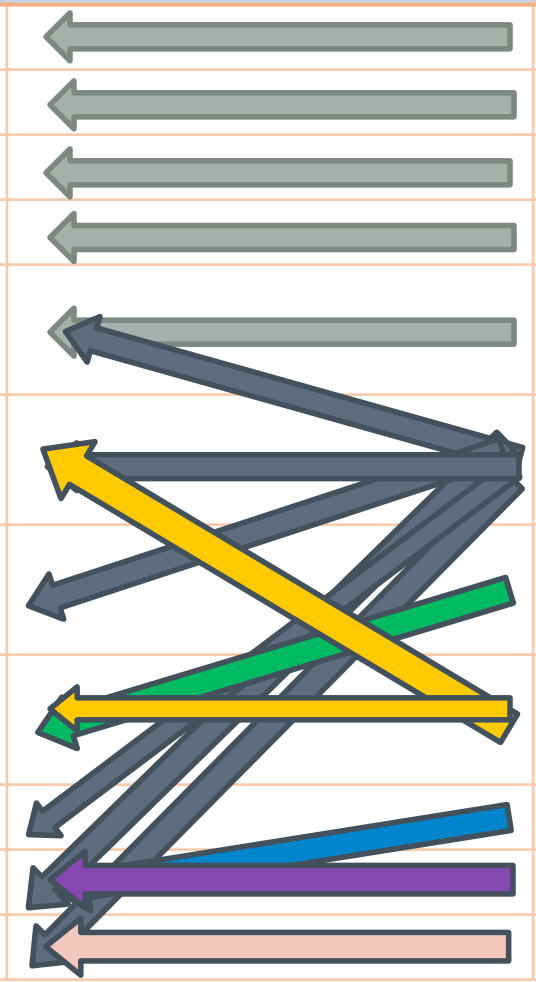
DAY 1

ISO 27001 新舊版差異說明

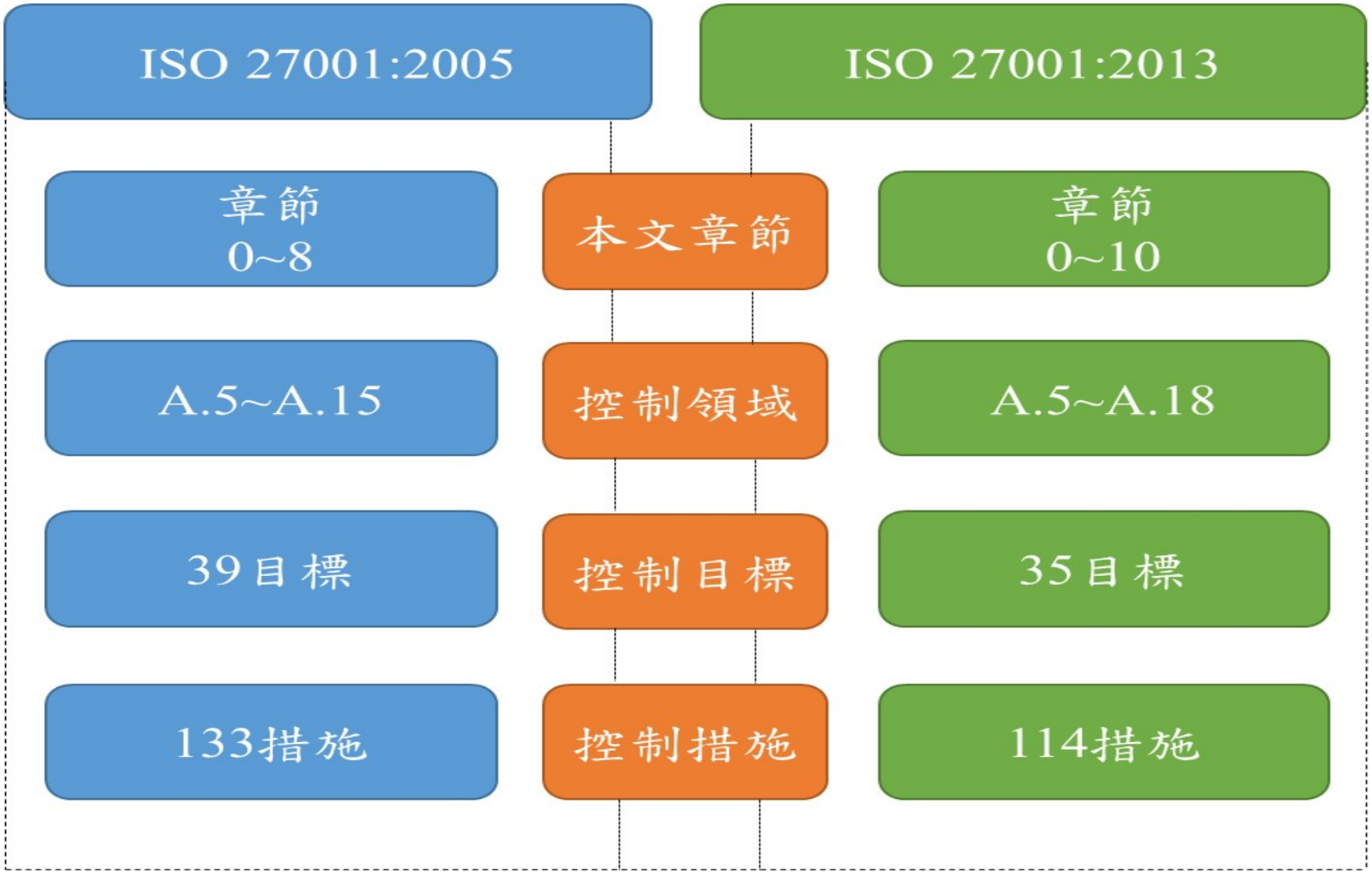
新版 ISO 27001主要修正方向

- 架構改成與其他ISO標準一致
- 與其他國際標準高度結合
  - 名詞釋義參照ISO/ IEC 27000
  - 風險評鑑方法論參照ISO 31000
- 強調組織內外部的議題、與外部團體的關係及要求，且需與組織目標結合，透過可量測的方式展現績效
- 重疊的內容進行整併、刪除過時的項目與內容，加入新增的項目

改版差異(本文)

ISO 27001:2013		ISO 27001:2005
0. Introduction		0. Introduction
1. Scope		1. Scope
2. Normative references		2. Normative references
3. Terms and definitions		3. Terms and definitions
4. Context of the organization		4.1 General
5. Leadership		4.2 Establish and managing the ISMS
6. Planning		4.3 Documentation requirements
7. Support		5. Management Responsibility
8. Operation		6. Internal ISMS audit
9. Performance evaluation		7. Management Review
10. Improving		8. ISMS improving

ISO 27001:2013 & ISO 27001:2005

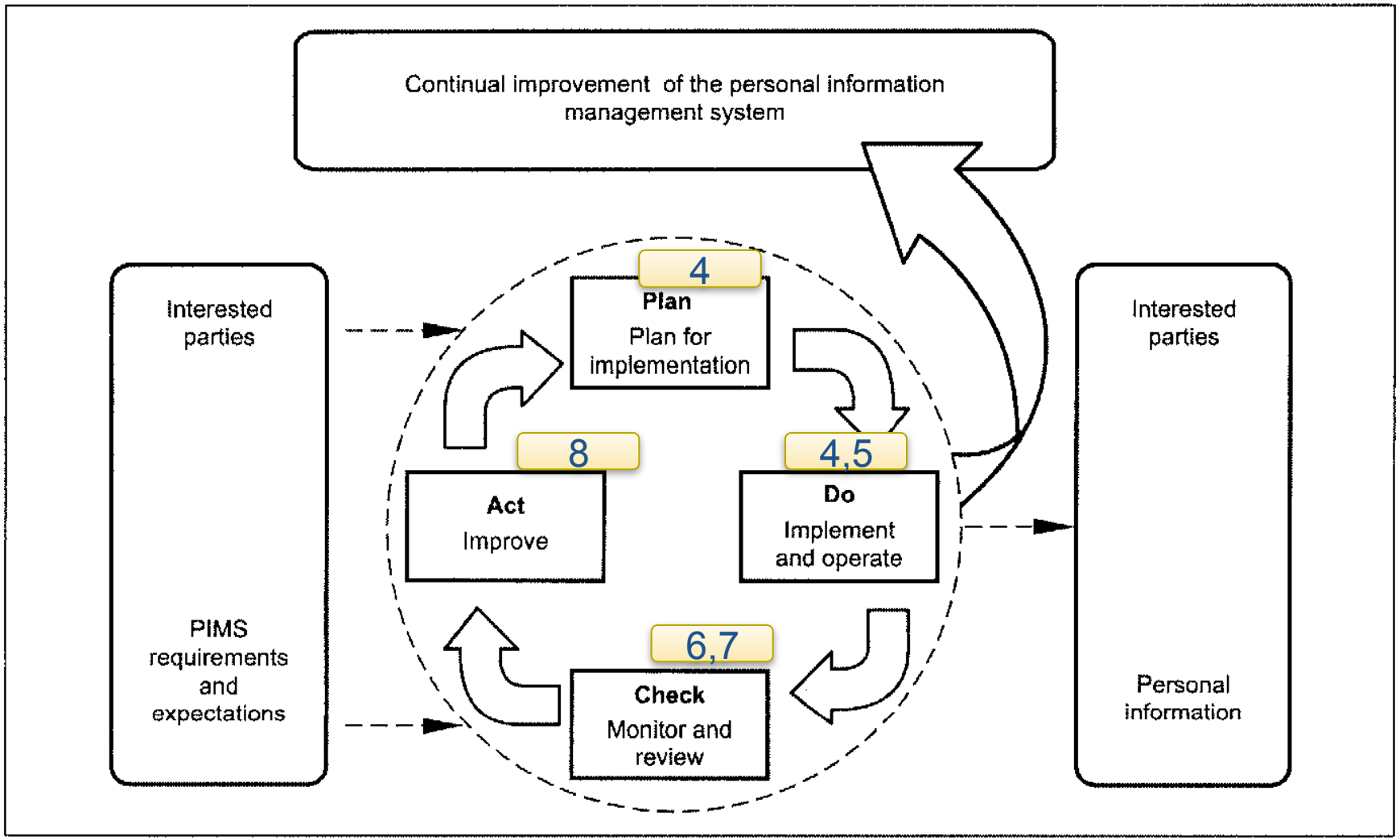


ISO27001架構

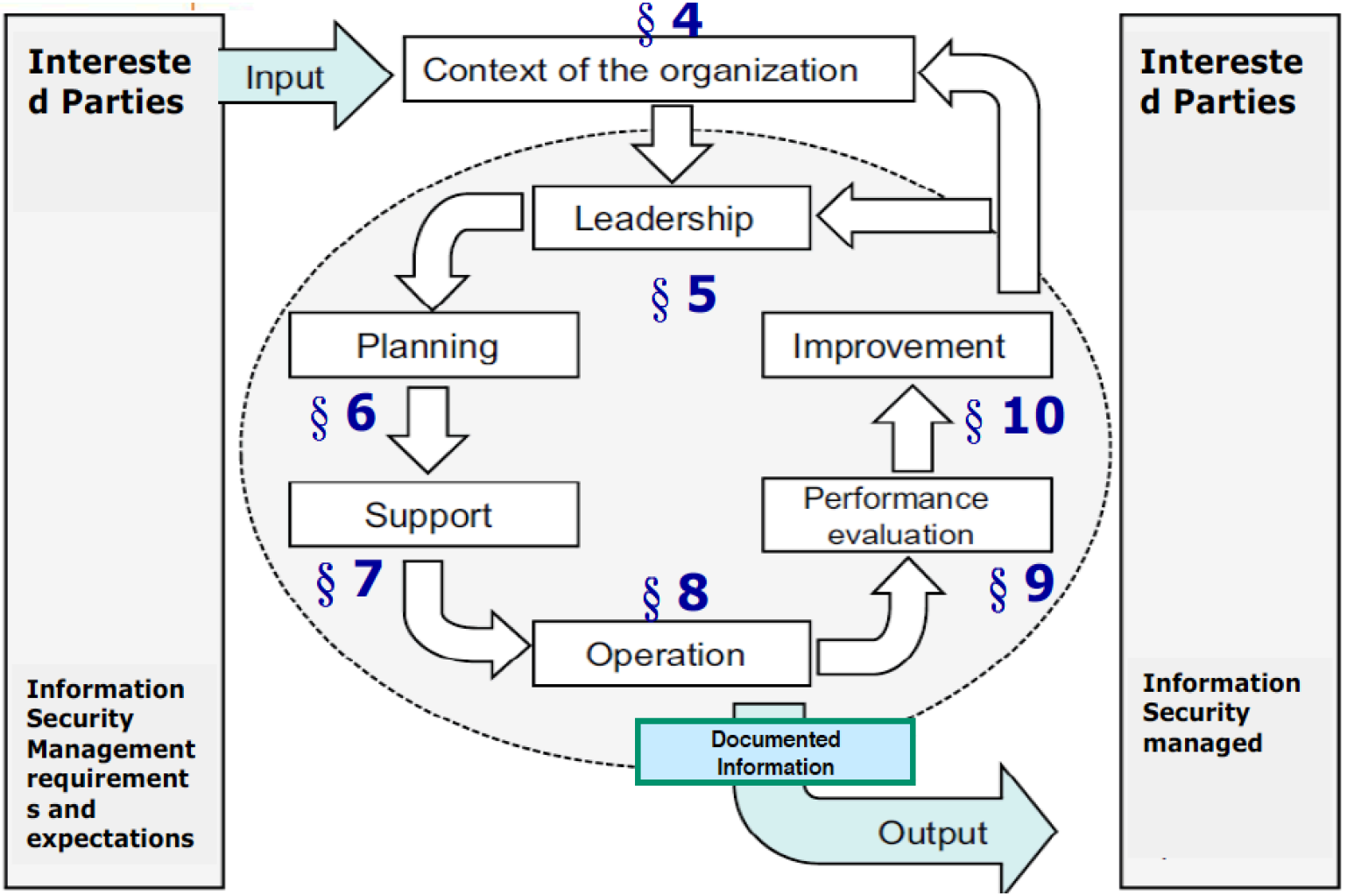
- 1.Scope範圍
- 2.Normative references 參考標準
- 3.Terms & definitions 名詞與定義
- 4.Context of the organization 組織環境（全景）
- 5.Leadership 領導
- 6.Planning 規劃
- 7.Support支援
- 8.Operation運作
- 9.Performance evaluation 績效評估
- 10. Improvement 改善
- Annex A (normative)

本文架構

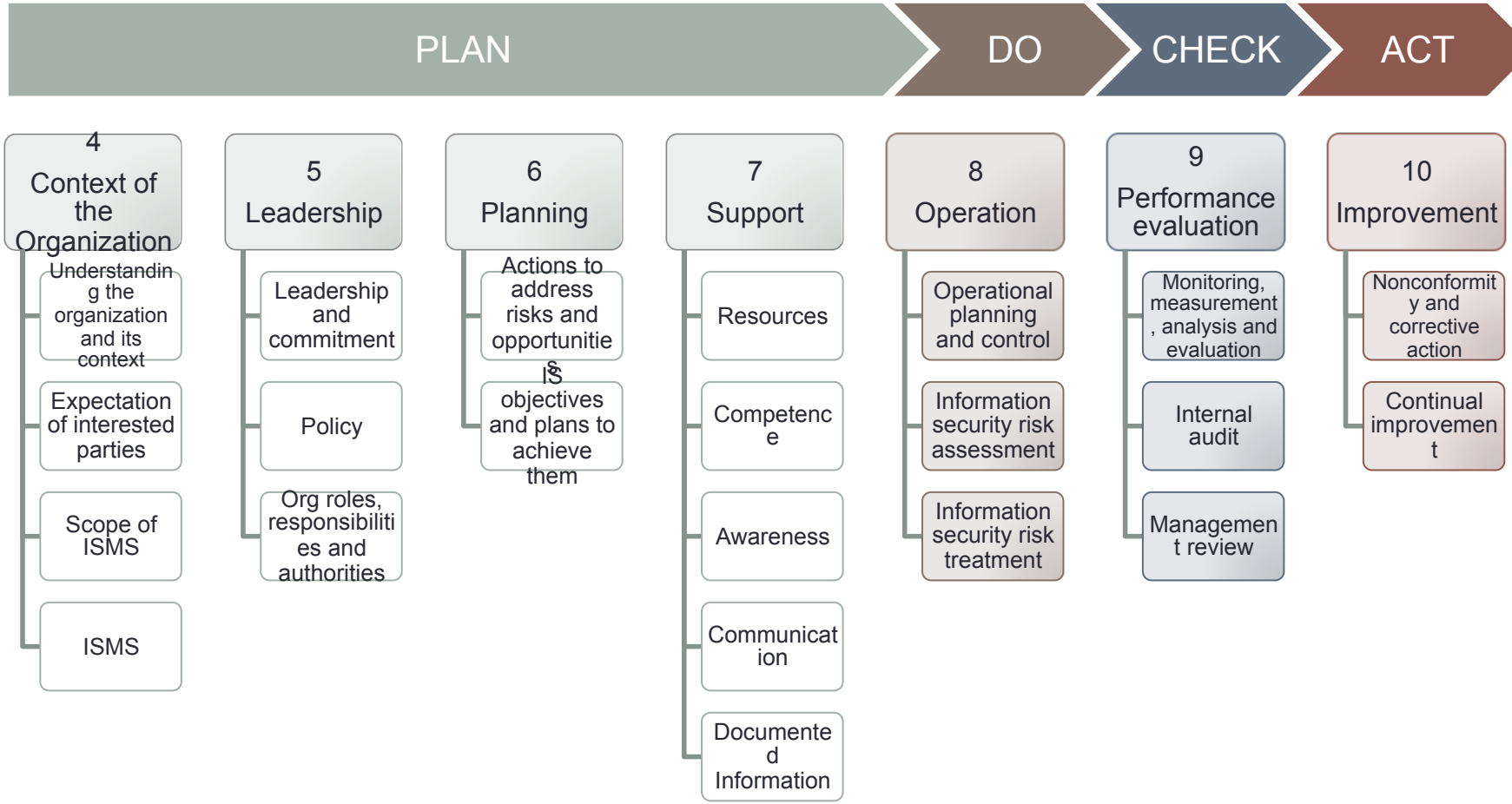
ISO 27001:2005 (PDCA) cycle



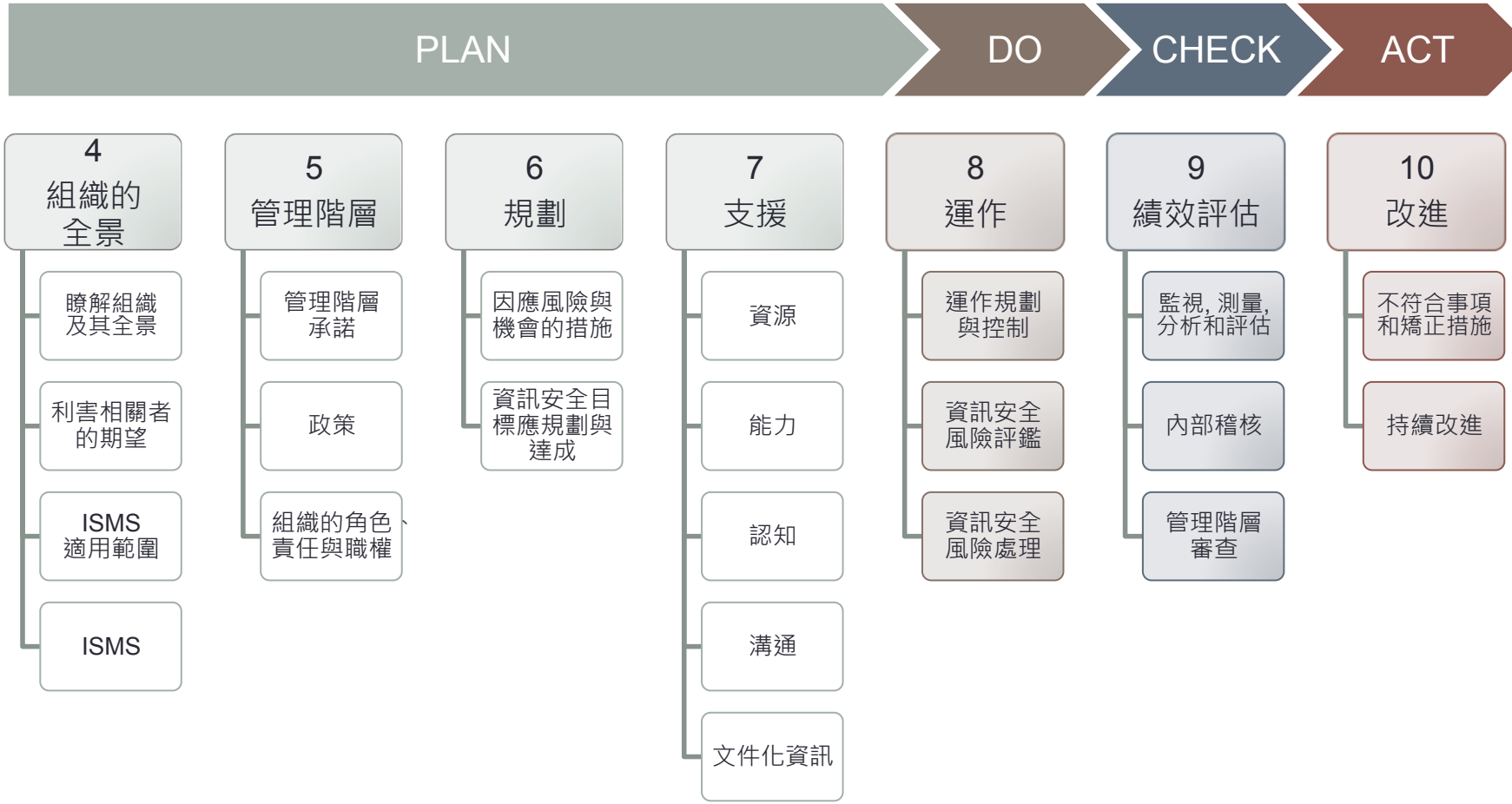
採用ISO Annex SL之高階架構



ISO 27001:2013 新版框架



ISO 27001:2013 新版框架



附錄A架構

ISO 27001:2013 Annex A

14領域;35控制目標;114控制項目

- A.5 Information security Policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

本文内容

- 1.Scope範圍
  - 4~10章節不可排除
- 2.Normative references 參考標準
  - 以ISO27000為參考
- 3.Terms & definitions 名詞與定義
  - 以ISO27000為參考

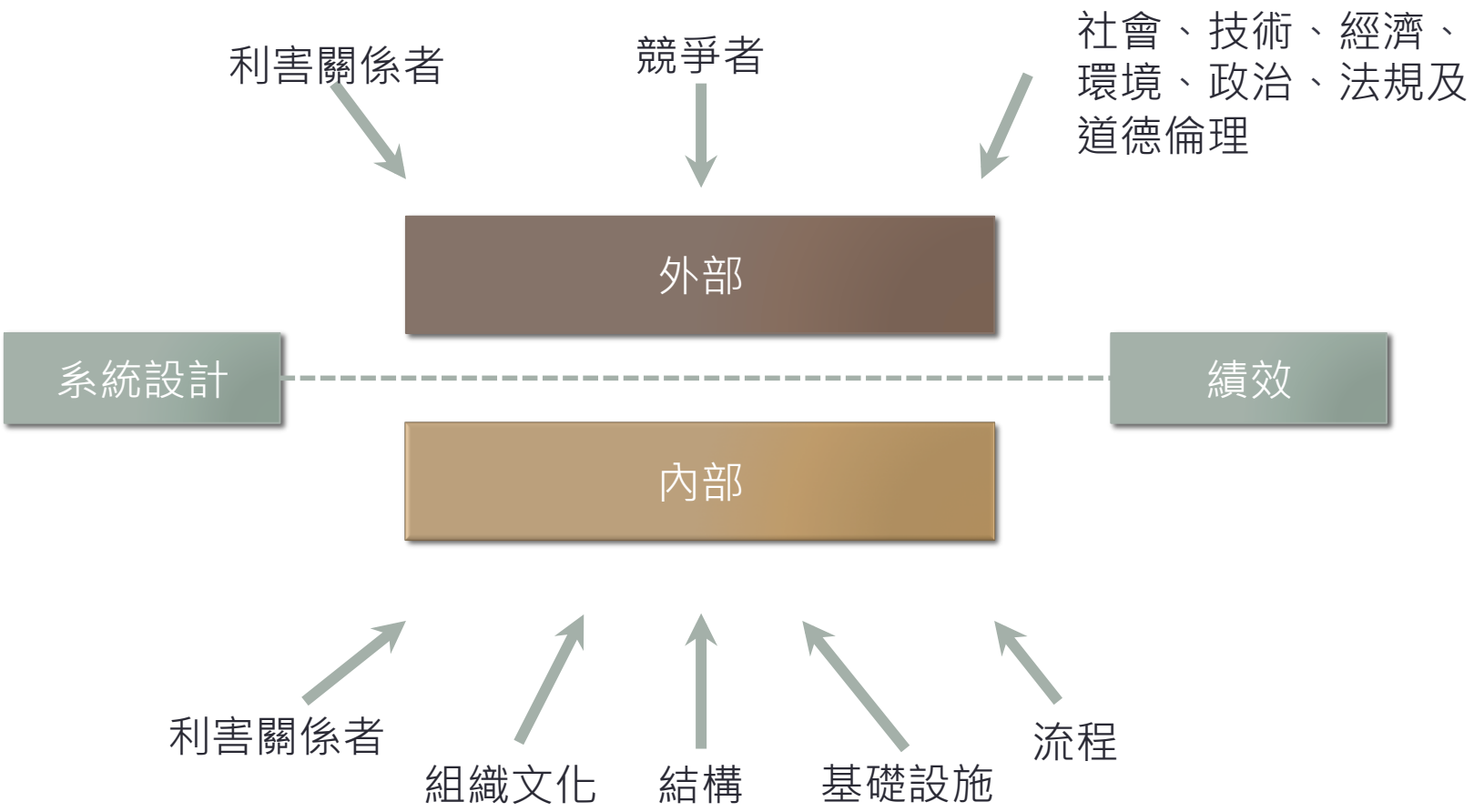
4.Context of the organization 組織環境（全景）<->4.1,4.2

- 4.1 瞭解組織及其全景

  組織應決定與組織目標相關，並會影響達成資訊安全管理系統預定成果的外部與內部議題

  內外部議題可參考ISO31000條文5.3建立外部與內部環境（全景）
- 4.2 瞭解利害相關者的需求與期望
  - ISMS相關的利害關係團體
  - 利害關係團體對資訊安全相關的要求事項（法律、法規、合約）
- 4.3 定義ISMS適用範圍 <-> 4.2.1.a
  - 範圍應考慮a)4.1 b)4.2 c)在組織與其他組織執行活動間的介面與相依性
  - 範圍必須文件化
- 4.4 ISMS<->4.1
  - 組織應建立、實作、維持及持續改進ISMS，以符合國際標準之要求
  - Dynamic response

組織內外部情境



參考：ISO31000:2009

討論一

了解組織及全景、
了解利害相關者的需求與期望
決定資訊安全管理制度範圍

5. Leadership 領導 <->4.2,5

- 5.1 領導與承諾 <-> 5.1.b~e
  - 如何展現確保
  - A) 政策與目標的建立切合組織策略方向
  - B) 整合ISMS要求於流程中
  - C) 所需資源可得
  - D) 溝通的重要性在有效的資訊安全管理與符合ISMS要求
  - E) 達到預期的結果
  - F) 指導與支援人員貢獻有效性
  - G) 促進持續改善
  - H) 支援其他相關角色以展現領導能力

5. Leadership 領導 <->4.2,5

- 5.2 政策 <-> 5.1.a;4.2.1.b(統一為資訊安全政策）
  - A) 達成組織目標
  - B) 包含資訊安全的目標或提供設定的框架
  - C)包含滿足資訊安全相關適用要求的承諾
  - D)包含持續改善ISMS的承諾
- 資訊安全政策應該
  - E) 提供文件化資訊
  - F) 於組織內溝通
  - G) 適當的被利害相關者所取用
- 5.3 組織的角色、責任與職權（人員對既有控制熟悉程度）(RACI)
  - A) 確保ISMS符合國際標準
  - B) 對高階管理階層報告ISMS的績效
- 備註：高階管理階層也可以指派報告績效的責任和授權

6.Planning 規劃 <->4.2

- 6.1 因應風險與機會的措施
- 6.1.1 概述（重點在現在及未來如何做）
  - 規劃ISMS時，應考量4.1,4.2的要求事項，及決定應被提出的風險與機會
  - A) 確保ISMS能達成預定效益
  - B) 預防或降低非預期的影響
  - C) 達到持續改進
- 組織應如何規畫
  - D) 因應風險與機會的行動
  - E) 1)如何整合及實作行動至ISMS的流程中以及
  - 2)評估其有效性

6.Planning 規劃 <->4.2

- 6.1.2 資訊安全風險評鑑 :建立RA標準、與可接受標準、識別、分析、評估風險，並文件化 <-> 4.2.1.c~f
- 組織應定義並建立資訊安全風險評鑑流程
  - A) 建立與維護資訊安全風險準則
    - 1) 風險接受準則
    - 2) 執行資訊安全風險評鑑的準則
  - B) 確保重複執行的資訊安全風險評鑑結果能一致性，有效性和可比較性
  - C) 鑑別資訊安全的風險
    - 1) 採用風險評鑑流程來辨識ISMS範圍中CIA的風險
    - 2) 識別風險擁有者
  - D) 分析資訊安全風險
    - 1) 評估潛在（6.1.2 c)1)）後果
    - 2) 評估發生（6.1.2 c)1)）的可能性
    - 3) 決定風險等級
  - E) 評估資訊安全風險
    - 1) 將風險分析結果與準則（6.1.2 a)）做比較
    - 2) 訂定風險處理的優先順序
- 組織應維持有關資訊安全風險評鑑流程的文件化程序

6.Planning 規劃 <->4.2

- 6.1.3 資訊安全風險處理 :製訂適用性聲明、資訊安全風險處理計畫，並文件化 <-> 4.2.1.g~j
- 組織應採用資訊安全風險處理流程(a~f)
  - A) 考量風險評鑑結果，選擇風險處理選項
  - B) 決定所有需要執行風險處理項目的控制措施
  - C) 與附錄A比較，以釐清有無必要的控制措施被省略
  - D) 適用性聲明書包含上述（6.1.3 b) c)）之選擇，無論選擇與否皆需進行說明
  - E) 產生風險處理計畫
  - F) 由風險擁有者核准風險處理計畫並接受殘餘風險
- 組織應維持有關資訊安全風險處理流程的文件化資訊
  - 備註：本標準中的資訊安全風險評鑑和處理流程，應與ISO31000提供的原則與一般性指引相符

6.Planning 規劃 <->4.2

- 6.2資訊安全目標與達成
- 規劃組織應於適當的功能和層級建立資訊安全目標
- 資訊安全目標應(a~e)
  - A) 與資安政策一致
  - B) 是可量測的
  - C) 考慮資訊安全要求、風險評鑑及風險處理的結果
  - D) 可溝通的
  - E) 適時更新
- 組織應維持有關資訊安全目標的文件化資訊
- 當規劃如何達到目標（f~j）4W1H
  - F) What will be done,（作什麼）
  - G) What resource will be required,（需要哪些資源）
  - H) Who will be responsible,（誰負責）
  - I) When it will be completed, and （何時完成）
  - J) How the results will be evaluated（如何評估結果）

討論二

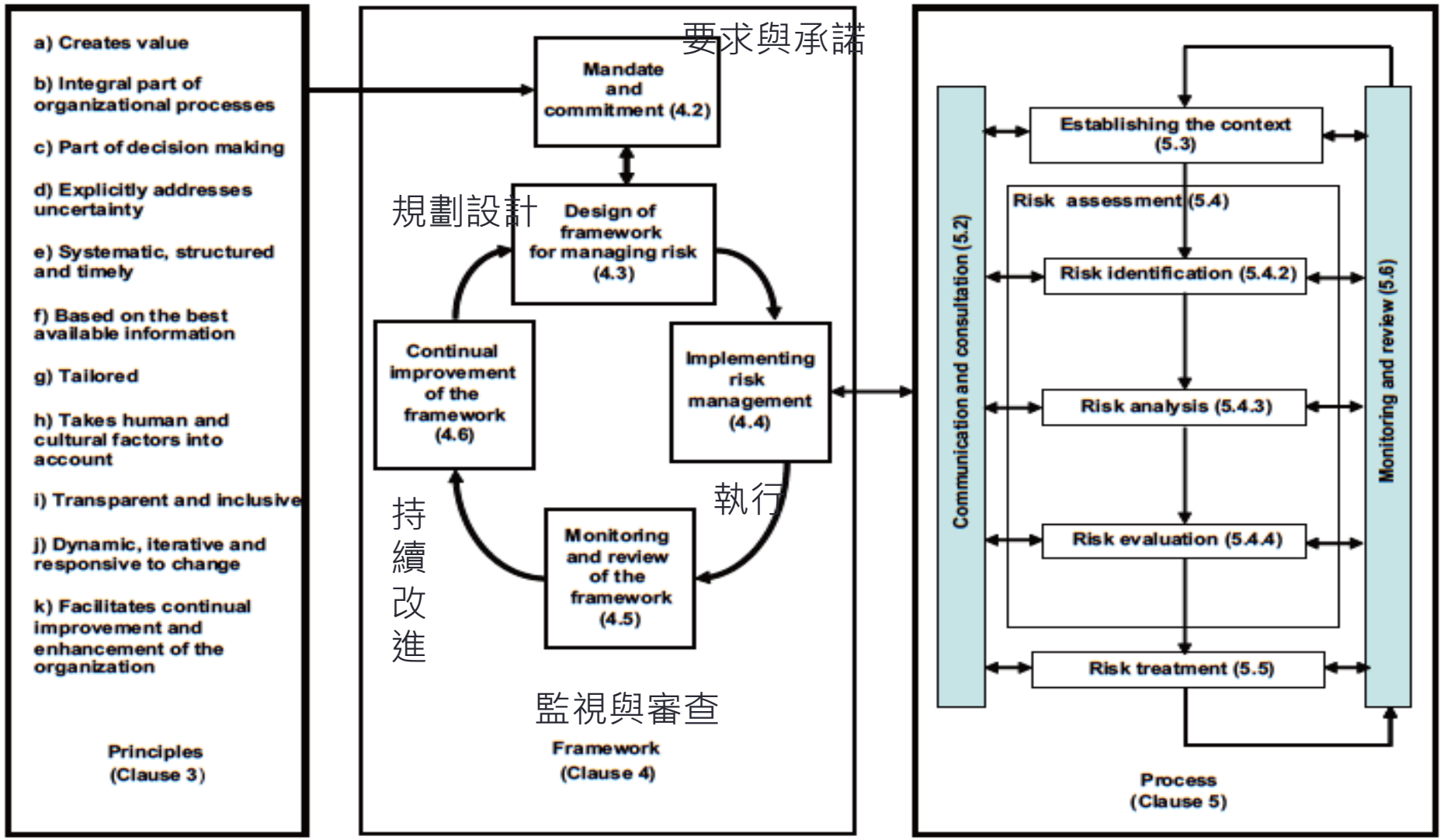
組織角色、責任

請建立組織角色責任表

ISO31000:2009

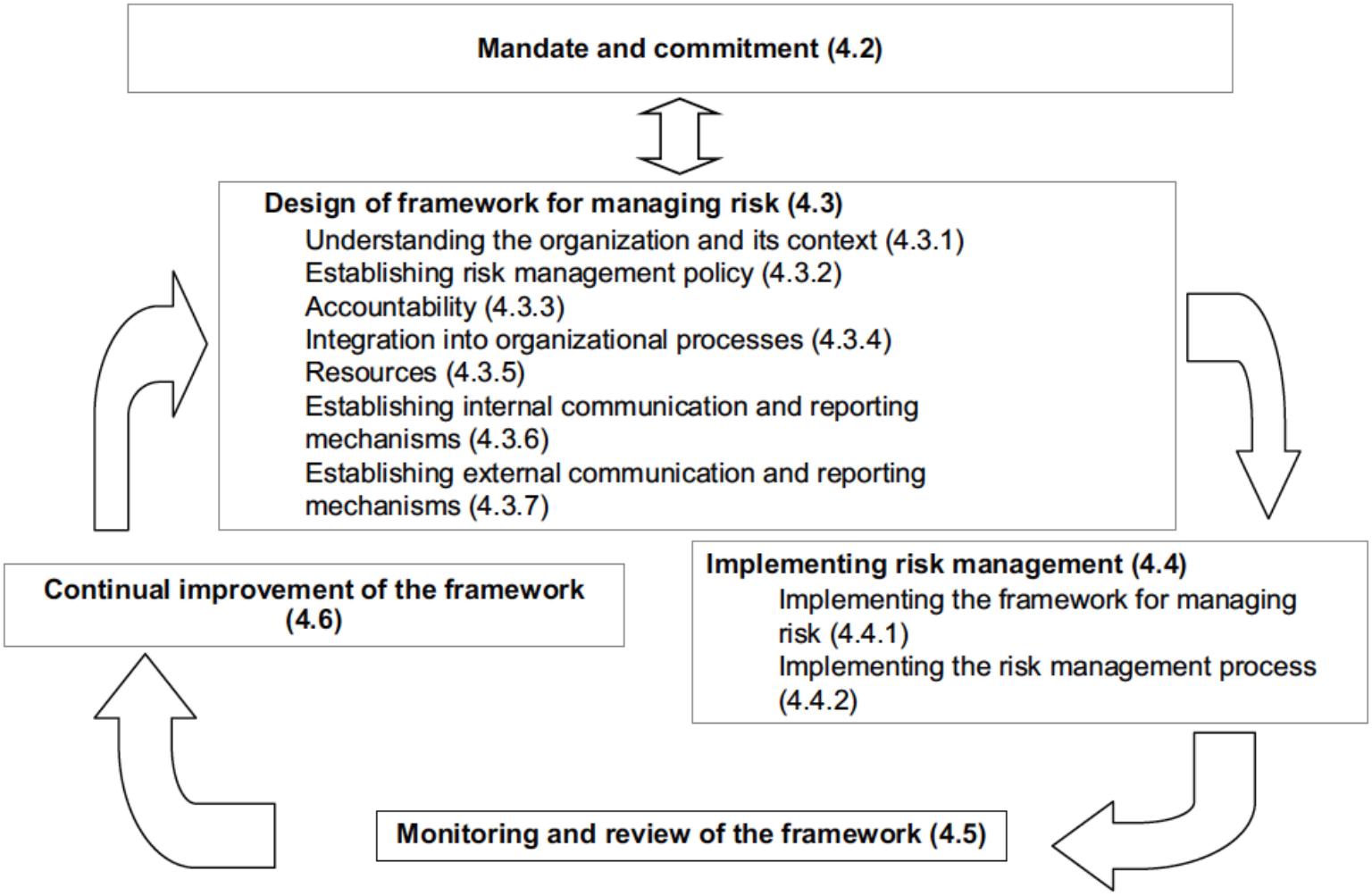
風險管理原則與指導綱要

風險管理原則、架構與流程關係圖



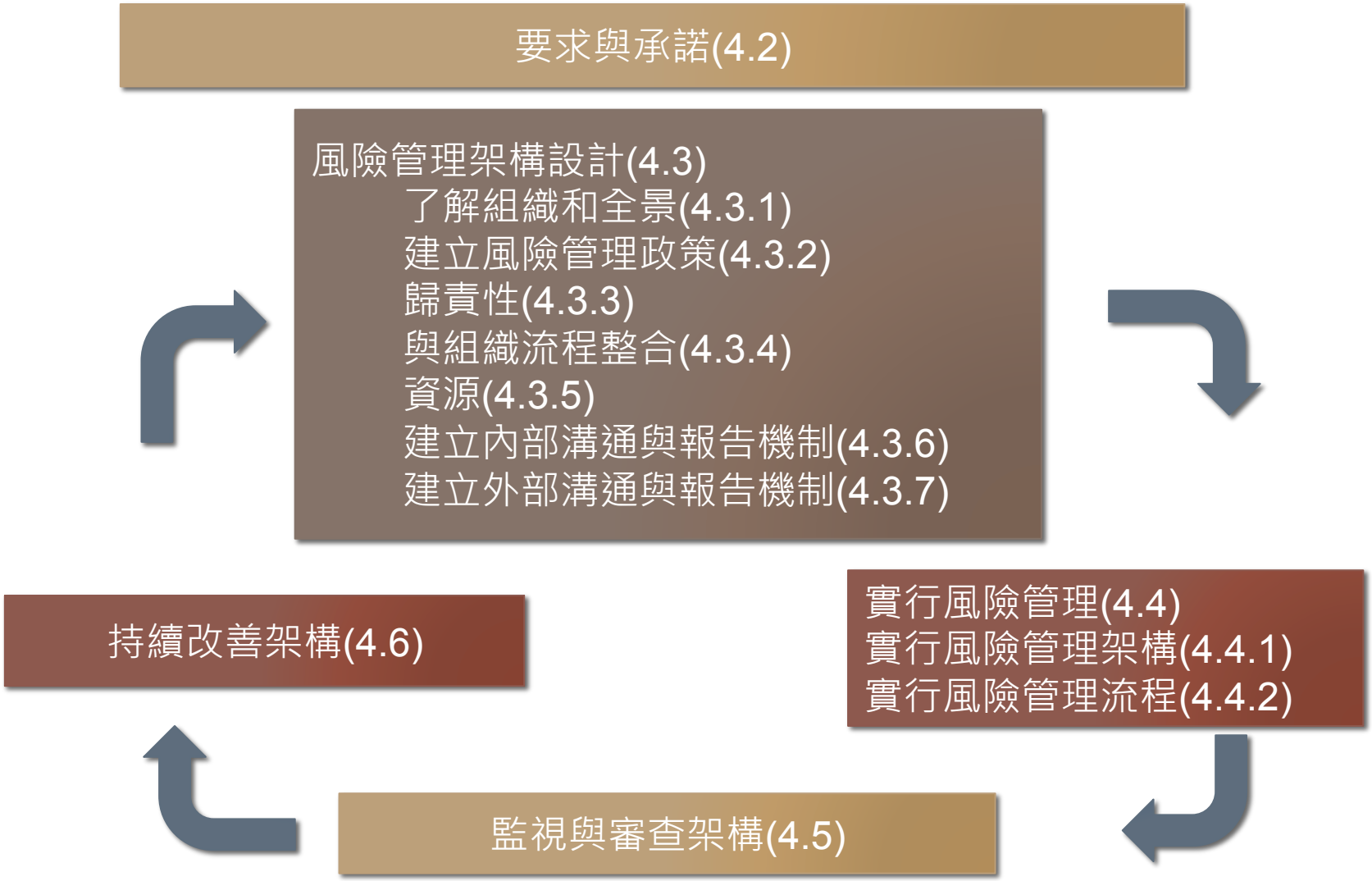
參考：ISO31000:2009

風險管理架構



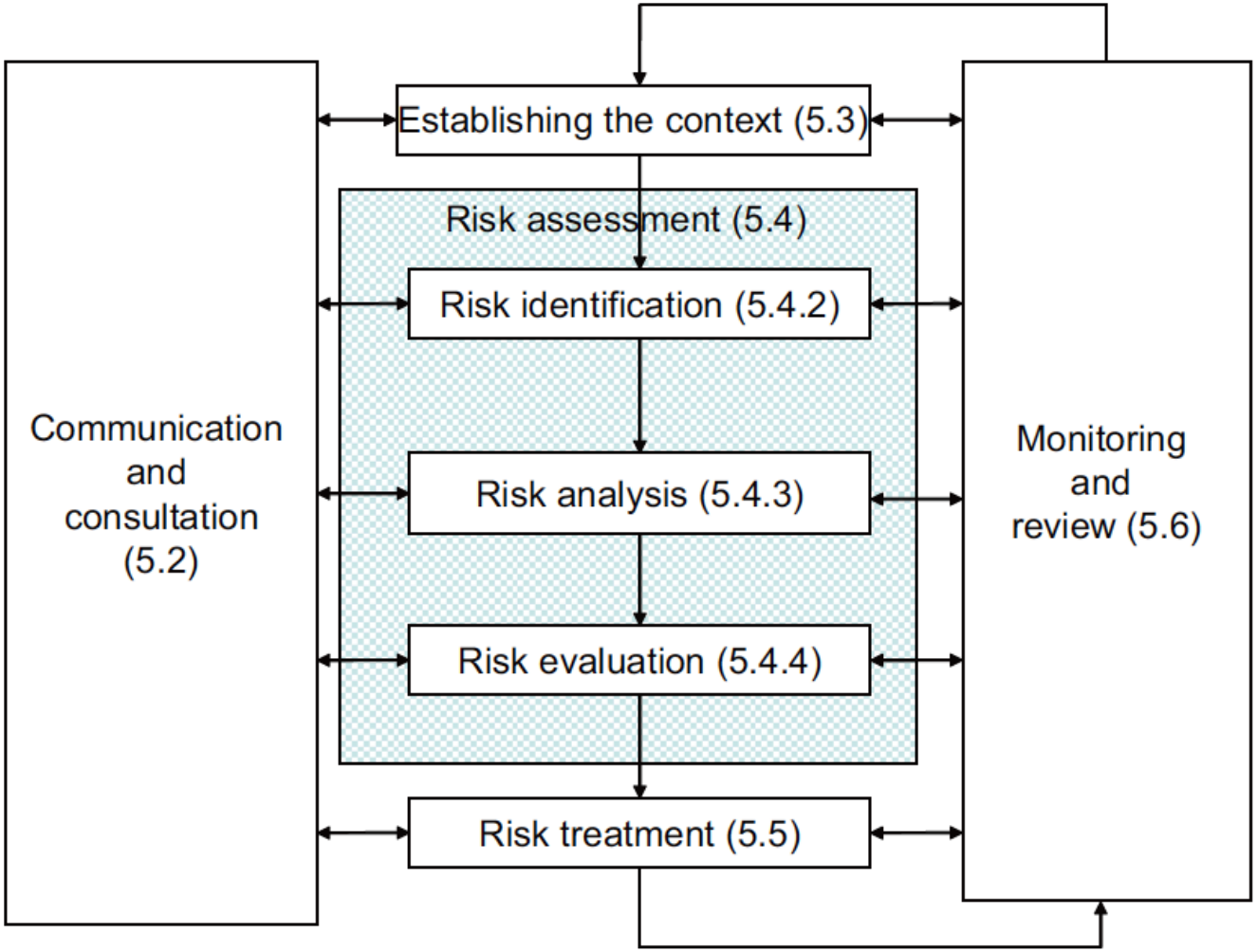
參考：ISO31000:2009

風險管理架構



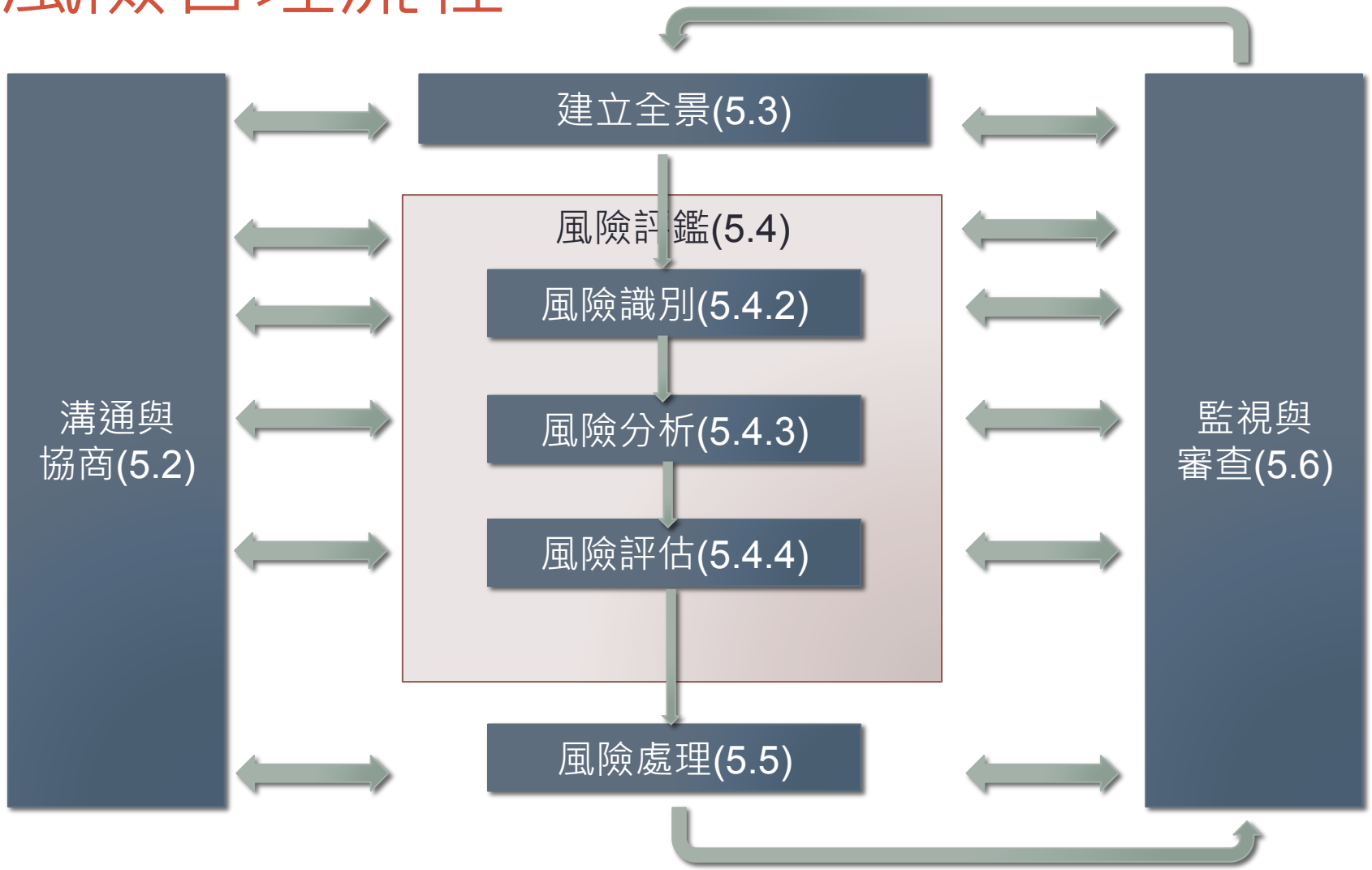
參考：ISO31000:2009

風險管理流程



參考：ISO31000:2009

風險管理流程



參考：ISO31000:2009

定義風險準則

- 組織應定義要用於評估風險的重要性的準則。該準則應該反映組織的價值、目標和資源。風險準則應與組織的風險管理政策相一致（見4.3.2），在任何風險管理程序的開端定義，並不斷檢討。
- 當定義風險準則，需要考慮的因素應包括以下內容：
  - 原因的本質和類型和可能發生的結果以及將如何進行測量
  - 可能性如何定義
  - 可能性和/或結果的時間表
  - 風險水準如何決定
  - 利害相關者的意見
  - 風險可接受或可容忍的水準
  - 應考慮到是否為多風險的組合，如果是，哪些組合應予以考慮

參考：ISO31000:2009

風險處理流程

- 風險處理涉及一個循環的流程：
  - 評估風險處理
  - 決定剩餘風險水準是否是可以容忍
  - 如果無法容忍，產生新的風險處理
  - 評估處理的成效。
- 風險處理方案並不一定是相互排斥的，或適用於所有情況。該選項可以包括以下內容：
  - a）避免風險，不繼續執行或從事相關風險活動
  - b）尋求新機會
  - c）去除的危險來源
  - d）變更可能性
  - e）變更情況
  - f）與另一方或多方（包括合約和風險融資）分擔風險
  - g）藉由選擇或放棄讓風險自留

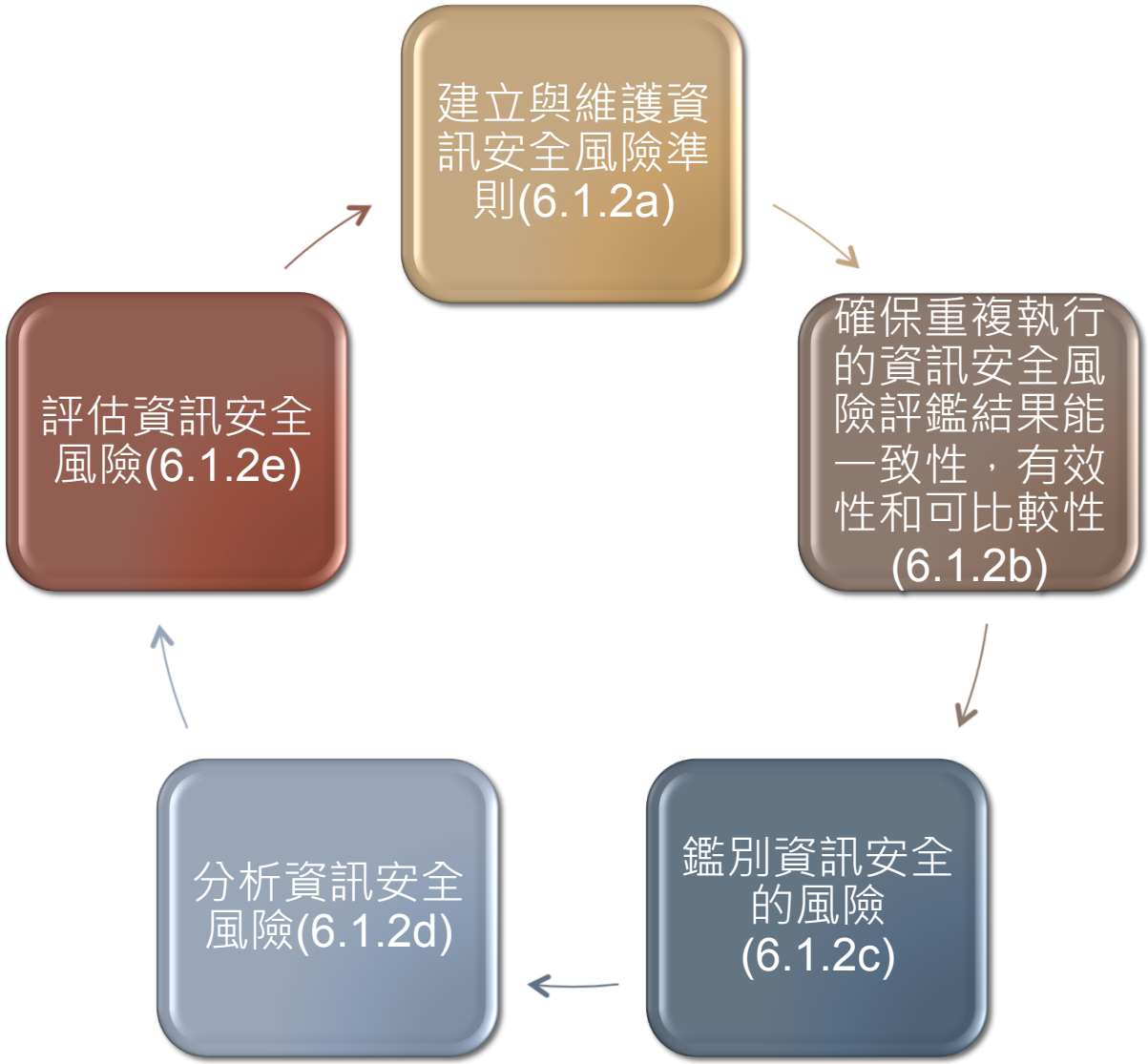
參考：ISO31000:2009

準備和實施風險處理計劃

- 風險處理計劃的目的是記錄如何選擇處理方案將得到執行。
- 在處理計劃中提供的資訊應包括：
  - 選擇處理方案原因，包括可以得到的預期收益
  - 誰負責批准計劃和負責實施計劃
  - 提議的行動
  - 資源需求，包括突發事件
  - 執行措施和限制
  - 報告和監測要求
  - 時機和進度。

參考：ISO31000:2009

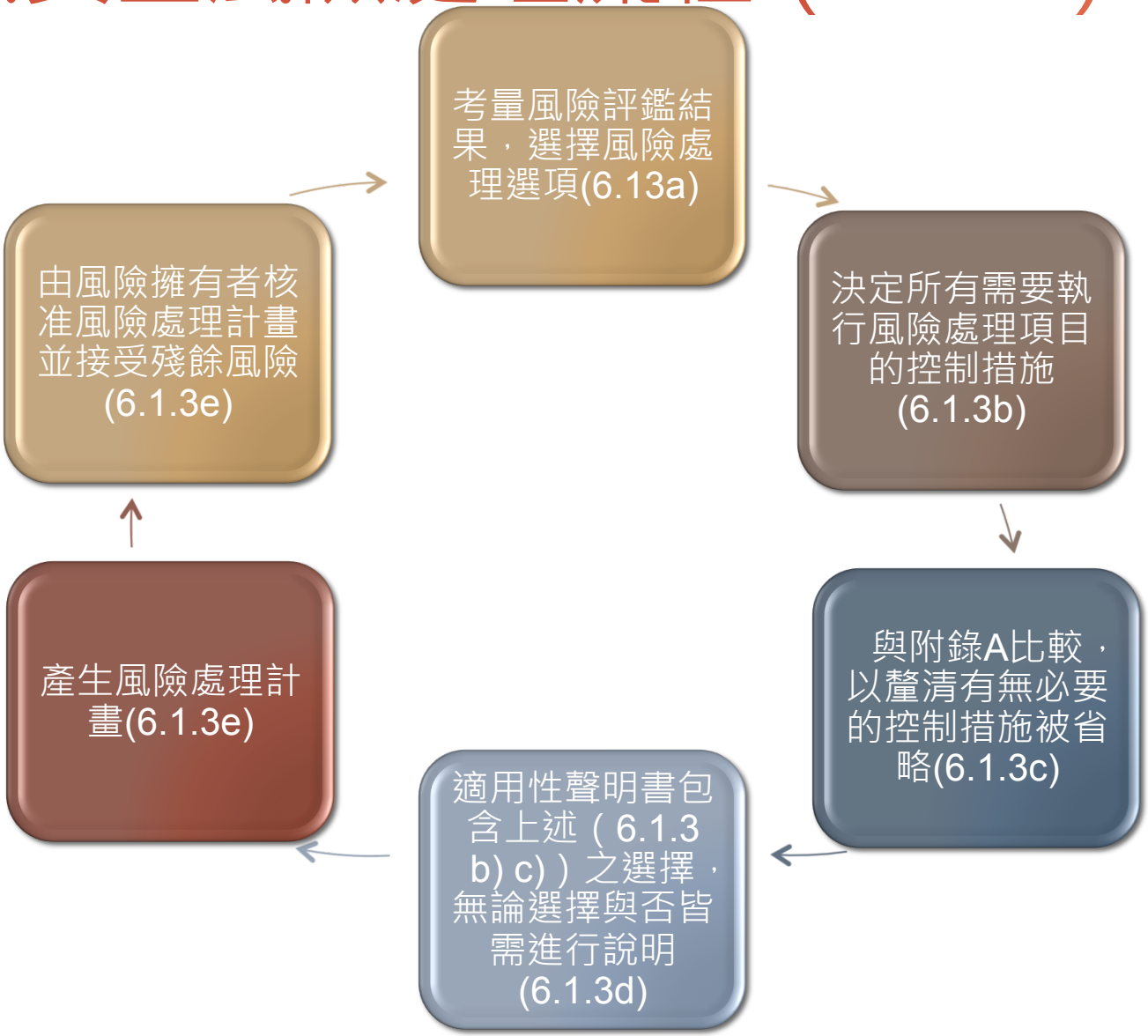
資訊安全風險評鑑流程（6.1.2）



資訊安全風險評鑑

- 6.1.2 資訊安全風險評鑑：
- 組織應定義並建立資訊安全風險評鑑流程
  - A) 建立與維護資訊安全風險準則
    - 1) 風險接受準則
    - 2) 執行資訊安全風險評鑑的準則
  - B) 確保重複執行的資訊安全風險評鑑結果能一致性，有效性和可比較性
  - C) 鑑別資訊安全的風險
    - 1) 採用風險評鑑流程來便是ISMS範圍中CIA的風險
    - 2) 識別風險擁有者
  - D) 分析資訊安全風險
    - 1) 評估潛在（6.1.2 c)1)）後果
    - 2) 評估發生（6.1.2 c)1)）的可能性
    - 3) 決定風險等級
  - E) 評估資訊安全風險
  - 1) 將風險分析結果與準則（6.1.2 a)）做比較
  - 2) 訂定風險處理的優先順序
- 組織應維持有關資訊安全風險評鑑流程的文件化程序

資訊安全風險處理流程（6.1.3）



資訊安全風險處理

- 6.1.3 資訊安全風險處理
- 組織應採用資訊安全風險處理流程(a~f)
  - A) 考量風險評鑑結果，選擇風險處理選項
  - B) 決定所有需要執行風險處理項目的控制措施
  - C) 與附錄A比較，以釐清有無必要的控制措施被省略
  - D) 適用性聲明書包含上述（6.1.3 b) c)）之選擇，無論選擇與否皆需進行說明
  - E) 產生風險處理計畫
  - F) 由風險擁有者核准風險處理計畫並接受殘餘風險
- 組織應維持有關資訊安全風險處理流程的文件化資訊
  - 備註：本標準中的資訊安全風險評鑑和處理流程，應與ISO31000提供的原則與一般性指引相符

本文内容

7.Support支援 <->4.3,5

- 7.支援
- 7.1 資源
  - 組織應決定並提供建立、實行、維護與持續改善ISMS所需的資源
- 7.2 能力
  - A) 決定在影響資訊安全績效控制措施下，員工所必備的能力
  - B) 確保人員在適切的教育、訓練或經驗中具備能力
  - C) 適當時採取措施以獲得必要的能力，並評估該措施的有效性（可回訓）
  - D) 維持適切的文件化資訊成為能力的證據
  - 備註：適用措施可包含如對現有員工的訓練提供、監督與重新指派任務，或對於適任人員的招募與簽約等
- 7.3 認知
- 組織控制下人員認知
  - A) 資訊安全政策
  - B) ISMS有效性及改進其效益的貢獻
  - C) 不遵循ISMS要求的影響（後果）

討論三

內外部溝通要求

7.Support支援 <->4.3,5

- 7.4 溝通
  - 組織應決定有關內外部溝通的需求，包含：5W
  - A) on what to communicate（內部：角色、工作職掌、程序、辦法、法令、法規。外部：資安規範要求、利害相關團體、媒體），
  - B) When to communicate（內部：定時、不定時。外部：簽約前）
  - C) with whom to communicate（內部：高階主管、員工。外部：廠商、利害相關團體、媒體）
  - D) Who shall communicate（內部：分層負責。外部：）
  - E) and the processes by which communication shall be effected哪些影響溝通的流程（會議記錄、公文、跨部門）
- 7.5 文件化資訊（Document procedures, records)
- 7.5.1 概述（組織的ISMS應包含）
  - A) 本標準與組織要求的文件化資訊
  - B) 組織決定ISMS有效性所需的文件化資訊
  - 備註：ISMS文件化資訊範圍，應依據組織而有所不同，根據：
  - 1) 組織規模與其活動力、流程、產品及服務型態
  - 2) 流程與其互動得複雜度
  - 3) 人員能力

7.Support支援 <->4.3,5

- 7.5.2 製作與更新
- 製作與更新文件化資訊時，組織應確保：
  - A) 識別與描述（如：標題、日期、作者或參考標號）
  - B) 格式（如：語言、軟體版本、繪圖）與媒體（如：紙本、電子格式）
  - C) 對適切性與正確性的審查與核准
- 7.5.3 文件化資訊的控制
- ISMS與本標準所要求的文件化資訊應被管控，以確保：
  - A) 所在地點與時間均適合可用
  - B) 適當保護（如：機密性喪失、不當使用或完整性喪失）
- 文件化資訊管控應於可行時進行下列活動：
  - C) 分發、存取、檢索與利用
  - D) 儲存與維護，包含保存的可讀性
  - E) 變更控制（如：版本控制）
  - F) 保存與銷毀
  - 由組織決定規劃與執行ISMS所需的外部文件化資訊，應加以適切的識別與控制
  - 備註：存取表示對文件化資訊僅可閱讀或是可讀寫等授權的決定

8.Operation運作 <->4.2

- 8.運作
- 8.1 運作規劃與控制
- 組織應規劃、實作與控制達成資訊安全要求事項所需的流程與6.1決定實行的行動方案。組織也應執行計畫來達成6.2所決定的資訊安全目標
- 組織應保存必要程度有信心的流程已依計畫執行的文件化資訊
- 組織應控制所規劃的變更並審查非預期變更的結果，當必要時採取行動以減輕任何不利的影響
- 組織應確保委外之流程確定與控管(A.15)
- 8.2 資訊安全風險評鑑
- 組織應定期或於預訂或執行重大變更時，執行風險評鑑並考量6.1.2 a)所建立的準則
- 組織應保存資訊安全風險評鑑結果的文件化資訊
- 8.3 資訊安全風險處理
- 組織應執行資訊安全風險處理計畫
- 組織應保存資訊安全風險處理結果的文件化資訊

練習一

文件化資訊

9.Performance evaluation 績效評估 <->4.2,6,7

- 9.績效評估
- 9.1 監視, 測量, 分析和評估
- 組織應評估資訊安全績效與ISMS的有效性
- 組織應決定（5W）
  - A) What need to be monitored and measured什麼需要監視與量測，包含資訊安全流程和控制措施
  - B) the methods as applicable監視、量測、分析與評估方法於可行時確認其結果有效度

  備註：選擇的方法一產生可以比較與重製結果，以確認其有效
  - C) When the m&m shall be performed何時執行監視與量測,
  - D) Who shall m&m,監視與量測執行人員
  - E) When the result from m&m shall be analyzed and evaluated監視與量測結果分析與評估的時機
  - F) Who shall a&e)分析與評估執行的人員
- 組織應保存作為監視與量測結果證據的適切化文件資訊

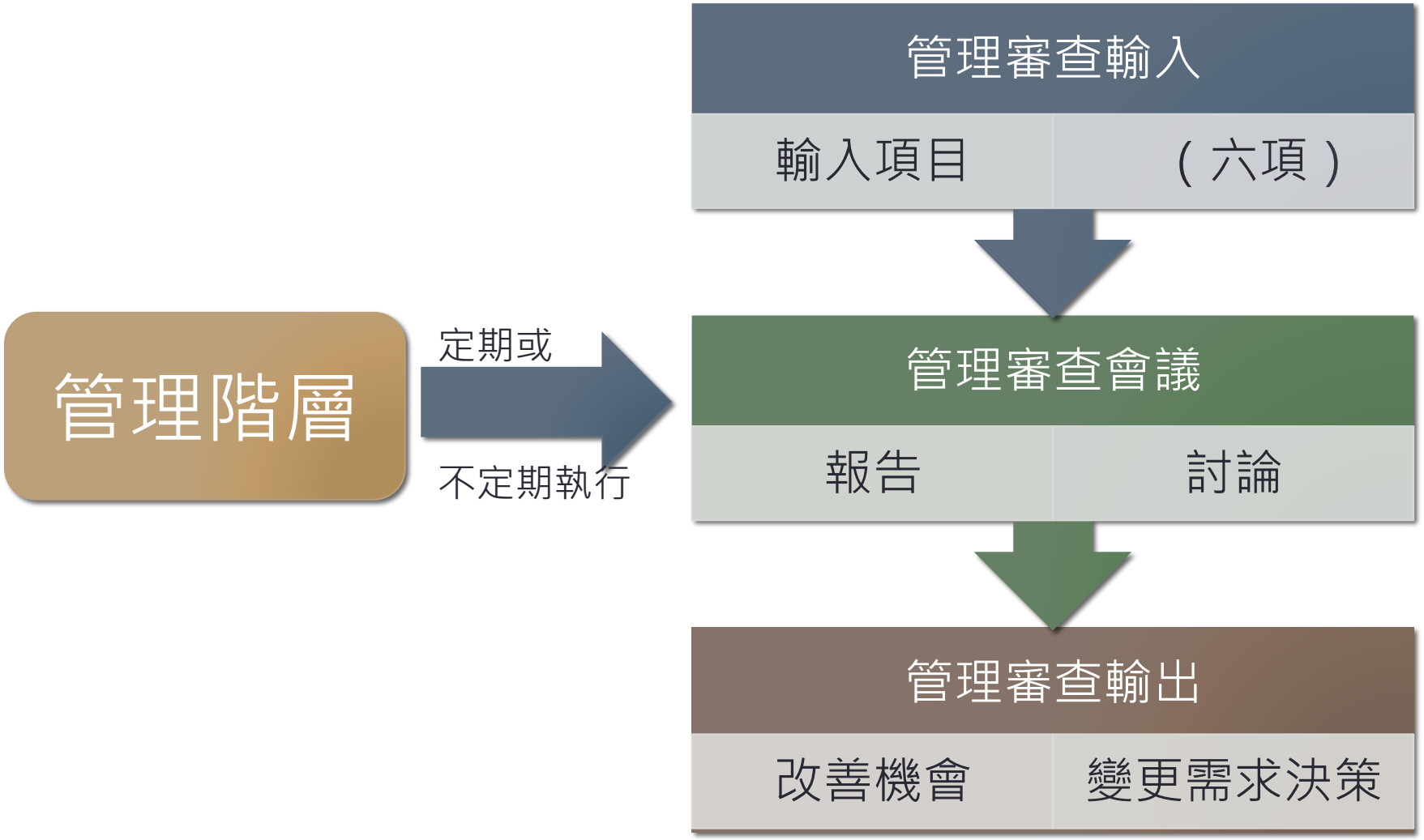
9.Performance evaluation 績效評估 <->4.2,6,7

- 9.2 內部稽核 <-> 6
- 組織應定期執行內部稽核以提供資訊，來確認ISMS是否：
  - A) 符合
    - 1) 組織對ISMS的要求事項
    - 2) 本標準的要求
  - B) 有效實行與維護
- 組織應：
  - C) 規劃、建立、實作與維護稽核計畫（programme(s)），包含頻率、方法、責任、規劃要求事項與報告等。稽核計畫（programme(s)）應涵蓋重要的流程與前次稽核的結果
  - D) 界定稽核準則與稽核範圍
  - E) 稽核員選擇與稽核執行應確保稽核流程的客觀性與公平性
  - F) 確保稽核結果向相關管理單位報告
  - G) 保存作為稽核計畫（programme(s)）與稽核結果證據的文件化資訊

9.Performance evaluation 績效評估 <->4.2,6,7

- 9.3 管理階層審查 <-> 7
- 高階管理階層應定期審查組織ISMS以持續確保適切性、充分性與有效性
- 管理審查應考量：
  - A) 前次管審措施狀態
  - B) ISMS內外部議題的變更
  - C) 資訊安全績效回饋，包含下列趨勢：
    - 1) 不符合事項與矯正措施
    - 2) 監視與量測結果
    - 3) 稽核結果
    - 4) 資訊安全目標符合度
  - D) 利害相關團體回饋
  - E) 風險評鑑結果與風險處理計畫狀態
  - F) 持續改善的機會
- 管理審查的輸出項目應包含ISMS持續改善機會與變更需求的決策
- 組織應保存作為管理審查結果證據的文件化資訊

管理階層審查


管理審查輸入
輸入項目
（六項）
管理階層
定期或
不定期執行
管理審查會議
報告
討論
管理審查輸出
改善機會
變更需求決策

練習二

流程要求，描述個流程的要求

10. Improvement 改善 <->4.2,8

- 10. 改善 <-> 8
- 10.1 不符合事項與矯正措施<-> 8.2
- 不符合事項發生時組織應：
  - A)因應不符合事項，如適用：
    - 1) 採取控制與矯正措施
    - 2) 處理其後果
  - B)評估消除不符合事項原因措施，以使其不再發生的需求：
    - 1) 審查不符合事項
    - 2) 決定不符合事項原因
    - 3) 決定類似的不符合事項是否存在或可能發生
  - C)實作所需的措施
  - D)審查採取措施的有效性
  - E)於需要時對ISMS進行變更
- 矯正措施應切合不符合事項所受到的影響
- 組織應保存文件化資訊以作為下列證據：
  - F) 不符合事項本質與所採取的措施
  - G) 矯正措施的結果
- 10.2 持續改善 <-> 8.1
- 組織應持續改善ISMS的適切性、充分性與有效性

練習三

可量測指標、評估有效性


Q & A……

文件化

- 4.3 ISMS範圍
- 5.2 ISMS政策
- 6.1.2 風險評鑑流程
- 6.1.3 風險處理流程
- 6.1.3 適用性聲明書
- 6.2 資訊安全目標
- 7.2 能力證明
- 8.1 流程依據規劃實行的證據
- 8.2 風險評鑑結果
- 8.3 風險處理結果
- 9.1 監督與量測活動結果的證據
- 9.2 內部稽核方案與稽核結果
- 9.3 管理審查結果
- 10.1 不符合事項與矯正行動成果

流程要求

- 6.1.2 風險評鑑流程
- 6.1.3 風險處理流程
- 8.1 委外流程
- 9.1 稽核流程

可量測指標、評估有效性

- 5.1(f)
- 5.3
- 6.1.1
- 7.2
- 7.3
- 9.1
- 9.2
- 9.3
- 10.1
- 10.2