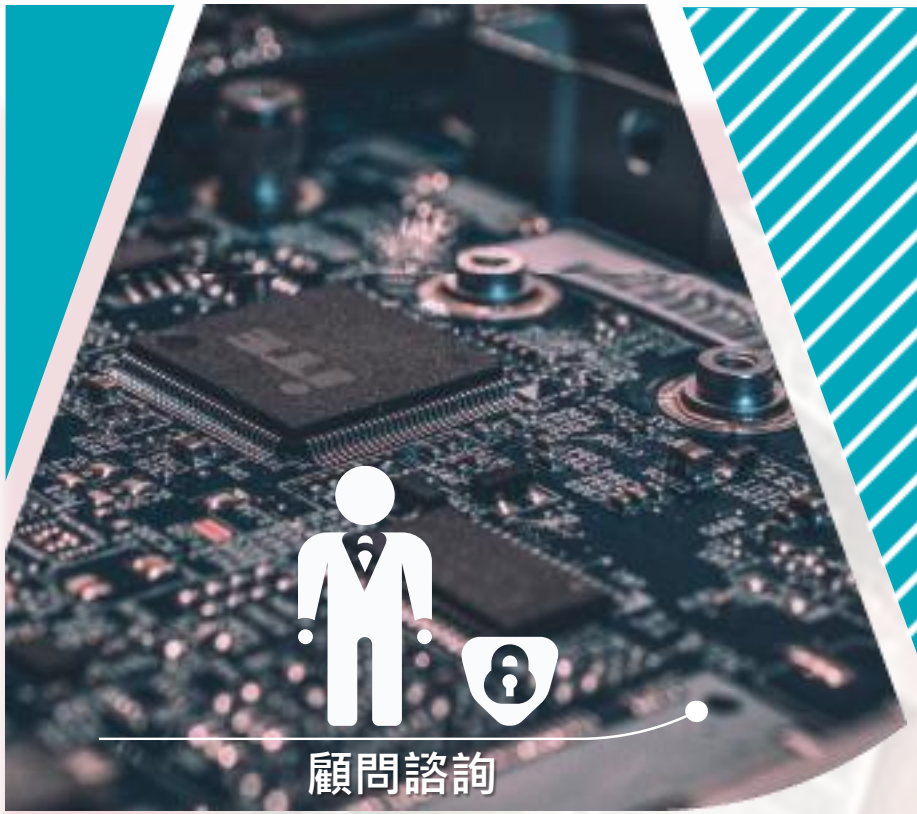


國立臺南大學

113年度內部稽核實務
教育訓練

漢昕科技 楊雯珺

輔導顧問

20240723

BCCS 漢昕科技

資安整備專家

納管對象

- 對人民生活、經濟活動及公眾或**國家安全**有重大影響者
- 分為「公務機關」、「特定非公務機關」各有不同的法遵義務

資安管理法第3條第5款

公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。

資安管理法施行細則第2條

所稱軍事機關，指國防部及其所屬機關（構）、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款及第二項規定之機關。

公務機關

- 中央與地方機關(構)(含學校)
- 公法人(含行政法人)
- 不包括**軍事機關**及**情報機關**

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 社會捐助之財團法人

資安等級

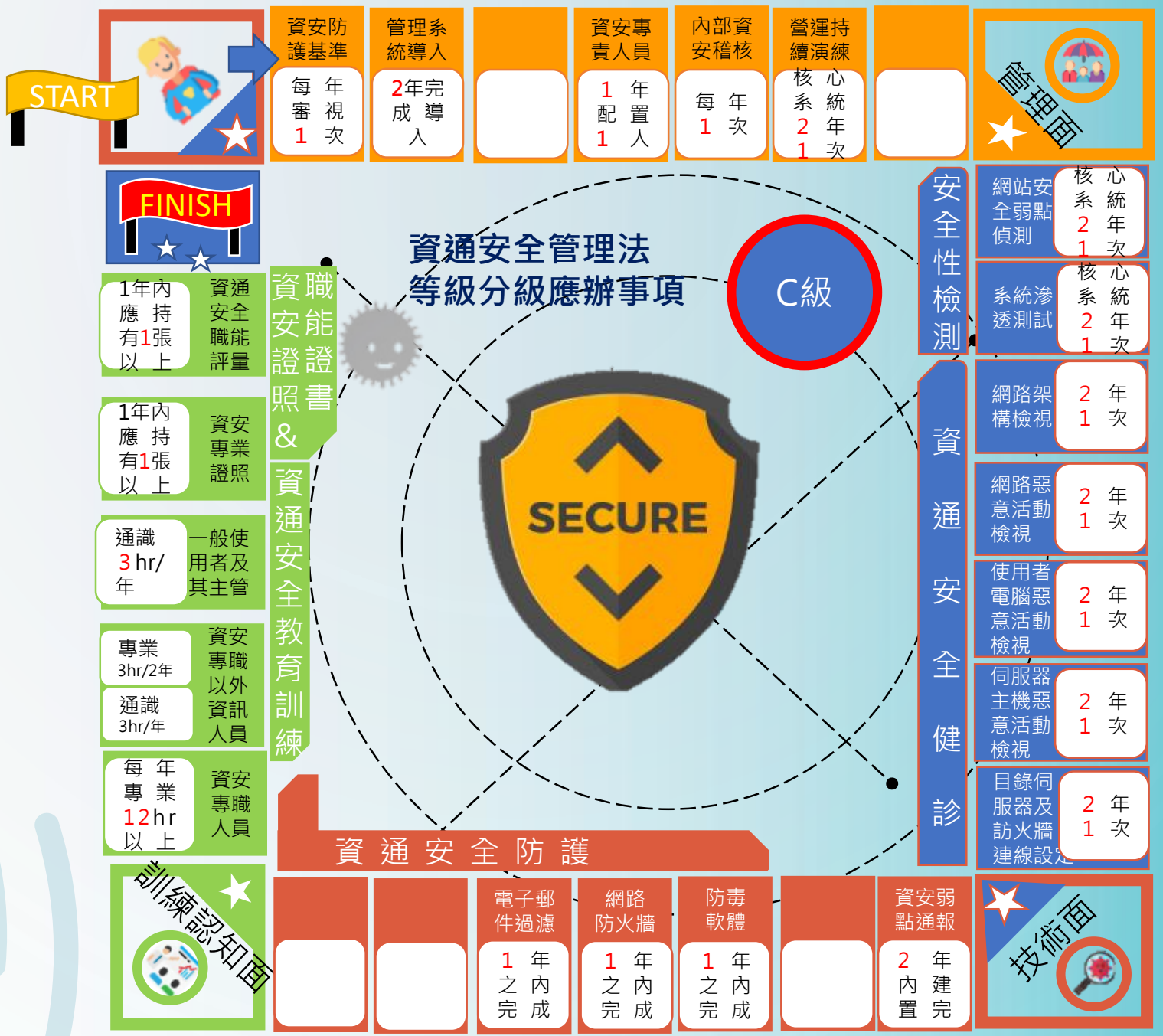
資通安全責任等級為何？

START

- 業務涉及國家機密？ 是 → A級
- 否 → 業務涉及外交、國防或國土安全？ 是 → A級
- 否 → 業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運？ 是 → A級
- 否 → 屬公務機關且業務涉及全國性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項？ 是 → A級
- 否 → 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響？ 是 → A級
- 否 → 屬公立醫學中心？ 是 → A級
- 否 → 業務涉及公務機關捐助或研發之敏感科學技術資訊之安全維護及管理？ 是 → B級
- 否 → 業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運？ 是 → B級
- 否 → 業務涉及區域性或地區性民眾個人資料檔案之持有？ 是 → B級
- 否 → 屬公務機關且業務涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項？ 是 → B級
- 否 → 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響？ 是 → B級
- 否 → 屬公立區域醫院或地區醫院？ 是 → B級
- 否 → 各機關維運自行或委外開發之資通系統者？ 是 → C級
- 否 → 各機關自行辦理資通業務，未維運自行或委外開發之資通系統？ 是 → D級
- 否 → 無資通系統且未提供資通服務？ 是 → E級
- 否 → 屬公務機關，且其全部資通業務由其上級或監督機關兼辦或代管？ 是 → E級
- 否 → 屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關兼辦或代管？ 是 → E級

BCCS 漢昕科技

等級應辦事項



大富翁.png

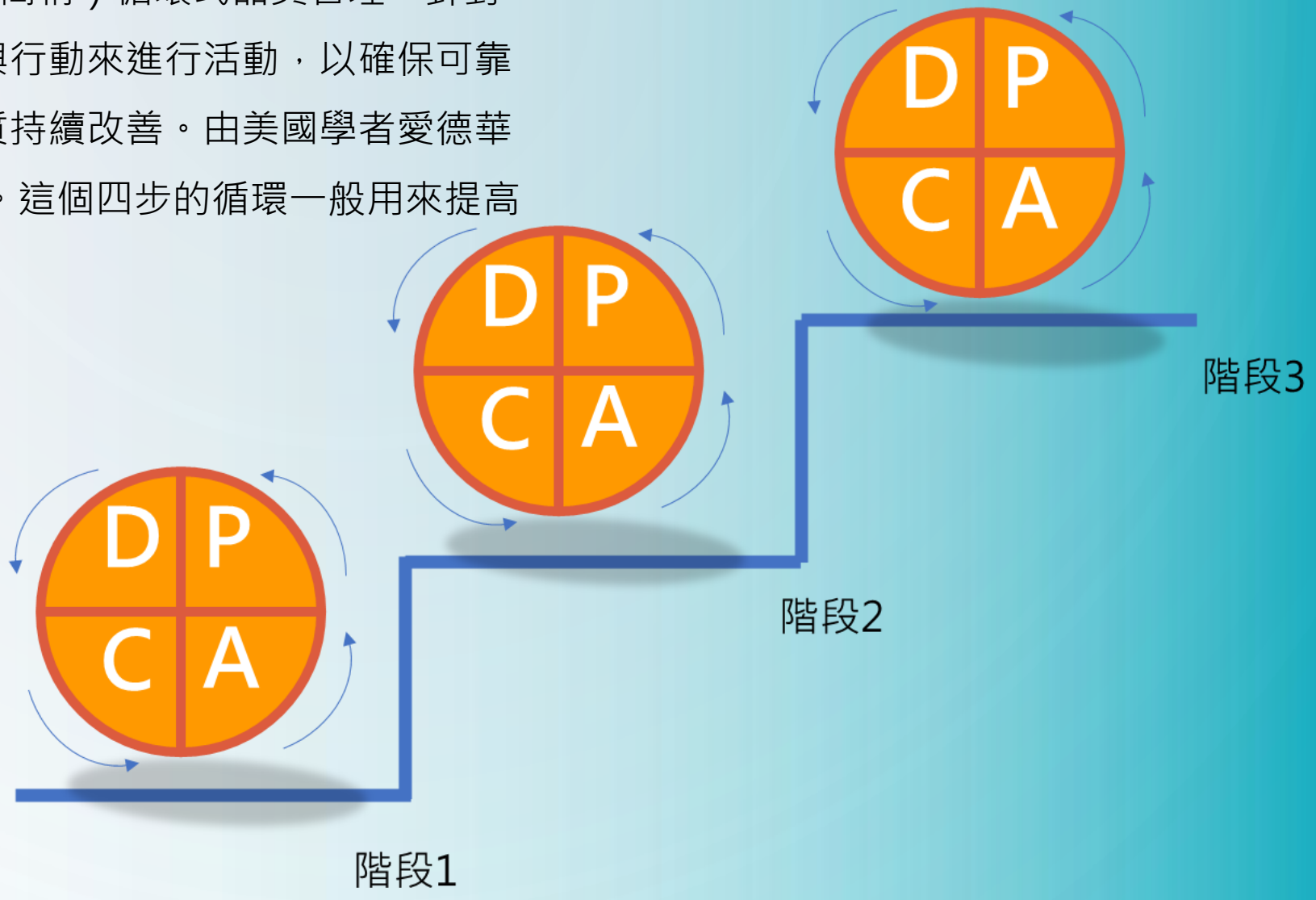
BCCS 漢昕科技

為何要做內部稽核？

- ✓ 為了確保組織對管理資訊安全的作法持續合適、適切且有效，內部稽核是必要的。
- ✓ 內部稽核有助於管理階層規劃並啟動定期獨立審查，評估改善機會以及評估變更資訊安全作法的需要。
- ✓ 透過獨立於受審查範圍之人員執行審查，確保審查的客觀性和獨立性，並確保審查人員具備適切的能力。
- ✓ 最終，內部稽核的結果應向管理階層和最高管理層報告，並維護相關紀錄。

PDCA循環

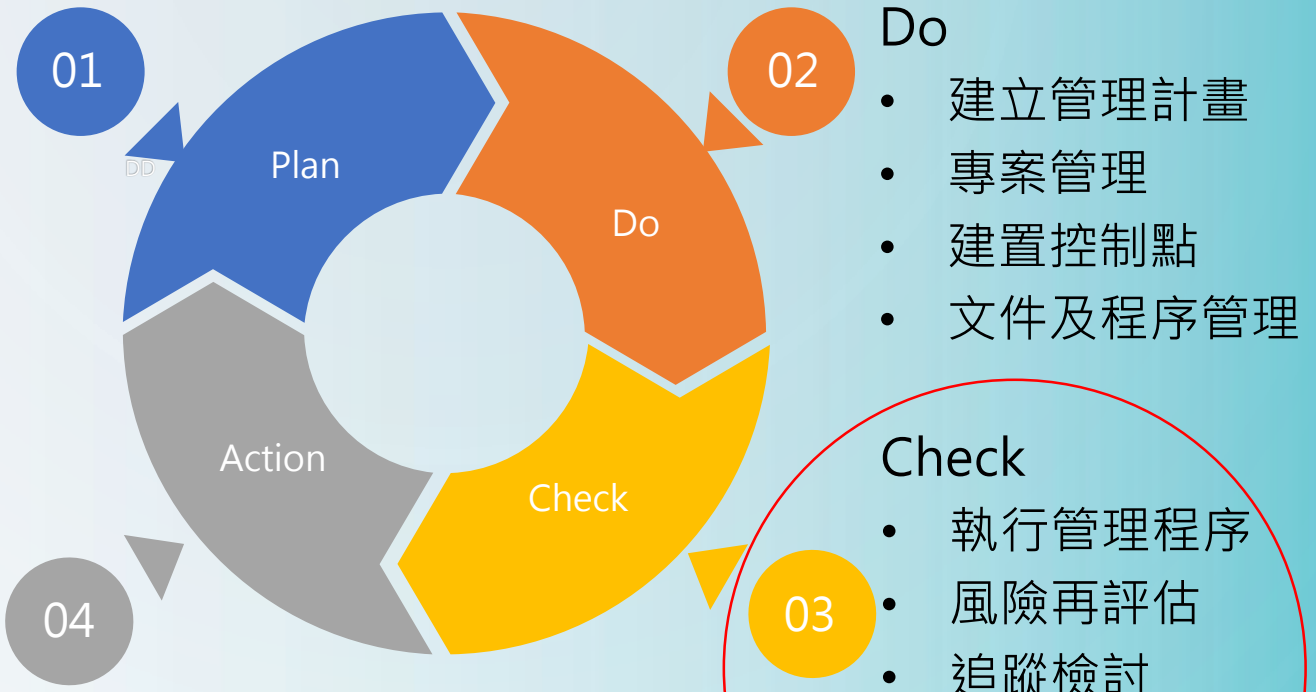
PDCA（Plan-Do-Check-Act的簡稱）循環式品質管理，針對品質工作按規劃、執行、查核與行動來進行活動，以確保可靠度目標之達成，並進而促使品質持續改善。由美國學者愛德華茲·戴明提出，因此也稱戴明環。這個四步的循環一般用來提高產品品質和改善產品生產過程。



ISO / IEC 27001:2022循環

Plan
- 定義ISMS範圍
- 風險評估
- 確認控制目標
- 選擇控制點

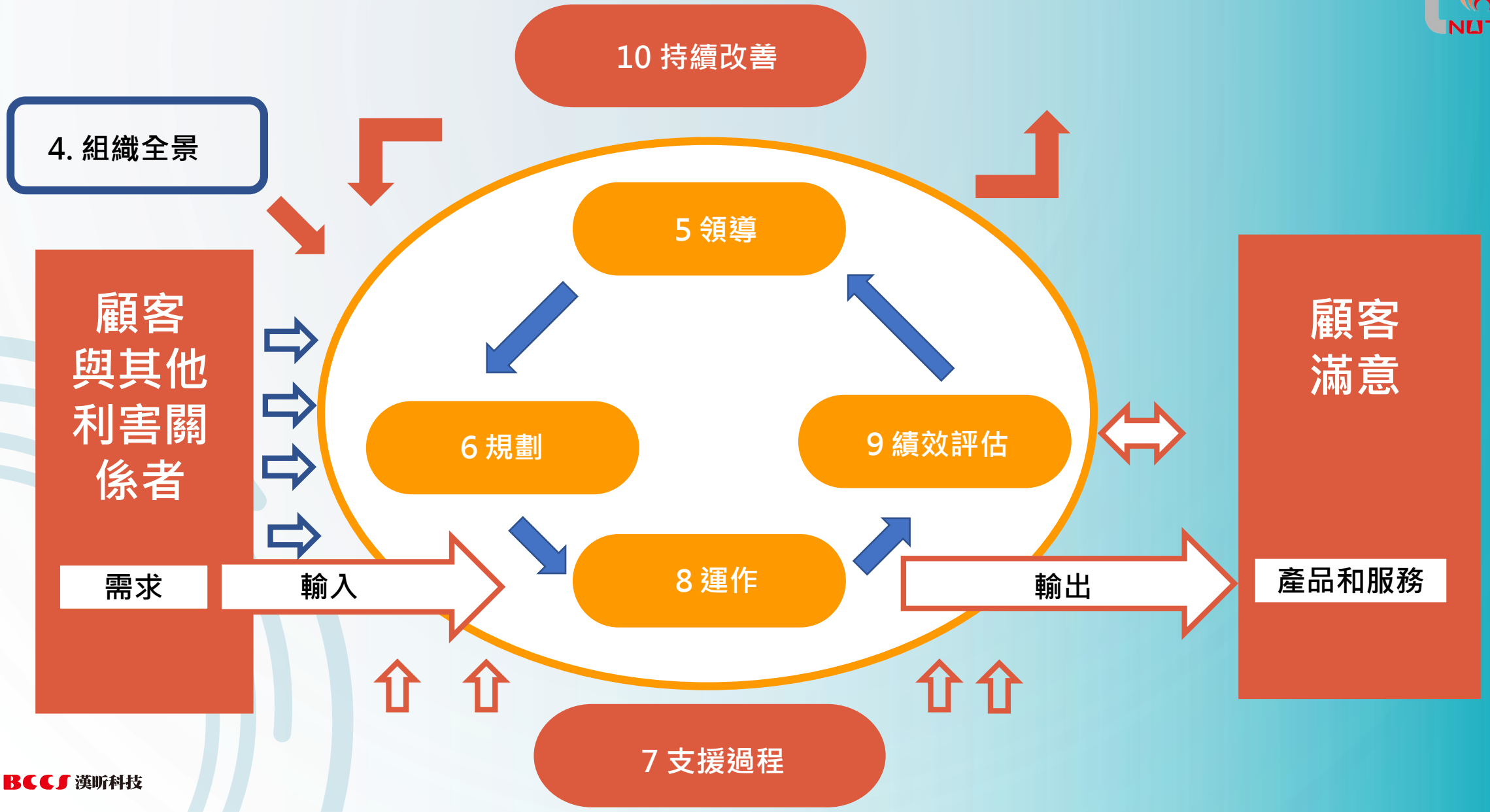
Action
- 執行適當修正
- 實施成果目標
- 確認目標達成
- 持續改善



Do
- 建立管理計畫
- 專案管理
- 建置控制點
- 文件及程序管理

Check
- 執行管理程序
- 風險再評估
- 追蹤檢討
- 定期稽核
- 績效評估

ISO / IEC 27001:2022架構



大綱

資訊管理系統稽核簡介

- 資訊系統稽核目的
- 資訊系統稽核說明

資訊管理系統稽核實務流程

- 本次稽核計畫
- 稽核重點與應關注事項

課後測驗

資訊管理系統
稽核簡介

資訊系統稽核目的

資訊系統稽核說明

稽核目的➔

控制風險

企業風險管理範疇

摘自於UMC網頁

稽核的定義

稽核：為一項具有獨立性與系統性的查核，以辨別作業活動及相關結果是否符合原先計畫內容，以及這些計畫內容是否有效地實施，且適宜於達成目標。

稽核的理由(為確保.....)

01 制定的流程符合標準或規範

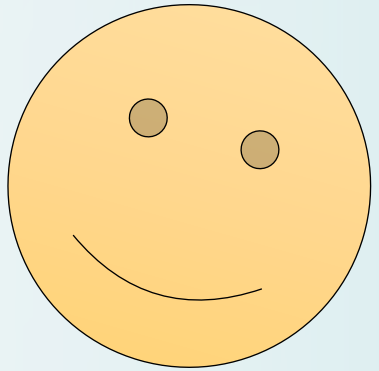
02 執行流程是符合標準或規範的

03 制定的流程是有效的

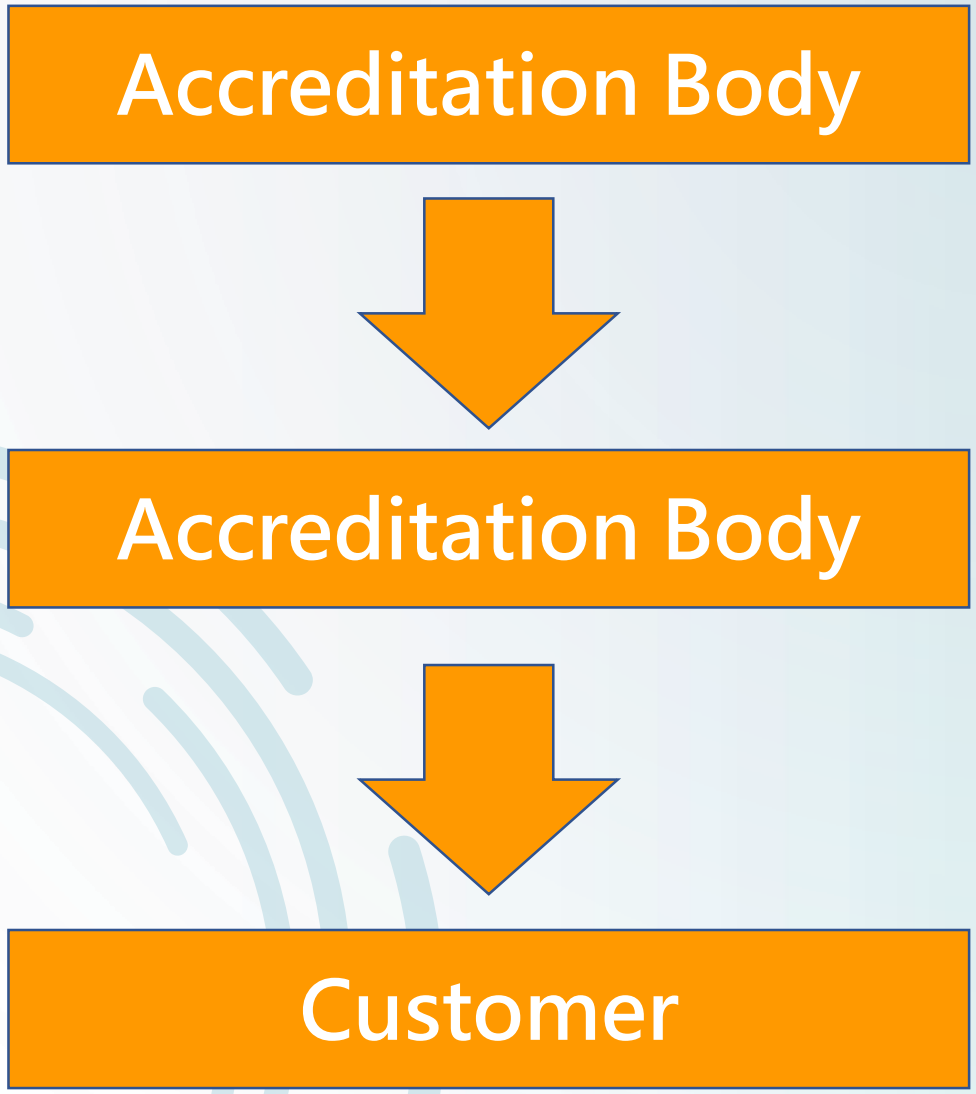
04 執行的成果是有品質的

customer

satisfaction



Management System Certification Scheme



ISO17021 符合性評鑑

Conformity assessment -- Requirements for bodies providing audit and certification of management systems

ISO27006針對審查及認證資訊安全管理系統的實體之要求

Requirements for bodies providing audit and certification of information security management systems

ISO19011 稽核準則

Management system standards, e.g.
ISO 9000;
ISO/IEC 27001 ;
ISO/IEC 20000-1 ;
ISO 22301 ;
BS 10012...

ISO27001系統管理

稽核參考標準為~~

ISO19011

ISO 19011:2018

稽核
計畫

稽核
執行

稽核報告
與
矯正措施

稽核後續活
動的實施

ISO 9001:2015 Standard

Quality Concepts and Principle

ISO 19011 品質與環境管理系統稽核指導綱要

此國際標準提供**管理稽核計畫的指引**，以執行**品質與環境**

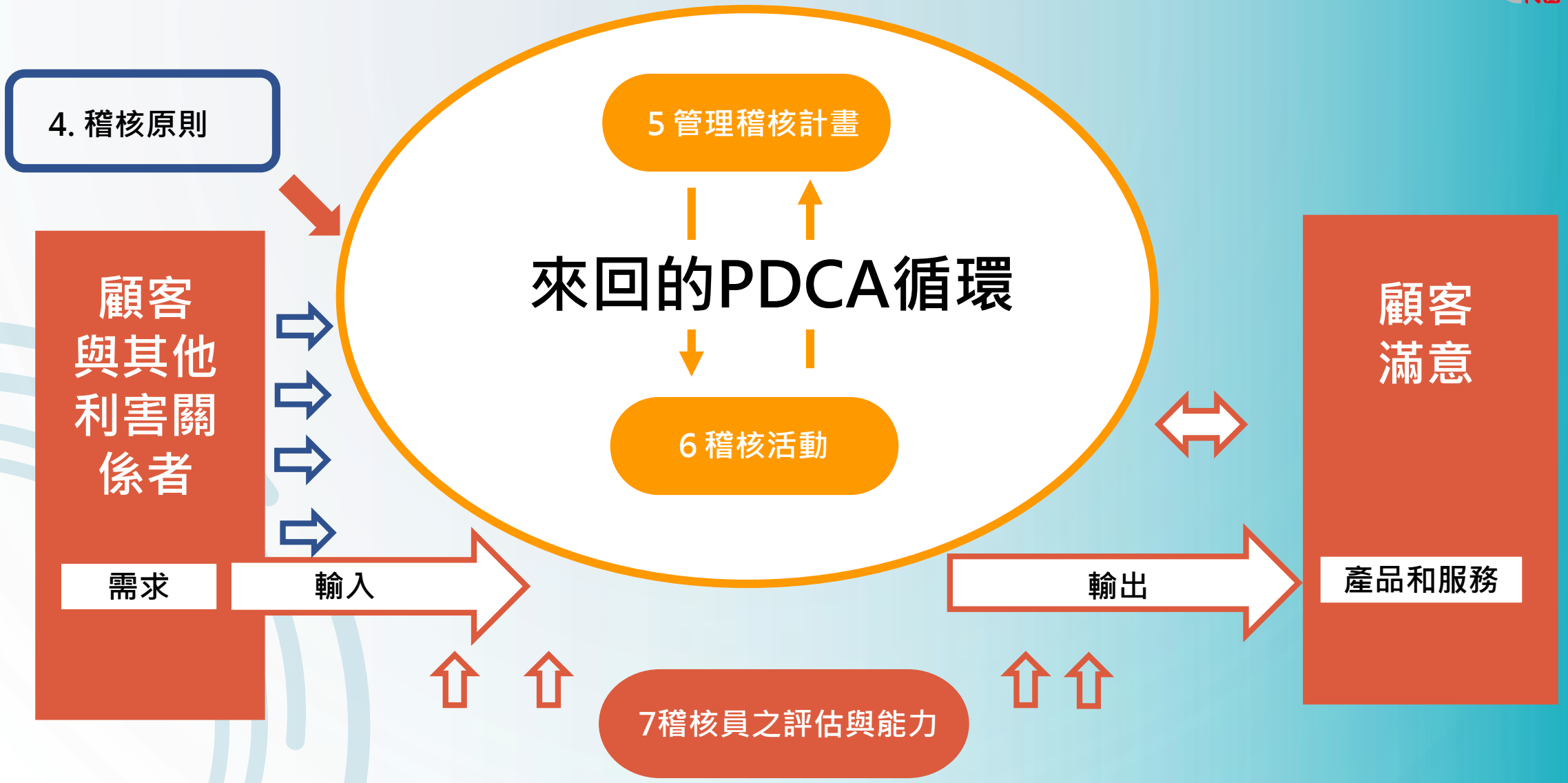
管理系統內部或外部稽核，以及**對稽核員的能力與評鑑** 。

藉由PDCA

稽核

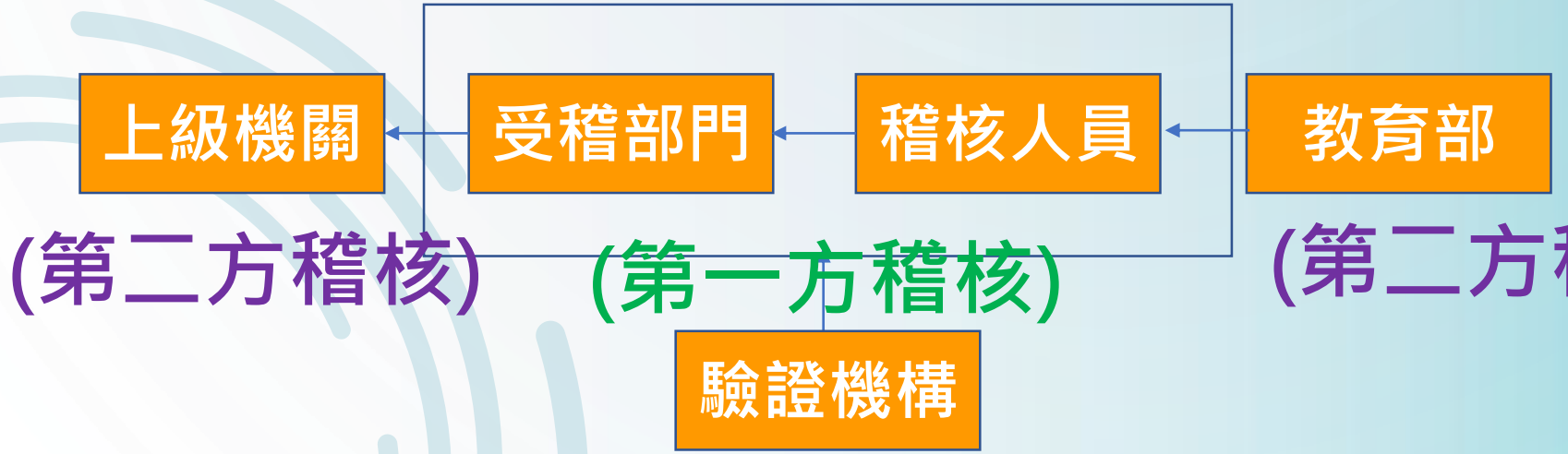
ISO 19011 三大面向

ISO / IEC 19011:2018架構



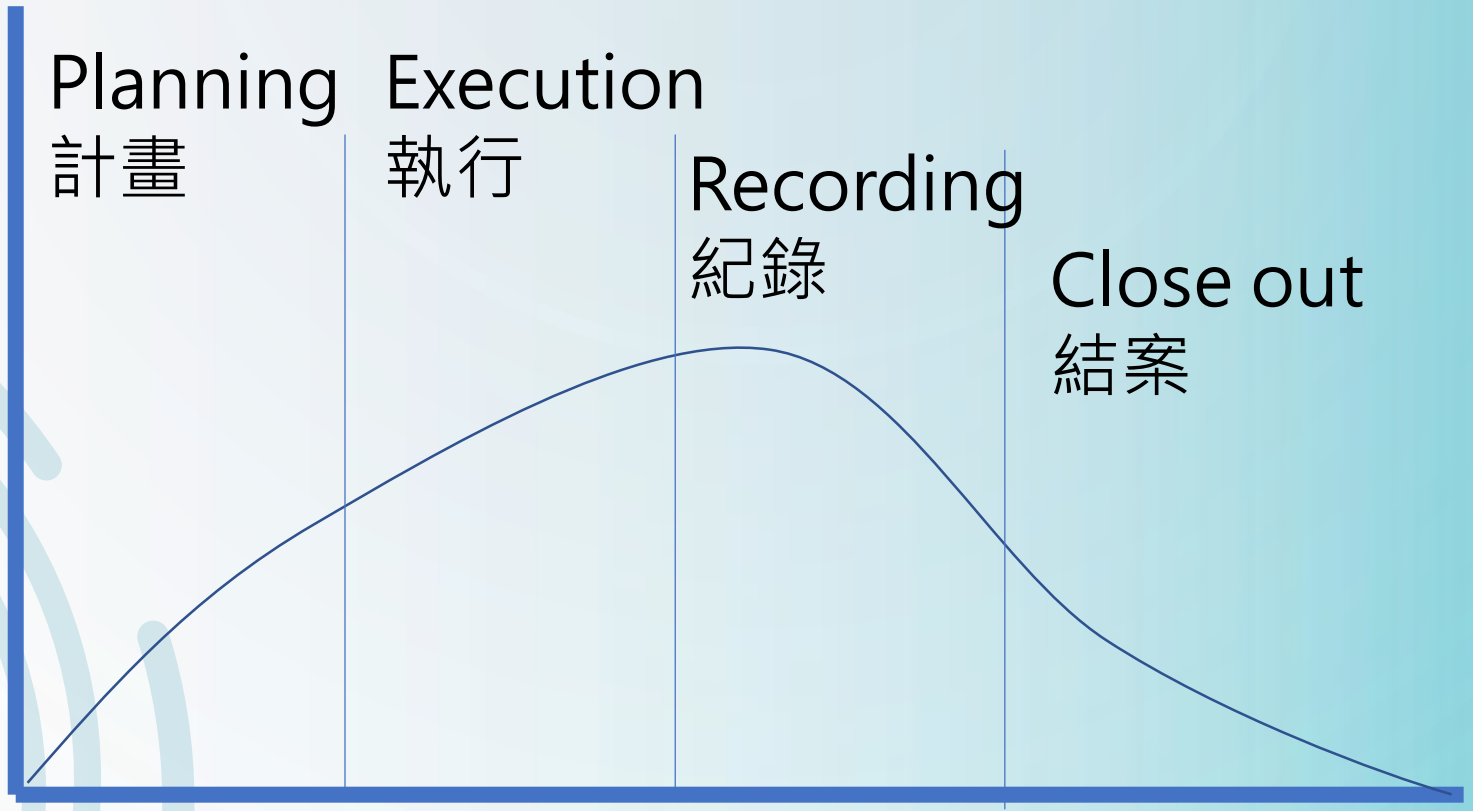
稽核類型

第一方稽核	第二方稽核	第三方稽核
• 內部稽核	• 上級機關 • 教育部	• 驗證公司 • SGS、BSI…



稽核之Life Cycle

- 稽核的生命週期通常稱為P.E.R.C



稽核角色

- ” 稽核” 稱職的角色扮演為何
- “顧問” 與 “稽核”

主導稽核員（ Lead Auditor ）

一個被指定管理稽核的稽核員。

Accountable

稽核員（ Auditor ）

一個有資格去執行稽核的人。

Responsible

被稽核方（ Auditee ）

組織中被稽核的人。

資訊管理系統
稽核實務流程

本次

稽核計畫

稽核重點與應

關注事項

稽核計畫

- 本次稽核安排於，7月29~30日與8月13~14日
- 稽核涵蓋面向：

Microsoft Word 文件

Microsoft Word 文件

稽核內容

- 本次稽核安排於，7月29~30日與8月13~14日

Microsoft Word 文件

國立臺南大學－資安暨個資稽核查檢表

適用範圍：本校113年資安暨個資稽核各行政及教學單位

單位名稱(全銜)：＿＿＿＿＿＿＿＿填表人員：＿＿＿＿＿＿＿＿填表日期：＿＿年＿＿月＿＿日

編號	查檢項目	查檢說明	自評結果	查檢結果
1	資訊資產暨個人資料風險評鑑作業(本文柒)	1. 個資處理人是否就已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險及可能面臨的風險等級？ 2. 資產管理人是否就資訊資產之分析評估可能產生之風險及可能面臨的風險等級？	□是 □否	□符合 □不符合
2	資訊資產暨個人資料盤點作業(A.8.1.1)	1. 是否已識別電資訊及資訊處理設施相關聯之資產，製作資訊資產之清冊，且每年至少清查一次所保有之資訊資產現況。 2. 是否已確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍及個人資料留存於單位之期間，且每年至少清查一次所保有之個人資料現況。	□是 □否	□符合 □不符合
3	已完成電腦作業系統帳號密碼設定(A.9.4.2)	1. 應設定登入密碼(不可設為自動登入)，作業系統重新開機查看是否需要輸入密碼。 2. 至少每 6 個月更換一次密碼。 3. 密碼長度至少 8 碼。 4. 密碼應包含大小寫字母、數字、符號。	□是 □否	□符合 □不符合
4	已完成設定螢幕保護裝置，並啟動密碼設定(A.11.2.9)	1. 設定螢幕保護裝置 15 分鐘以內，並勾選繼續執行後，顯示登入畫面。 2. 離開座位時，應將電腦鎖定及設定螢幕保護裝置，並啟動密碼以保護電腦資料安全。	□是 □否	□符合 □不符合
5	無未授權軟體或來路不明軟體(A.12.2.1)	1. 禁止使用非本校購買授權使用商用軟體。 2. 禁止使用遊戲影音等來路不明軟體。 3. 如有發現來路不明或未授權檔案，請移除。	□是 □否	□符合 □不符合
6	開啟系統或軟體自動更新功能(A.12.2.1)	應配合進行系統或軟體(例如 Windows、Java、Flash Player、Adobe Reader、7zip 等)更新，修補漏洞，保持更新至最新狀態，勿關閉系統自動更新程式。	□是 □否	□符合 □不符合
7	已安裝防毒軟體並更新病毒碼(A.12.2.1)	1. 檢查電腦是否有安裝本校購買之正版防毒軟體並更新病毒碼至最新。 2. 使用外來檔案，應先掃毒，請勿任意移除或關閉防毒軟體。	□是 □否	□符合 □不符合
8	郵件軟體安全管理(A.12.6.2)	1. 關閉郵件軟體中所有資料夾郵件預覽功能。 2. 開啟起電子郵件純文字模式。 3. 不開啟或轉寄來路不明的電子郵件及其附件檔案或連結。	□是 □否	□符合 □不符合

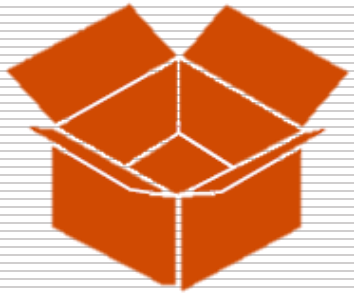
你看到的只是冰山一角?

稽核是以【抽樣方式】來確認落實度

稽核方式

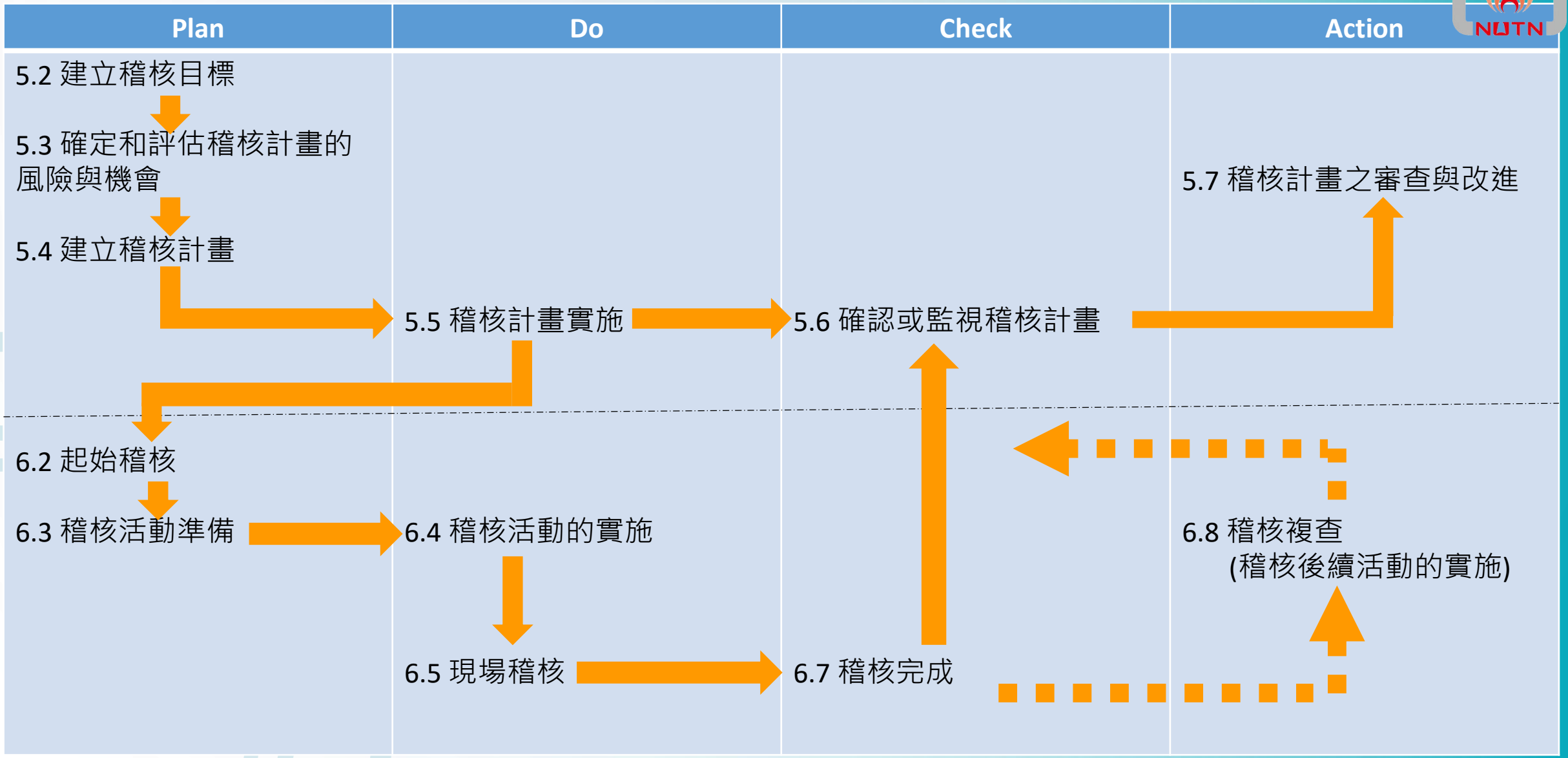
- 訪談
- 觀察
- 審查文件
- 審查紀錄
- 抽樣

收集客觀證據



對資訊安全管理系統的狀態和有效性做出綜合判斷

稽核管理的流程


Plan
Do
Check
Action
5.2 建立稽核目標
5.3 確定和評估稽核計畫的風險與機會
5.4 建立稽核計畫
5.5 稽核計畫實施
5.6 確認或監視稽核計畫
5.7 稽核計畫之審查與改進
6.2 起始稽核
6.3 稽核活動準備
6.4 稽核活動的實施
6.5 現場稽核
6.7 稽核完成
6.8 稽核複查
(稽核後續活動的實施)

稽核計畫-稽核說明

依據	適法性-法律授權
對象	其他四院及其地方政府
類型	一般稽核與專案查核
目的	依據資安維護計畫架構

一般稽核

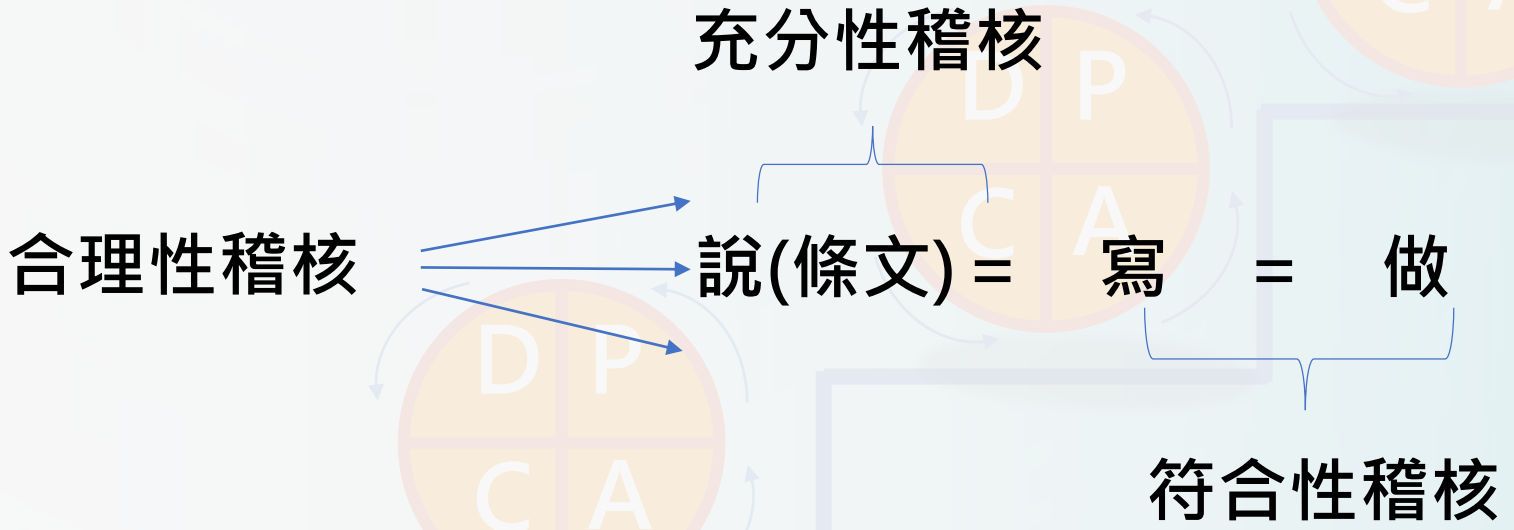
- 公務機關
  - 行政院各部會處署
- 特定非公務機關
  - 關鍵基礎設施提供者
  - 公營事業
  - 政府捐助之財團法人

專案查核

- 資料庫查核
- 資安事件
- 教育部稽核

稽核方向

- 充分性
- 符合性
- 合理性



稽核方式-訪談

目的

- 了解實際作業流程與控制點
- 確認受稽核單位人員熟知作業流程、控制點與書面一致
- 確認受稽核單位人員是否了解發生的風險

稽核重點

- 詢問同仁是否了解資安政策
- 詢問同仁是否了解組織內資訊安全相關組織
- 思考同仁的作業內容是否造成資安的風險

稽核過程形式

- 請受稽單位提供相關文件（程序書、作業手冊及表單等）以證明其所敘述
- 採用開放式問題
- 發覺不一致的資訊，例如：同一控制但不同單位說法不一

稽核方式-觀察

目的

- 瞭解正式作業流程與控制點
- 檢視環境
- 現場查核受稽單位同仁實際執行情形
- 確認受稽核單位同仁是否實依規範執行相關控制作業

稽核重點

- 觀察受稽核範圍之實體環境
- 觀察系統畫面
- 觀察受稽核人員之作業方式、流程及反應

稽核過程形式

- 觀察受稽核單位之辦公區域、同仁作業情形
- 觀察其他同仁行為及態度
- 不一定依照計畫規劃的路線或執行計畫規劃的流程

稽核方式-審查文件

目的

- 確認是否有正式文件制度供所相關單位同仁遵循
- 瞭解正式作業流程與規範
- 確認作業流程與控制點是否適當設定
- 確認受稽核單位同仁是否實依規範執行相關控制作業

稽核重點

- 審查部內正式核准並公布之政策、制度及規範
- 審查部內規範之標準作業程序
- 審查紙本及電子表單、紀錄

稽核過程形式

- 請受稽核單位人員提供相關文件（程序書、作業手冊及表單等）以證明其所敘述
- 取得內部政策、規範及標準等正式文件的最新版本，以比對稽核單位之作業流程
- 稽核人員以現場即時取得之文件為主要依據

稽核方式-審查紀錄

目的

- 確認相關單位同仁是否遵循內部規範制度備存紀錄
- 確認作業流程、控制點是否與紀錄相符
- 確認受稽核單位同仁是否實依規範留存相關控制紀錄

稽核重點

- 審查中心政策及制度，於實際作業程序行時是否有依規範留存紀錄
- 審查紙本及電子表單、紀錄

稽核過程形式

- 請受稽核單位人員提供相關文件（程序書、作業手冊及表單等）以證明其所敘述
- 取得內部政策、規範及標準等正式文件的最新版本，以比對稽核單位之作業流程
- 稽核人員以現場即時取得之文件為主要依據

稽核方式-抽樣

目的

- 確認相關單位同仁是否遵循內部規範制度備存紀錄
- 確認作業流程、控制點是否與紀錄相符
- 確認受稽核單位同仁是否實依規範留存相關控制紀錄

稽核重點

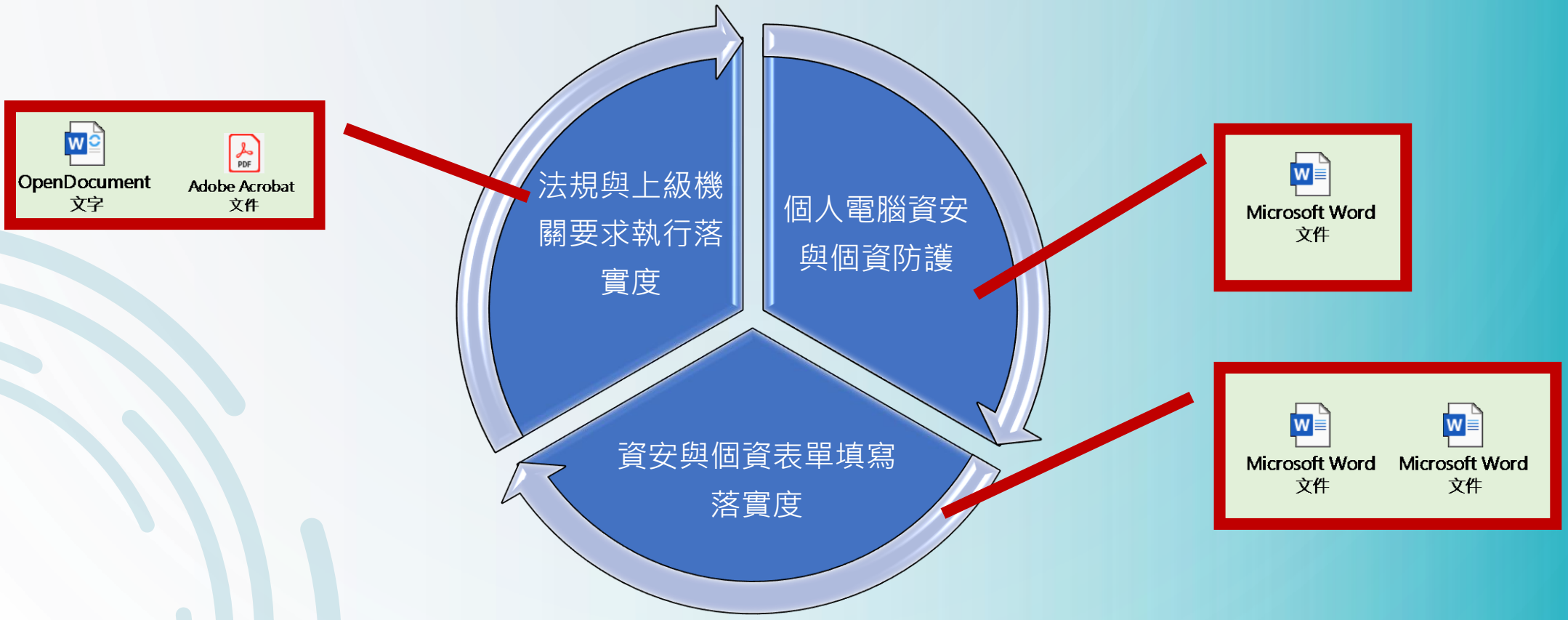
- 抽查文件與紀錄
- 抽查實際作業程序中或所留存之紀錄
- 抽查已填寫之紙本電子表單與紀錄

稽核過程形式

- 請受稽核單位人員提供相關文件（程序書、作業手冊及表單等）以證明其所敘述
- 取得部內政策、規範及標準等正式文件的最新版本，以比對稽核單位之作業流程
- 稽核人員以現場即時取得之文件為主要依據

稽核計畫

- 本次稽核安排於，7月29~30日與8月13~14日
- 稽核涵蓋面向：



課後測驗

https://forms.gle/BLWbFgr8PCcuRaox6

問題與討論