內部稽核心得分享

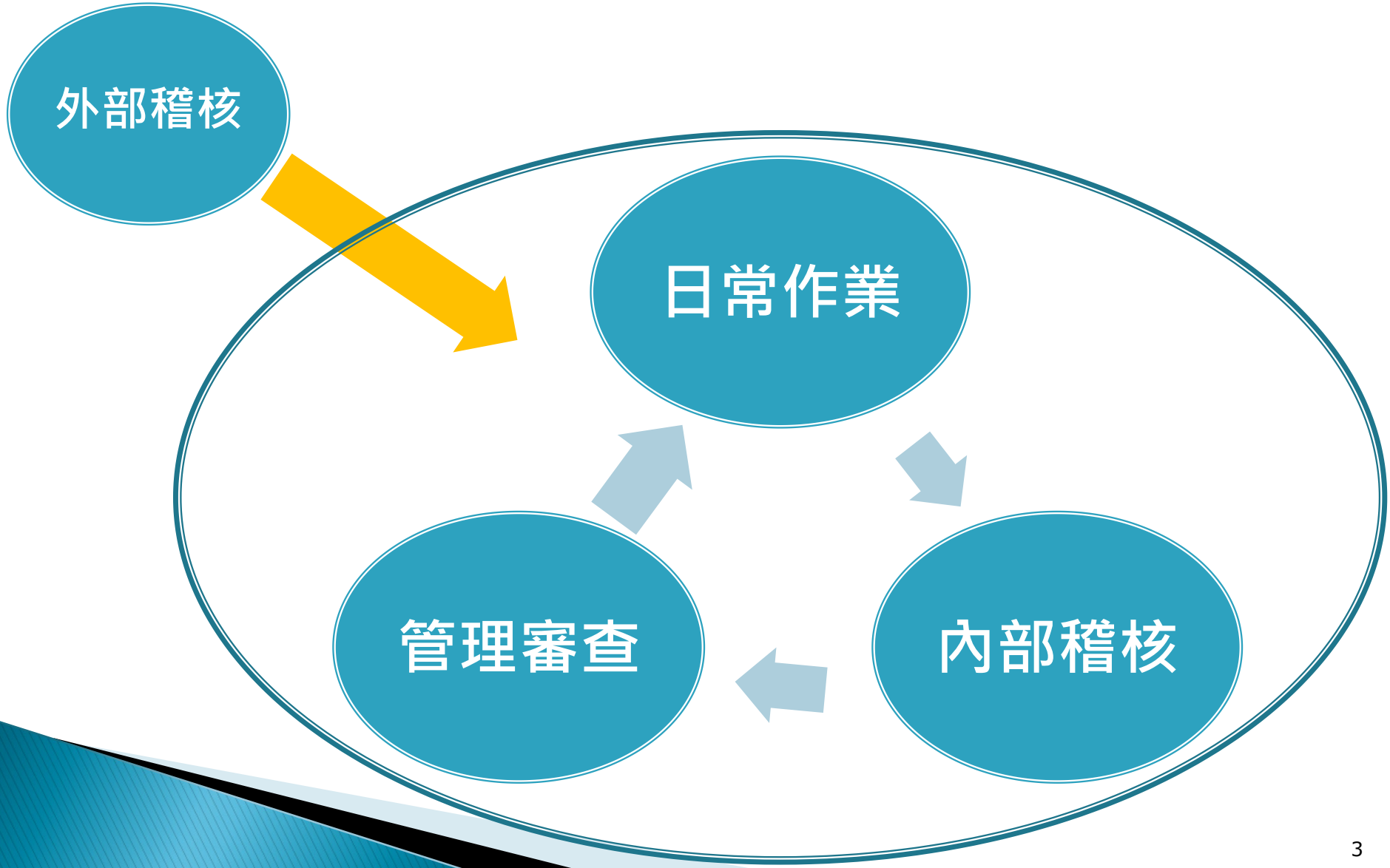
淡江大學 資訊處 教學支援組 組長
林東毅

- 本文件建議印表方式:
雙面列印、每面印4頁,本文件可使用省碳模式列印,
- 請愛惜地球資源,盡量不要印表

驗證標準相關經歷

- ISO27001:2013(資訊安全管理系統)(ISMS)
  轉版、內稽
- ISO20000-1:2011(資訊服務管理系統)(SMS)
  部門導入、內稽、轉版
- BS10012:2017(個人資料管理系統)(PIMS)

ISO27001、BS10012作業循環



稽核目的

- 查核組織PIMS對標準(BS10012)的符合性
- 查核管控程序落實程度與管理成效
- 協助發現缺失
- 提供改善建議
- 達成控制風險、管理品質改善的目的

稽核作業程序

- 確認稽核目標及範圍
- 確認稽核方法/人員訪談/抽樣測試/實地觀察
- 規劃稽核計劃/確認風險所在
- 執行稽核/完成工作底稿
- 討論/填寫稽核報告

內部稽核心得1

- 內部稽核的重點是協助改善相關的管理機制(PIMS)，而不是找缺失，認知錯誤容易造成稽核立場對立
- 稽核雙方一定要建立較高的信任度,才有利於稽核進行
- 內部稽核比外部稽核還重要
- 管理機制要規範的有彈性、易執行、易修正，也要考慮人性特質，才容易落實
- 落實作業程序比應付稽核輕鬆

內部稽核心得2

- 導入PIMS 確實可以改善組織的管理機制(例如:SOP落實與建立、備援機制增強、服務品質改善…)
- 取得驗證通過，不代表組織的管理機制是絕對的安全或制度良好，管理機制需要組織自行持續改善
- 透過驗證機制運作，可以讓管理機制改善的更好、更快

內部稽核心得3

- 缺失會因為環境的改變而產生，面對缺失時，不要過度反彈，單位主管也不必過度責難，應該共同找出改善方法，以免妨礙管理機制的改善
- 導入過多標準會造成組織的成本增加效率降低，應適時的整併作業，包括表單、文件、作業程序…等
- 導入ISO要成功，全員需配合組織及流程變革

內部稽核心得4

- 資訊安全、服務管理的要求應視狀況分等級，不能無限要求，更要了解高階管理階層的想法與組織的難處，給予配合調整
- PIMS會因為PDCA的循環而一直改善與改變，不要視別人的建議與修正(包括文件、管理流程)是對自己尊嚴與職權的挑戰
- 人都犯錯，但求不二過
- 真正完全落實個資保護—真不容易

與外稽人員的應對之道

- 不要質疑外稽人員的提問與專業
- 不要回答過多問題外的內容
- 外稽人員很容易在日常生活中套話, 要注意
- 多讚美對方可開啟雙方溝通管道
- 發現缺失時, 表達願意立即改善的誠意

與外稽人員的應對之道

- 若外稽人員的改善建議很難達成, 要虛心溝通讓其了解
- 內稽人員應盡量陪同外稽人員，以學習稽核技巧

優秀稽核員的典範

- 能使受稽方心甘情願把工作改善好，又不得罪人，又能讓管理階層在狀況內

謝謝大家~