InfoSec Taiwan 2025
國際資安組織大會
07.09-10

DATE : 2025 / 07 / 10

面對資安的有效風險管理框架

PRESENTER : 莊盛祺

兆益數位股份有限公司總經理
淡江大學會計學系兼任講師
中華民國電腦稽核協會理事暨專業發展委員會主委(CAA & ISACA TW)
台灣舞弊防治與鑑識協會理事(ACFE TW)
中華民國內部稽核協會理事(IIA)

各類資訊系統風險

一、資訊安全風險（Information Security Risk）
- ■資料洩漏（Data Breach）
- ■非法存取（Unauthorized Access）
- ■惡意程式（Malware / Ransomware）
- ■身分冒用（Identity Theft）

二、系統風險（System Risk）
- ■系統故障（System Failure）
- ■軟體缺陷（Software Bugs / Errors）
- ■版本更新風險（Patch / Upgrade Issues）
- ■系統整合錯誤（Integration Risk）

三、基礎設施風險（Infrastructure Risk）
- ■網路中斷（Network Outage）
- ■資料中心故障（Data Center Failure）
- ■電力問題（Power Failure / UPS Risk）
- ■雲端服務中斷（Cloud Outage）

四、第三方風險（Third-Party / Vendor Risk）
- ■外包服務中斷（Service Interruption）
- ■供應商資安事件（Vendor Breach）
- ■契約與合規風險（Contractual / SLA Failure）

五、合規與法規風險（Regulatory / Compliance Risk）
- ■未遵循資安法規（如GDPR、PDPA、HIPAA）
- ■稽核失敗（Audit Failure）
- ■政策不符（Policy Non-compliance）

六、資料管理風險（Data Risk）
- ■資料遺失（Data Loss）
- ■資料品質問題（Data Quality Issue）
- ■備份失效（Backup Failure）

七、操作風險（Operational IT Risk）
- ■人為錯誤（Human Error）
- ■權限配置錯誤（Privilege Mismanagement）
- ■缺乏變更管理（Lack of Change Control）

八、策略與專案風險（Strategic / Project Risk）
- ■IT 專案失敗（IT Project Failure）
- ■技術選擇錯誤（Wrong Tech Adoption）
- ■系統實施延期 / 超支（Delay / Cost Overrun）

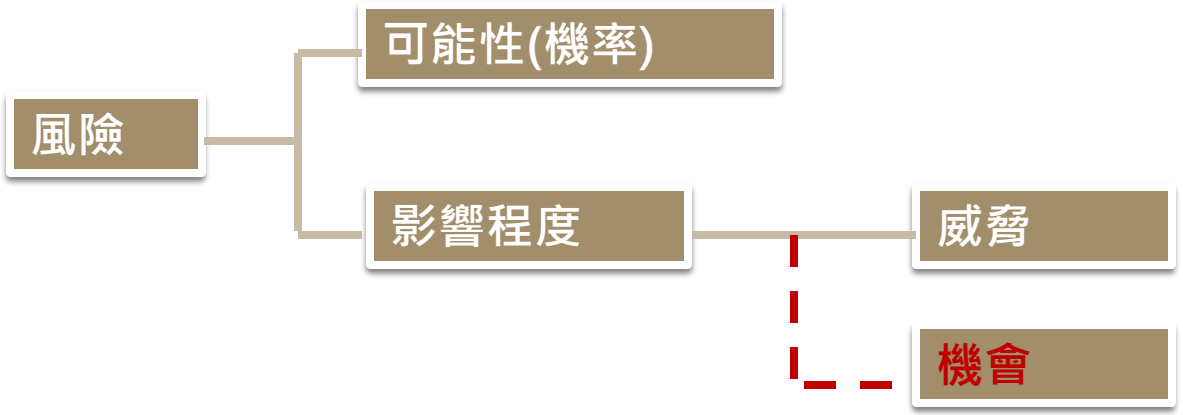
九、網路與通訊風險（Network and Communication Risk）
- ■DDoS 攻擊（Distributed Denial of Service）
- ■傳輸資料被攔截（Man-in-the-Middle）
- ■通訊協議漏洞（Protocol Vulnerabilities）

十、新興風險（Emerging IT Risk）
- ■AI 風險（AI Output Reliability / Bias / Abuse）
- ■IoT 安全風險（IoT Device Security）
- ■量子計算威脅（Post-quantum Cryptography Risk）

風險的定義

風險(Risk):一個事件潛在影響組織目標達成的機率及影響程度。

- 機率(Likelihood):用來描述頻率及或然率的實際數值。
- 影響(Consequences):一個事件的結果，以定量或定性來表示，可能是損失、傷害、賠錢或獲利。一個事件有許多不同的可能結果。



資訊技術相關的風險相對於其他主要風險類別的範圍

摘錄自ISACA 資訊技術風險框架 第2版

風險管理原則

摘錄自ISACA 資訊技術風險框架 第2版

風險管理工作流程

摘錄自ISACA 資訊技術風險框架 第2版

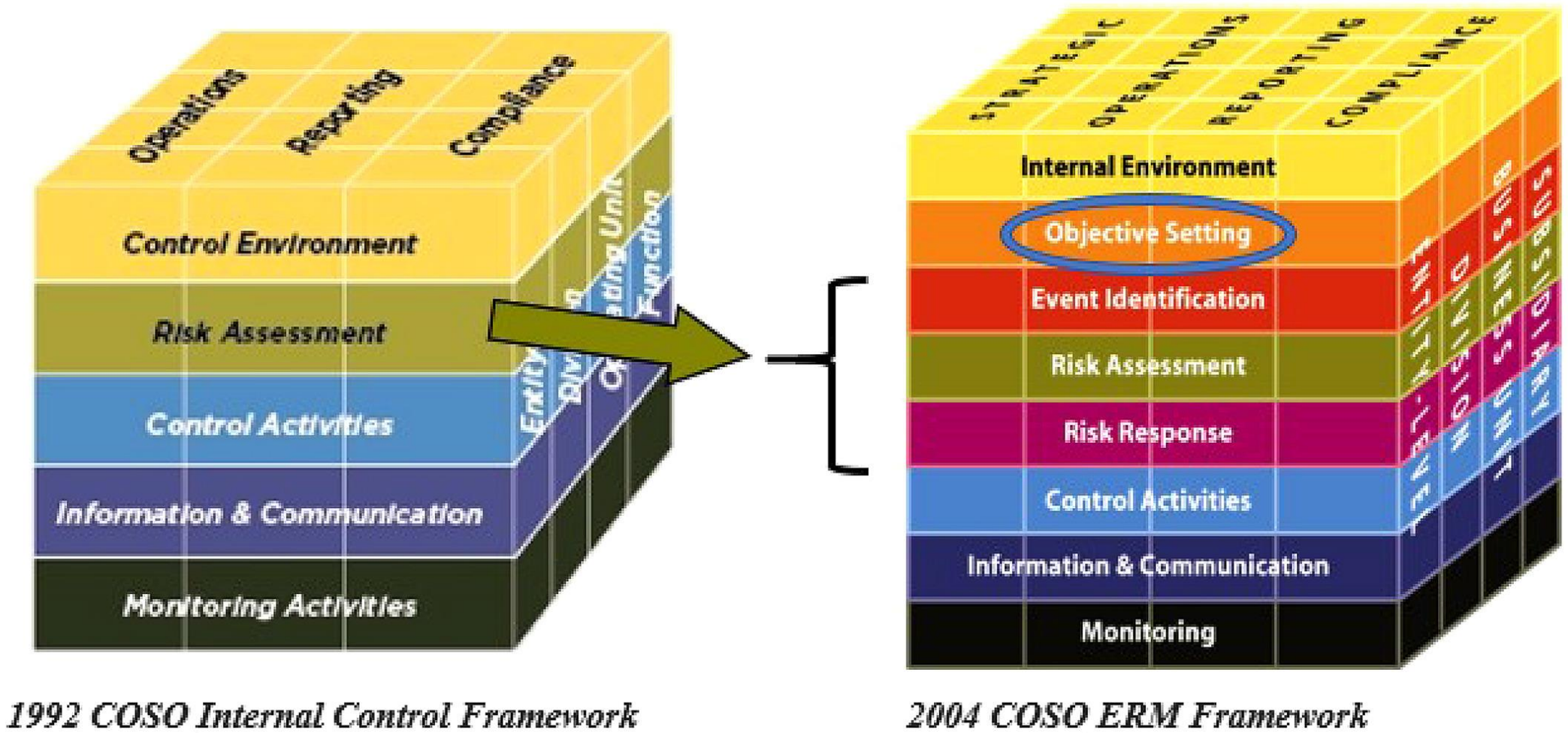
風險情境/損失事件架構及組成

摘錄自ISACA 資訊技術風險框架 第2版

資訊與技術(I&T)風險溝通的組成

摘錄自ISACA 資訊技術風險框架 第2版

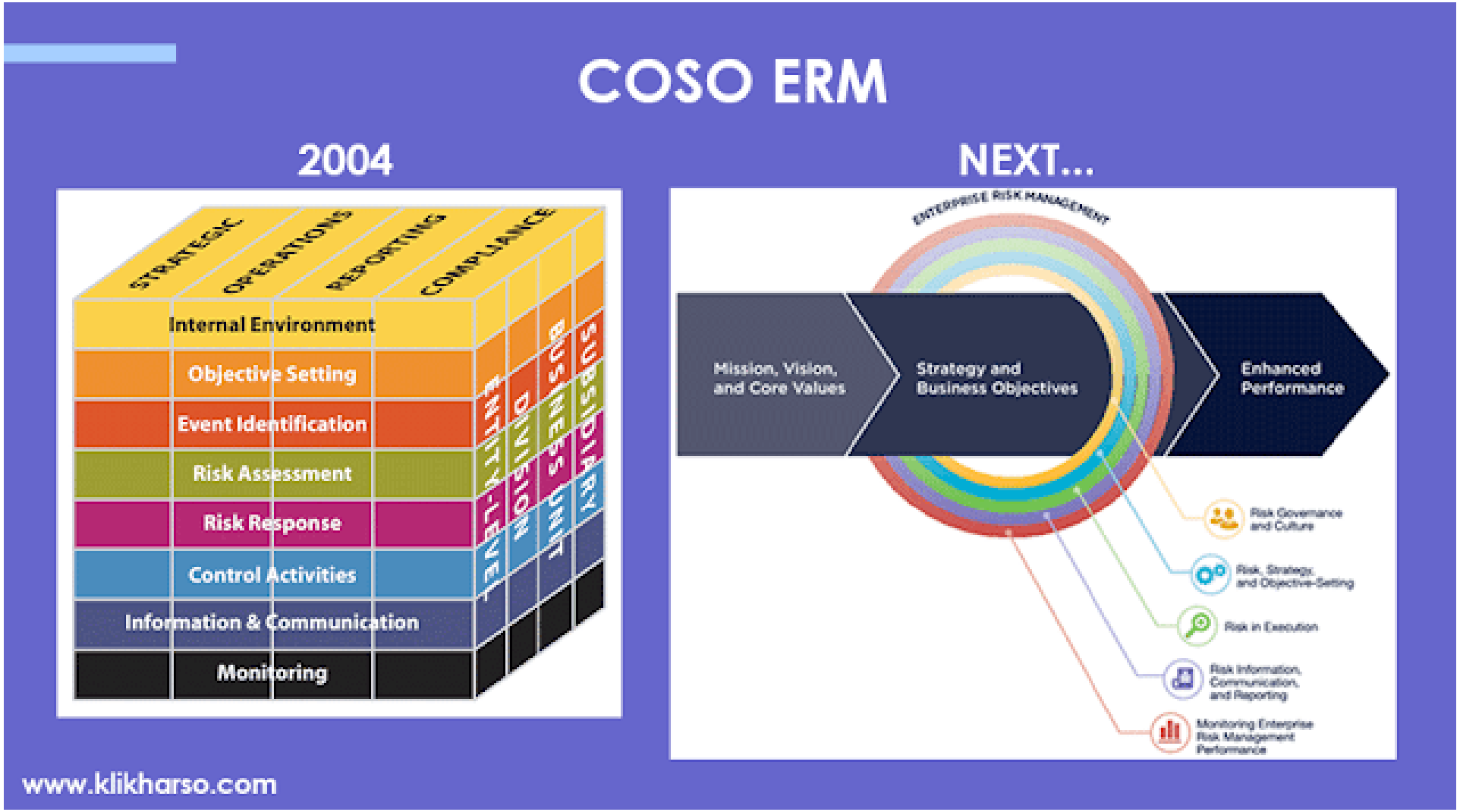
COSO 內控五大要素與ERM 八大要素



1992 COSO Internal Control Framework

2004 COSO ERM Framework

COSO ERM 焦點的移轉

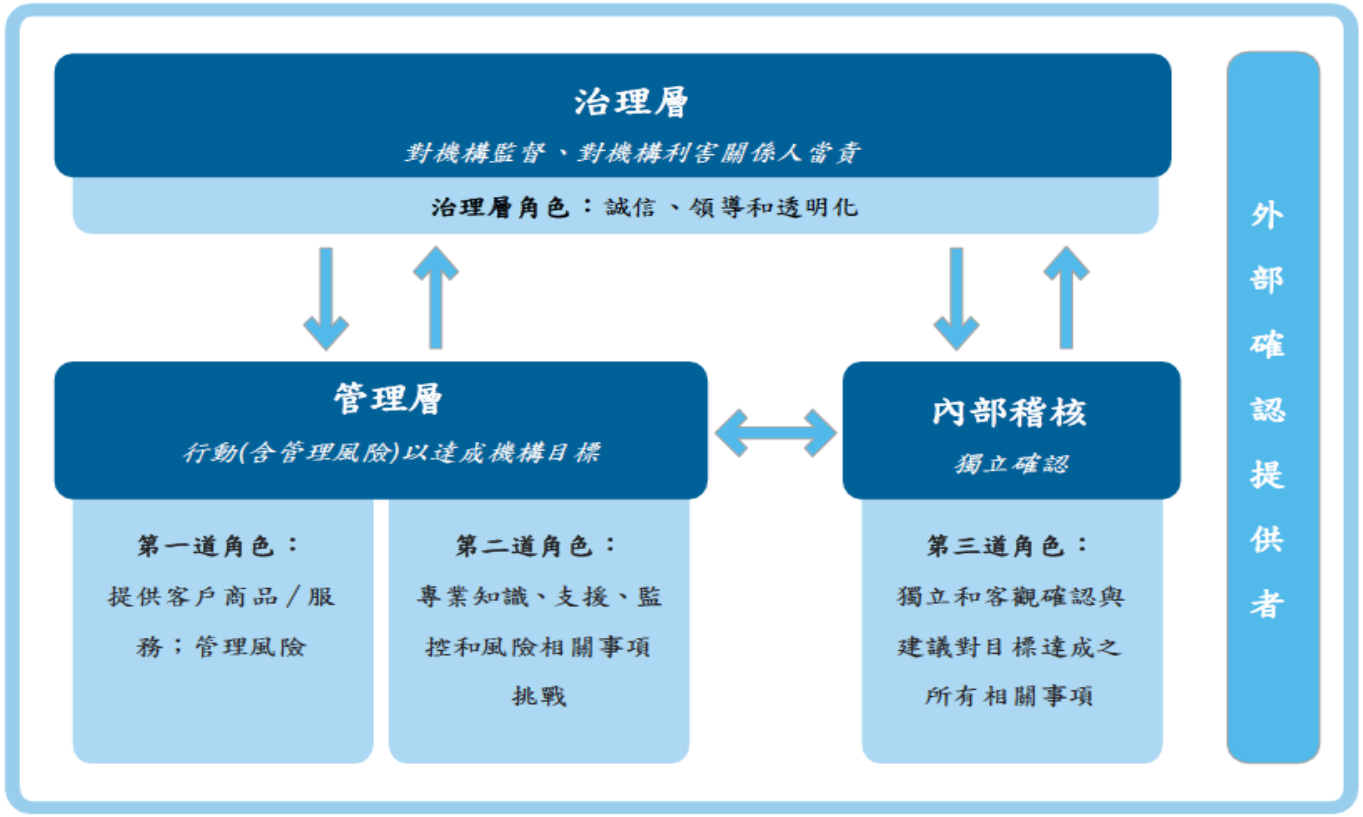


企業風險管理整合策略與績效

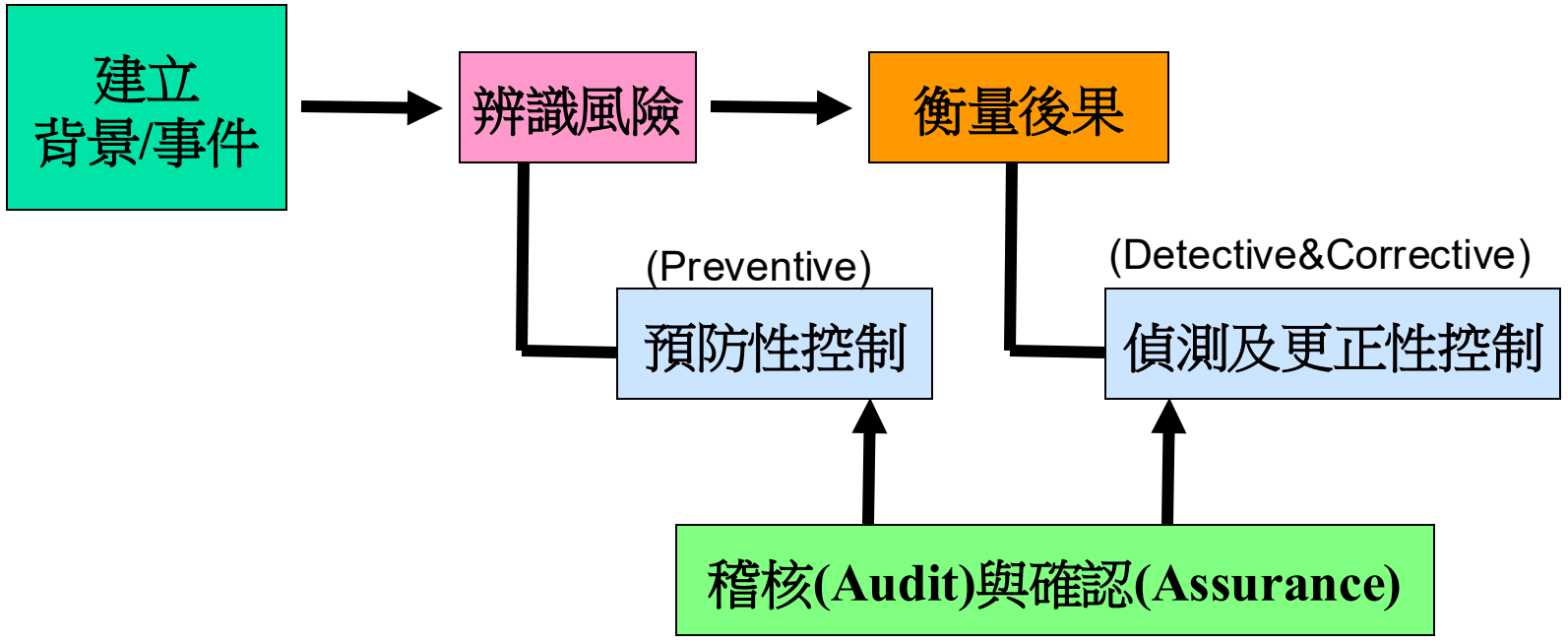
國際內部稽核協會三道模型

國際內部稽核協會三道模型

Sep. 9, 2020



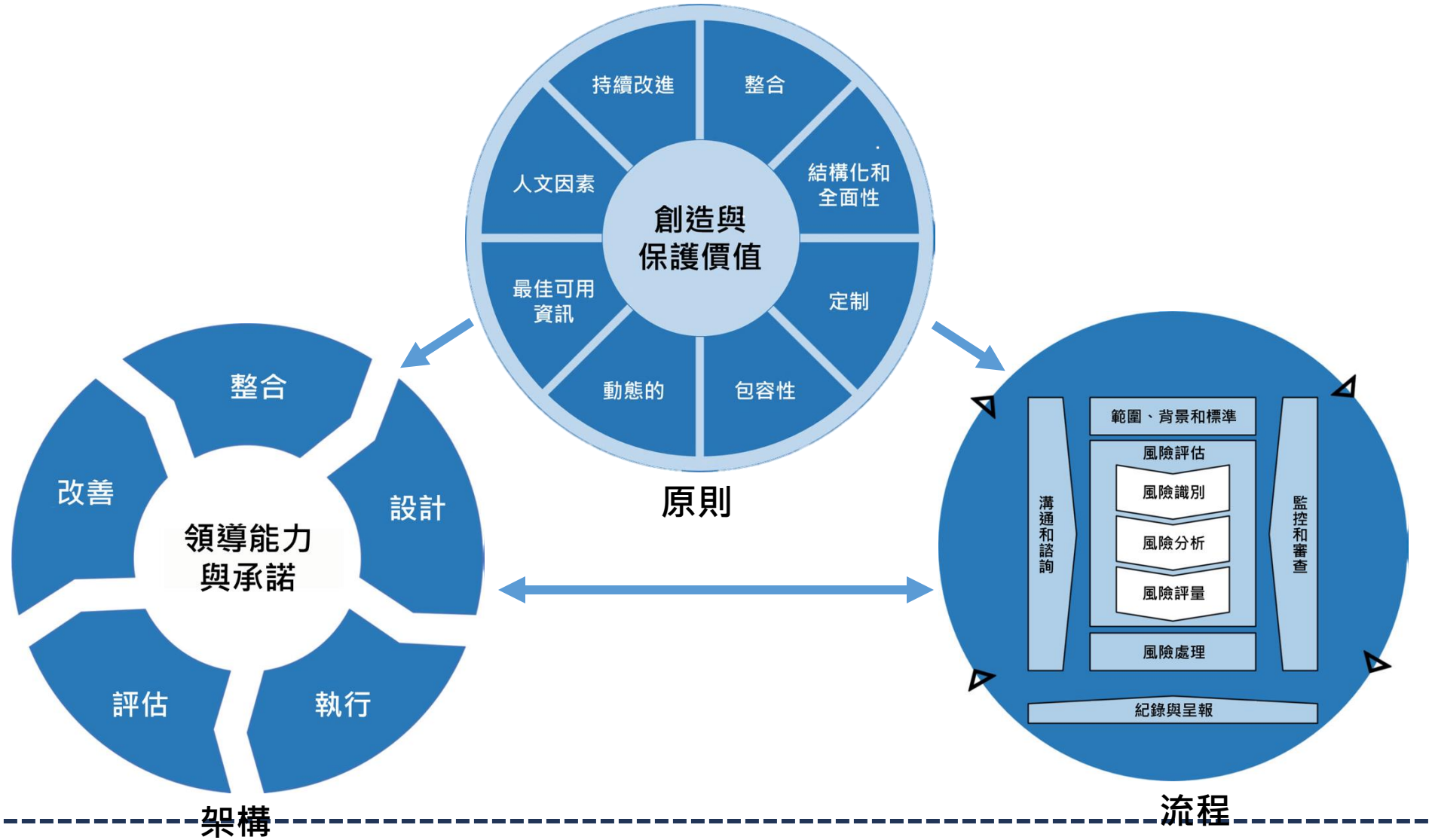
風險管理方法



查核控制的適當性與執行的有效性

從簡單開始實施 → 再發展到複雜的層面

ISO31000:2018風險管理原則、架構和流程關係圖



GRC執行架構

ISO31000:2018風險管理原則、架構和流程關係圖

稽核分析能力成熟度模型

有效風險管理與內部控制三道防線(模型)

治理層

對機構監督、對機構利害關係人當責

治理層角色：誠信、領導和透明化

管理層

行動(含管理風險)以達成機構目標

第一道角色：提供客戶商品/服務；管理風險

第二道角色：專業知識、支援、監控和風險相關事項挑戰

內部稽核

獨立確認

第三道角色：獨立和客觀確認與建議對目標達成之所有相關事項

外部確認提供者

主管機關

風險項目擁有者/主管	風險控管與法遵	風險項目確認
■營運管理	■有限獨立性 ■主要向管理部門呈報	■內部稽核 ■更大的獨立性 ■向管理機構呈報

會計師

基本的持續確保架構

操作上的管理擁有及管理風險	預測風險的功能, 例如:符合風險管理)	內部稽核提供獨立的確保

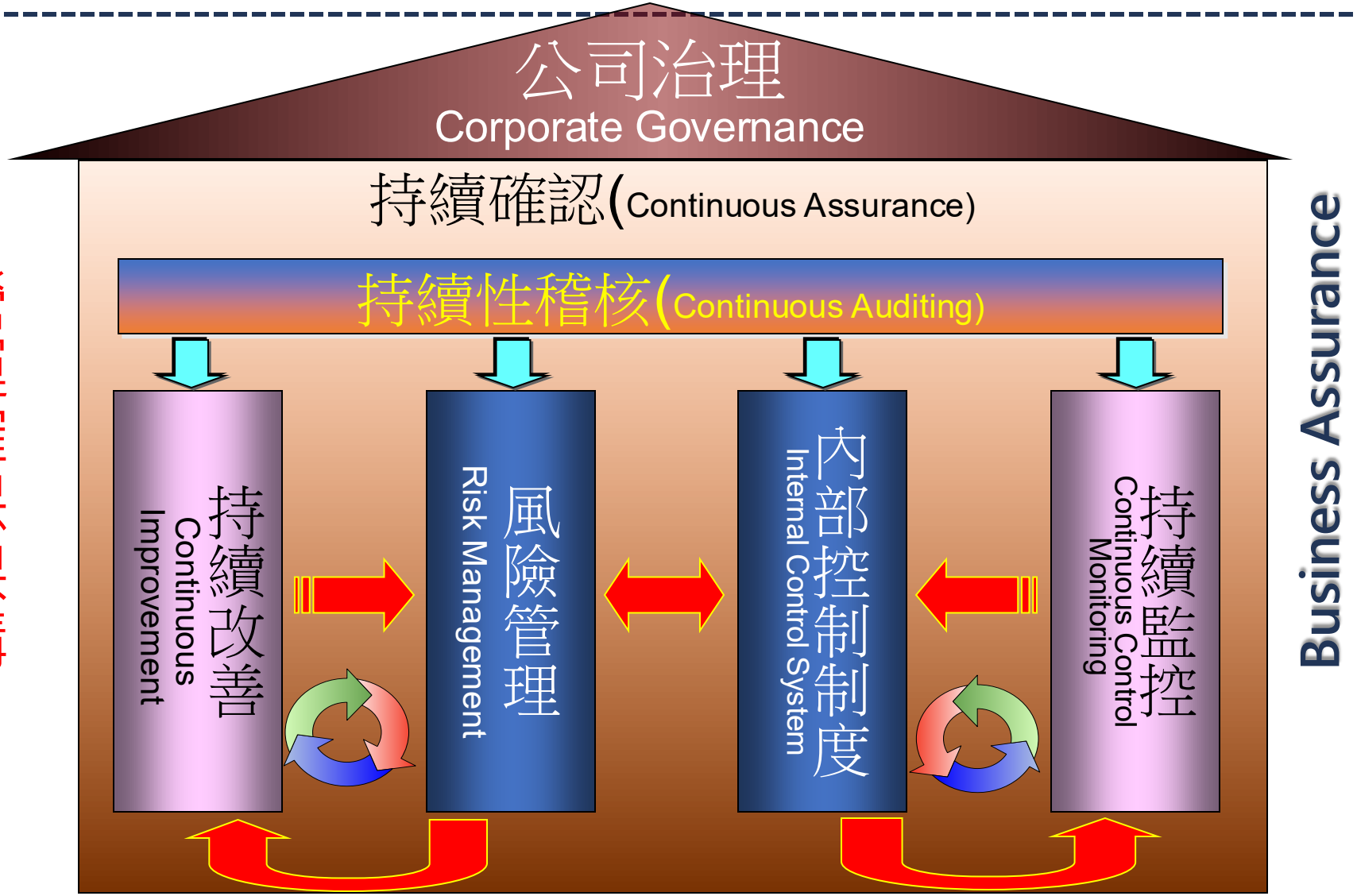
持續性監控

第一道及第二道防線持續性監控的稽核測試

持續稽核,是透過科技做持續風險及控制評估

透過內部稽核活動達到持續的確保：
- 第一道及第二道防線持續性監控的稽核測試
- 持續性稽核

我們共同的目標



Thanks!

Do you have any questions?

youremail@twcsa.org
+886 6 3125518
yourcompany.com