Chapter 01
資訊治理、風險、控制與稽核概論

莊盛祺 CFE, 舞弊稽核師
台北商業大學會計資訊系兼任講師
淡江大學會計學系兼任講師
兆益數位股份有限公司總經理

David Chuang の觀網
blog.uprofit-tw.com
UProfit 兆益數位學苑

個人簡介

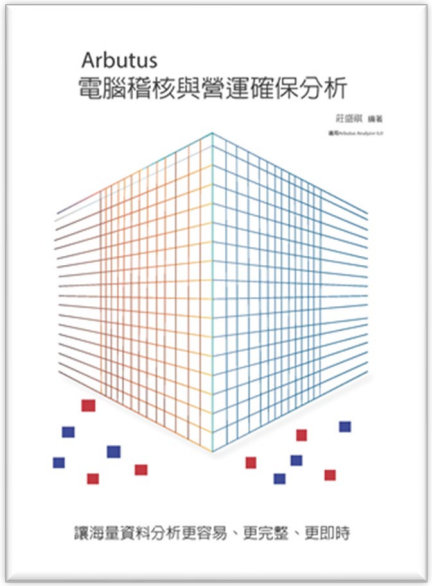
莊盛祺

現　任：

台北商業大學會計資訊系	兼任講師
淡江大學會計學系	兼任講師
兆益數位股份有限公司	總經理
中華民國電腦稽核協會	常務理事暨專業發展委員會主委
台灣舞弊防治與鑑識協會(ACFE TW)	理事
中華民國內部稽核協會	理事
台北大龍峒扶輪社理事	理事暨祕書

歷　任：

傑克商業自動化股份有限公司	總經理
行政院風險管理研習班講師/風險管理服務團顧問	
中華民國電腦稽核協會	祕書長
安侯建業會計師事務所	協理
友邦信用卡股份有限公司	財務經理
安麗日用品股份有限公司	財務經理
眾信聯合會計師事務所	財務主任



著　作:

Arbutus電腦稽核與營運確保分析

Arbutus電腦稽核實務分析

課程大綱

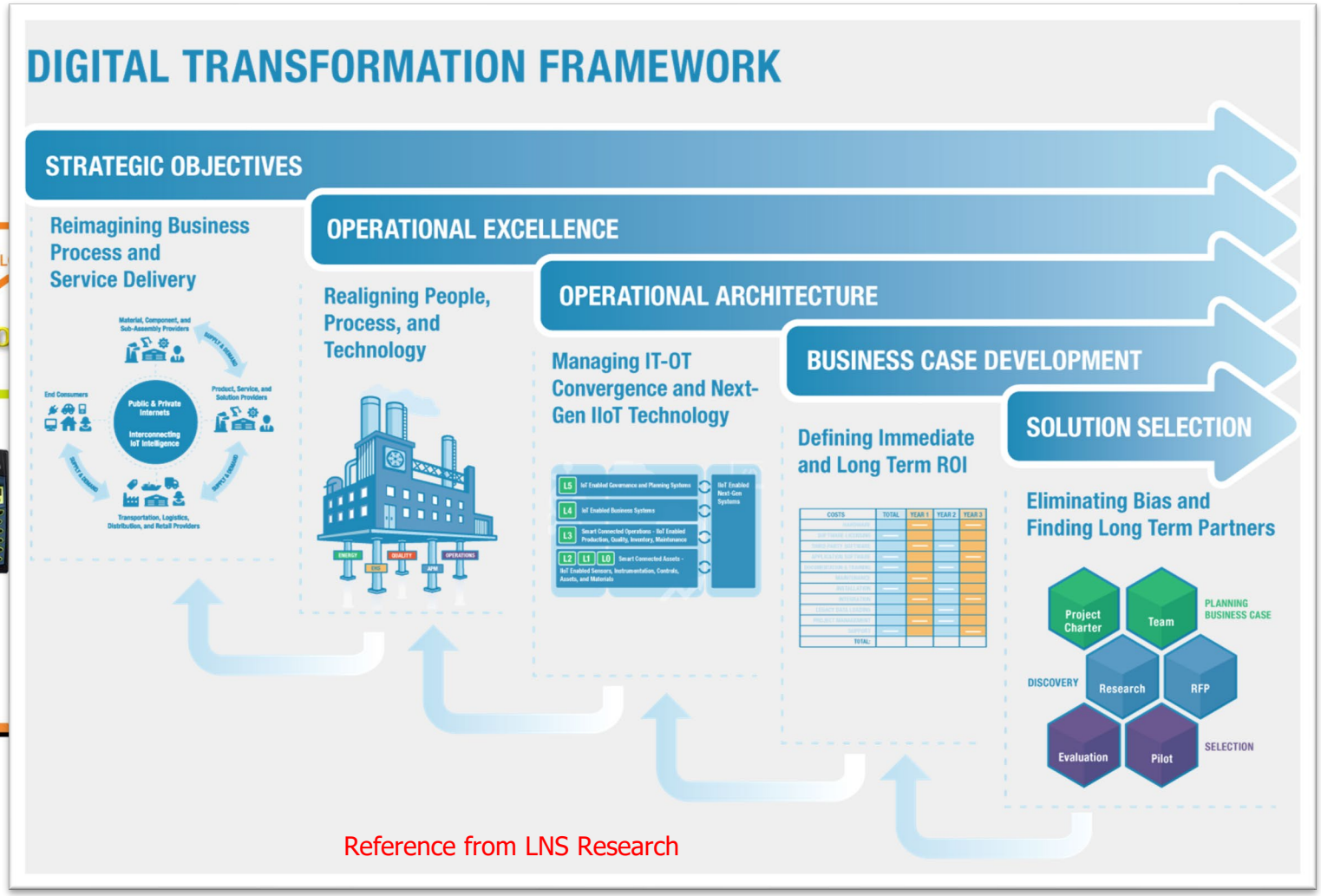
1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

如何提升企業營運效率…….

Timeline:



Reference from LNS Research

Overview

- 為什麼我應該要瞭解資訊科技風險和控制？
  - ✓『確認和可靠』。
- 什麼是要被保護的?
  - ✓信賴是應該被保護的。
- 資訊科技控制可以應用在那裡?
  - ✓每一個地方。
- 誰要負責?
  - ✓每一個人。
- 什麼時候要評鑑資訊科技風險與控制?
  - ✓經常性。
- 要多少控制才足夠?
  - ✓管理當局必須基於風險胃納、容忍度、要求規範來決定。

資訊治理

- 是討論資訊科技控制主題時的重要考量因素
- 提供確保IT能夠支援組織整體營運需求的架構
- 對資訊科技管理人員的重要在於對組織用於符合其營運流程的目的和達到由行政管理層和董事會所提出的目標，進行深度的瞭解。
- 資訊治理不但要說明被辨識出來風險的控制項組成，同時是一個整合IT實務和人員的結構，必須與組織整體策略與目標緊密連結並促使達成。

正確應用資訊治理原則能夠去影響和衝擊整個組織和資訊科技如何與組織營運進行互動

- 資訊科技風險的辨識與管理及改善資訊科技作業的啟動
- 加強企業營運與資訊科技間的關係：
- 能見到資訊管理實現目標的能力
- 為企業營運與資訊科技結果所做的風險管理和辨別持續改善的機會
- 資訊治理持續改善資訊科技適應性, 以改變經營與資訊科技環境

當內部稽核活動評估組織的資訊治理結構與實行時，有幾項產生有效資訊治理的關鍵組成部分會被審查評估

- 領導統御。
- 組織結構
- 資訊科技作業
- 風險管理
- 控制活動

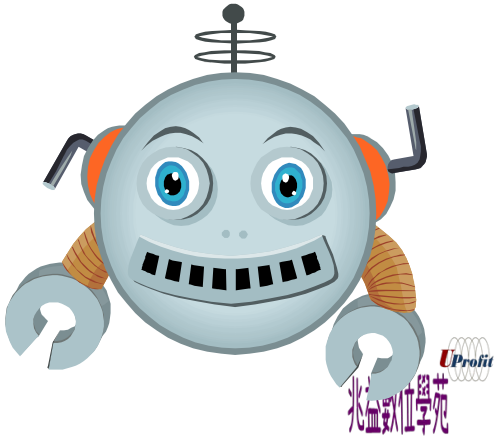
IT之運用

管理交易(Transaction)、資訊(Information)

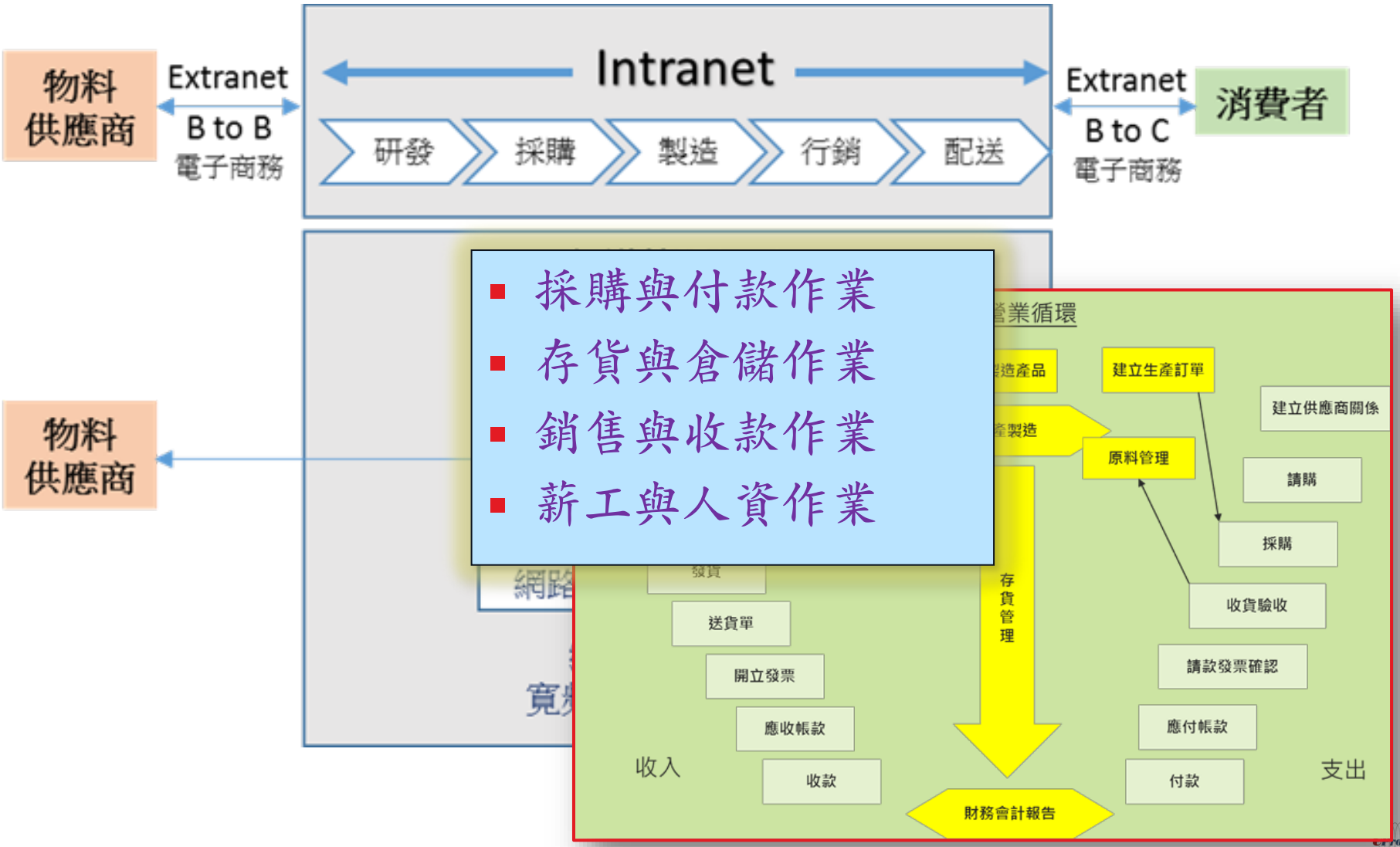
與知識(Knowledge) 之重要工具

支援及維持營運與促成營運成長之基礎

整體營運不可分之一部份

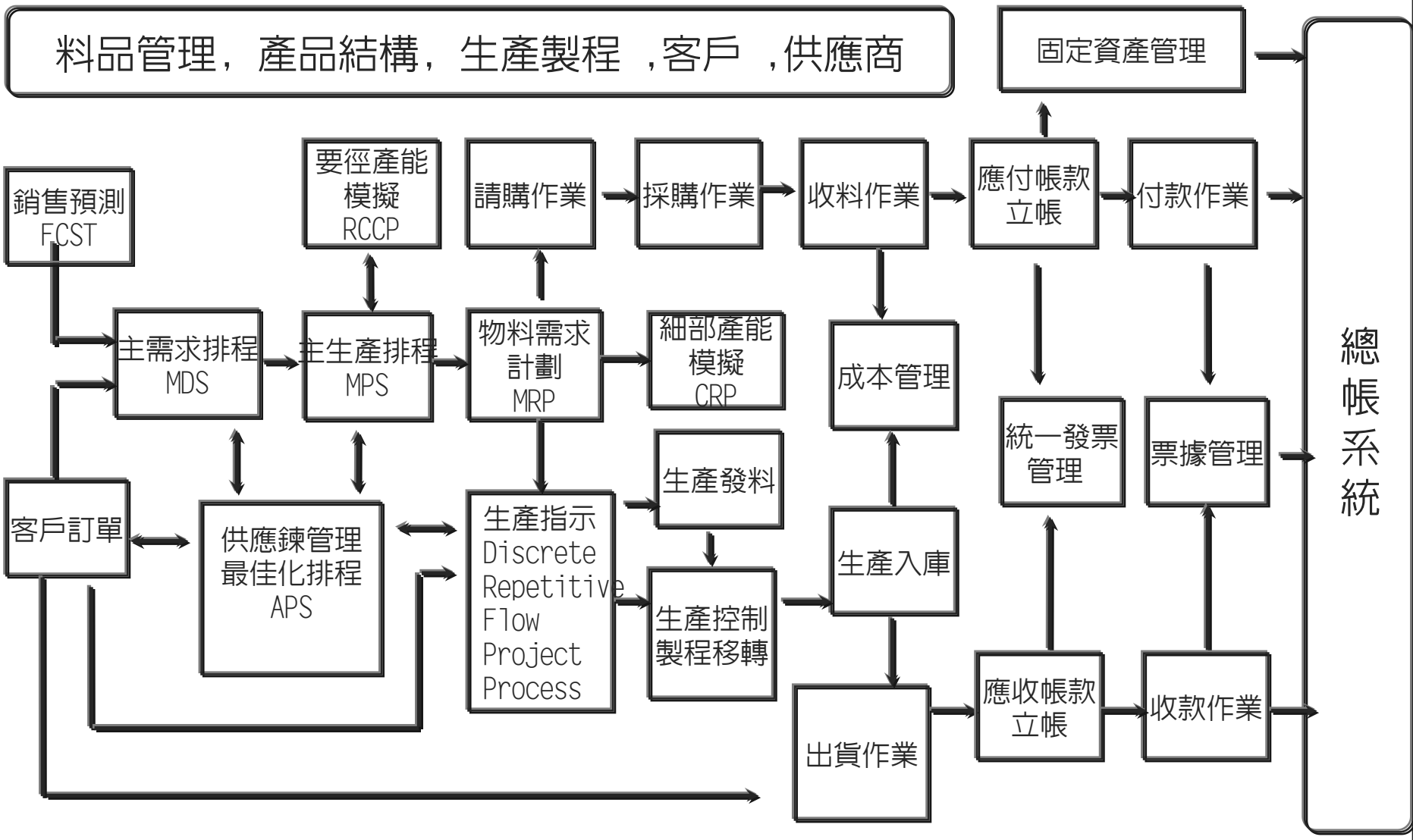


資訊化的企業經營環境



- 採購與付款作業
- 存貨與倉儲作業
- 銷售與收款作業
- 薪工與人資作業

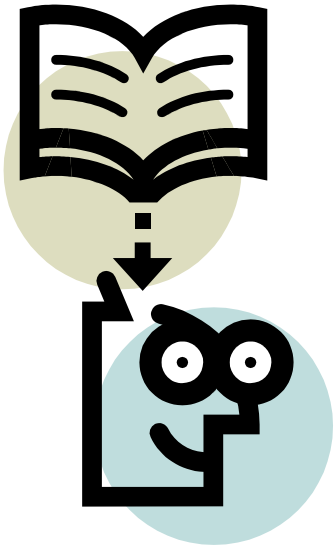
資訊系統流程


料品管理，產品結構，生產製程 ，客戶 ，供應商
固定資產管理
銷售預測
FCST
要徑產能
模擬
RCCP
請購作業
採購作業
收料作業
應付帳款
立帳
付款作業
主需求排程
MDS
主生產排程
MPS
物料需求
計劃
MRP
細部產能
模擬
CRP
成本管理
統一發票
管理
票據管理
總帳系統
客戶訂單
供應鍊管理
最佳化排程
APS
生產指示
Discrete
Repetitive
Flow
Project
Process
生產發料
生產控制
製程移轉
生產入庫
出貨作業
應收帳款
立帳
收款作業

目前電腦環境下之內部控制風險

- 缺乏交易軌跡或有交易軌跡卻無法稽核
- 處理程式一致，因而處理程式或程序的錯誤將導致大量資料或資訊錯誤
- 缺乏職能分工：會計單位不再擔任交易記錄之角色，傳統職能分工與系統權限不相符，發生錯誤及舞弊之可能性增高
- 交易由電腦自動產生或執行，資訊錯誤將誤導重大決策
- 資料未予適當保護造成機密洩漏與資料流失
- 未適度了解個別資訊產品的特性及既有控制或稽核功能，而無法辨識控制風險與稽核績效

你真得信賴您資訊系中
所處理的資料及交易記錄的
完整性與正確性嗎



Can you rely on the integrity of all your data and transactions

Assurance

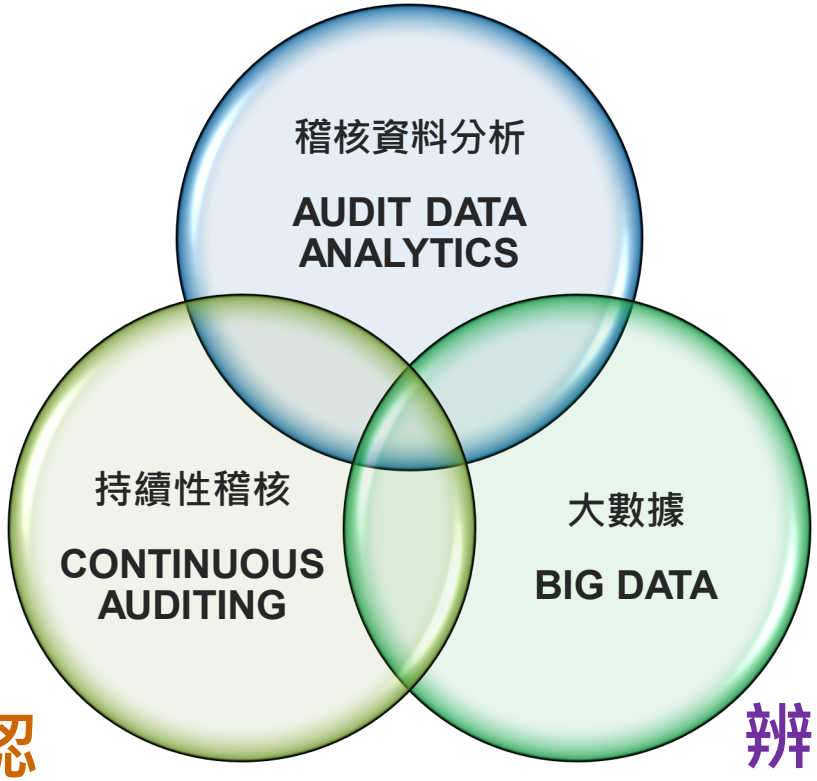
Assurance is necessary and sufficient evidence that information (or information systems and technology) meet their recipients' (or their users') knowledge (or belief, trust or confidence) requirements in support of rational action in one or more specific contexts.

(Will and Whobrey 2003)

『確認』是指資訊能夠符合其接受者（或其使用者）的知識（或信仰、信任或信心）需求，以支援在一或多個特定背景中之合理行為的充份必要證明。

轉型中的稽核作業

有效查核與舞弊偵測



持續性確認

辨別多種行為

課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

組織在確認資訊科技控制的角色與責任

- 董事會及其他治理組織
- 管理階層－定義、核准、執行資訊科技控制或瞭解它的使用
- 稽核
  - 內部稽核-確保 (assurance)
  - 外部稽核-定期查核

一般來說，在任何組織中 IT 使用的目標是：

✓ *將有效率地交付可靠的資訊與保護 IT 服務，和組織的策略、政策、外部需求與風險胃納一致 (line with)。*
✓ *保護利害關係人的利益。*
✓ *為達成營運目標與客戶、商業夥伴和其他外界人士啟動 (enable) 互益關係。*
✓ *要適當地識別和回應威脅與可能違反控制。*

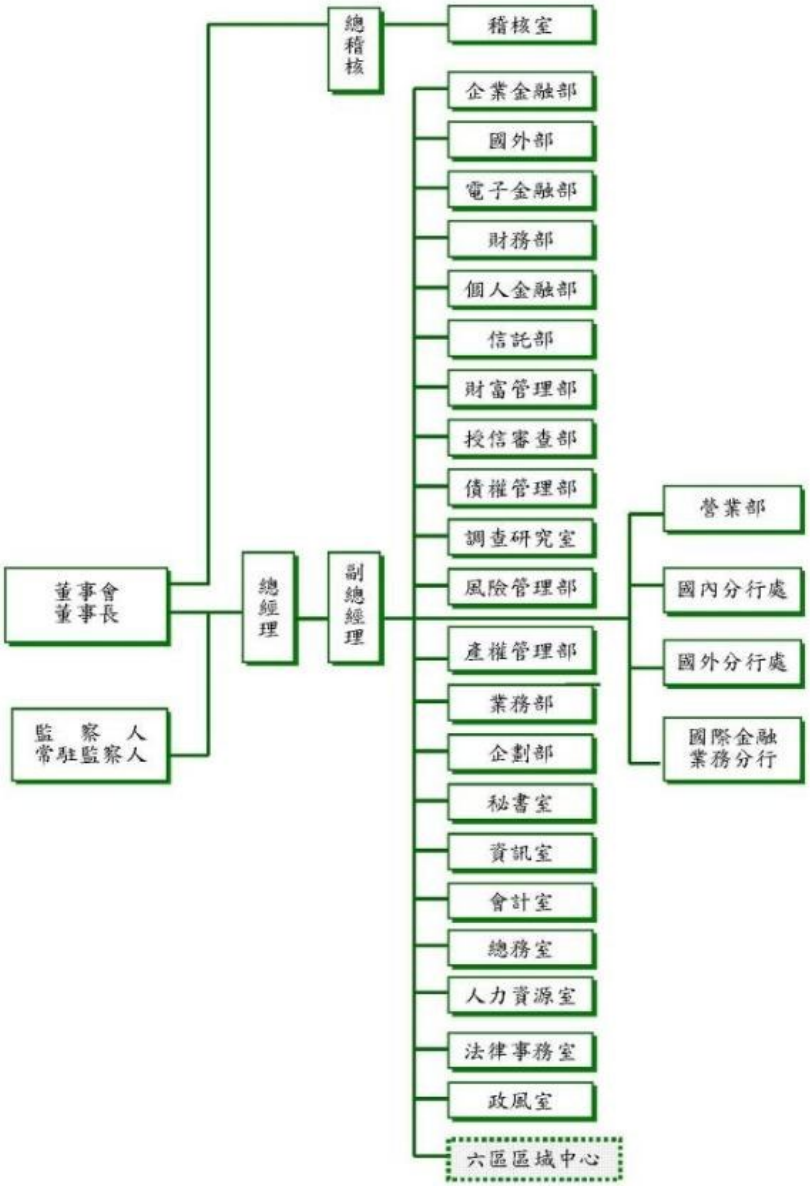
董事會及其他治理組織

- 董事會
  - 審計委員會
  - 薪酬委員會
  - 治理委員會
  - 風險管理委員會
  - 財務委員會
  - 其他

角色	職責
董事會	董事會應該： ● 了解資訊科技職能的策略性價值。 ● 變成熟知資訊科技對企業的角色和衝擊 ● 設定策略方向和預期回報。 ● 考慮管理階層如何分派職責。 ● 監督轉換如何發生。 ● 了解在管理運作間的制約因素。 ● 監督企業走向。 ● 指示管理部門透過資訊科技傳達可衡量價值。 ● 監督企業的風險。 ● 支援學習、成長和資源管理 ● 監督績效該如何衡量 ● 取得確保

管理階層

- 執行長
- 財務長
- 資訊長
- 安全長
- 資訊安全官
- 首席法律顧問
- 風險長



執行者管理階層角色與職責

角色	職責
執行者 管理階層	管理階層應該: ● 成為熟知資訊科技在企業中的角色和 衝擊。 ● 將策略、政策和目標串聯成系列散佈到企業裡，並將資訊科技組織與企業目標聯成一氣。 ● 確定所需要的能力和投入資源。 ● 分配責任。 ● 維持目前的營運。 ● 提供必要的組織結構和資源。 ● 為風險管理與資訊科技控制嵌入清楚的權責。 ● 衡量績效。 ● 關注於資訊單位必須支持的核心營運競爭力。 ● 關注在改善營運價值的重要資訊科技作業。 ● 建立一個有彈性的、適應的企業， 它可以充分利用訊息和知識。 ● 加強價值傳遞。 ● 發展策略以優化資訊科技成本。 ● 要有明確的外部資源策略。

資深主管角色與職責

角色	職責
資深主管應該	資深主管應該: ● 管理關於IT業務和執行預期。 ● 推動IT策略的制定和施行。 ● 將資訊科技預算連結策略目標和目的。 ● 確保可衡量的價值準時及在預算範圍內提出。 ● 實現所需要的資訊科技標準、政策和控制架構。 ● 告知及教育行政主管人員有關資訊科技問題。 ● 檢查增加資訊科技價值貢獻的方法。 ● 確保資訊科技專案良好的管理。 ● 提供資訊科技基礎設施，以促進成本效益的創造和商業智慧的分享。 ● 確保合適的資訊科技資源、技能和基礎建設提供，以符合目標及創造價值。 ● 評估風險、有效地減輕、使風險狀態對利害關係人透明化。 ● 確保重要對於管理資訊風險的職能是有適當的定義與人力配置。 ● 確保對資訊科技作業與控制的日常管理與驗證。 ● 直接且明確地連結到策略實行績效評估。 ● 專注於核心資訊科技能力。

內部稽核活動

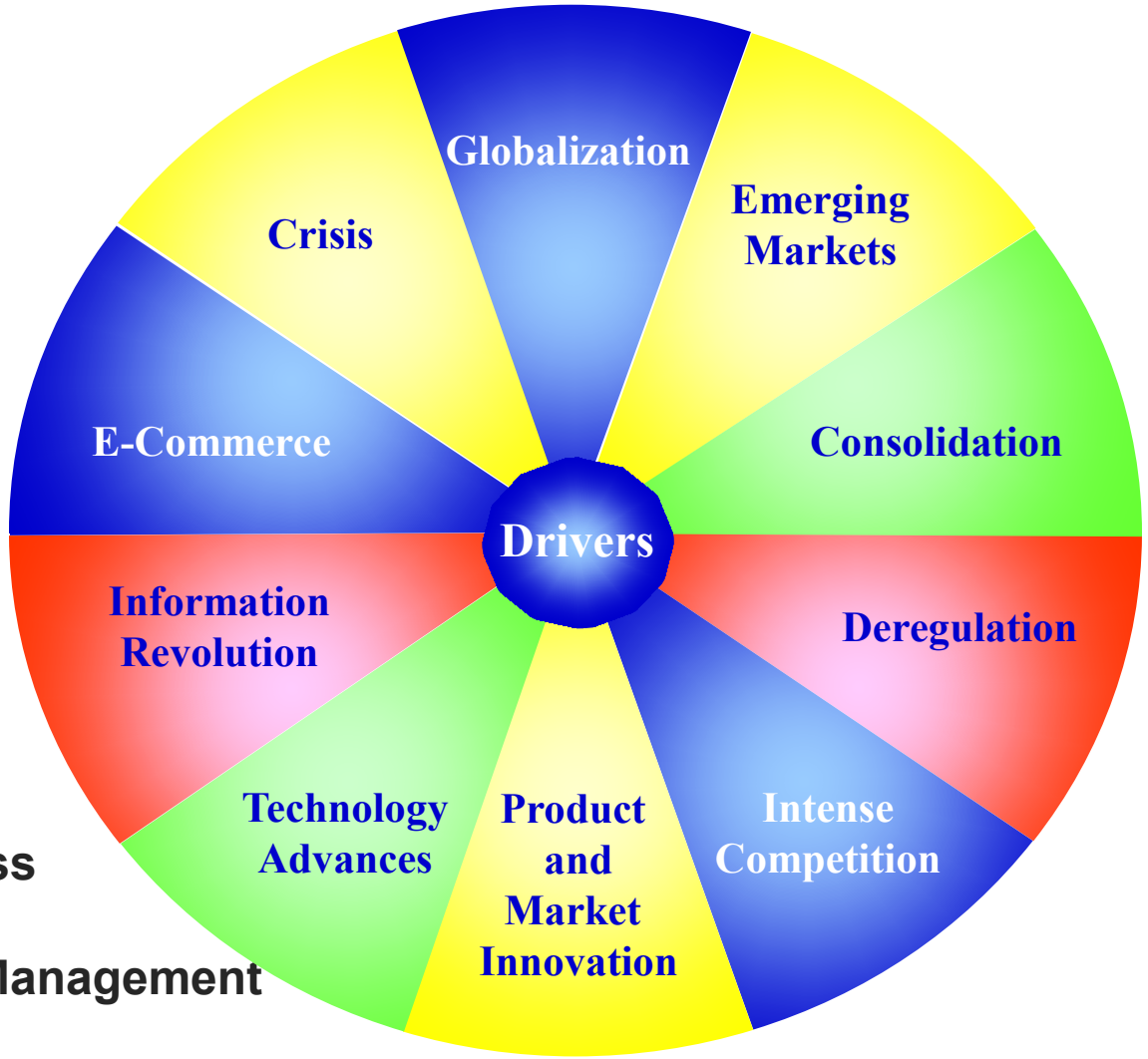
- 確保在部門內的資訊科技稽核專業知識有足夠基礎水準。
- 包括在規劃過程中對資訊科技的評價。
- 評估在組織中資訊治理是否維持和支援策略和目標。
- 辨識和評估關於組織資訊系統的曝險。
- 評估對應到組織資訊系統間風險的控制。
- 確保稽核單位具備資訊科技專業知識可以執行查核專案。
- 考慮使用適當地以資訊科技為基礎的稽核技術

課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

Drivers of Enterprise Business Risk

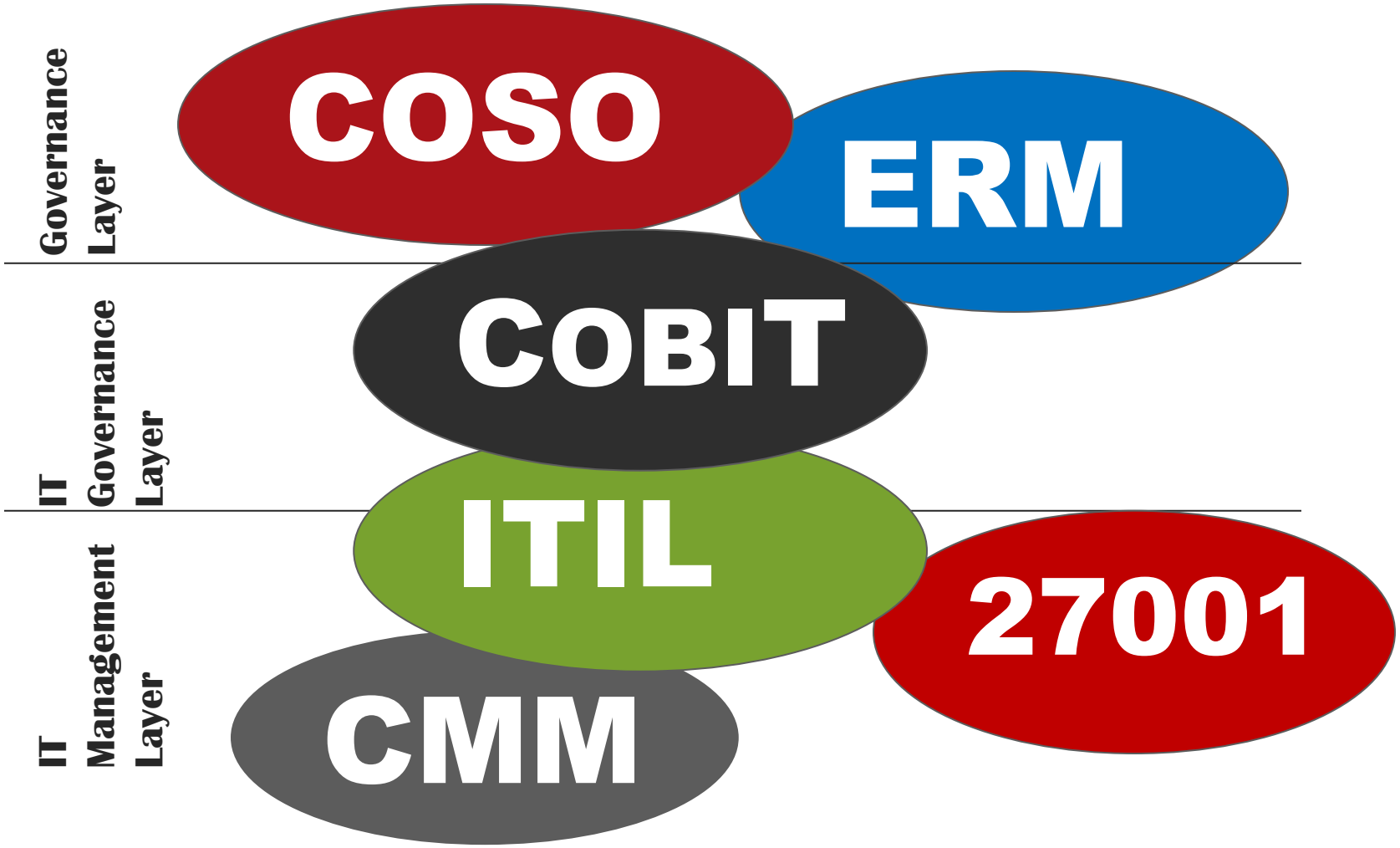
Increased Change Driven By…



Leads to…

- **Increased Exposure to Loss**
- **Need for Enterprise Risk Management**

COBIT and other Frameworks



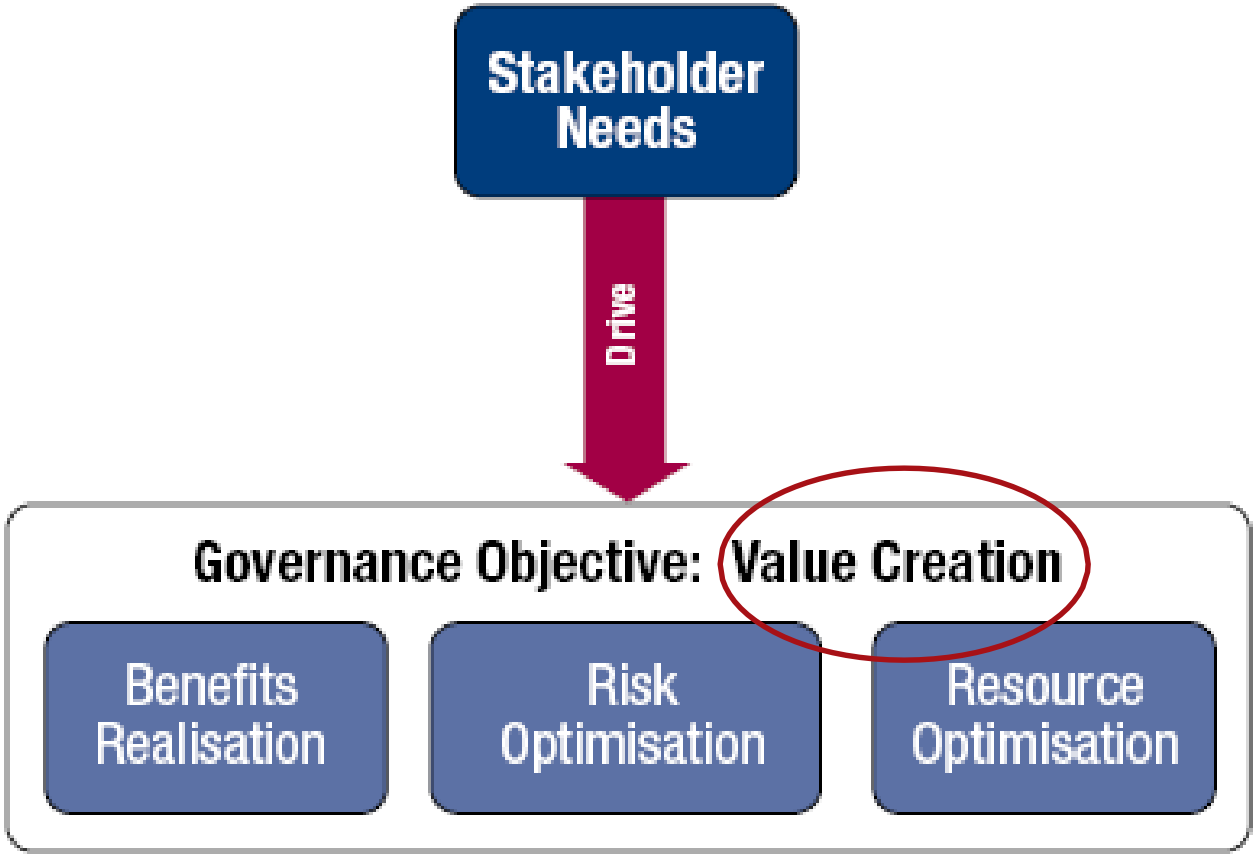
The Context of Enterprise Governance of Information and Technology

Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*, 2nd ed., Springer International Publishing, Switzerland, 2015, *https://www.springer.com/us/book/9783319145464*

參考自ISACA COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY

1.滿足利害關係人需求

- 企業存在的目的是為利害關係人**創造**價值



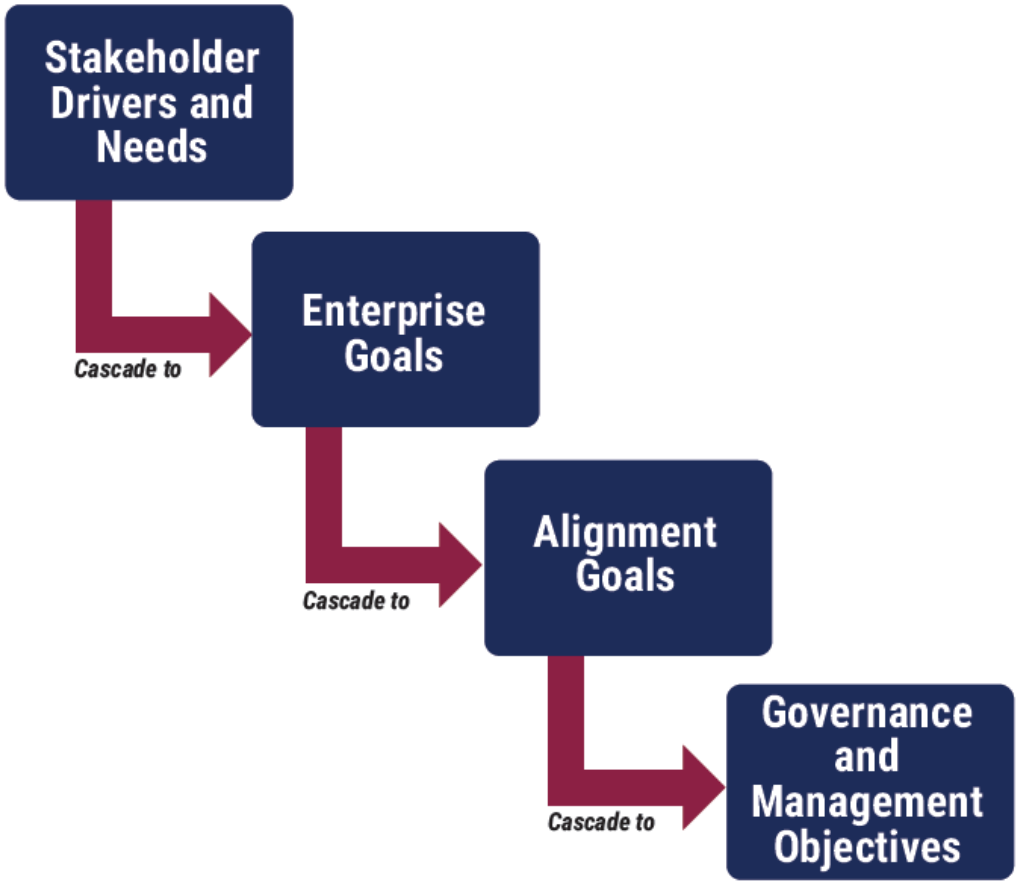
Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.

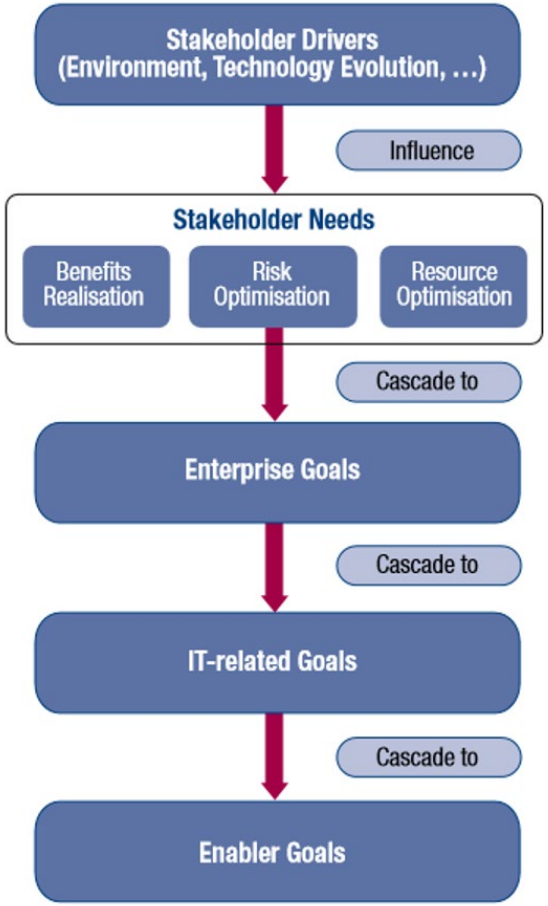
Governance (COBIT) Stakeholders

Stakeholder	Benefit of COBIT
Internal Stakeholders	
Boards	Provides insights on how to get value from the use of I&T and explains relevant board responsibilities
Executive Management	Provides guidance on how to organize and monitor performance of I&T across the enterprise
Business Managers	Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for new strategic opportunities
IT Managers	Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.
Assurance Providers	Helps to manage dependency on external service providers, get assurance over IT, and ensure the existence of an effective and efficient system of internal controls
Risk Management	Helps to ensure the identification and management of all IT-related risk
External Stakeholders	
Regulators	Helps to ensure the enterprise is compliant with applicable rules and regulations and has the right governance system in place to manage and sustain compliance
Business Partners	Helps to ensure that a business partner's operations are secure, reliable and compliant with applicable rules and regulations
IT Vendors	Helps to ensure that an IT vendor's operations are secure, reliable and compliant with applicable rules and regulations

參考自ISACA COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY

COBIT Goals Cascade





參考自ISACA COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY

分析風險

IT 控制是基於其被設計來管理風險而選擇與實施。
當風險被識別 – 透過經驗或正式風險評估（assessment） –
合宜的風險回應（risk responses）被決定，從都不做/管（doing nothing）到將風險視為營運成本而應用廣泛的包含保險之具體控制。

稽核長應考量是否:

- 組織的 IT 環境與組織的風險胃納一致。
- 內部控制架構是適當的，以確保組織的效能維持在其聲明（stated）的風險承受/容忍度內。

在決定資訊科技控制適當性時的風險考量

- IT環境
  - ✓包含硬體、軟體、通訊、應用程式、協定（規則）和資料，在實體空間（physical space）、組織結構內及組織與其外部環境間實施。
- 組織所面對的IT風險
  - ✓與資訊長及流程擁有者討論 IT 風險問題，透過 IT 的使用和其角色在應用與保持有效的控制，來確保所有關係人（related parties）對組織所面對的技術風險有適當的認知和瞭解。
- 風險胃納和風險承受／容忍度
  - ✓風險胃納和承受/容忍度的定義必須與所有相關主管溝通，最終決策必須由風險委員會決定 – 從審計委員會提出建議 – 由全體董事會認可

Continue….

在決定資訊科技控制適當性時的風險考量

- 執行風險分析
  - ✓ 在風險中的資產與其機密性、完整性和可用性的價值是什麼？
  - ✓ 發生什麼事會對資訊資產價值有不利的影響（威脅事件）？ 此問題隱含弱點分析與弱點對映於威脅，及潛在對資訊資產的影響。
  - ✓ 若發生威脅事件，其衝擊會有多壞？
  - ✓ 事件可能多常發生（發生的頻率）？
  - ✓ 對前 4 個問題的答案有多確定（不確定性分析）？
  - ✓ 能夠做什麼來降低風險？
  - ✓ 它將花費多少錢？
  - ✓ 它是有成本效益（cost-efficient）嗎？

降低風險策略

- 接受風險
- 規避風險
- 分擔風險
- 控制/降低風險

課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

南山今年已有七案被罰

2019年南山遭金管會裁罰大事記

		罰鍰	糾正及人員裁處
2月13日	防制洗錢專案金檢疏失	-	6項糾正
4月18日	片面變更收費員制度	600萬	1項糾正 總經理許妙靜停職半年；副總吳雲嬌、范嘉玲停職5個月
4月19日	有價證券投資業務專案檢查	180萬	5項糾正
5月17日	電子商務專案檢查	240萬	4項糾正
5月30日	投資主管Line群組報明牌	660萬	5項糾正 解任炒股經理人葉時雙，五年內不能重回保險業
9月17日	一般業務檢查	180萬	2項糾正
9月17日	境界專案檢查	3000萬	5項糾正 董事長杜英宗停職兩年；前總稽核楊玠青減薪30%， 為期一年，三年內不得擔任總稽核
	合計	4860萬	28項糾正

資料來源：金管會

案例

南山人壽保險股份有限公司辦理「境界成就計畫專案」，違反保險法令裁罰案，依保險法規定，核處罰鍰新臺幣(下同)3,000萬元整，以及予以5項糾正，令該公司停止投資型保險商品新契約業務，直至投資型保險商品資訊系統改善完成，經本會認可之第三方專業機構查核驗證通過，並報經本會同意，始得恢復辦理；併令該公司調降前總稽核楊○○薪酬30%為期1年，且3年內不得再任總稽核；併停止董事長杜○○其董事及董事長職務2年，令該公司於杜○○停止董事及董事長職務期間，不得支付或給予杜○○任何形式之報酬及福利。

四、違反事實理由：

(一)南山人壽：

1.專案控管作業：專案管理團隊之建立未落實內控三道防線架構，且未就該專案重要內容之研商過程與決議事項建立妥適之內控監督機制，不利內控之有效運作；該公司內部稽核單位於103.4.30啟動該專案後，遲至106.11.6始就該專案辦理專案查核，未將該專案管理團隊是否有效評估及控制合約內容可能衍生之風險，及履約過程是否建立妥適之內部控制監督機制等項目納入查核，致無法適時提供相關改進建議，不利董事會之有效監督；又境界系統上線未進行平行測試，或相關完備之替代測試方案，草率匆促取代舊系統上線，致產生諸多問題，影響保戶權益甚鉅；因系統測試範圍不完整及程式功能未完成修復，導致投資型保險商品之系統功能頻繁出錯；因系統功能問題進行修復，所為之暫停寄發催告通知書及進行系統鎖單動作，亦持續發生保單給付金額錯誤、未正常寄發繳費通知單等情事；依該公司於108.5.9所報「境界計畫具體改善規劃」，截至108.7.31經第三方驗證機構查核驗證結果，仍未依該公司函報時程改善完成，嚴重影響保戶權益及公司正常營運；境界系統有發生作業重大缺失事項，卻未依規定即時向本會辦理重大偶發事件通報，其處理流程欠妥。

2.採購控管作業：境界專案之採購係直接與特定廠商合作，未依一般採購程序辦理及比價，該公司初始採購即未依其內部採購作業準則辦理，且未能在採購前完整評估掌握專案需求及時程，致專案進度延遲並大幅追加預算；該公司董事會對於合約中攸關合作模式之重要約定及可能風險未詳予審議，並建立控管及因應措施，且其審計委員會對於該專案主要風險之評估監控及該專案重要事項如執行進度及預算控管等之追蹤處理等有欠妥情事，公司治理之功能有待提升；董事會及審計委員會辦理該專案之預算審議及合約簽署事宜，有未取得或分析外部會計師及律師之意見等欠妥情事。

3.財務控管作業：該公司因境界系統上線後之投資型保險商品帳務處理系統錯誤，導致帳務不正確，影響財務報表記載不實，且該公司仍無法確認調節金額，影響金額龐大。

(二)相關人員：

1. 南山人壽董事長杜○○應負決策失當，未善盡督導南山人壽辦理「境界成就計畫專案」之責，嚴重影響保戶權益及公司正常營運，有礙公司健全經營，杜○○自104.8.13起擔任南山人壽董事長，亦為該專案主要負責人，該專案辦理過程進度嚴重落後及追加預算金額龐大，且本專案於重新議約並調整合作模式時，杜○○卻未尋求外部專家意見並審慎評估，決策顯有失當，另境界系統上線不採平行測試，所採行之替代測試方案亦不完備，嚴重影響系統運作及穩定性，致後續上線後產生諸多問題，又杜○○承諾境界系統於108年6月底前能穩定運作，依南山人壽於108.5.9所報「境界計畫具體改善規劃」，亦載明可於108年6月底完成改善，惟經第三方認證機構之查核驗證結果，截至108年7月底發現許多項目未依公司所報時程改善完成，杜○○未確實善盡督導南山人壽辦理「境界成就計畫專案」之責，嚴重影響保戶權益及公司正常營運，有礙公司健全經營。

2. 南山人壽前總稽核楊○○未就本專案辦理情形進行完整查核，未落實第三道內稽防線機制，未善盡執行內部稽核制度之職責，核有輕忽廢弛職務之情事，嚴重有礙公司健全經營。

五、裁罰結果：

(一)南山人壽：

1. **專案控管缺失**：該公司就境界專案未建立內控內稽制度，內部稽核監督功能不彰，且未確實執行系統開發、程式修改及測試程序之控制作業及辦理重大偶發通報，其處理流程欠妥，違規事實明確，嚴重影響保戶權益，且有礙健全經營之虞，核與保險法第148條之3第1項授權訂定之保險業內部控制及稽核制度實施辦法第4條、第5條、第6條及第7條規定不符，依保險法第171條之1第4項規定，核處罰鍰1,200萬元，及依保險法第149條第1項規定予以糾正。又鑑於該公司投資型保險商品系統功能頻繁出錯，且未依該公司規劃時程改善系統完成，罔顧保戶權益，依保險法第149條第1項第1款規定，令該公司自裁處書送達之翌日起令其停止投資型保險商品新契約業務，直至投資型保險商品資訊系統改善完成，經本會認可之第三方專業機構查核驗證通過，並報經本會同意，始得恢復辦理。

2. **採購控管作業缺失**：**該公司董事會及審計委員會決策該專案過程未發揮董事會及審計委員會治理監督責任及未考量商業模式改變之影響，違規事實明確，情節重大**，核與保險法第148條之3第1項授權訂定之保險業內部控制及稽核制度實施辦法第4條規定不符，依行為時保險法第171條之1第4項，核處罰鍰600萬元；又該公司未依內部採購作業準則辦理該專案採購及未考量並審慎評估該專案合作廠商如未依約履行對專案及公司所造成之影響，違規事實明確，情節重大，核與保險法第148條之3第1項授權訂定之保險業內部控制及稽核制度實施辦法第4條、第5條規定不符，依保險法第149條第1項規定，予以2項糾正。又，上開事實缺失核有礙健全經營之虞，併依保險法第149條第1項規定，予以糾正。

3. **財務控管作業缺失**：**該公司帳務錯誤，違規事實明確，情節重大且有礙健全經營之虞**，核與保險法第148條之3第1項授權訂定之保險業內部控制及稽核制度實施辦法第5條規定不符，依保險法第171條之1第4項，核處罰鍰1,200萬元，及依保險法第149條第1項規定予以糾正。

(二)相關人員：

1. 有關南山人壽董事長杜○○應負決策失當，未善盡督導南山人壽辦理「境界成就計畫專案」之責，嚴重影響該公司正常營運及保戶權益，有礙該公司健全經營，又為避免杜○○在職影響南山人壽經理部門有效辦理系統改善，及對專案履約工作之執行及檢討，實有必要於相當期間內停止其董事及董事長職務，應依保險法第149條第1項第6款規定，停止其董事及董事長職務2年，併依同條項第7款規定，令南山人壽於杜○○停止該公司董事及董事長職務期間，不得支付或給予杜○○任何形式之報酬及福利(包括但不限於薪酬、交際費、差旅費、房屋津貼或租金、獎金紅利等各項類似性質之給付) 。

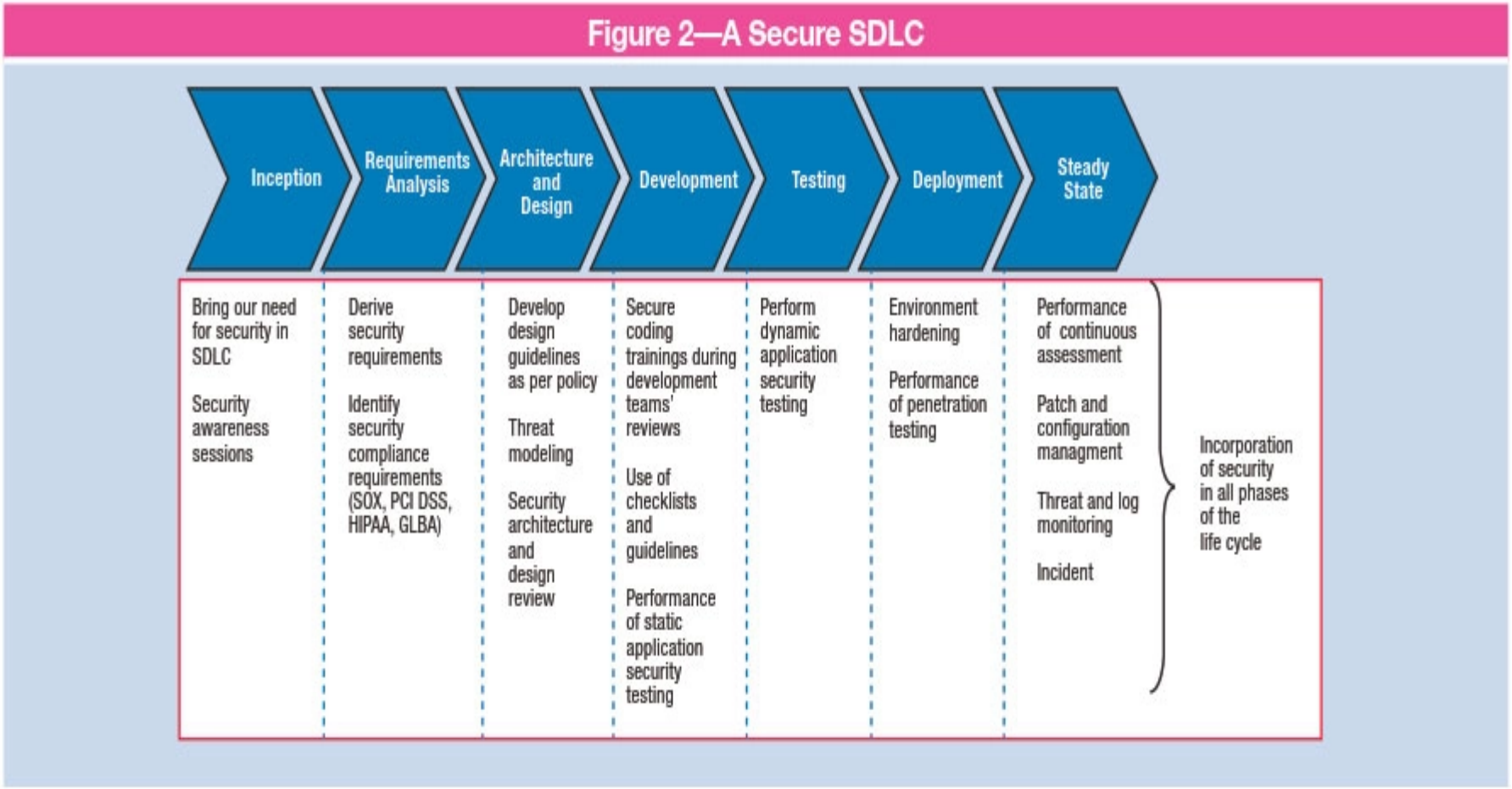
2. 有關南山人壽內部稽核監督功能不彰，未落實執行境界專案稽核作業，前總稽核楊○○核有輕忽廢弛職務之情事，依保險法第149條第1項第7款規定，令該公司自裁處書送達之翌日起調降楊○○薪酬30%為期1年，及3年內不得再任總稽核。

六、其他說明事項：

(一)金管會呼籲，保險業有別於一般行業，其資金大部分來自於保戶，應依保險法令規定建立相關內部控制制度並落實執行，以發揮**內控制度設計及執行之有效性**，**且就系統建置轉換上線，應確保保戶權益不受影響**。

(二)**良好之公司治理係保險業健全經營之基石，公司治理制度包括建立良好之公司組織及文化、內部控制制度及法令遵循機制，而公司治理之落實，有賴專業經理人責任及董事會職能之強化**。保險業應確實依保險法相關規定，依業務性質及規模，按內部牽制原理訂定內部控制制度並落實執行，並應強化公司治理及法令遵循機制，以維護保戶權益、共同維護保險市場秩序。

系統發展生命周期
(System Development Life Cycle,SDLC)



Source: S. Subramanian and B. Swaminathan. Reprinted with permission.

Systems Development and Project Management Audit/Assurance Program

Systems Development and Project Management
Audit/Assurance Program

ISACA

Systems Development and Project Management Audit/Assurance Program

VI. Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1 . PLANNING AND SCOPING THE AUDIT									
1.1 Define audit/assurance objectives. The audit/assurance objectives are high level and describe the overall audit goals.									
1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.									
1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.									
1.2 Define boundaries of review. The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment.									
1.2.1 Perform a high-level walkthrough of the project to be reviewed.									
1.2.1.1 Determine what phase the project is in.									
1.2.1.2 Obtain a list of implemented changes to production for the test period.									
1.2.1.3 Determine the applications and/or operating environments serviced by the project.									
1.2.1.4 Obtain a list of the Sarbanes-Oxley critical applications.									
1.2.1.5 Obtain a list of implemented new systems or major enhancements to existing systems for the period under test.									
1.2.2 Establish initial boundaries of the audit/assurance review.									
1.2.2.1 Identify limitations and/or constraints affecting audit of specific systems.									
1.2.3 Review all phases and steps within this audit/assurance program.									
1.2.3.1 Select those steps within the phase that are applicable to the scope and boundaries established.									
1.2.3.2 Consider additional steps as required based on the scope established.									
1.2.3.3 Consider using additional audit/assurance programs for application specific and IT									

誰負責內部控制作業

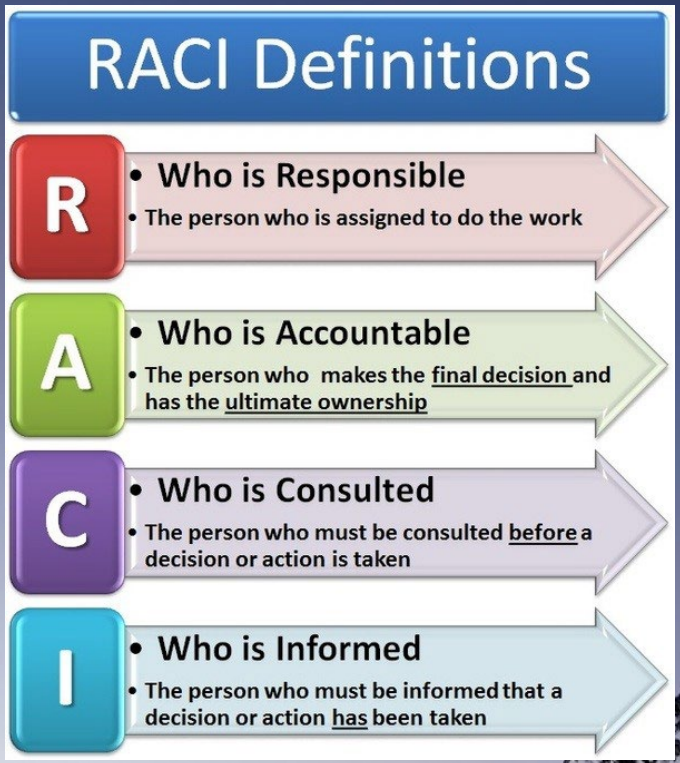

RACI Definitions
R
• Who is Responsible
• The person who is assigned to do the work
A
• Who is Accountable
• The person who makes the final decision and has the ultimate ownership
C
• Who is Consulted
• The person who must be consulted before a decision or action is taken
I
• Who is Informed
• The person who must be informed that a decision or action has been taken

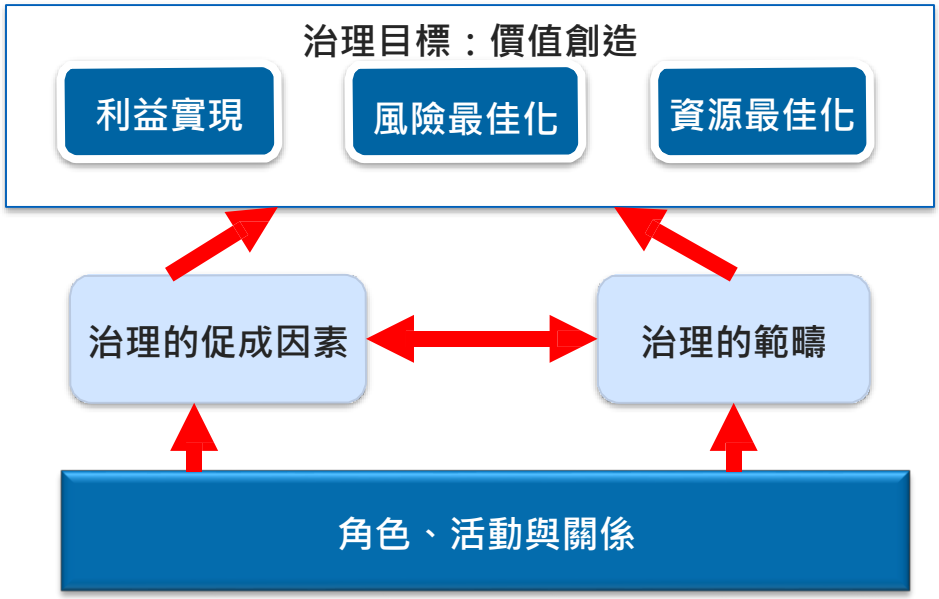
Figure 3—RACI Chart for MEA02 *Monitor, evaluate and assess the system of internal control*

MEA02 RACI Chart

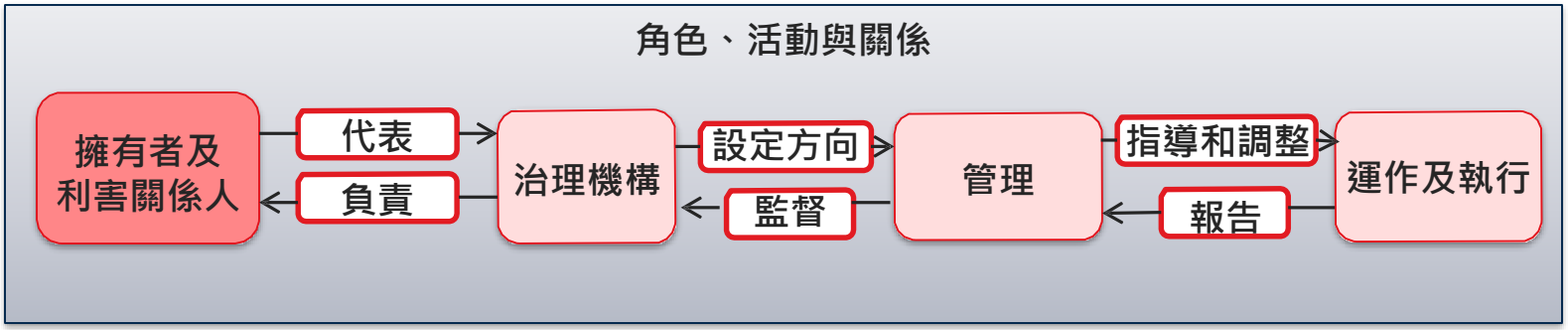
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA02.01 Monitor internal controls.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.02 Review business process controls effectiveness.	I	I	R	I	A	R	I				I	I				R	R	C			C		C	C	C	
MEA02.03 Perform control self-assessments.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.04 Identify and report control deficiencies.		I	C	I	C	R			R		I	I				R	R	A	I	R	R	R	R	R	R	R
MEA02.05 Ensure that assurance providers are independent and qualified.						R										A	A	R								
MEA02.06 Plan assurance initiatives.		A			C	R			C							C	C	R	C	C	C	C	C	C	C	C
MEA02.07 Scope assurance initiatives.				R	R	R			C							C	A	R	C	C	C	C	C	C	C	C
MEA02.08 Execute assurance initiatives.	I	I			C	R			C		I	I				C	A	R	C	C	C	C	C	C	C	C

2.含蓋企業端到端業務(續)

治理系統關鍵要素



Source: COBIT® 5, figure 8. © 2012 ISACA® All rights reserved



Source: COBIT® 5, figure 9. © 2012 ISACA® All rights reserved.

Common Element of Organization

Executive Management

Executive management establishes and incorporates strategy into business activities. At the enterprise or entity level, business objectives are set, policies are established, and decisions are made on how to deploy and manage the resources of the organization. From an IT perspective, policies and other enterprisewide guidelines are set and communicated throughout the organization.
Business processes are the

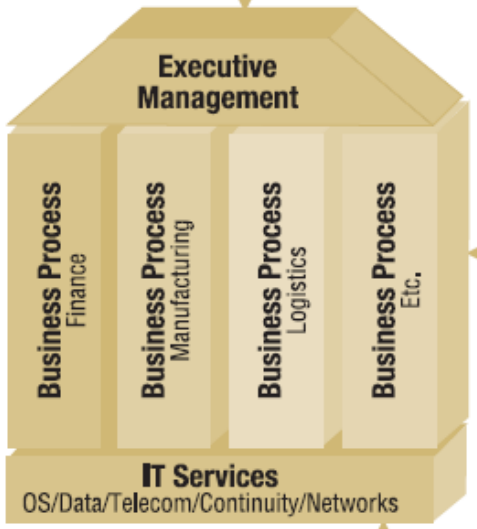
IT Services

for operations and are provided across the organization, rather than segregated by business process or business unit. IT services commonly include network management, database management, operating system management, storage management, facilities management and security administration, and are often managed by a central IT function.

Entity-level Controls

Entity-level controls set the tone and culture of the organization.
IT entity-level controls are part of a company's overall control environment.

Controls include:
- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit



IT General Controls

Controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls

Controls include:
- Program development
- Program changes
- Access to programs and data
- Computer operations

Application Controls

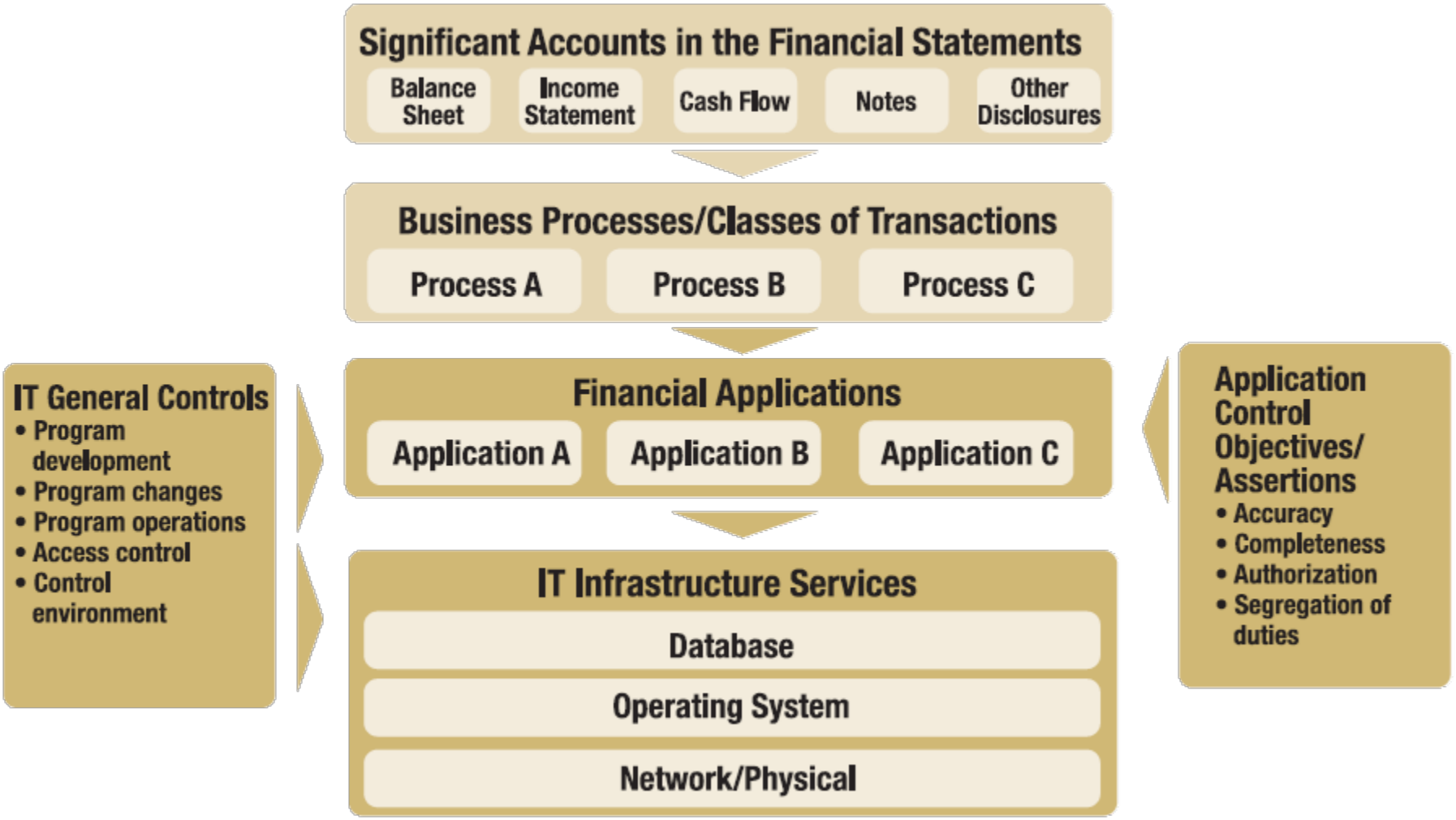
Controls embedded within business process applications directly support financial control objectives. Such controls can be found in mos financial applications including large systems such as SAP and Oracle as well as smaller OTS systems such as ACCPAC.

Control objectives/assertions include:
- Completeness
- Accuracy
- Existence/authorization
- Presentation/disclosure

Business Process

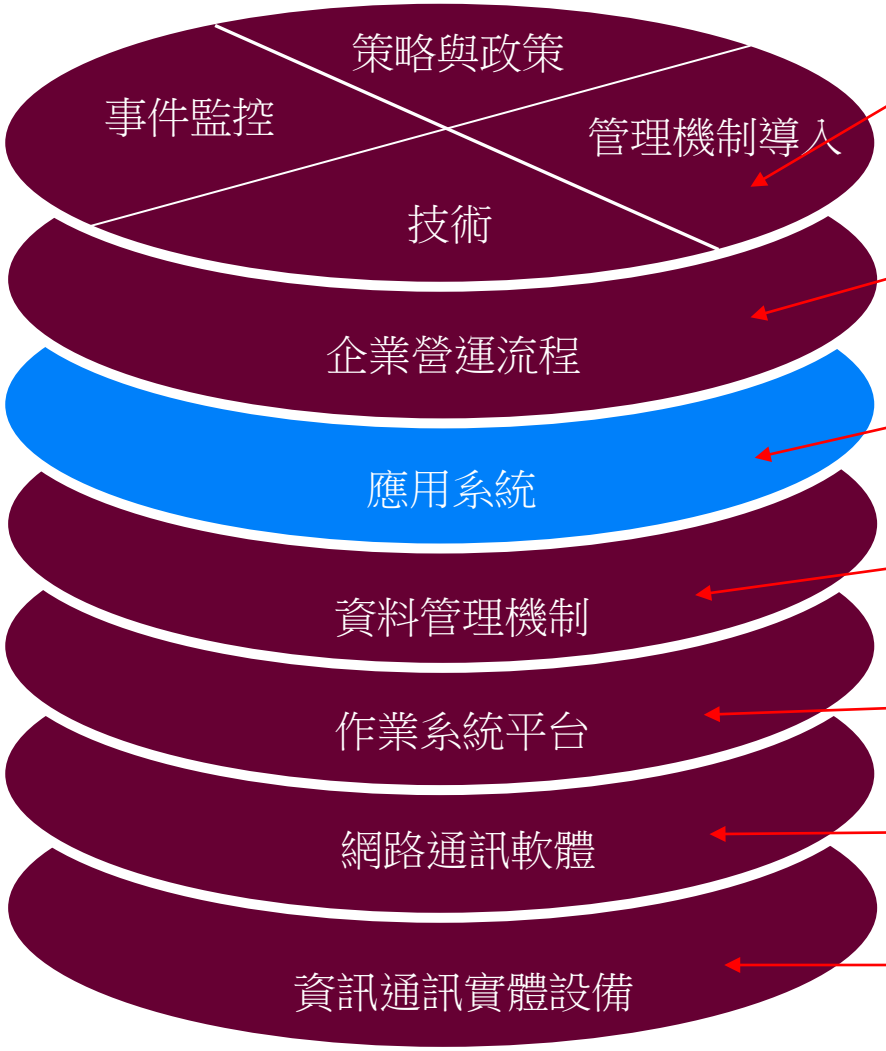
organization's mechanism of creating and delivering value to its stakeholders. Inputs, processing and outputs are functions of business processes. Increasingly, business processes are being automated and integrated with complex and highly efficient IT systems.
IT services form the foundation

Scoping the IT Control Project—Top Down



參考自ISACA:IT CONTROL OBJECTIVES FOR SARBANES-OXLEY

資訊系統基礎架構之控制標的



- 資訊計／政策
- 電腦核／事件處理
- 安全管制技術認知

- 銷售／營收／採購／支出
- 行銷／銷公關／製造／庫存
- 財會／人事／資訊／

- 進銷存／總帳
- ERP/MRP/人事薪資
- Web/FTP/News/Telnet/BBS/VoIP等

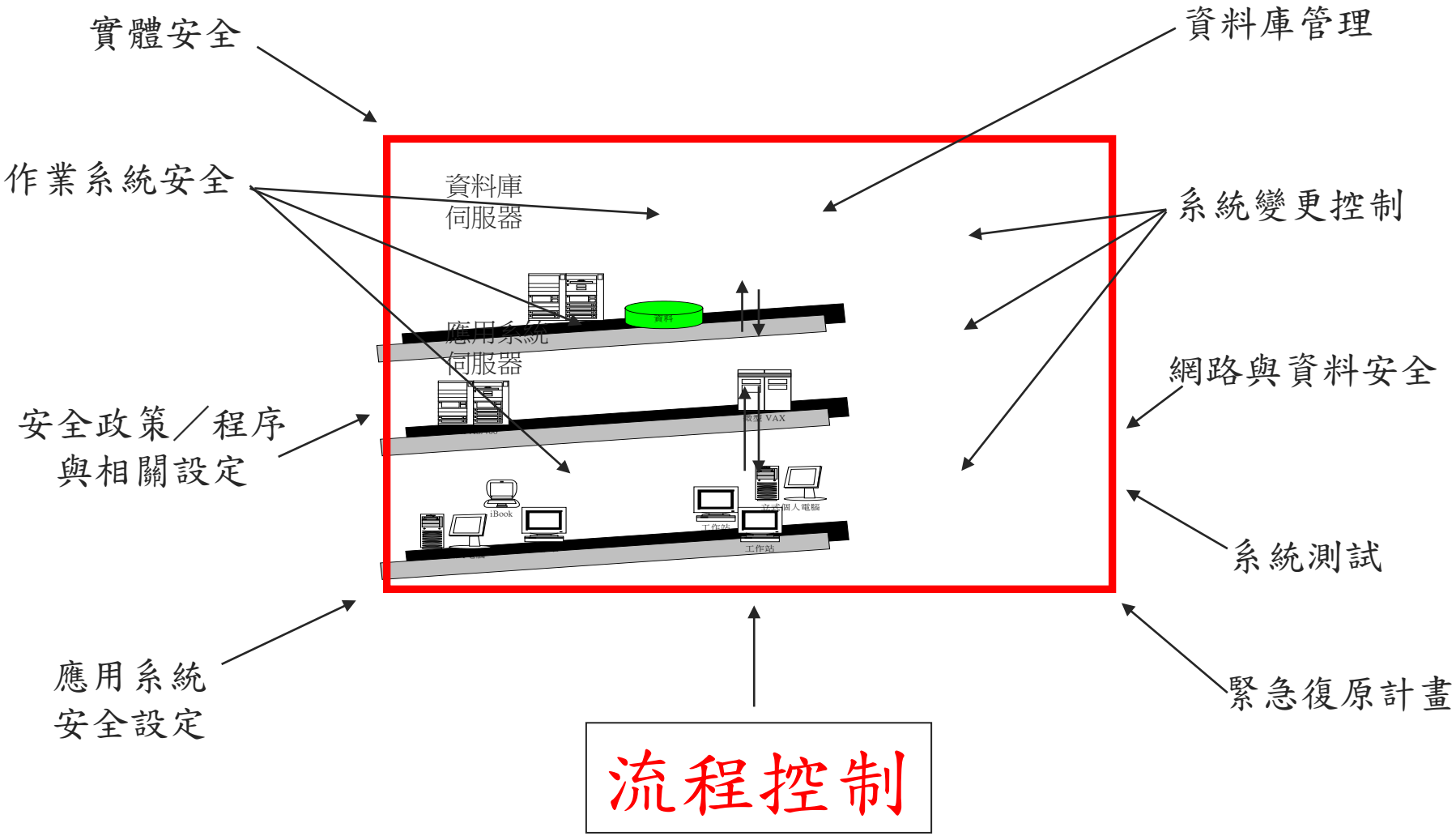
- COBOL File / DB2
- MS SQL / Access / DBF
- Oracle / Sybase / Informix

- DOS / Windows 9X / NT / 2000
- UNIX 家族 / Novell
- OS400 / VMS /OS2 / Tandem

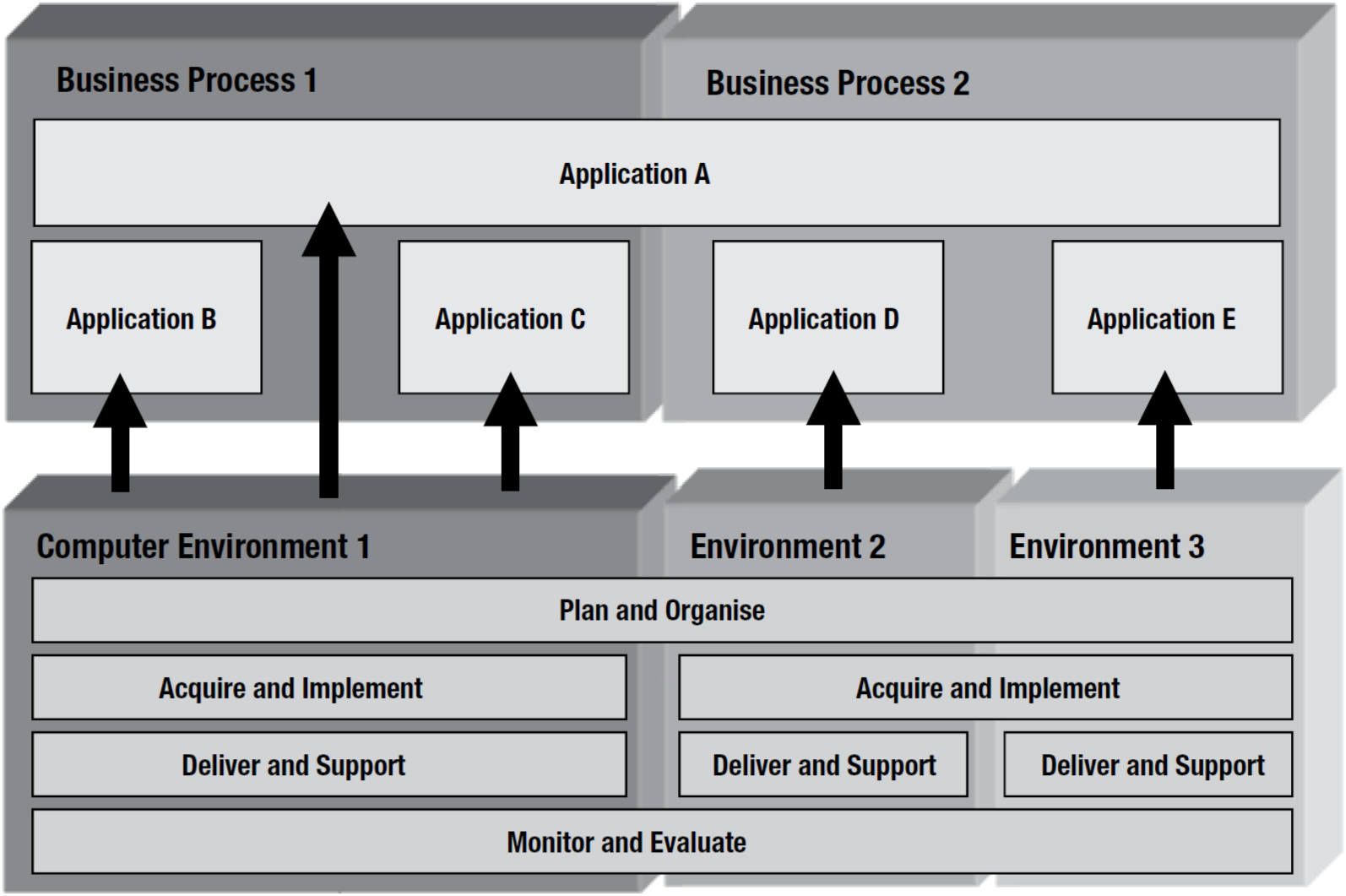
- PC-Anywhere / RAS / Dial UP服務
- TCP / UDP / IP / UUCP LAN等
- 防火牆 / IDS / IOS / Socket等

- 電腦 / 手機 / 數據機 / 網路卡 / 網路埠
- 集線器 / 交換器 / 路由器 / 閘道器
- 纜線 / ADSL數據機

資訊系統一般控制環境


實體安全
資料庫管理
作業系統安全
資料庫
伺服器
系統變更控制
應用系統
伺服器
網路與資料安全
安全政策／程序
與相關設定
系統測試
應用系統
安全設定
緊急復原計畫
流程控制

Understanding Computer Processing Environments



UProfit 兆益數位學苑

ITGC Overview

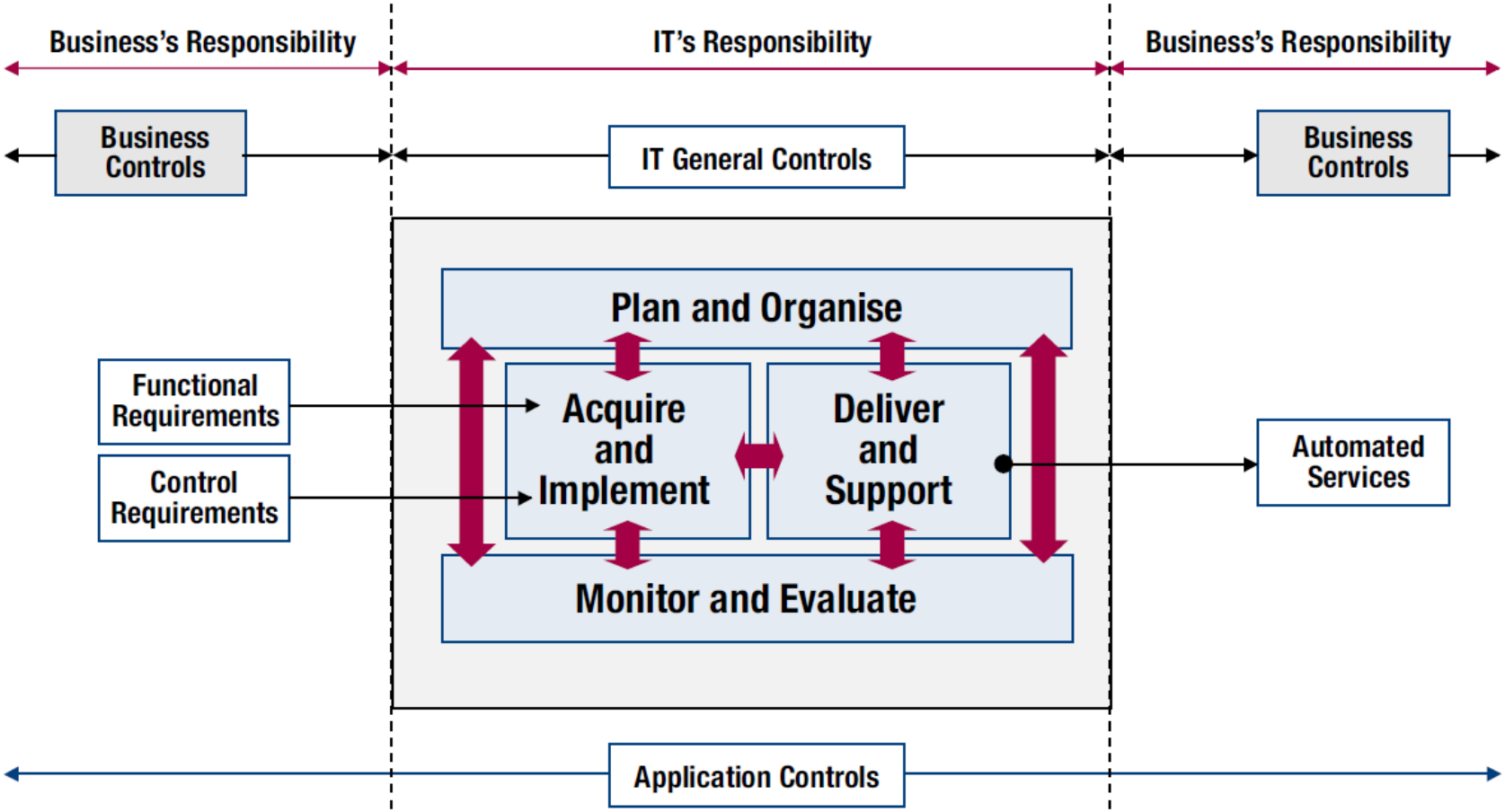
ITGC Section I – Key Application Identification

Identified Significant Business Process	Application Name	Underlying Infrastructure (Database, Operating System, Hardware)	Location Where Application is Hosted	IT General Controls			
				System Security / Access	Change Management	System Development	Computer Operations
Purchasing	GKPS	Oracle, Unix	NY Data Center	ITGC-1	ITGC-1	ITGC-1	ITGC-1
Purchasing	Purchman	MS SQL, Win2k	NY Data Center	ITGC-2	ITGC-2	ITGC-2	ITGC-1
Sales	MS Access	MS Access, Win 2k	Sales Mgrs office	PAD - X	PAD - X	ITGC-2	PAD - X

IT General Controls around end-user computing environment could be documented in the Process Analysis Document (PAD) and the working paper reference should be entered in Section I table of the ITGC document.

If more than one IT general control process exists in a given category (e.g.: two change management processes exist, each for a different application or data center), both should be documented in separate ITGC documents.

Boundaries Amongst Business, IT General Controls and Application Controls



課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

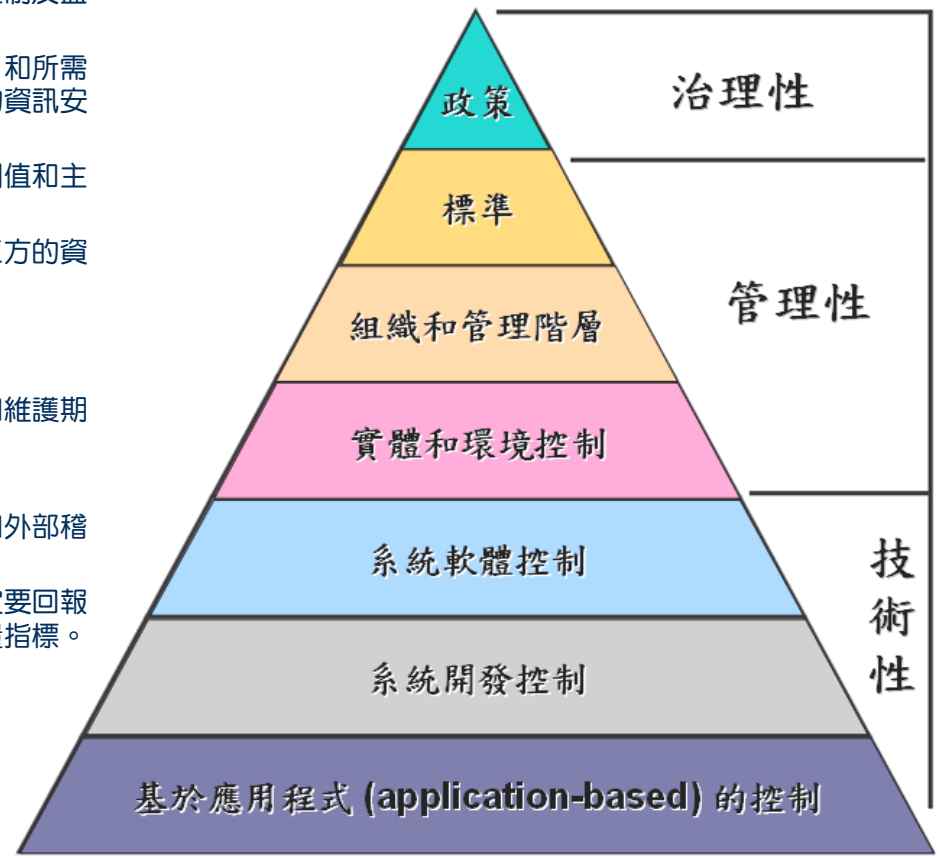
瞭解資訊科技控制

- **資訊科技控制**含蓋這些提供對**資訊**與**資訊服務**確認及協助降低組織使用資訊科技相關**風險**的作業。
- **兩個重要元素**
  - 營運控制自動化
  - 資訊技術控制

瞭解資訊科技控制

・管理階層

- 建立資訊安全管理政策和控制及監督遵循。
- 指派資訊安全角色、責任、和所需技能與執行以角色為基礎的資訊安全存取權限。
- 評估資訊風險，建立風險閾值和主動地管理風險抵減。
- 確保對策略夥伴和其他第三方的資訊安全要求之實施。
- 識別和分級資訊資產。
- 實施和測試營運持續計畫。
- 核准在取得、開發、運作和維護期間之資訊系統架構。
- 保護實體環境。
- 確保資訊安全計畫的內部和外部稽核有及時追蹤跟催。
- 與負責安全人員協作來指定要回報給管理階層的資訊安全衡量指標。



資訊科技控制層級

・治理（董事會）：

- 監督屬於資訊安全（例如，沙氏法案、美國醫療保險可攜性及責任法案、金融服務業現代化法案）的風險管理和遵循計畫。
- 核准和採用廣泛的資訊安全計畫原則，與核准負責資訊安全重要經理職位的指派。
- 基於資訊安全努力保護所有利害關係人的利益。
- 審查有關策略夥伴和其他第三方之資訊安全政策。
- 努力確保營運持續。
- 審查資訊安全計畫之內部和外部稽核的規定。
- 與管理階層協作來指定要被回報給董事會之資訊安全衡量指標。

・技術上的

- 建立完整的資訊安全計畫需要注意下列的技術的計畫要素：
- 使用者識別和身分認證。
- 使用者帳戶管理。
- 使用者權限。
- 組態管理。
- 事件和活動紀錄與監督。
- 通訊、電子郵件和遠端存取安全。
- 軟體變更管理，包含修補。
- 防火牆。
- 備份和回復。
- 事故和弱點偵測與回應。
- 與管理階層協作來指定回報給管理階層的技術衡量指標。

iProfit 兆益數位學苑

資訊科技控制層級

政策：

- 一個在整個組織的安全和隱私權保護層級之全面性政策。
- 在資訊分級（classification）和在每一階層存取權限上的條文。
- 資料和系統擁有權概念，與對建立（originate）、修改、刪除資訊必要性之授權（authority）的定義。
- 定義使用者能部署智慧型工作站來建立其自身應用程式之範圍的一般政策。
- 人員晉用政策（personnel policies）能對在敏感區域中的員工定義和限制前提條件（conditions）。
- 整體營運持續計畫要求的定義。 這些政策應確保在中斷（disruption）或災難（disaster）－ 不只是 IT 要件 － 事件中所有企業的面向有被考慮到。

SANS Security Policy Resource: http://www.sans.org/security-resources/policies

資訊科技控制層級

組織與管理階層：

- 職能分工(separation of duties)
- 財務控制(financial controls)
- 變更管理(change management)
- 其他管理性控制(如資訊安全計畫)

資訊科技控制層級

※標準也驅使組織更有效率地維護整個 IT 作業環境

標準：

- 系統開發流程（system development processes）
- 系統軟體組態（systems software configuration）
- 應用程式控制（application controls）
- 資料結構（data structures）
- 記錄（documentation）
- 其他標準

資訊科技控制層級

實體與環境控制：

- 將伺服器置於已上鎖、存取有限制的房間。
- 限制伺服器的存取給特定的人。
- 提供火災偵測和滅火裝置（suppression equipment）。
- 遠離有環境危害的地點，像是低窪積水地面或存放易燃液體之處，放置敏感設備、應用程式和資料。
- 緊急應變計畫(DRP & BCP)

資訊科技控制層級

系統軟體控制：

- 系統軟體產品驅使 IT 設備被應用系統和使用者所使用。
  - ✓ 這些產品包含作業系統像是 Windows、Unix 和 Linux；網路與通訊軟體；防火牆；防毒產品；和資料庫管理系統（DBMS）像是 Oracle 與 DB2。
- 根據組織所描述的政策分配和控制存取權限。
- 透過系統軟體和其他組態控制來執行職能分工 (division of duties)。
- 入侵和弱點評估（assessment），用在預防和偵測且持續監控。
- 定期執行入侵測試。
- 加密服務 (encryption services) 應用在有宣稱需要保密的情況。
- 變更管理流程 – 包含修補管理 – 有存在，來確保對軟體、系統、網路元件和資料應用所有變更和修補時，有嚴格控制的作業。

資訊科技控制層級

系統開發與取得控制：

- 使用者需求應被記錄，且其完成度應被衡量。
- 系統設計應遵循正常程序來確保使用者需求和控制有被設計進系統中。
- 系統開發應被以結構化的方法導入，來確保需求和設計功能有在最終完成的產品中被採用（incorporated）。
- 測試應確保單獨系統元件是有依需求運作、系統介面有依期望作業、使用者有參與測試流程，且期望的功能（intended functionality）有被提供。
- 應用程式維護流程應確保在應用系統中的變更遵循一致性的控制模式（pattern of control）。變更管理應以結構化的確認驗證程序。

資訊科技控制層級

以應用為基礎的控制

應用控制的定義-有關個別營運作業範圍或應用系統控制包括資料編輯、營運作業分工、處理總數平衡、交易日誌及錯誤異常報表。

應用系統內部控制目的：

- 所有輸入資料是精確的、完整的、有經授權的和正確的。
- 所有資料有依計畫處理。
- 所有儲存的資料是精確的且完整的。
- 所有輸出是精確的且完整的。
- 紀錄被維護來追蹤（track），從輸入到儲存且到最終的輸出之資料流程。

應用系統中常見的一般控制：

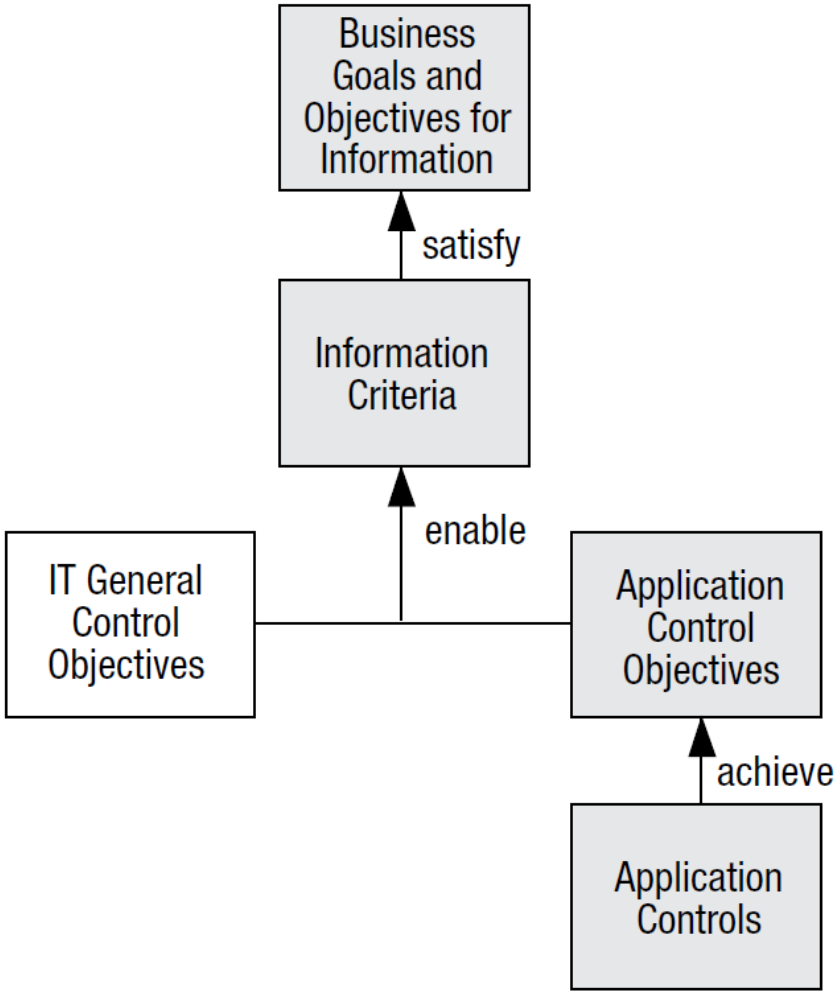
- 輸入控制（input controls）
- 處理控制（processing controls）
- 輸出控制（output controls）
- 完整性控制（integrity controls）
- 管理軌跡（management trail）

應用系統控制目的與資訊要件

Application Control Objectives	Information Criteria: Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
AC1 Source Data Preparation and Authorisation	S	P	S	P		S	
AC2 Source Data Collection and Entry	S	S	S	P		S	
AC3 Accuracy, Completeness and Authenticity Checks	S	P	S	P	S	P	P
AC4 Processing Integrity and Validity			P	P	P	P	P
AC5 Output Review, Reconciliation and Error Handling	P	S	P	P	P	P	P
AC6 Transaction Authentication and Integrity		S	P	P		P	

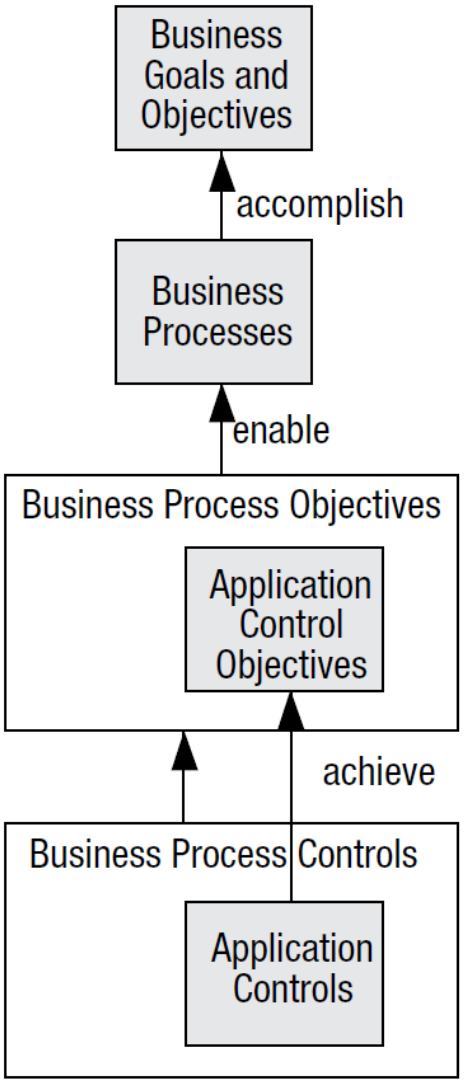
P = Primary; S = Secondary

應用控制(Application Control)的目標



營運流程與應用控制

- 營運風險與資訊流程
  - 不完整及不正確地資訊處理作業
  - 無效地或是未授權的交易被處理
  - 未授權地變更常設資料
  - 繞過、擅權、人為輸入規避控制
  - 無效率
  - 失去機密性
  - 無法及時提供資訊
  - 缺乏整合與可靠性



應用控制種類

- 輸入控制
  - 檢查輸入應用系統資料的一致性，資料是否直接由員工、交易夥伴遠端、或者透過網頁程式、或者介面輸入;檢查輸入資料確保維持在參數內。
- 處理控制
  - 提供自動化的方法確保處理是完整、精確和有被授權的。
- 輸出控制
  - 此項控制顯示資料處理被完成的結果，比較實際與預期輸出結果是否一致。
- 一致性控制
  - 監督資料從開始處理到儲存，確保維持一致性及正確性。
- 管理軌跡
  - 可讓管理者辨別交易及記錄追蹤交易從原始資料到輸出往回追溯事件，以確認控制作業有效性及辨別發生錯誤的來源。

應用控制分類要件

- 預防性控制(Preventive Control)
  - 檢查確保資料輸入符合應用系統程式邏輯一致性
- 偵測性控制(Detective Control)
  - 偵測一旦應用系統程式邏輯錯誤，能夠先發現異常資料被輸入系統
  - 支持人工控制與監督控制

Responsibility for Application Control Design and Implementation: RACI Chart

	Activities	Business Executives	Business Process Owners/Application Owners	Business Analysts	End Users	Project Managers	Programmers/IT Specialists/IT Application Owners	Risk and Control (and/or Security) Specialists	Internal and External Auditors
		Stakeholders							
Identify Relevant Control Objectives	Identify key stakeholders and assig application control-related roles and responsibilities	A	R	C	C	C		C	I
	Perform an assessment of information-related risk and information processing-related risks.	C	A	R	C	I		R	C
	Identify and document relevant control objectives.	C	A	R	C	I		R	C
	For third-party software, include control requirements in the RFP.	C	A	R	C	I		R	I
Design/Build/Configure Application Controls	Develop a detailed application specification design (including automated application controls).	C	A	R	C	R	C	C	C
	Evaluate vendor solution (including fit with control requirements.		A	R	C	R	C	R	C
	Develop future state business process design (including design of manual application controls to meet control objectives).		A	R	C	R	C	R	C
	Assess and determine sufficiency of the design of application controls.	A	R	C	C	R	C	C	C
	Develop program code and debug automated application controls as part of software development.		C	C	C	A/R	R	C	
	Install and configure commercial applications, including configurable controls.		C	R	C	A/R	R	C	I
Document Controls and Train Users	Develop/update application control documentation.		A	R	C	R	C	C	C
	Develop/update user training materials and provide training as required to affected staff.		A	R	R	R	C	C	I
	For new employees, provide full training on the application and relevant application controls.		A		R				
Test and Approve Application Controls	Develop, document and approve the test plan.		A	R	C	R	R	I	I
	Conduct application control testing in accordane with the test plan.		R	C	C	A/R	R	R	C
	Identify, log priorities and resolve errors and issues identified during testing.		R	C	C	A	R	R	I
	Document and interpret the final test results, including unresolved issues.		A	R	C	R	R	C	
	Approve test results.	A	R	C	C	R	C	C	I
	Approve design and implementation of application controls.	A	R	C	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

資訊安全

資訊安全政策

資訊安全組織

資產分類與控制

人員的安全管理

硬體及環境的安全管理

通訊及操作設備的安全管理

系統發展及維護上的安全管理

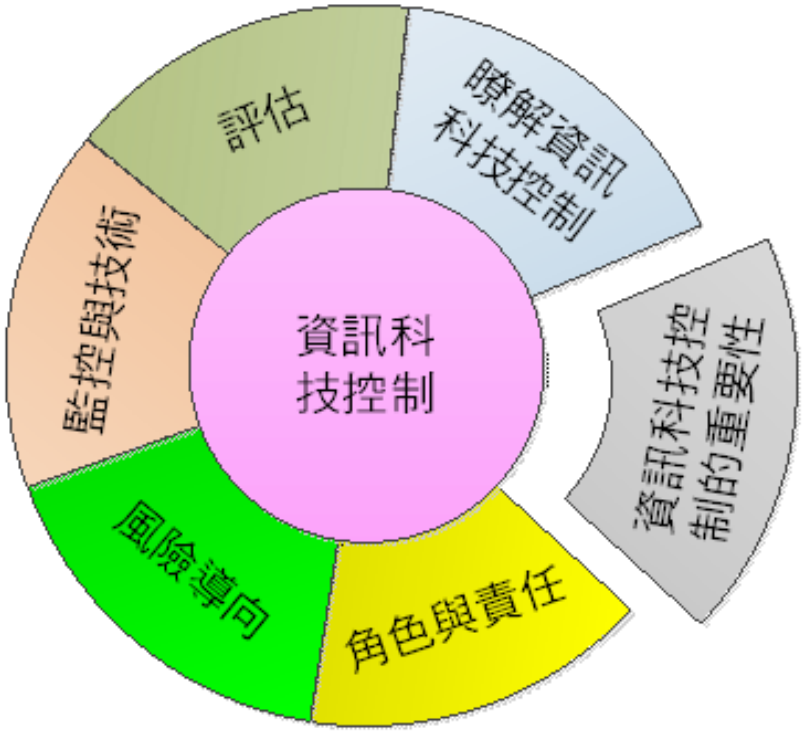
存取控制

商業持續性管理

符合性

資訊科技控制的重要性

- 對資訊科技控制的需求，例如：
  - 控制成本
  - 維持競爭力
  - 保護資訊資產
  - 法規遵循 (SOX)
- 實行有效的資訊科技控制，以改善營運效率、可靠性及確認性證據的可提供性。



課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

依據IIA國際專業實務架構-IPPF，
內部稽核人員被期望去適用，並堅持四個原則：
誠正，客觀，保密和適任，
適任／能力的原則要求內部稽核人員從事只有他們具備的知識、技能和經驗的服務項目。

IIA Attribute Standard 1210: Proficiency states －
『內部稽核人員須具備執行其個別職責所需之知識、技能及其他能力。
內部稽核單位整體須具備或取得履行其職責所需之知識、技能及其他能力』。

稽核長應該知道對查核所標訂的營運風險上的控制有效性，需要什麼樣的IT技能與能力水準，下列表格對應營運風險和所需要的IT控制，以及需要執行稽核的技能/能力展示一些範例:

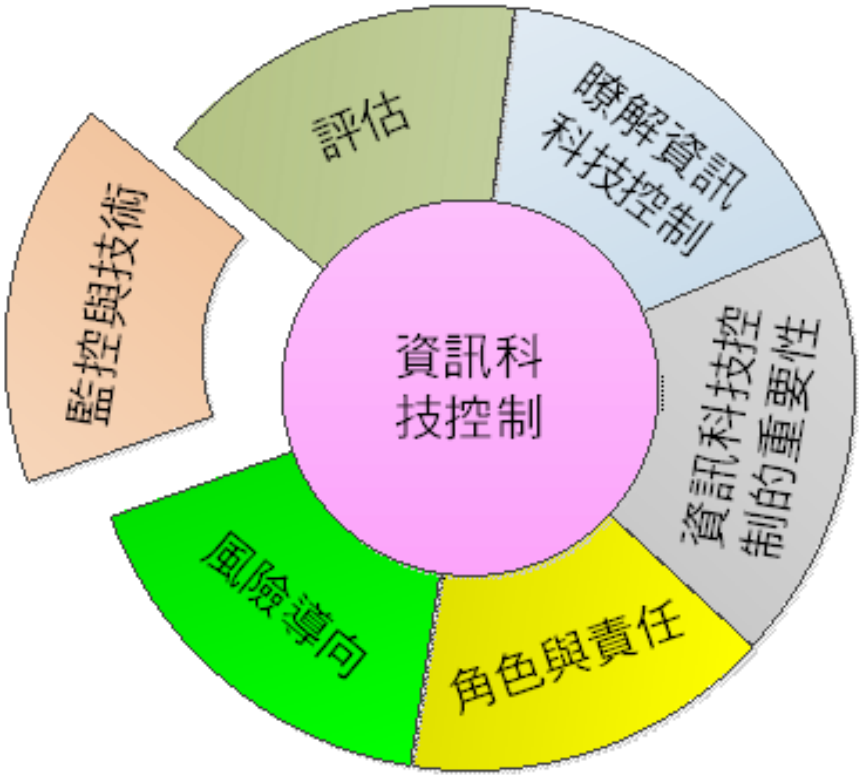
營運風險	資訊科技控制	資訊科技技能和能力
資訊安全管理	健全合理的邏輯安全控制	安全管理；網路存取控制、作業系統資料庫和應用系統層級
重要營運中斷	確保重要營運應用系統的可用性	營運持續性和災難復原計畫的IT設備(包括網路基礎建設、操作系統 、資料庫和應用程序)
不準確和不完整的財務和管理報告	保護資料的機密性和可用性	應用控制，變更控制和系統開發生命週期（SDLC）控制

課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

監控與技術

- 監控與評估資訊科技控制
  - ✓ 選擇控制架構
  - ✓ 持續監督/專案審查/自動化持續性稽核



科技技術控制的 COSO 模型

監督：

- 科技技術效能每月衡量指標
- 科技技術成本和控制效能之分析
- 定期科技技術管理評估
- 企業科技技術的內部稽核
- 高風險區域的內部稽核

控制活動：

- 複核變更管理委員會
- 比較科技技術推動、投資計畫和報酬
- IT計畫和系統架構的核准和文件化
- 遵循資訊和實體安全標準
- 定期實施營運持續風險評估
- 遵循科技技術標準

資訊與溝通：

- 公司定期宣達（內部網路，電子郵件、會議、郵寄）
- 持續對科技技術最佳實務的認知
- IT效能之調查
- IT和安全教育訓練
- 服務台問題之解決及追蹤

風險評估：

- IT風險被包含於整體公司風險評估
- IT整合進營運風險評估
- 區分高風險營運區塊 / 部門的 IT 控制
- IT內部稽核評估
- IT保險評估

控制環境：

- 從最高層的管理態度/風氣 – IT和安全控制被視為重要的
- 整體科技技術政策和資訊安全政策
- 公司科技技術治理委員會
- 科技技術架構和標準委員會
- 所有業務單位充份參與

監督IT控制

管理階層是負責監督和評估（assessing）風險。 稽核人員進行之監督和評估是要獨立證實（attest）管理階層對控制適當性的主張。

- 持續監督
  - ✓每日/定期
  - ✓事件驅動
  - ✓持續
- 專案審查
  - ✓年度(每季)控制評估-內控聲明
  - ✓稽核審查－Risk-Based Audit

要使用何種查核方法論?

- 從傳統查核方法到自動化系統處理重要商務交易之作業分析。
- 內部稽核專業實務的國際標準 (International Standards for the Professional Practice of Internal Auditing)
- 現今，沒有特定的查核方法論能被視為目前惟一僅有的最佳實務。
  - ✓ 當進行沙氏法案（Sarbanes-Oxley）要求的評估（assessment）時，以系統為基礎的（system-based）查核方式可能是最佳的方法。
  - ✓ 舞弊調查可能需要稽核軟體的使用來分析資料和找尋證據。 稽核軟體提供強的分析能力，加上能夠檢驗所有相關記錄和檔案。
  - ✓ 進行支援主要內部稽核目標之年度稽核作業大部分將可能循著以風險為基礎的（risk-based）方式實施。

測試IT控制和持續之確保

- 自動化持續監控
- 自動化的內部控制分析工具
- 自動化風險分析

課程大綱

1. IT相關的營運風險與控制基礎的介紹
2. 內部利害關係人與IT責任
3. 分析風險
4. 評估資訊科技-綜覽
5. 瞭解資訊科技控制的重要性
6. IT稽核能力和技能
7. 採用控制架構
8. 結論

總結

- 評估IT控制是個持續性的過程，查核方法要持續改善
- IT控制評估是首要考慮的稽核議題
- 稽核IT控制是個持續的學習過程
- 應用控制是具有成本效益的一種方法，可用來管理風險
- 內部稽核人員應該要判定他們組織內應用控制設計是否適當？且是否有效執行？
- 考量標竿可做為進一步減少測試工作的方式
- 有效地評估IT控制的關鍵，是與技術人員、管理階層和董事會成員的溝通。

Technology for GRC & Business Assurance

11070台北市信義區基隆路一段141號9樓之8
TEL:02-27601798 FAX:02-27601797
Mobile phone: 0937054999
E-mail: david_chuang@uprofit-tw.com
Web Site: www.uprofit-tw.com
Facebook 專頁: david.sc.chuang

Facebook 粉絲專頁:
兆益數位訊息網 - https://www.facebook.com/UprofitDigital
大衛營 Uprofit Connection - https://www.facebook.com/Uprofit.Connection
兆益電腦稽核論壇 - https://www.facebook.com/UprofitForum
全國大專院校電腦稽核個案競賽暨專題研討會 - https://www.facebook.com/ACLAward

David Chuang の觀網
blog.uprofit-tw.com

兆益數位學苑