<<會計資訊系統課程講義>>

# 企業資訊系統風險與控制

~電腦舞弊、COSO、COBIT及PKI架構探討~

周國華
國立屏東大學會計學系

初版：2007/12/10
本次修正：2023/03/31

# 目錄

# 智慧財產權聲明

- 本文件係由周國華老師獨自撰寫，除引用之概念屬於原文作者外，其餘文字及圖形內容之智慧財產權當然屬於周老師獨有。
- 任何機構或個人，在未取得周老師同意前，不得直接以本文件做為學校、研究機構、企業、會計師事務所、政府機關或財團法人機構舉辦教學或進修課程之教材，否則即屬侵權行為。
- 任何機構或個人，在未取得周老師同意前，不得在自行編撰的教材中直接大量引用本文件的內容。若屬單頁內部分內容之引用，亦請註明出處。

# 企業風險層次

- Dunn et al. (EIS, 2005)將企業面臨的風險分為五個層次：
  - 經濟體風險(economy risk)：影響整個經濟體(國家、區域)的風險，例如：景氣反轉、戰爭、SARS、恐怖攻擊、環境惡化等。
  - 產業風險(industry risk)：個別產業內所有公司都受影響的風險。
  - 企業風險(enterprise risk)：個別企業面臨的內、外部風險。前者包含道德欠缺、士氣低落、技能不足等；後者包含競爭加劇、產品或企業形象下降、供應鍊伙伴出現危機、突發性災難導致營運中斷、其他企業的併購行為影響本公司的競爭力等。
  - 企業程序風險(business process risk)：與企業程序內之個體(資源、事件、代理人)及個體間之關係有關的風險。
  - 資訊程序風險(information process risk)：與企業程序內各項資訊之紀錄、維護、報導有關的風險。➡ 本講義重點所在！

# 電腦舞弊及濫用

- 電腦舞弊及濫用(computer fraud and abuse)是資訊系統安全最大的威脅，它不僅與資訊程序風險攸關，也與其他層級的企業風險息息相關。
- Romney et al.(AIS, 15 ed, 2021)整理了五十多種與電腦舞弊及濫用有關的犯罪技術，以下為幾種常見項目：
  - 被駭電腦群組(botnet, bot herders), 殭屍電腦(zombies)
  - 阻斷服務攻擊(denial-of-service attack)
  - 竊聽(eavesdropping)
  - 駭客入侵(hacking)
  - 劫持(hijacking)
  - 身份盜用(identity theft)
  - 鍵盤動作紀錄(key logger)

- 密碼破解(password cracking)
- 導引至虛假的網站(pharming)
- 網路釣魚(phishing)
- 攢聚利息尾數(round-down)
- 微量監守自盜(salami technique)
- 在字紙簍中拼湊出秘密(scavenging/dumpster diving)
- 軟體盜版(software piracy)
- 垃圾郵件(spamming)
- 間諜軟體(spyware)
- 使用特殊軟體繞過系統安全檢查(superzapping)
- 後門程式(trap door)
- 木馬程式(Trojan horse)
- 網址類似的虛假網站(typosquatting/URL hijacking)
- 病毒(virus)
- 蠕蟲(worm)

# 電腦網路安全防護

- 為預防電腦舞弊及濫用造成的危害，無論家用或企業電腦，都應盡可能建立以下基本防護措施：
  - 電腦開機或登錄入口網頁應設置密碼。行動裝置可透過指紋辨識技術強化安全。
  - 每部電腦均應安裝防毒軟體，並定期更新病毒碼。
  - 電子郵件系統應強化病毒及垃圾郵件過濾功能。
  - 安裝軟體或硬體防火牆(firewall)。
  - 設置入侵偵測/預防系統(IDS/IPS)。
  - 作業系統及應用程式定期進行更新(例如：Windows update 或Microsoft update)，以及時修補程式安全漏洞。
  - 重要檔案應定期備份，重要應用系統應有備援系統。
- 行動裝置需注意GPS定位、資料自動上傳等設定，以免在不知覺中暴露行蹤、私密資料曝光。下載App軟體亦須注意資料存取權設定。
- 此外，企業應設置完善的內部控制制度，以降低企業資訊系統的風險，並確保營運程序及資訊處理程序的正確性及完整性。

# ChatGPT引發的資安疑慮



## 憂對手從ChatGPTGPT探知公司營業祕密

引自**2023/3/28**聯合報

本報求證台積電相關人員，原來ChatGPT具備深度學習程序，台積電擔心競爭對手只要每天向ChatGPT提問台積電員工最近都問哪些問題，如果ChatGPT整理出台積電員工詢問事項，三星就能從台積電可能觸及的事務，例如研發工程師可能詢問開發進度碰到瓶頸，不經思考就想考考ChatGPT能做出什麼回覆，殊不知也可能讓聊天機器人透過深度學習，蒐集有人問這類的問題，讓有心窺探台積電先進製程開發進度的三星，掌握台積電可能碰到的問題，或從對話中找到解決方法。

雖然台積電未明確指出要如何控管員工向ChatGPT詢問與公司有關的營業祕密，但由此也可見，ChatGPT應用泛濫，確實已有業者擔心可能成為洩露公司營業祕密破口。台積電限員工使用ChatGPT範圍，也可能喚起相關企業資安保護意識，尤其製程研發及設備研發工程師，或營業等掌握公司營業祕密重要單位，有必要在AI的浪潮下提高保護公司營業祕密的警戒，否則對公司的損害，可能不亞於遭駭客入侵。

# CERT/CC

- Morris & CERT/CC：
  - Robert T. Morris 在1988/11/2透過MIT的電腦網路散佈全球第一支網路蠕蟲(Internet Worm)，對剛起步的全球資訊網造成重大危害。有鑑於此類行為未來可能層出不窮，美國國防部在當時(1988/11)即出資在卡耐基美隆大學設立全球第一個電腦危機反應協調中心(Computer Emergency Response Team / Coordination Center)。此外，美國聯邦政府國土安全部在2003年另外設立US-CERT，做為政府與民間合作維護電腦網路安全的中介機構。
  - R. T. Morris在1989年被依違反美國「1986年電腦舞弊及濫用法」定罪，是全球第一個類似定罪案例。他後來從哈佛大學取得博士學位，目前任教於MIT。[台灣類似法例：刑法第三十六章「妨害電腦使用罪」]
- 世界各國隨後紛紛成立類似的機構。台灣目前也有多個CERT：
  - 台灣電腦網路危機處理暨協調中心(TWCERT/CC)：是台灣最早設立的CERT(成立於1998年)。已加入First.org。
  - 政府網路危機處理中心(GSN CERT/CC)：由行政院國家發展委員會設置。
  - 國家電腦事件處理中心(TWNCERT)：由資策會設置。已加入First.org。
  - 臺灣學術網路危機處理中心(TACERT)：設於高雄中山大學。
  - ✓ First.org：由各國CERT組織組成的區域性聯盟，便於迅速交換資安訊息。

# CSIRT

- 前頁介紹的CERT/CC在位階上屬於國家層級。由於電腦安全事件屢見不鮮，對個別企業的營運構成重大危害。因應此類事件，許多企業未雨綢繆紛紛成立電腦安全事件反應團隊(Computer Security Incident Response Team, CSIRT)，以因應此類事件的突發。
- 台灣目前已成立CSIRT、並加入First.org的機構有以下11家：
  - 奧義智慧科技(CCCSIRT)。
  - 勤業眾信會計師事務所(DTTW-CSIRT)。
  - 金融資安資訊分享與分析中心(F-ISAC Taiwan)
  - 中山科學院資訊通信研究所(NCSIST-CSIRT)。
  - 安華聯網(Onward CSC)。
  - 威聯通科技(QNAP PSIRT)。PSIRT的P代表產品。
  - 群暉科技(Synology PSIRT)。
  - 趨勢科技公司(TM CSIRT) 。
  - 台灣電腦網路危機處理暨協調中心(TWCERT/CC)。
  - 國家高速網路與計算中心(TWCSIRT) 。
  - 國家電腦事件處理中心(TWNCERT)。

# 內部控制

- 針對各種潛在的風險，企業都應規劃內部控制及危機處理程序，但須符合成本效益原則。
- 對企業內部控制制度現況的評估，是會計師進行財務報表審計的基礎。
- 內部控制可按事前、事後分成以下三種類型：
  - 預防性控制(preventive control)：能防止問題發生。
  - 偵測性控制(detective control)：能察覺出已發生的問題。
  - 修正性控制(corrective control)：能針對已發生的問題做改正。

# 內部控制制度相關法令

- 國內主要法令：
  - 證券交易法第14條之1 (授權金管會訂定相關準則)。
  - 公開發行公司建立內部控制制度處理準則 (金管會按證交法授權訂定，以下簡稱**內控準則**)。(最新修正日期：111/12/15)
  - 審計準則公報第48號：瞭解受查者及其環境以辨認並評估重大不實表達風險。
  - 金融控股公司及銀行業內部控制及稽核制度實施辦法。
- 美國主要法令：
  - Foreign Corrupt Practices Act (1977)：內控法治化的起點。
  - Statements of Auditing Standards (SAS) No. 78 & 94
  - Sarbanes-Oxley Act (2002, 簡稱SOX)：安隆案後的亡羊補牢。
  - Dodd-Frank Act (2011, 全名 Dodd-Frank Wall Street Reform and Consumer Protection Act)：2008 金融風暴後對華爾街進行的大整肅。

# 內部控制：八大循環 3-1

- 內控準則第7條：公開發行公司之內部控制制度應涵蓋所有營運活動，遵循所屬產業法令，並應依企業所屬產業特性以營運循環類型區分，訂定對下列循環之控制作業：

一、銷售及收款循環：包括訂單處理、授信管理、運送貨品或提供勞務、開立銷貨發票、開出帳單、記錄收入及應收帳款、銷貨折讓及銷貨退回、客訴、產品銷毀、執行與記錄票據收受及現金收入等之政策及程序。

二、採購及付款循環：包括供應商管理、代工廠商管理、請購、比議價、發包、進貨或採購原料、物料、資產和勞務、處理採購單、經收貨品、檢驗品質、填寫驗收報告書或處理退貨、記錄供應商負債、核准付款、進貨折讓、執行與記錄票據交付及現金付款等之政策及程序。

# 內部控制：八大循環 3-2

三、生產循環：包括環境安全管理、職業安全衛生管理、擬訂生產計畫、開立用料清單、儲存材料、領料、投入生產、製程安全控管、製成品品質管制、下腳及廢棄物管理、產品成分標示、計算存貨生產成本、計算銷貨成本等之政策及程序。

四、薪工循環：包括僱用、職務輪調、請假、排班、加班、辭退、訓練、退休、決定薪資率、計時、計算薪津總額、計算薪資稅及各項代扣款、設置薪資紀錄、支付薪資、考勤及考核等之政策及程序。

五、融資循環：包括借款、保證、承兌、租賃、發行公司債及其他有價證券等資金融通事項之授權、執行與記錄等之政策及程序。

# 內部控制：八大循環 3-3

六、不動產、廠房及設備循環：包括不動產、廠房及設備之取得、處分、維護、保管與記錄等之政策及程序。

七、投資循環：包括有價證券、投資性不動產、衍生性商品及其他投資之決策、買賣、保管與記錄等之政策及程序。

八、研發循環：包括對基礎研究、產品設計、技術研發、產品試作與測試、研發記錄與文件保管、智慧財產權之取得、維護及運用等之政策及程序。

公開發行公司得視企業所屬產業特性，依實際營運活動自行調整必要之控制作業。

# 電腦化資訊系統內控作業 2-1

- 內控準則第9條：公開發行公司使用電腦化資訊系統處理者，其內部控制制度除資訊部門與使用者部門應明確劃分權責外，至少應包括下列控制作業：

  一、資訊處理部門之功能及職責劃分。

  二、系統開發及程式修改之控制。

  三、編製系統文書之控制。

  四、程式及資料之存取控制。

  五、資料輸出入之控制。

  六、資料處理之控制。

  七、檔案及設備之安全控制。

# 電腦化資訊系統內控作業 2-2

八、硬體及系統軟體之購置、使用及維護之控制。

九、系統復原計畫制度及測試程序之控制。

十、資通安全檢查之控制。

十一、向本會(註：金管會)指定網站進行公開資訊申報相關作業之控制。

# 內部控制參考架構

- COSO 架構：由美國COSO委員會在1992年提出的內部控制整體架構，及COSO 2013更新版，已成為許多國家(包含台灣)制訂企業內部控制法令的重要參考資料。
- ERM 架構：由美國COSO委員會在2004年提出的企業風險管理架構，將過去以控制為基礎的1992 COSO架構，調整為以風險為基礎的2004新架構。此架構包含(而非取代)COSO 1992架構的內容，並增加新的元素，使其內容更完整且更有彈性。COSO在2017推出ERM更新版。
- COBIT 架構：由國際電腦稽核協會(ISACA)在1996年制訂的資訊科技內控架構(目前最新版本：COBIT 2019)，是許多AIS教科書討論企業資訊系統內部控制的主要參考資料。
- ITIL：由英國政府商務辦公室提出的資訊科技基礎架構庫，是一套與IT服務和管理有關的概念及實務彙整。
- ISO 27000系列：由ISO針對資訊安全議題制定的指引。

# COSO 架構 2-1

- COSO委員會(Committee of Sponsoring Organizations)在1992年提出的內部控制整體架構(Internal Control – Integrated Framework)，包含五個組成要素(以下說明內容取材自金管會制訂的內控準則第6條)：

一、控制環境(control environment)：係公司設計及執行內部控制制度之基礎。控制環境包括公司之誠信與道德價值、董事會及監察人治理監督責任、組織結構、權責分派、人力資源政策、績效衡量及獎懲等。董事會與經理人應建立內部行為準則，包括訂定董事行為準則、員工行為準則等事項。

二、風險評估(risk assessment)：風險評估之先決條件為確立各項目標，並與公司不同層級單位相連結，同時需考慮公司目標之適合性。管理階層應考量公司外部環境與商業模式改變之影響，以及可能發生之舞弊情事。其評估結果，可協助公司及時設計、修正及執行必要之控制作業。

# COSO 架構 2-2

三、控制作業(control activities)：係指公司依據風險評估結果，採用適當政策與程序之行動，將風險控制在可承受範圍之內。控制作業之執行應包括公司所有層級、業務流程內之各個階段、所有科技環境等範圍及對子公司之監督與管理。

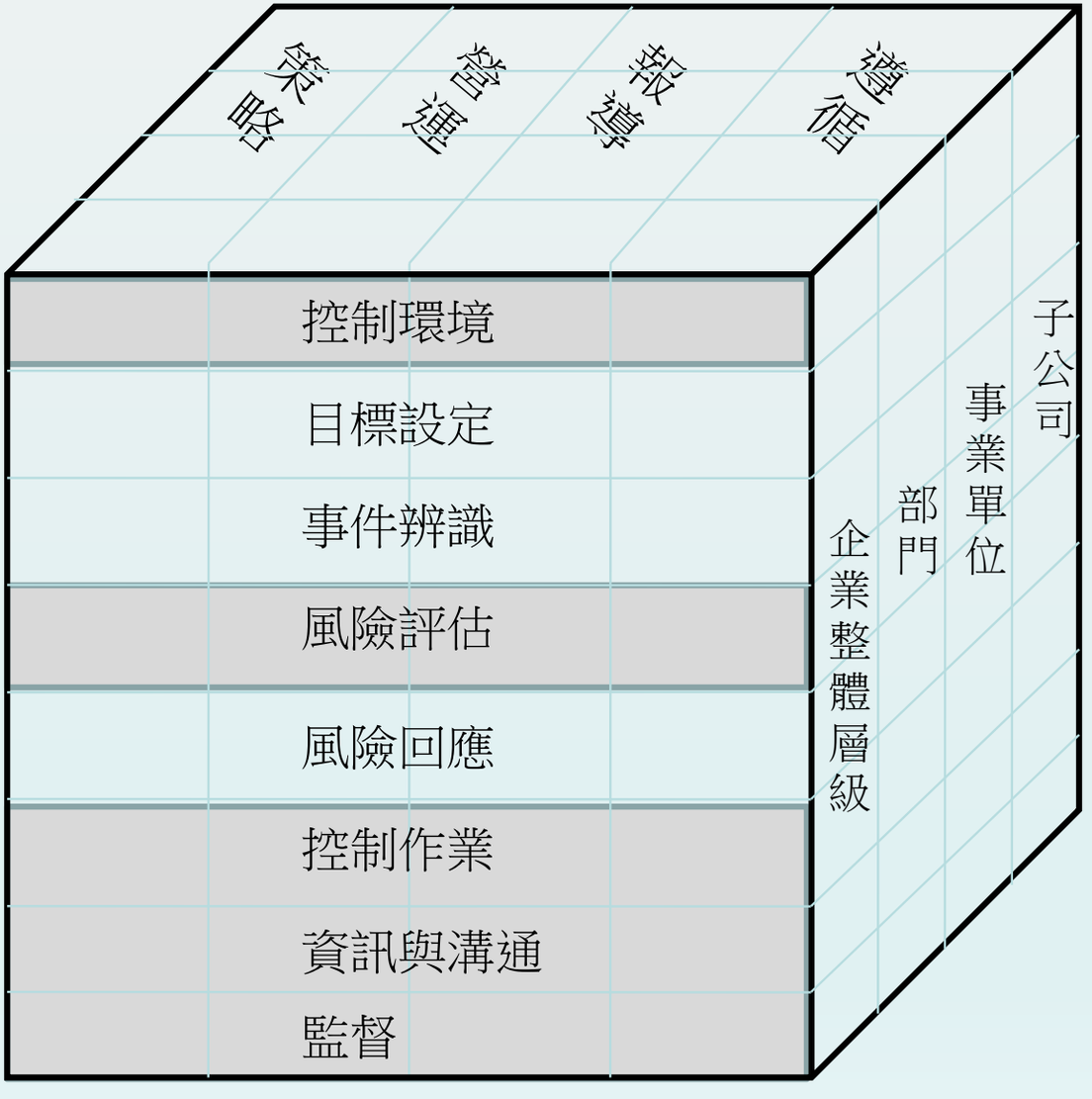
四、資訊與溝通(information and communication)：係指公司蒐集、產生及使用來自內部與外部之攸關、具品質之資訊，以支持內部控制其他組成要素之持續運作，並確保資訊在公司內部，及公司與外部之間皆能進行有效溝通。內部控制制度須具備產生規劃、執行、監督等所需資訊及提供資訊需求者適時取得資訊之機制。

五、監督作業(monitoring)：係指公司進行持續性評估、個別評估或兩者併行，以確定內部控制制度之各組成要素是否已經存在及持續運作。持續性評估係指不同層級營運過程中之例行評估；個別評估係由內部稽核人員、監察人或董事會等其他人員進行評估。對於所發現之內部控制制度缺失，應向適當層級之管理階層、董事會及監察人溝通，並及時改善。

# ERM (Enterprise Risk Management) 架構

- 美國COSO委員會提出企業風險管理整體架構(ERM, 2004)，以4類目標、8種組成要素及4種企業單位層級等三個構面建立企業風險管理模型：

＊ 右圖中有淡灰底色的五個要素為COSO 1992架構的內容。



# COBIT 架構

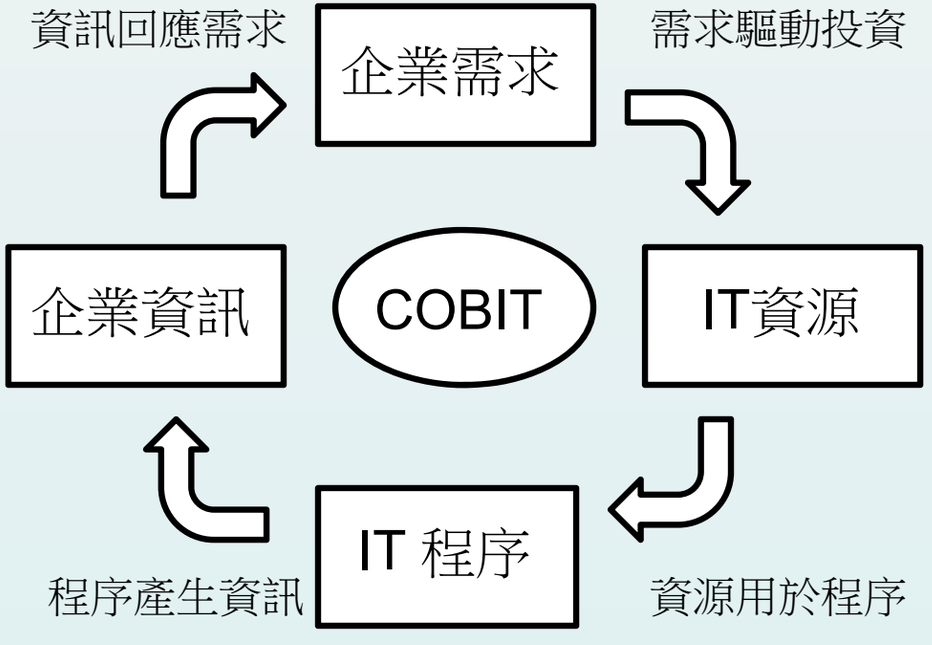
- ISACA在1996年制訂COBIT架構(**C**ontrol **Ob**jectives for **I**nformation and related **T**echnology)第一版。隨著國際IT治理協會(ITGI)在1998年成立，後續更新版本的制訂工作轉交由ITGI負責。
  - COBIT 最近幾個版本：4.1版 (2007年發佈)。COBIT 5 (2012年發佈)， COBIT 5以COBIT 4.1版為基礎，並將Val IT 2.0及Risk IT這兩套架構整合在內。COBIT 2019，在上述基礎上進行必要更新。

➢ 本講義以下說明仍以COBIT 4.1版核心內容為準。

- 為滿足IT治理的需求，ITGI採取四個導向制訂COBIT：
  - 以企業為焦點(business-focused)
  - 程序導向(process-oriented)
  - 以控制為基礎(controls-based)
  - 用衡量來驅動(measurement-driven)

# COBIT導向一：以企業為焦點

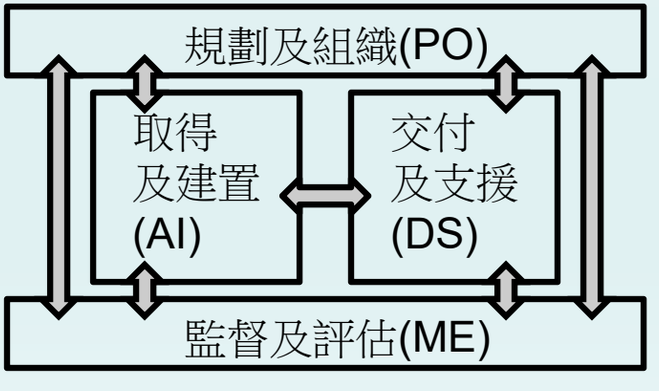
- COBIT架構的訴求對象並不限於IT人員，而是包含全體管理人員及企業程序負責人。
- 右圖顯示COBIT架構的基本原則：要取得為達成企業目標所需的資訊，企業必須投資在IT資源上，這些資源應使用結構化的程序來加以管理及控制，俾提供相關服務以產生所需資訊。



# COBIT導向二：程序導向

- COBIT將IT作業定義在34種通用程序內，這些程序分別歸屬於四個相互關聯的領域。這四個領域(domain)是：
  - 規劃及組織(plan and organize, PO)：對AI及DS提供指引。
  - 取得及建置(acquire and implement, AI)：提供解決方案並將其投入服務。
  - 交付及支援(deliver and support, DS)：取得解決方案並將其適用於終端使用者。
  - 監督及評估(monitor and evaluate, ME)：監督每個程序以確保其遵循PO所提供的指引。

四個領域彼此互動：



# COBIT導向三：以控制為基礎

- COBIT為34種通用IT程序分別制訂多項控制目標(control objective)，以PO1程序為例，有以下6項控制目標：
  - PO1.1：IT價值管理。
  - PO1.2：企業與IT協調一致。
  - PO1.3：目前能量與效能之評估。
  - PO1.4：IT戰略性規劃。
  - PO1.5：IT戰術性規劃。
  - PO1.6：IT群組管理。
- COBIT除了為每種IT程序制訂專屬的控制目標外，也制訂了6項適用於所有程序的通用程序控制(PC)(見次頁)。個別程序的專屬控制目標加上通用程序控制，構成完整的控制規範。

# 通用程序控制

- COBIT制訂6項適用於所有程序的通用程序控制(process control, PC)：
  - PC1：定義及傳達程序目的及目標。
  - PC2：指定一位程序負責人，並明訂其角色及責任。
  - PC3：程序應設計成可重複運作並產生一致的結果，並具有足夠彈性以處理意外狀況。
  - PC4：定義程序內的關鍵作業及最終產品，為關鍵作業指派角色及責任[: 使用RACI圖表(詳後述)]。
  - PC5：定義及傳達政策、計畫及程序如何驅動特定IT程序。
  - PC6：找出一組能對特定程序的成果及效能提供洞察力的衡量指標。

# RACI 圖表

- COBIT使用RACI圖表來說明每個程序內各項作業的角色及責任，RACI代表：
  - Responsible (R)：負責將任務完成。
  - Accountable (A)：提供指引及批准作業，負最終責任。
  - Consulted (C)：被諮詢。
  - Informed (I)：被告知。
- 例如，PO1程序的RACI圖表如下：

**RACI Chart**

| Activities \ Functions | CEO | CFO | Business Executive | CIO | Business Process Owner | Head Operations | Chief Architect | Head Development | Head IT Administration | PMO | Compliance, Audit, Risk and Security |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Link business goals to IT goals. | C | I | A/R | R | C | | | | | | |
| Identify critical dependencies and current performance. | C | C | R | A/R | C | C | C | C | C | | C |
| Build an IT strategic plan. | A | C | C | R | I | C | C | C | C | I | C |
| Build IT tactical plans. | C | I | | A | C | C | C | C | C | R | I |
| Analyse programme portfolios and manage project and service portfolios. | C | I | I | A | R | R | C | R | C | C | I |

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

# 企業內控及IT控制

- COBIT把企業內部控制系統對IT的影響分成三個層次：
  - 高階主管層：企業高階主管負責制訂企業政策及目標，其中包含公司治理方法及控制架構。IT控制環境則由此套政策及目標所導引。
  - 企業程序層：企業程序內的每一項作業都需要控制。大部分企業程序都已自動化，並且與IT應用系統整合，因此相關的控制也採自動化處理。企業程序層的控制稱為應用控制(application control)，包含由IT部門提供的自動化控制服務，以及仍有必要的人工化控制(例如：交易授權、工作劃分、人工調節等)。
  - IT整合性服務：企業各部門所使用的網路、資料庫及通用軟硬體等IT相關服務在大多數企業內是以整合性的方式由IT部門提供，IT部門對這些整合性的服務必須做適當的控制，這類控制稱為一般性控制(general control)。
    - 一般性控制是應用控制的前提：唯有在一般性控制提供可靠性後，應用控制的可靠性才能達成。

# IT 一般性控制及應用控制

- IT一般性控制內建在前述34種通用IT程序及服務內，例如：
  - 系統發展。
  - 變革管理。
  - 安全性。
  - 電腦運作。
- IT應用控制內建在個別企業程序的應用系統內，例如：
  - 完整性(completeness)。
  - 精確性(accuracy)。
  - 適當性(validity)。
  - 已獲授權(authorization)。
  - 工作劃分(segregation of duties)。
- COBIT認為，IT一般性控制的責任在IT部門，IT應用控制的責任則由IT部門及企業各部門共同承擔。

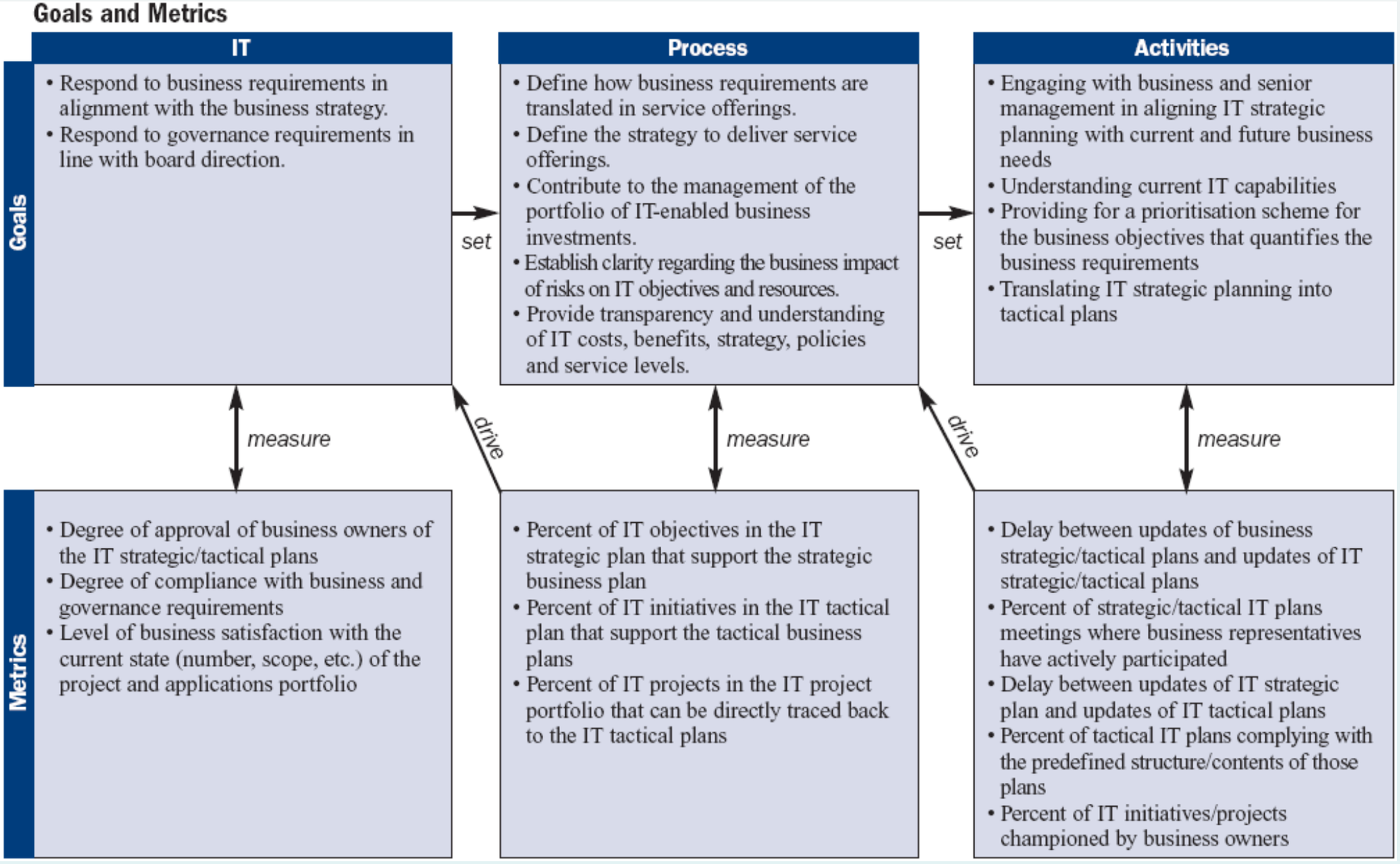
# 應用控制目標

- COBIT的核心內容是IT一般性控制，但它也提供了6項建議性的應用控制目標：
  - AC1：原始資料編製及授權。
  - AC2：原始資料蒐集及登錄。
  - AC3：精確性、完整性及確實性檢查。
  - AC4：處理完整性及適當性。
  - AC5：輸出檢核、調節及錯誤處理。
  - AC6：交易授權及完整性。

# COBIT導向四：用衡量來驅動

- 管理當局必須對IT系統是否達到預期目標做出客觀的評價，以做為進一步改進的參考。
- COBIT對於如何評價每一種IT程序的現狀及效能，提供一套系統性的方法：
  - IT、程序及作業的績效目標及衡量指標(範例見次頁)。
  - 成熟度模型(maturity model)：COBIT借用軟體工程領域的CMM方法，把IT程序的管理及控制成熟度分成(0)到(5)等六個等級：
    - (0) 不存在：並無任何管理控制。
    - (1) 剛起步：有管控程序，但缺乏組織。
    - (2) 以直覺方式重複：管控程序已遵循某種樣式。
    - (3) 程序已定義：管控程序已文件化並在組織內傳達。
    - (4) 已管理並且可衡量：管控程序已受監督及衡量。
    - (5) 達到最適化：管控程序遵循最佳實務且自動化進行。

# 績效目標(goal)及衡量指標(metric)範例：PO1程序



# 成熟度模型的應用

- COBIT的成熟度模型主要用來評估企業在個別IT程序的管控現狀之相對性，例如，以＊代表企業現狀、☆代表產業平均狀況、◆代表企業的改進目標，則可套用在某一特定IT程序上：

| 成熟度： | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 現狀及改進目標： | | | ＊ | ☆ | ◆ | |

# COBIT架構的侷限

- COBIT架構的內容主要是針對IT程序的一般性控制提出詳細規範。它雖然也對企業程序的應用控制提出六項建議性控制目標，但並未針對個別企業程序如何操作這六項應用控制目標提出指引。
- 個別企業程序之探討是會計資訊系統課程的核心內容，因此大多數AIS教科書都會針對個別企業程序的應用控制做深入探討。

# 控制矩陣

- Gelinas et al. (AIS, 11th ed., 2017)針對個別企業程序的IT應用控制，以控制矩陣(control matrix)的方式加以描述，其結構如下(以收款程序為例)：

| | 營運程序控制目標 | | | 資訊程序控制目標 | |
|---|---|---|---|---|---|
| | 確保營運效能 | 確保資源使用效率 | 確保資源安全性 | 收現資料，確保輸入適當性、完整性、精確性 | 應收帳款主檔資料，確保更新完整性及精確性 |
| 已存在控制 | | | | | |
| P-1 支票立即背書 | | | | | |
| P-2 去回性文件 | | | | | |
| …. | | | | | |
| 未設之控制 | | | | | |
| M-1 定期編製銀行調節表 | | | | | |

# 電子化企業平台安全控制

- 目前大多數企業已建置電子化企業(e-business)平台。透過此平台，一方面建立與供應商及客戶之間的B2B或B2C電子商務(e-commerce)交易網絡，另方面可建立內部文件無紙化(paperless)審核流轉機制。
- 資料在網路中移轉的安全問題，是電子化企業平台最重要的議題之一。此問題，可透過公開金鑰基礎架構(public key infrastructure, PKI)及衍生的電子簽章技術(digital signature)來加以處理。

# 電子簽章法 與 PKI 架構

- 台灣的電子簽章法自2002/4/1起實施，該法對PKI架構的基本名詞定義如下：
  - 電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。
  - 電子簽章：指依附於**電子文件**並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。
  - 數位簽章：指將電子文件以**數學演算法**或其他方式運算為一定長度之數位資料，以簽署人之**私密金鑰**對其加密，形成**電子簽章**，並得以**公開金鑰**加以驗證者。
  - 加密：指利用數學演算法或其他方法，將電子文件以**亂碼**方式處理。
  - 憑證機構：指簽發憑證之機關、法人。
  - 憑證：指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。
  - 憑證實務作業基準：指由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。

# 加密演算法 及 金鑰

- 電子化企業平台的交易安全核心，是以數位金鑰(即:憑證)透過加密演算法把文件加密。數位金鑰主要分為兩類：
  - 對稱性金鑰：資料發出方以金鑰將明文(plain text)轉成密文(cipher text)，資料接收方以同一份金鑰將密文解譯為明文。對稱性金鑰的處理效率較高，適用於處理大量交易；但因收、發方使用同一份金鑰，故該金鑰需具有絕對私密性。處理跨行提款及轉帳的金融資訊系統，即使用對稱性金鑰。
  - 非對稱性金鑰：資料發出方以資料接收方的公開金鑰(public key)將明文轉成密文，資料接收方再以自己的私密金鑰(private key)將密文轉成明文。目前許多企業、學校或政府機構的網站，網址以https開頭，s表示該網址是一個安全網站，受到SSL加密機制保護(在Chrome瀏覽器下於網址列左側顯示 符號)，使用者所輸入的資料會在傳輸前以該網站的公開金鑰加密，網站伺服器收到資料後，再以私密金鑰解密。(註：有些網站使用SSL的進階版TLS，但均以SSL為通用名稱)

# 電子簽章與加解密

- 以SSL (或TLS)加解密的電子商務交易，消費者不需要申請憑證，其功能主要在保障資料傳輸的安全性。但SSL並無法確認使用者身份，且消費者如果事後抵賴，商家很難在舉證上站得住腳。
- 為強化交易的身份驗證性及不可抵賴性，商家可要求消費者加上電子簽章。其運作模式為：
  1. 消費者將電子交易文件透過**雜湊函數**(hash function)轉成二進位碼。
  2. 消費者以自己的私密金鑰將上述二進位碼轉成電子簽章。
  3. 消費者將電子交易文件以商家的公開金鑰轉成密文。
  4. 消費者將電子交易密文、電子簽章及雜湊函數傳遞給商家。
  5. 商家以自己的私密金鑰將電子交易密文解譯成明文。
  6. 商家以消費者的公開金鑰將電子簽章解譯為二進位碼。
  7. 商家將電子交易文件明文以相同雜湊函數轉成二進位碼。
  8. 比對6及7的內容，若相同，則證明是該消費者所發出的交易文件。

# 憑證機構

- 在PKI架構下，使用者可向經核准設立的憑證機構(certificate authority, CA)申請金鑰對。金鑰對包含公開金鑰及私密金鑰各一份，通常CA會保留一份公開金鑰，私密金鑰則由使用者自行保管。
- 台灣目前已有許多憑證機構：
  - 政府部分：內政部自然人憑證管理中心，負責審核發放自然人憑證，此憑證亦通稱為電子身份證。其他由政府設立的CA有：研考會的政府憑證管理中心、經濟部的工商憑證管理中心…等。
  - 民間部分：台灣網路認證公司(金融交易憑證)、網際威信、是方、聯傳、博訊…等。許多證券公司亦設置CA，讓投資人申請憑證做為網路交易的驗證機制。
  - 許多大型企業及教育機構，為推動無紙化公文簽核機制之需要，在資訊部門或電算中心設置CA，讓員工申請金鑰對，做為公文電子簽章的驗證基礎。

# 相關證照及服務 2-1

- 市場上目前有三種與資訊系統風險控管相關的主流證照：
  - CISA (certified information system auditor)：台灣稱為國際電腦稽核師，由ISACA辦理認證考試，考題為150題單選選擇題。
  - CISSP (certified information systems security professional)：資訊安全管理師，由(ISC)$^2$辦理認證考試。
  - CISM (certified information security manager)：資訊安全管理師，由ISACA辦理認證考試。
- 美國會計師協會(AICPA)針對資訊系統及網路安全推出兩類型認證服務：
  - WebTrust：由會計師針對網站交易安全性及CA運作安全性提供認證服務。
  - SysTrust：由會計師針對供應鏈伙伴的資訊系統可靠性提供認證服務。

# 相關證照及服務 2-2

- 鑑識會計(forensic accounting)：
  - 新興的會計服務領域，由企業或政府聘請具有豐富學識及實務經驗的會計專家從事舞弊的偵察。
  - 在美國，許多鑑識會計專家受過FBI、IRS或其他執法機構的犯罪偵防訓練。
- 舞弊稽核師(certified fraud examiner, CFE)：
  - 由美國舞弊稽核師協會(ACFE)頒發的證照。
  - CFE證照考試內容涵蓋舞弊防制、財務交易(包含會計、審計、內部控制等主題)、舞弊調查、舞弊的法律要素等四個領域。每個領域每次考試都會出125個題目。
- 內部稽核師(certified internal auditor, CIA)：
  - 由國際內部稽核協會(IIA)頒發的證照。
  - CIA證照考試內容包含內部稽核基礎(125題)、內部稽核實務(100題)及內部稽核知識要素(100題)等三科。考題均為4選1單選題。