Lecture 5：企業資訊系統風險與控制 (AIS Risks and Controls)

編撰：國立屏東大學 周國華老師 日期：2026-03-25

一、課程回顧與導論

過去幾週，我們從基礎的關聯式資料庫，一路探討到能讓數據極速運算的 SAP HANA 引擎，以及實現單一真相來源的通用日記帳 (ACDOCA)。然而，當企業引進 ERP（如 SAP）在提升營運效率的同時，也高度集中了資訊風險。本週我們將探討企業面臨的風險層次、電腦舞弊的手法，以及如何透過國際風險控制框架與 SAP 系統設定，建立堅不可摧的內部控制防線。

二、企業面臨的風險層次與 AIS 的定位

在探討系統控制前，我們必須先具備宏觀的風險視野。根據 Dunn et al. (2005) 的研究，企業面臨的風險可區分為五個層次：

1. **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。
2. **產業風險 (Industry Risk)**：個別產業內所有公司都受影響的系統性風險。
3. **企業風險 (Enterprise Risk)**：個別企業面臨的內、外部風險。
    - 內部：包含道德欠缺、士氣低落、技能不足等。
    - 外部：包含競爭加劇、產品或企業形象下降、供應鏈伙伴危機、突發性災難導致營運中斷、其他企業併購行為影響競爭力等。
4. **企業程序風險 (Business Process Risk)**：與企業程序內之個體（即我們學過的 REA：資源、事件、代理人）及個體間之關係有關的風險。
5. **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。

學習重點：第五個層次「資訊程序風險」正是本課程 (AIS) 的核心！當所有會計數據都數位化後，這個層次的風險若失控，將直接導致財務報表不實。

三、電腦舞弊與濫用 (Computer Fraud and Abuse)

在資訊程序風險中，對企業殺傷力最大、最難防範的就是人為的惡意行為。要防範舞弊，我們必須先了解舞弊是如何發生，以及它們在系統中的哪個環節被執行。

1. **舞弊的發生要件：舞弊三角理論 (The Fraud Triangle)**。美國犯罪學家 D. Cressey 在 1953 年提出，所有的職場舞弊幾乎都具備三個共同要素。這也是我們設計內部控制時必須考量的人性盲點：

- **壓力 (Pressure)**：員工面臨財務困難（如投資失利、負債）或公司給予的業績壓力。
- **機會 (Opportunity)**：這是 AIS **內部控制唯一能積極介入的環節**！當系統缺乏職能分工 (SoD)、密碼管理鬆散、或沒有三方吻合檢查時，就創造了讓員工能執行並掩飾舞弊的機會。
- **合理化 (Rationalization)**：舞弊者說服自己的藉口，例如「我只是先借用，發薪水就還」、「公司對我不公，這是我應得的」。

* Wolfe & Hermanson (2004) 認為光有上述三個要素還不構，舞弊者還必須具備**能力(Capability)**，才能真正完成犯罪。這四個要素合起來稱為**舞弊鑽石理論(Fraud Diamond Theory)**。

2. 依「資料處理循環」劃分的五大舞弊節點。電腦舞弊並不僅僅是電影裡駭客敲敲鍵盤的畫面。在會計資訊系統中，舞弊可以發生在資料處理的任何一個階段：

- **輸入舞弊 (Input Fraud) - 最常見且最簡單：**
  - **資料竄改 (Data Diddling)：**在資料輸入系統前或輸入當下，非法修改資料。例如：會計人員在輸入薪資單時，偷偷把自己的加班時數灌水；或是竄改供應商的匯款銀行帳號。
- **處理器舞弊 (Processor Fraud)：**
  - 未經授權使用系統資源。例如：員工利用公司強大的伺服器算力來「挖礦（加密貨幣）」，或是利用公司網路經營私人網拍事業。
- **電腦指令舞弊 (Computer Instructions Fraud)：**
  - 透過惡意程式碼來操縱系統運算邏輯。
  - **沙拉米技術 (Salami Technique)：**從大量帳戶中各自偷取極微小的金額（如利息計算時無條件捨去的尾數），累積到舞弊者的帳戶中。因為單筆金額極小，極難被傳統的報表稽核發現。
  - **邏輯炸彈 (Logic Bomb) / 木馬程式 (Trojan Horse)：**IT 人員在系統中埋入惡意程式，設定在自己被解雇的那一天自動觸發，刪除公司核心資料庫。
- **資料舞弊 (Data Fraud)：**
  - 非法複製、瀏覽、竊取或破壞公司的核心資料庫。例如：離職員工偷偷用 USB 下載全公司的客戶名單與產品配方，賣給競爭對手。這也是企業近年面臨最嚴重的「營業秘密外洩」風險。
- **輸出舞弊 (Output Fraud)：**
  - 攔截、竊取或偽造系統產出的報表。例如：從印表機拿走未公開的機密財務報表，或是螢幕偷窺 (Shoulder Surfing) 主管畫面上的機密數據。

3. 現代常見的網路攻擊與社交工程手法。除了內部員工舞弊，企業系統還面臨外部無所不在的攻擊威脅：

- **社交工程 (Social Engineering) 與釣魚攻擊 (Phishing)：**駭客不直接攻擊防火牆，而是利用人性弱點（如恐懼、貪婪、好奇）。例如：發送偽裝成「SAP 系統緊急密碼重設」的釣魚郵件，騙取高階主管的帳號密碼。
- **勒索軟體 (Ransomware)：**例如將企業的資料庫（包含所有會計帳冊）惡意加密，導致 ERP 系統全面癱瘓，並要求企業支付比特幣等高額贖金才給予解密鑰匙。
- **阻斷服務攻擊 (DDoS)：**透過殭屍網路發送海量無效的存取請求，塞爆企業的伺服器頻寬，導致正常的客戶與員工無法登入系統。

四、法規遵循與國際主流風險控制框架

為了遏止舞弊與控制系統風險，國際法規與專業組織制定了嚴格的框架。現代會計人必須了解，IT 控制不僅是技術問題，更是「法律責任」。

1. 法律與規範的強制要求 (Compliance)

- **美國沙賓法案 (Sarbanes-Oxley Act, SOX，2002 年)：**
    - **SOX 404 條款：**要求上市櫃公司的管理階層必須出具「財務報導內部控制 (ICFR) 有效性」的聲明，且外部會計師必須對其進行查核並出具意見。
    - **核心鐵律：**現代企業財務數據由 ERP 產出，因此「沒有有效的 IT 系統控制，就不可能有有效的財務報表控制」。
    - 創立「**公開發行公司會計監督委員會 (PCAOB)**」，將會計師行業由過去的「自我監管」轉為「政府獨立監管」。
    - **限制非審計服務：**嚴格限制會計師事務所向其審計客戶提供特定的諮詢服務，以確保查核的獨立性。
- **台灣《公開發行公司建立內部控制制度處理準則》(**最新修正：113/4/22)。金管會的內控準則規範與時俱進，除了跟進國際法規趨勢(納入後述 COSO 架構的五大要素)，近年大幅強化資安監管力道，要求企業落實以下控制：
    - **第 9 條（電腦化資訊系統的 11 大控制）。**企業的內部控制必須專章規範系統作業，這也是會計師 IT 查核的法定項目：
        1. 資訊處理部門之功能及職責劃分（即 IT 部門的 SoD）。
        2. 系統開發及程式修改之控制（對應 SAP 的 TMS 傳輸管理）。
        3. 編製系統文書之控制。
        4. 程式及資料之存取控制（對應 SAP 的 BASIS 權限與密碼管理）。
        5. 資料輸出入之控制。
        6. 資料處理之控制。
        7. 檔案及設備之安全控制（如機房實體門禁）。
        8. 硬體及系統軟體之購置、使用及維護之控制。
        9. 系統復原計畫制度及測試程序之控制（災難復原 DRP 與備份演練）。
        10. 資通安全檢查之控制（防範駭客、勒索軟體與惡意攻擊）。
        11. 向主管機關指定網站進行公開資訊申報相關作業之控制（確保上傳至公開資訊觀測站的財報與重訊安全無誤，防範提早外洩或竄改）。
    - **第 9-1 條（資安治理提升至高階管理層）：**明訂公開發行公司應配置適當人力與設備執行資安管理。符合一定條件者，更被強制要求指派高階主管兼任「資訊安全長 (CISO)」，並設置資安專責單位與人員。(參閱 **附錄 1：台積電的資訊安全控制**)

2. 兩大國際控制架構 (COSO 與 COBIT)

- **COSO 內部控制整合架構 (**COSO Internal Control Integrated Framework，1992 年初版)：全球通用的企業內部控制架構，包含五大要素：**控制環境、風險評估、控制作業、資訊與溝通、監督作業**。
    - COSO 提出的五大要素已成為各國制定內控法規的基本規範，前述台灣的內控準則也完整納入 (內控準則第 6 條)。
    - COSO 架構於 2013 年更新，在五大要素下增加 17 項原則，2023 年再發佈 ICSR 指引將 17 項原則適用到 ESG 報告。

- COBIT (Control Objectives for Information and Related Technology) 是由**國際電腦稽核協會 (ISACA)** 所發布的國際公認 IT 治理與管理框架。
    - **核心定位：**如果說 COSO 框架是適用於全公司的「廣泛性健康指南」，那麼 COBIT 就是專門為資訊科技 (IT) 環境量身打造的「作業與查核手冊」。
    - **解決的痛點：**企業高層懂業務不懂技術，IT 人員懂技術不懂商業風險。COBIT 的核心價值在於提供一套共通語言，**完美橋接「業務目標」、「IT 風險」與「技術控制」之間的鴻溝**。
    - **實務應用：**它提供了非常詳細的「控制目標」與「成熟度模型」。例如，當法規要求企業必須做好「系統變更管理」時，查核人員就會直接翻開 COBIT 框架，逐一核對企業的作法是否符合其中的標準指標。
    - **CISA 證照：**ISACA 也主辦國際電腦稽核師(CISA)證照考試，內容涵蓋 COBIT 規範及其他電腦稽核專業知識。(參閱 **附錄 2：IT 查核領域的黃金證照**)

3. 進階風險視角：COSO ERM (企業風險管理整合架構，2004 年初版)。隨著商業環境日益複雜，傳統的內部控制已不足以應付全面性的危機。因此，COSO 委員會進一步擴展了原有的內控框架，提出了 **ERM (Enterprise Risk Management) 架構**。

- **ERM 的核心精神：**內部控制主要偏向「防弊與合規（保護價值）」；而 ERM 則進一步結合了企業的「策略設定（創造價值）」，強調在追求利潤的同時，如何將風險控制在企業的「風險胃納 (Risk Appetite)」之內。
- **風險管理的四種回應策略 (Risk Response)。**當企業辨識出資訊系統風險（例如：伺服器遭受駭客攻擊、SAP 系統當機）後，管理階層必須採取以下四種策略之一來應對：
    1. **規避 (Avoid)：**停止產生該風險的活動。例如：評估後發現自建機房風險太高，決定廢除自建機房。
    2. **降低 (Reduce)：**採取控制措施來降低風險發生的機率或影響程度。例如：導入防火牆、嚴格設定 SAP 存取權限、實施職能分工 (SoD)。**（這是內部控制最主要的發揮領域）**
    3. **分擔/移轉 (Share/Transfer)：**透過轉嫁將風險的衝擊降低。例如：購買資訊安全保險，或是將 ERP 系統委外給專業的雲端供應商（如 SAP HEC，參閱 **附錄 3**）代為維護管理。
    4. **接受 (Accept)：**當風險發生的機率與影響極低，且採取控制的成本大於風險損失時，企業選擇不採取任何行動，直接承擔風險。

五、達成安全目標的現代技術：公開金鑰基礎建設 (PKI)

在無紙化與電子商務時代，要確保交易的「機密性、完整性與不可否認性」，必須仰賴 PKI 架構 (Public Key Infrastructure)。這是一種使用「金鑰對（公開金鑰與私密金鑰）」的非對稱加密技術。

1. 電子交易的加密與驗證流程 (以消費者向商家網購為例)：

A. 商家與消費者皆需擁有自己的金鑰對。

B. 消費者用商家的公開金鑰(public key)，將交易文件明文加密成「電子交易密文」。(確保機密性)

C. 消費者將交易文件明文透過雜湊函數 (Hash Function) 轉換為二進位碼。

D. 消費者再用自己的私密金鑰(private key)，將這串二進位碼加密成「電子簽章」。(確保不可否認性)
E. 消費者將「電子交易密文」、「電子簽章」及「雜湊函數」傳遞給商家。
F. 商家用自己的私密金鑰解開交易密文，得到明文。
G. 商家用消費者的公開金鑰解開電子簽章，得到消費者原始的二進位碼。
H. 商家將解開的交易明文，用相同的雜湊函數轉成二進位碼，並與步驟 G 的結果比對。若兩者完全相同，則證明該文件確實由該消費者發出且未被竄改 (確保完整性)。

2. 憑證機構 (Certificate Authority, CA)

為了證明「公開金鑰」真的是某個人的，必須有公正的 CA 來核發與管理憑證。

- 台灣政府 CA：內政部自然人憑證管理中心（電子身分證）、經濟部工商憑證管理中心..等。
- 台灣民間 CA：台灣網路認證公司(TWCA，處理金融交易憑證）、網際威信、中華電信通用憑證管理中心..等。
- 企業內部 CA：許多大型企業與教育機構為推動無紙化公文簽核，會在資訊中心自建 CA。

六、SAP 實務防線：ITGC、ITAC 與稽核軌跡

理解了理論後，我們來看 SAP S/4HANA 如何透過具體的交易代碼 (T-Code) 落實這些控制防線：

1. 資訊科技一般控制 (ITGC) 與權限安全

這是針對整個系統基礎建設的控制，確保環境安全。

- 存取安全與密碼策略 (RZ10)：BASIS 管理員透過此工具設定密碼長度、複雜度、定期更換與登入失敗鎖定，防範帳號被暴力破解。
- 正式環境保護 (SCC4)：可將正式系統 (PRD) 設定為「不可更改配置 (No changes allowed)」，確保所有變更都必須嚴格走 TMS 傳輸機制，防範 IT 人員在正式區偷偷修改底層設定。

2. 資訊科技應用控制 (ITAC) 與財務防護

這是針對特定業務流程的自動化防禦機制，有效防止輸入錯誤或越權操作。

- 過帳期間控管 (OB52)：會計主管月底結帳後，必須在此關閉舊的會計期間。系統會自動擋下所有企圖倒填日期 (Backdated) 的跨期作帳行為。
- 限額檢查與員工容忍度 (OBA4)：會計主管可設定群組權限（如限制初階會計員單筆分錄最高 $100,000）。超過金額系統將亮起紅燈並阻擋存檔。
- 三方吻合 (Three-Way Match)：防範採購舞弊的最強武器。系統自動比對：採購單(PO) → 收貨單(GR) → 發票(Invoice)。若金額不符，系統將自動凍結該筆付款 (Block for Payment)。

3. 稽核軌跡 (Audit Trail) 與日誌監控

當防線被突破，或者需要追查「凡走過必留下痕跡」的鐵證時，這是稽核人員必查的工具。

- 變更文件評估 (AUT10)：查核舞弊的終極工具。若有人竄改供應商銀行帳號，此工具能精準調出「改動前/後」的數值、修改時間戳記 (Timestamp) 以及作案帳號。

- 資安稽核日誌 (RSAU_CONFIG)：記錄系統層級的異常行為，例如「誰在半夜三點嘗試登入失敗」、「誰試圖執行無權限的 T-code」。

七、會計內控的靈魂：職能分工 (Segregation of Duties, SoD)

這是預防舞弊的核心原則：「任何人都不能同時掌握一項交易的所有環節，以防止一人獨大並掩飾舞弊。」 常見的絕對衝突點包括「採購 vs. 付款」、「維護供應商主檔 vs. 開立發票」等。

在 SAP 中，我們透過以下工具來落實並稽核 SoD 衝突矩陣：

- 角色與帳號切割 (SU01 / PFCG)：嚴格劃分每個帳號能使用的 T-code，確保權限不重疊。
- 權限稽核神兵 (SUIM 使用者資訊系統)：這是稽核人員的最愛。可以瞬間查出「全公司有誰同時擁有採購與付款權限」，或「誰在過去 90 天內未曾登入系統」，藉此揪出潛在的 SoD 漏洞與幽靈帳號。

八、結語與預告

再強大的 HANA 引擎，都需要嚴謹的控制框架 (COSO/COBIT)、先進的密碼學技術 (PKI) 以及系統實務控制 (ITGC/ITAC/SoD) 來防範五大層次的企業風險。內部控制不是阻礙業務，而是確保財務資訊正確可靠。

下次課程我們將正式踏入核心業務循環，從「銷售與配銷模組 (SD)」開始，體驗從客戶詢價到開立發票的 Order-to-Cash (O2C) 完整流程！

附錄 1：台積電的「資訊安全控制」

[參考資料：台積電 113 年永續報告書、台積電 2024 年報、台積電企業網頁、iThome 專題報導]

台積電（TSMC）將資訊安全視為公司生存的命脈，其資安控制體系不僅是為了保護自身製程領先地位，更是為了維護全球半導體供應鏈的穩定。

台積電的資安控制主要圍繞**「機密資訊保護（PIP, Proprietary Information Protection）」**展開，並結合了高度自動化的技術防禦與嚴格的人員管理：

1. 組織架構與治理

- **資安長 (CISO) 制度**：台積電設有資安長(由資深高階主管兼任)，直接向執行長與董事會報告，確保資安決策具備最高層級的授權。
- **資安委員會**：定期審查全球廠區的資安風險，並針對新興威脅（如供應鏈攻擊、勒索軟體）制定應變策略。

2. 多層次防禦架構 (Defense in Depth)

台積電採取「零信任（Zero Trust）」原則，將控制點佈署在多個維度：

- **網路隔離 (Network Segmentation)**：將辦公區域網路與晶圓廠（Fab）生產網路嚴格隔離，防

止惡意程式橫向擴散。

- **端點防護**：所有入廠設備（包含筆電、USB）皆須經過掃毒與資安合規檢查，並對員工使用的電腦進行高強度的側錄與監控。
- **雲端安全**：針對採用雲端運算的研發環境，實施嚴格的資料加密與存取權限管理（IAM）。

3. 機密資訊保護 (PIP) 控制 [PIP: Proprietary Information Protection]

這是台積電內控中最具特色的一環，針對「文件」與「資料」進行精細化管理：

- **文件標籤化與加密**：所有敏感文件皆會自動上標（如：Confidential, Top Secret），且具備動態浮水印，追蹤所有存取與列印紀錄。
- **數位權限管理 (DRM)**：即便文件被帶離公司環境，若未經授權也無法開啟，且可遠端撤銷存取權。[DRM: Digital Rights Management]
- **通訊管制**：廠區內禁止攜帶具有攝影與傳輸功能的智慧型手機（或需張貼禁拍標籤），並嚴格監控對外電子郵件與通訊軟體的內容。

4. 供應鏈資安管理

台積電深知資安缺口往往來自合作夥伴，因此：

- **供應商稽核**：要求所有設備供應商與委外夥伴必須符合台積電的資安規範，並進行定期的資安成熟度評鑑。
- **入廠維修管控**：針對設備商進入廠區維護的工具機（Tools），設有專門的病毒過濾機制（Scrubbing Station），確保外部設備不會帶入感染源。

5. 自動化監控與事件應變 (SOC) [SOC: Security Operations Center]

- **24/7 資安監控中心 (SOC)**：利用 AI 與機器學習技術，即時偵測異常流量或員工異常行為。
- **演練與紅隊測試**：定期進行駭客攻擊模擬與紅隊測試（Red Teaming），以驗證內部防禦系統是否仍具備韌性。

6. 國際標準合規

台積電已取得 **ISO 27001**（資訊安全管理系統）與 **SEM 規格 (SEMI E187)** 等國際認證。值得注意的是，台積電也是推動半導體設備資安標準（SEMI E187）的主要推手，要求設備商在出廠前就必須符合特定的資安防禦規範。

附錄 2：CISA (國際電腦稽核師)：IT 查核領域的黃金證照

CISA (Certified Information Systems Auditor) 由 ISACA 發行，是全球歷史最悠久、最具權威性的電腦稽核專業證照。

- **專業地位：**在四大會計師事務所的「風險諮詢 (Risk Advisory)」或「電腦稽核 (IT Audit)」部門，CISA 是晉升與執業的必備敲門磚，其含金量在特定領域經常與會計師 (CPA) 證照齊名。
- **考試核心領域：**CISA 的測驗內容完美對應了我們 Lecture 5 教學的知識點，包含：
    1. 資訊系統稽核流程
    2. IT 治理與管理 (充分融入 COBIT 精神)

3. 資訊系統的取得、開發與建置 (如系統上線控制)
4. 資訊系統營運與企業韌性 (如災難復原、日常維運)
5. 資訊資產的保護 (即資安 CIA、密碼學與網路安全) [CIA: Confidentiality 機密性、Integrity 完整性、Availability 可用性]

- **學生的職涯優勢：**傳統會計系學生通常缺乏 IT 背景，資管系學生又不懂審計準則與財報。若會計系學生能透過 AIS 課程打底，未來考取 CISA 證照，將成為就業市場上極度稀缺的「跨領域雙棲人才」。

附錄 3：SAP HEC

SAP HEC，全名是 SAP HANA Enterprise Cloud (HANA 企業雲)。

如果用一個簡單的比喻：企業導入 SAP S/4HANA 就像買了一台頂級的超跑。過去，企業必須自己蓋一個恆溫車庫、自己聘請頂級技師來保養（這稱為**地端自建，On-Premise**）；而現在，企業可以選擇把這台超跑停在 SAP 原廠直營的 VIP 專屬車庫裡，由 SAP 的原廠技師團隊來幫你做 24 小時的維護、保養與升級，這就是 SAP HEC 。

它是 SAP 專為大型企業推出的一種「託管式私有雲 (Managed Private Cloud)」服務。從我們 AIS 課程的內部控制與查核角度來看，它具有以下幾個核心意義：

一、 為什麼企業要使用 SAP HEC？

1. **解決 IT 人才荒與維運負擔：**維護 HANA 這種高階的記憶體內資料庫（In-Memory Database）需要非常專業的 BASIS 人員與硬體專家。透過 HEC，企業等於將底層作業系統、資料庫備份、系統修補程式（Patch）等繁重工作，全數交給 SAP 原廠處理。
2. **私有雲的最高安全性：**財務數據是企業的命脈。與一般大眾共用的公有雲不同，HEC 提供的是「專屬隔離」的運算資源，完美滿足大型企業或金融業對「機密性 (Confidentiality)」的嚴格法規要求。

二、 SAP HEC 與「電腦稽核 (IT Audit)」的關聯

當企業將 ERP 系統搬到 SAP HEC 後，會計師的查核方式也會跟著改變：

- **完美詮釋「風險移轉 (Risk Transfer)」。**企業面臨「機房斷電、硬碟損毀、駭客癱瘓伺服器」等 IT 基礎建設風險時，透過付費給 SAP，將這些「資訊科技一般控制 (ITGC)」的責任（如災難復原 DRP、實體機房門禁、資料備份）轉移給了雲端服務商。
- **會計師怎麼查？(SOC 報告的登場)。**雖然機器不在公司裡，但法規（如 SOX 或台灣內控準則）還是要求企業必須對這套系統的內控負責。因此，企業的電腦稽核人員（CISA）每年必須向 SAP 索取所謂的 SOC (Service Organization Control) 查核報告。這是一份由獨立第三方會計師去查核 SAP HEC 機房後出具的背書報告，用來證明「SAP 代管的環境是安全且符合內控標準的」。