AIS Lecture 5 課後練習題

編撰：屏東大學 周國華老師 2026-03-25

第一部分：風險層次 × AIS（1–12）

1.某上市公司導入 ERP 後，因會計人員誤輸匯率，導致財報大幅偏差，進而影響投資人決策並造成股價下跌。此案例中「最根本的風險來源」為何？

A 經濟體風險（股價變動）
B 企業風險（投資人信心）
C 企業程序風險（交易流程）
D 資訊程序風險（資料處理錯誤）

答案：D

解析
AIS 核心關注「資訊處理錯誤」，財報失真源於資料處理問題，而非市場反應

易錯點
很多人選 B，但那是結果不是來源

2.某公司因 AI 技術落後而失去市場競爭力，進一步導致 ERP 投資無法回收。此案例最主要的風險層次為何？

A 經濟體風險
B 產業風險
C 企業風險
D 資訊風險

答案：C

解析
問題發生在公司競爭策略層級

易錯點
學生常選 B（產業），但題目強調「該公司」

3.某企業供應鏈中斷，導致採購系統無法取得原料資料，使 ERP 無法完成訂單處理。最直接影響的是：

A 資訊程序風險
B 企業程序風險

C 經濟體風險
D 網路風險

答案：B

4.某公司 ERP 系統設計不良，導致採購、驗收與付款流程混亂。此最屬於：

A 資訊程序風險
B 企業程序風險
C 產業風險
D 經濟體風險

答案：B

5.某企業 ERP 資料庫被內部員工竄改，但流程本身沒有問題。最直接風險層次為：

A 企業程序風險
B 資訊程序風險
C 產業風險
D 經濟體風險

答案：B

6.某公司因員工士氣低落，導致 ERP 操作錯誤頻繁。此屬於：

A 外部企業風險
B 內部企業風險
C 資訊風險
D 系統風險

答案：B

7.ERP 導入後，企業資料集中，任何錯誤都會快速擴散。此主要增加的是：

A 系統效能
B 資訊風險
C UI 風險
D CPU 負載

答案：B

8.某企業 ERP 系統正常，但報表邏輯錯誤導致錯誤決策。此風險最屬於：

A 程序風險
B 資訊程序風險

C 企業風險
D 市場風險

答案：B

9.某公司 ERP 系統設計完善，但市場需求突然消失。此風險為：

A 資訊風險
B 企業程序風險
C 經濟體風險
D 企業風險

答案：D

10.REA 模型中「事件（Event）」設計錯誤會導致：

A UI 問題
B 程序風險
C 網路風險
D SQL 錯誤

答案：B

11.ERP 導入後，最需要強化的風險控制是：

A 市場分析
B 資訊控制
C UI 設計
D CPU

答案：B

12.AIS 課程最關注的核心問題是：

A 系統效能
B 財務報表
C 資訊正確性與控制
D UI

答案：C

第二部分：舞弊三角 × 舞弊鑽石 × 恩隆（13–25）

13.某 CFO 因股價壓力而操縱盈餘。最主要因素為：

A 機會
B 壓力
C 能力
D 合理化

答案：B

14.某公司內控薄弱，使員工可同時建立供應商與付款。此強化的是：

A 壓力
B 機會
C 合理化
D 能力

答案：B

15.某員工認為「公司虧待我」而進行舞弊。此屬於：

A 壓力
B 機會
C 合理化
D 能力

答案：C

16.恩隆案中，SPE（特殊目的實體）主要代表：

A 壓力
B 能力
C 機會
D 控制

答案：C

17.恩隆高層設計複雜金融結構，最符合：

A 壓力
B 機會
C 能力
D 合理化

答案：C

18.審計失靈在舞弊鑽石中代表：

A 壓力
B 能力
C 機會
D 合理化

答案：C

19.「為了公司長期利益」進行舞弊，屬：

A 壓力
B 能力
C 合理化
D 機會

答案：C

20.舞弊鑽石相較三角多出：

A 控制
B 能力
C 技術
D 權限

答案：B

21.SoD 控制主要降低：

A 壓力
B 機會
C 合理化
D 能力

答案：B

22.高層權力集中會提高：

A 壓力
B 機會
C 能力
D 合理化

答案：C

23.舞弊最容易發生在：

A 壓力 + 機會
B 壓力 + 能力
C 機會 + 能力
D 三者同時存在

答案：D

24.員工財務困難但控制完善時，舞弊機率：

A 高
B 低
C 不變
D 無關

答案：B

25.舞弊控制最有效切入點：

A 壓力
B 機會
C 合理化
D 能力

答案：B

三、SoD × 舞弊 × 控制設計（26–35）

26.某公司在 SAP 系統中進行角色設計時，發現某員工同時擁有「建立供應商主檔」與「批准付款」的權限。系統管理員認為該員工資深且可信任，因此未進行調整。數月後，公司發現該員工建立虛假供應商並成功取得付款。此案例最關鍵的控制失敗為何？

A 未設置輸入驗證（Input Validation）
B 未建立 SoD 衝突矩陣並執行預防性控制
C 未加密付款資料
D 未建立備份機制

答案：B

解析
SoD 矩陣應在權限設定時即阻止衝突（預防性控制）

易錯點
學生常選 A（Input），但問題在「權限組合」

27.某企業進行內部稽核時，發現多名員工因職務調動而累積過多權限（舊權限未移除，新權限又增加），但尚未發生舞弊。此情境最適合歸類為：

A Input Fraud
B SoD Preventive Control
C Privilege Creep（權限蔓延）
D Output Fraud

答案：C

解析
講義明確指出：權限蔓延會在矩陣中顯現

28.某公司在 SoD 衝突矩陣中標示「建立供應商 × 批准付款」為高風險，但允許某高階主管保留此權限，並透過每月人工審查補強。此控制類型最適合分類為：

A 預防性控制
B 偵測性控制
C 更正性控制
D 補償性控制（Compensating Control）

答案：D

解析
高風險 SoD 衝突允許存在，但透過額外審查降低風險

29.某公司將 SoD 控制完全依賴「事後稽核報表」，而未在系統中阻擋衝突權限。此設計最主要問題為：

A 成本過高
B 缺乏預防性控制
C SQL 效率低
D UI 設計不佳

答案：B

30.在 SoD 架構中，若同一人同時負責「Authorization（核准）」與「Custody（資產保管）」職能，最可能導致：

A 資料輸入錯誤
B 無法執行 SQL
C 舞弊機會顯著增加
D 系統效能下降

答案：C

解析
ARC 分離原則：核准 + 保管 = 高風險

31.某企業在設計 SoD 矩陣時，僅考慮兩兩權限衝突，但忽略三個以上權限組合（例如：建立供應商 + 修改銀行帳號 + 批准付款）。此設計缺陷最可能導致：

A SQL 錯誤
B 權限衝突未被完全識別
C UI 錯誤
D 系統崩潰

答案：B

解析
矩陣應涵蓋所有組合（講義：窮舉組合）

32.某 SAP 系統中，會計人員無法直接付款，但可修改付款金額後由主管核准。主管僅檢查總額未核對細項。此控制缺陷最接近：

A SoD 完全失敗
B ITGC 缺失
C ITAC 設計不足
D 網路安全問題

答案：C

解析
應用控制未檢查細節（application control weakness）

33.某企業將 SoD 視為「只需限制高階人員」，而對基層員工不設限制。此觀念最可能導致：

A 控制成本上升
B 系統效能下降
C 舞弊風險增加
D SQL 錯誤

答案：C

34.某企業建立 SoD 矩陣，但未定期更新。此最可能導致：

A SQL 錯誤
B 權限蔓延未被發現
C UI 問題
D CPU 過載

答案：B

35.SoD 矩陣中「安全」的組合代表：

A 無風險
B 無需控制
C 無直接衝突但仍需監控
D 系統錯誤

答案：C

四、舞弊節點 × AIS（36–40）

36.某員工在輸入銷售訂單時刻意修改價格，使公司少收款。此舞弊最精確分類為：

A Data Fraud
B Input Fraud
C Processor Fraud
D Output Fraud

答案：B

37.某 IT 人員修改薪資計算程式，使特定員工獲得額外獎金。此最屬於：

A Input Fraud
B Data Fraud
C Processor Fraud
D Output Fraud

答案：C

38.某員工透過查詢系統下載客戶資料並外洩。此最精確分類為：

A Output Fraud
B Data Fraud
C Processor Fraud
D Input Fraud

答案：B

39.某員工在系統中未修改資料，但利用列印功能取得敏感報表並外洩。此最適合分類為：

A Data Fraud
B Output Fraud

C Input Fraud
D Processor Fraud

答案：B

40.某公司發現舞弊主要發生在資料輸入階段，最有效的控制措施為：

A 增加報表
B 強化輸入驗證與權限控制
C 增加備份
D 增加 UI

答案：B

五、網路攻擊 × 控制（41–45）

41.某 CFO 收到「銀行通知」並輸入帳密，導致公司帳戶被盜。最根本的控制缺陷為：

A 防火牆不足
B 使用者安全意識不足
C SQL 錯誤
D RAM 不足

答案：B

42.某公司 ERP 系統遭勒索病毒攻擊，資料被加密。最有效的預防措施組合為：

A 防火牆 + SQL 優化
B 定期備份 + 權限控管
C UI 改善
D CPU 升級

答案：B

43.某企業網站遭大量假請求攻擊，導致服務中斷。此攻擊主要影響 CIA 中哪一項？

A Confidentiality
B Integrity
C Availability
D Authentication

答案：C

44.某企業僅依賴技術防護，未對員工進行資安教育。此最可能導致：

A SQL 錯誤
B Social Engineering 成功率提高
C UI 錯誤
D CPU 過載

答案：B

45.某公司導入多因素驗證（MFA）後，Phishing 攻擊仍成功。最可能原因為：

A SQL 錯誤
B 使用者仍主動提供驗證資訊
C RAM 不足
D UI 問題

答案：B

六、COSO × COBIT × ERM（46–52）

46.某企業已建立完整的內部控制制度（如授權、分工與稽核），但在面對市場變化時，仍無法將風險納入策略決策，導致重大投資失敗。此案例最主要缺乏的是：

A COSO 控制環境
B COBIT IT 治理
C ERM（企業風險管理）
D ITGC

答案：C

解析
ERM 強調「風險與策略整合」，不只是控制

易錯點
學生會選 COSO，但 COSO 偏「內控」，不是策略

47.某公司 IT 系統高度複雜，資料不一致且缺乏標準化管理，雖然財務內控流程良好，但 IT 風險持續升高。此情境最適合導入：

A COSO
B COBIT
C SOX
D ERM

答案：B

解析
COBIT 專注 IT 治理與控制

48.某上市公司 CFO 簽署財報時，需確認內部控制有效性並承擔法律責任。此要求最直接來自：

A COSO
B COBIT
C SOX 404
D ERM

答案：C

49.某公司建立內部控制制度，包含：控制環境、風險評估、控制活動、資訊與溝通、監督。此架構最符合：

A COBIT
B COSO
C SOX
D ERM

答案：B

50.某企業 IT 部門建立完整治理架構，使 IT 投資能支持企業策略並降低風險。此最符合：

A COSO
B COBIT
C ERM
D SOX

答案：B

51.某企業決定接受部分 IT 風險，以換取市場擴張機會。此屬於：

A 風險降低
B 風險轉移
C 風險接受
D 風險避免

答案：C

52.某企業將 ERP 系統外包至雲端服務商，並由第三方負責備份與災難復原。此屬於：

A 風險降低
B 風險轉移

C 風險避免
D 風險接受

答案：B

七、ITGC vs ITAC × SAP 控制（53–57）

53.某 SAP 系統允許使用者同時建立供應商與付款，導致舞弊。此控制缺陷最屬於：

A ITAC
B ITGC
C Output Control
D Data Control

答案：B

解析
SoD 屬於 IT General Control

易錯點
學生常誤選 ITAC

54.某公司在 SAP 中設置三方比對（PO / GR / Invoice）以防止錯誤付款。此屬於：

A ITGC
B ITAC
C SoD
D Network Control

答案：B

解析
三方比對屬應用控制（Application Control）

55.某企業透過 SUIM 定期檢查使用者權限異常。此控制最適合分類為：

A 預防性 ITAC
B 偵測性 ITGC
C 預防性 ITGC
D 偵測性 ITAC

答案：B

解析
SUIM → 權限稽核 → 偵測性控制

56.某公司未設定 OB52，允許使用者跨期修改會計資料。此問題最本質為：

A ITAC 缺失
B ITGC 缺失
C SQL 問題
D UI 問題

答案：B

57.某 SAP 系統透過 RZ10 強制密碼複雜度與更換週期。

此屬於：

A ITAC
B ITGC
C Output Control
D Application Control

答案：B

八、PKI × 加密流程（58–60）

58.在電子交易中，客戶使用商家的公開金鑰加密資料。此主要確保：

A 完整性
B 機密性
C 可用性
D 驗證

答案：B

59.客戶使用自己的私密金鑰對訊息進行簽章。此主要確保：

A 機密性
B 完整性與不可否認性
C 可用性
D 備份

答案：B

60.某系統同時使用：公開金鑰加密資料 及 私密金鑰簽章。此最完整確保：

A CIA 三要素
B 機密性 + 完整性 + 不可否認性
C 完整性 + 可用性
D 可用性 + 機密性

答案：B

Lecture 5 附錄 (61–70)

61.某半導體企業為保護核心製程機密，將資訊安全長（CISO）設為由資深高階主管兼任，並直接向執行長與董事會報告。從治理角度看，這項安排最主要的控制意義為何？

A 讓資安部門可以直接執行所有採購付款權限
B 使資安決策具備足夠的組織權威與資源支持
C 讓資安長兼任內部稽核主管，以減少溝通成本
D 將資訊安全完全技術化，避免管理階層介入

答案：B

解析
附錄 1 指出，台積電設有 CISO，且直接向執行長與董事會報告，目的在於讓資安決策具有最高層級授權，不只是技術執行，而是治理層級的風險管理安排。

易錯點
很多人會誤以為 CISO 是純技術職，但講義強調的是**高階治理與授權**。

62.台積電將辦公網路與晶圓廠生產網路嚴格隔離。若從控制目標來看，這種作法最主要是為了防止哪一類風險擴散？

A 財務報表重分類錯誤
B 惡意程式或攻擊在不同網段間橫向移動
C 員工輸入資料時的鍵盤錯誤
D 因欄位定義錯誤而造成資料庫正規化失敗

答案：B

解析
附錄 1 在「多層次防禦架構」中明確提到 network segmentation，核心目的是阻止惡意程式在網路中橫向擴散，這是零信任與 defense in depth 的實務表現。

63.某公司將所有敏感文件自動加上 Confidential / Top Secret 標籤，並附加動態浮水印，同時記錄列印與存取紀錄。這種控制最接近台積電附錄中哪一種保護邏輯？

A 以 SQL 最佳化提升查詢效率
B 以 PIP 為核心的文件與資料精細化管理
C 以三方吻合控制採購舞弊
D 以 OB52 阻擋跨期作帳

答案：B

解析
附錄 1 強調台積電的特色控制是 **PIP（Proprietary Information Protection）**，對文件與資料做標籤化、加密、浮水印與追蹤，以保護營業秘密。

64.某高科技公司允許合作設備商進入廠區維修，但要求所有工具機先經過專門的病毒過濾站（scrubbing station）檢查後才能連入內部環境。這項控制最主要反映哪一個風險觀點？

A 企業認為內部員工永遠不會帶來風險
B 資安缺口往往來自供應鏈與外部夥伴
C 只要有 ISO 27001 就不需要任何技術控制
D 只要資料加密，外部設備是否感染並不重要

答案：B

解析
附錄 1 指出，台積電非常重視供應鏈資安，因為資安缺口常來自合作夥伴；scrubbing station 就是防止外部維修設備帶入感染源的具體控制。

65.若一家公司已建立 24/7 的 SOC，並運用 AI 與機器學習即時偵測異常流量與員工異常行為，這項控制最適合歸類為下列何者？

A 單純的更正性控制，只有事後修復功能
B 結合偵測性控制與事件應變能力的持續監控機制
C 純粹的預防性控制，完全不涉及監控
D 只與財務報表編製有關，與資安無直接關係

答案：B

解析
附錄 1 中的 SOC 是 24/7 持續監控中心，其功能在於偵測異常並支援應變，因此本質上是**偵測性控制 + 事件應變能力**。

66.一位會計系學生希望未來進入四大會計師事務所的風險諮詢或 IT 稽核部門。根據附錄 2，哪一張證照最具直接關聯性？

A CFA，因為主要評估投資組合績效
B CISA，因為核心涵蓋資訊系統稽核、IT 治理與資訊資產保護

C PMP，因為重點是專案時程控管
D FRM，因為重點是市場風險定價模型

答案：B

解析
附錄 2 明確指出，CISA 是 IT 查核領域的黃金證照，特別適合四大風險諮詢、IT Audit 路徑，且內容直接對應 Lecture 5 的控制與資安主題。

易錯點
有些學生會選 CFA 或 FRM，因為也很熱門，但講義談的是**電腦稽核 / IT Audit**，最直接就是 CISA。

67.根據附錄 2，CISA 的考試領域中，哪一項最能直接對應 Lecture 5 所談的「災難復原、日常維運與企業韌性」？

A 資訊系統營運與企業韌性
B 財務會計準則更新
C 行銷資料分析與顧客分群
D 網頁前端 UI/UX 設計

答案：A

解析
附錄 2 列出的 CISA 核心領域之一，就是「資訊系統營運與企業韌性」，其中直接涵蓋災難復原、日常維運等 Lecture 5 的重點。

68.某企業將 SAP S/4HANA 遷移到 SAP HEC，由 SAP 原廠負責底層作業系統、資料庫備份與 patch 維護。從風險回應角度看，這項安排最符合下列哪一種策略？

A 規避（Avoid），因為企業完全停止 ERP 活動
B 降低（Reduce），因為企業自行強化全部控制
C 分擔/移轉（Share/Transfer），因為基礎建設風險部分轉由服務商承擔
D 接受（Accept），因為企業選擇不採取任何行動

答案：C

解析
附錄 3 明確將 SAP HEC 與風險移轉連結：企業把機房斷電、硬碟損毀、伺服器維運等 ITGC 層級風險，透過託管式私有雲轉移給 SAP。

69.某公司 CFO 認為：「既然 ERP 系統已經放到 SAP HEC，機器不在公司裡，就不需要再對內控制負責。」根據附錄 3，這種說法最大的錯誤在哪裡？

A 因為 HEC 屬公有雲，所以公司仍須自建機房
B 因為法規仍要求企業對其財務報導內控負責，故需透過 SOC 報告取得外部服務商控制的查核證據
C 因為 HEC 只適用於中小企業，不適用大型企業
D 因為使用 HEC 後，所有 ITGC 都自動失效

答案：B

解析
附錄 3 強調：即使系統搬到 HEC，企業仍須對內控負責；因此稽核人員需向 SAP 取得 **SOC（Service Organization Control）報告**，作為外部代管環境安全性的查核證據。

易錯點
很多人會把「系統外包」誤解成「責任外包」，但講義清楚指出責任並未消失。

70.從 AIS 與內控角度看，SAP HEC 相較於一般公有雲，講義特別強調其對大型企業與金融業更具吸引力的主要原因為何？

A 因為 HEC 可讓企業完全不需要任何權限管理
B 因為 HEC 提供專屬隔離的託管式私有雲，更能滿足對財務資料機密性的高要求
C 因為 HEC 只用於 UI 設計，不涉及核心 ERP
D 因為 HEC 保證企業不再需要外部會計師查核

答案：B

解析
附錄 3 指出，HEC 的重要價值之一是「私有雲的最高安全性」：相對於一般共用式公有雲，HEC 提供專屬隔離資源，更符合大型企業或金融業對**機密性（Confidentiality）**的要求。