iPAS管理：責任、風險與復原

2026東海產投 / 第六週 / 考前速記 1/7
資訊安全管理概論 / 用情境辨識角色與證據

資產責任與風險處理

概念	判斷重點
資料擁有者 / 保管者 / 使用者	業務擁有者依政策決定分類與要求；保管者落實保護；使用者依授權使用。
資產 / 弱點 / 威脅 / 影響	訂單資料 / 離職帳號未停用 / 帳號被盜用 / 個資外洩與營運損失。
風險處理	規避、降低、移轉、接受。處理後仍需評估殘餘風險；移轉不讓責任自動歸零。

四種存取控制模型

模型	主要依據	讀題線索
DAC	資源擁有者決定	擁有者可授權
MAC	安全標籤與集中規則	機密等級與強制規則
RBAC	角色所對應的權限	客服、會計等職務角色
ABAC	主體、資源、動作、環境屬性	部門、資料類型、時間等條件

MFA使用不同因子：所知、所持、固有特徵。密碼 + 另一個PIN通常仍是同一類因子。驗證確認身分，授權決定能做什麼；兩者仍需最小權限與定期複核。

業務持續、系統復原與事件處理

名稱	目的與例子
BCP	讓關鍵業務持續，例如替代接單流程。
DRP	讓IT系統與資料在災難後復原，例如重建與還原。
事件應變	依授權程序辨識、通報、遏止、調查、復原與檢討，保留跡證。

RTO與RPO：時間目標，不是只看備份排程

指標	教學假設	實際結果
RTO：復原時間目標	2小時	10:00中斷，11:15恢復，共75分鐘，符合本例目標。
RPO：資料回復點目標	30分鐘	回復至09:40，距10:00中斷差20分鐘，符合本例目標。

數字均為課堂假設。RTO是復原時間目標，不能直接等同最大可容忍中斷時間MTD。

RAID容錯依等級而異，RAID 0無容錯。RAID、多AZ與同步副本都不能取代隔離備份及復原測試。

來源連結 / 查核日 2026-10-27

iPAS資訊安全工程師：官方學習資源與115年簡章 / ipd.nat.gov.tw
iPAS管理概論學習指引（2026-04-20版） / www.ipas.org.tw
NIST SP 800-61 Rev.3：事件應變 / csrc.nist.gov

iPAS技術：網路、網站與維運

2026東海產投 / 第六週 / 考前速記 2/7
資訊安全技術概論 / 先辨識攻擊，再選控制

常見連接埠

服務	常見埠	提醒
HTTP / HTTPS	TCP 80 / TCP 443	HTTP/3使用QUIC/UDP，通常也是443。
SSH / DNS	TCP 22 / UDP與TCP 53	DNS不能只背UDP。
SMTP / RDP	TCP 25 / TCP 3389	25常用於郵件伺服器轉送；提交另有587等。

防護設備的主要任務

控制	任務	常見誤會
Firewall	依規則允許或拒絕流量	開443不代表網站沒有弱點。
IDS	偵測並告警	告警後仍需人員研判。
IPS	部署在路徑中偵測與阻擋	阻擋規則仍可能誤判。
WAF	檢查HTTP應用請求	不能取代程式修補或所有主機防護。

SQLi、XSS與CSRF

攻擊	題目線索	主要控制方向
SQL injection	輸入被拼接成查詢語法	參數化查詢，並核對資料授權。
XSS	不可信腳本進入網頁	依輸出情境編碼，避免不安全DOM操作。
CSRF	利用已登入者送出非預期請求	伺服器驗證Token、適當SameSite與身分驗證設計。

安全檢測與維運證據

工作	目的與限制
弱點掃描 / 滲透測試	找可能缺陷 / 在授權範圍驗證攻擊風險。兩者都不保證找出全部弱點。
修補與複測	依暴露面、利用情況、資產重要性排優先；保留修正、回復與複測紀錄。
日誌 / SIEM / SOC	紀錄事件 / 集中關聯分析平台 / 結合人員、流程與工具的營運能力。

日誌需要時鐘同步、存取限制、完整性與保留規則。MAM偏應用程式及其資料管理；MDM偏裝置管理。SBOM列軟體元件與版本，幫助追查相依套件風險，並非「沒有漏洞」的證明。

設備可更改服務埠，產品能力也可能重疊。讀題須看功能、部署與保護目標；不可只憑一個縮寫作答。

來源連結 / 查核日 2026-10-27

iPAS技術概論學習指引（2026-04-20版） / www.ipas.org.tw
IANA：服務名稱與連接埠登錄表 / www.iana.org
OWASP Cheat Sheet Series：網站防護 / cheatsheetseries.owasp.org
NIST SP 800-218：安全軟體開發 / csrc.nist.gov

AES、RSA與量子遷移時間差

2026東海產投 / 第六週 / 考前速記 3/7
金鑰角色 / RSA白板算例 / Mosca框架

對稱式與非對稱式比較

比較	AES：對稱式	RSA：非對稱式
金鑰	共享秘密金鑰	公鑰、私鑰成對
用途	大量資料保密	保密與簽章採不同標準方案
成本	大量資料處理通常較有效率	模冪等公鑰運算通常較昂貴
長度	區塊128 bits；金鑰128/192/256 bits	以模數n的位元長度描述
安全使用	標準模式、參數；GCM避免同金鑰重複nonce	保密用收件者公鑰；需合適padding，例如OAEP
簽章	AES本身不是數位簽章	PSS等簽章：私鑰簽，公鑰驗

AES與RSA的金鑰位元數不能直接比較安全強度。實務常用公鑰機制建立或保護金鑰，再用對稱驗證加密處理大量資料。Hash是摘要，簽章驗證需文件、簽章與正確公鑰，結果為通過或失敗。

玩具RSA：65變成2790，再回到65

步驟	已驗算的數字
建立參數	p=61，q=53；n=pq=3233；φ(n)=60×52=3120。
選擇金鑰	e=17，d=2753；17×2753=15×3120+1。
公鑰運算	公鑰(e,n)：65^17 mod 3233 = 2790。
私鑰運算	私鑰(d,n)：2790^2753 mod 3233 = 65。

mod是除法餘數。此例只教模運算：小數字及沒有padding的裸RSA不具實際安全性，不能拿來保護真實資料。

Mosca框架：X + Y > Z表示估計情境下有保護缺口

符號	意義	本例假設
X	資料所需保密年限	8年
Y	完成系統遷移所需時間	3年
Z	從現在到相關破解能力可用的情境時間	10年

接近第3年才產生、仍用舊機制保護的資料，若須再保密8年，期限到第11年；情境第10年可能解開，出現約1年缺口：8 + 3=11 > 10。這不是Q-day預測，等號也沒有餘裕。

HNDL（harvest now, decrypt later）：攻擊者先保存密文，日後再解。系統更新不會清除對手已有的舊密文。先盤點資料壽命、演算法與供應商依賴，再測試與分批遷移；X + Y≤Z也不是安全保證。

來源連結 / 查核日 2026-10-27

NIST FIPS 197：AES / csrc.nist.gov
RFC 8017：RSA標準方案與編碼 / www.rfc-editor.org
Mosca (2015)：遷移時間框架原文 / eprint.iacr.org
National Academies：Quantum Computing，第4章 / www.nationalacademies.org

雲端：五個特性與服務用途

2026東海產投 / 第六週 / 考前速記 4/7
NIST五特性 / 三種服務模型 / AWS架構速記

雲端五個必要特性

特性	英文	情境記憶
隨需自助服務	On-demand self-service	自行開通需要的資源。
廣泛網路存取	Broad network access	透過網路與標準機制存取。
資源池化	Resource pooling	共享資源，依需求動態配置。
快速彈性	Rapid elasticity	資源隨需求快速增加或減少。
可量測服務	Measured service	使用量可計量、監控與報告。

網路存取不代表向所有人公開；資源池化不表示租戶能讀彼此資料；可量測服務也不限定單一計價方式。

三種服務模型與責任

模型	供應商提供	客戶仍需負責的例子
IaaS	運算、儲存與網路	OS、應用與資料。
PaaS	應用執行平台	程式、資料與設定。
SaaS	可直接使用的應用	資料、帳號、授權與使用設定。

AWS基本服務

服務	用途	常見混淆
EC2	虛擬運算執行個體	客戶仍管理OS與應用等責任。
S3	物件儲存	不是一般本機磁碟；權限須正確設定。
RDS	受管關聯式資料庫	資料、帳號與網路存取仍需客戶管理。
VPC	邏輯隔離的虛擬網路	私有子網仍需路由與安全規則。
IAM	身分與權限管理	最小權限、MFA與定期複核。
CloudTrail / CloudWatch	API活動紀錄 / 監控與可觀測性	紀錄範圍與保留依設定確認。

架構讀題：高可用與可還原

概念	核心用途
Region / AZ	Region是地理區域；AZ由一或多個離散資料中心組成，不能當成固定一棟樓。
HA / Backup	多AZ分散部分故障風險；備份保留可還原版本。副本可能同步誤刪或惡意修改。

書店常見路徑：瀏覽器經HTTPS進應用，應用依權限讀S3圖片與RDS訂單。服務可用性取決於整條依賴鏈；RAID容錯依等級而異，RAID 0無容錯。備份要用還原測試驗證。

來源連結 / 查核日 2026-10-27

NIST SP 800-145：雲端五特性與服務模型 / nvlpubs.nist.gov
AWS Cloud Practitioner考試指南 / docs.aws.amazon.com
AWS Regions與Availability Zones / aws.amazon.com
AWS RDS Multi-AZ文件 / docs.aws.amazon.com

雲端：成本四工具與支援方案

2026東海產投 / 第六週 / 考前速記 5/7
先分清費用分析與技術支援 / 依2026-10-27官方頁整理

成本管理四工具

工具	回答的問題	記憶詞
AWS Pricing Calculator	部署前，這個假設架構大約多少錢？	估算
AWS Cost Explorer	費用花在哪裡，用量與趨勢如何？	分析
AWS Budgets	實際或預測費用是否達到門檻？	預算
Cost Anomaly Detection	花費是否出現異常模式或突增？	異常

Budgets通知不等於全部資源自動停機；可另設定特定Actions。成本資料與通知有延遲，仍需核對實際用量、權限及處置流程。

現行AWS Support：四項包含Basic

方案	主要能力	讀題線索
Basic	帳務、文件與社群資源	基本支援
Business Support+	全天候技術支援	生產工作負載
Enterprise Support	指定TAM與主動指導	關鍵工作負載
Unified Operations	營運專家與持續監控等服務	加強營運韌性

支援回應時間是初次人工回應目標，不是修復完成保證。表格供概念複習，價格、範圍、地區與合約條件請查官方頁。

舊教材常見四類：按題目版次辨識

舊名稱	當時的能力線索	用途線索
Basic	帳務、文件與基本資源	基本支援
Developer	營業時間技術支援	開發與測試
Business	24/7技術支援	生產工作負載
Enterprise	指定TAM與主動指導	關鍵業務

過渡規則：Developer、Business、Enterprise On-Ramp在一般AWS區域的停止支援日為2027-01-01；AWS GovCloud (US)有例外。Developer / Business轉向Business Support+；Enterprise On-Ramp於2026年更新合約或分批轉向Enterprise。

Developer未選擇升級可能降為Basic。舊教材四類與現行四項不是同一組清單；不要把支援方案當成成本管理工具。

來源連結 / 查核日 2026-10-27

AWS Pricing Calculator / aws.amazon.com
AWS Cost Explorer / aws.amazon.com
AWS Budgets功能 / aws.amazon.com
AWS Cost Anomaly Detection文件 / docs.aws.amazon.com
AWS Support現行方案比較 / aws.amazon.com
舊Developer方案說明 / aws.amazon.com
舊Business方案說明 / aws.amazon.com
AWS Support舊方案停止支援與GovCloud例外 / docs.aws.amazon.com

產業：誰做硬體，誰提供服務

2026東海產投 / 第六週 / 考前速記 6/7
雲端供應鏈與台灣可接觸的軟體業雇主 / 非排名

企業按需要購買雲端服務，背後仍有晶片、伺服器、電力、網路與冷卻工程。一般供應鏈角色與特定客戶採購，是兩種不同證據。

資料中心與雲端的分工

層次	企業例	提供什麼
設計與平台	AWS / Annapurna Labs	Trainium晶片設計與雲端平台。
晶片與封裝	TSMC	半導體製造與先進封裝能力。
伺服器與整櫃	緯穎、廣達 / QCT	運算、儲存、系統整合與驗證。
供電與冷卻	台達、光寶	電源、配電、液冷與機櫃基礎設施。
企業應用	軟體商、SI、企業IT	開發、導入、整合、維運與資安。

已公開合作例：TSMC於2022-10-27新聞稿刊載AWS主管說明，Annapurna Labs與TSMC就Trainium、CoWoS等先進封裝合作到量產。這不代表本筆記掌握2026年的採購數量或完整料件表。

緯穎、QCT、台達、光寶在此是產業角色例；本次來源未確認各家特定AWS機櫃或材料採購關係，不把角色表直接當成AWS供應商清單。

軟體與資訊服務雇主例

企業	工作領域	產品或服務例
趨勢科技	全球資安產品，在台有研發	端點、混合雲與網路防護。
精誠資訊	資訊服務、雲地整合	系統建置、維運、DevOps。
叡揚資訊	企業軟體、SaaS與治理	CRM、知識協作、公文等。
鼎新數智	ERP與企業流程	製造、流通與企業管理。
訊連科技	影音創作與AI辨識	PowerDirector、FaceMe。

趨勢科技是全球企業，不以「在台研發」推成「總部在台灣」。精誠資訊與精誠軟體服務是不同法人；鼎新台灣品牌現名為鼎新數智。這份名單不是營收或規模排名。

技能不是只分軟體或硬體：伺服器韌體需要程式與硬體介面；水冷控制器也需要網路、更新與安全啟動。資安工作橫跨供應鏈與服務生命週期。

來源連結 / 查核日 2026-10-27

TSMC：2022年OIP 3DFabric與AWS引述 / pr.tsmc.com
Wiwynn公司與整櫃方案 / www.wiwynn.com
QCT資料中心產品型錄（2025） / go.qct.io
Delta資料中心產品 / www.deltaww.com
LITEON與QCT：官方OCP 2026合作新聞 / www.liteon.com
趨勢科技台灣徵才 / www.trendmicro.com
精誠資訊雲端維運職缺 / www.104.com.tw
叡揚官方產品與服務 / www.gss.com.tw
鼎新數智公司介紹 / www.digiwin.com.tw
CyberLink產品與公司介紹 / www.cyberlink.com

職涯：104職缺與第一份作品

2026東海產投 / 第六週 / 考前速記 7/7
2026-10-27職缺快照 / 完整條件與狀態以連結為準

把職缺當作能力地圖：先分必要、加分條件，再看經驗與學歷。下列是6個不同角色的當日公開內容，並非全部職缺統計；完成一項入門練習不等於符合全部資格。

六個職缺的技能與門檻

公司 / 短職稱	核心技能	經驗等條件
啄木科技 / 資安分析師	Log、SIEM、Windows/Linux、網路、事件紀錄	經歷不拘；大學以上等條件
精誠資訊 / SRE、DevOps	AWS/GCP、Docker、CI/CD、Python/Shell、監控	2年以上；大學以上
叡揚資訊 / Java全端	Java、SQL、API、Git、Spring、測試與Docker	2年以上；大學以上
緯穎 / BMC資深韌體	C/C++、Embedded Linux、OpenBMC、硬體介面	3年以上；大學以上
鴻海 / 伺服器熱流	熱傳、CFD、液冷、設計與驗證測試	經歷不拘；相關工程背景
台達 / 水冷控制韌體	Linux/BSP、C/C++、Secure Boot、測試	2年以上；碩士

選一項入門練習，保留可檢查的證據

方向	第一份練習	交付證據
SOC	判讀模擬登入日誌，說明異常與下一步。	紀錄、理由與處置報告。
雲端維運	部署簡單容器網站，加入監控與故障復原。	部署說明、監控與復原紀錄。
軟體開發	做書店CRUD，整理API與資料庫結構。	Git、文件與測試結果。
BMC韌體	閱讀Redfish規格，模擬設備狀態查詢。	程式、輸出與除錯紀錄。
熱流工程	畫出熱流路徑，練習讀溫度與功率曲線。	標註圖與數據解讀。
控制韌體	模擬感測資料、異常告警與更新流程。	介面說明、測試與操作紀錄。

共同能力：網路與系統基本功、問題分析、測試、文件、英文規格閱讀與團隊溝通。資深職缺可作長期目標；先用作品找出自己下一個需要補的技能。

證照複習連結：CIA與風險判斷、存取控制、加密、日誌、備份復原與雲端責任，可支持閱讀職缺與實作。課堂練習與正式考試資格、成績規則分開確認。

來源連結 / 查核日 2026-10-27

104：啄木科技資安分析師 / www.104.com.tw
104：精誠資訊雲端維運工程師 / www.104.com.tw
104：叡揚資訊Java全端工程師 / www.104.com.tw
104：緯穎BMC資深韌體工程師 / www.104.com.tw
104：鴻海伺服器熱流工程師 / www.104.com.tw
104：台達水冷控制韌體工程師 / www.104.com.tw