資訊安全工程師

初級能力鑑定學習指引

科目一：資訊安全管理概論

序

為提供授課教師及考生掌握評鑑方向，準備有所依循，本計畫委託委員會題庫組及規劃組領域專家，以科目評鑑內容為分項，展開重點說明及考題解析。

本手冊為學習指引，並非教材也非題庫，僅做為引導學習的考前準備工具手冊，並不保證考試通過之責，建議依循考試簡章所公告之評鑑主題內容準備考試。

目錄

職能基準

經濟部為有效提升產業人才素質，近年來持續致力於專業人才培訓發展。為了更明確產業對各類專業人才的能力需求，特別針對亟需人才的多項重點產業，邀集產官學專家，發展產業職能基準，提供各界依其內涵辦理培訓課程及規劃能力鑑定機制。

一、何謂職能?

為完成特定職業（或職類）工作任務，所需具備的能力組合（知識、技能、態度）。

二、資訊安全工程師職能基準

職類名稱	資訊安全工程師
工作描述	具備相關資訊安全知識，藉由組織內部能力或尋求外部廠商、專家協助，建立符合法規與組織安全需求之系統、網路與安全防護架構，並執行相關維運作業與協助其他單位執行資訊安全相關活動。
入門水準	1.大學或專科以上學歷，或具有資訊安全相關背景，資訊或電機相關科系尤佳。 2.具備英文閱讀能力，具跨領域學習特質者尤佳。
基準級別	4

完整的資訊安全工程師職能基準，可從 iPAS 網址下載：

https://www.ipas.org.tw/AbilityStandardDownload.aspx

第一章. 考科與評鑑內容

科目	評鑑主題	評鑑內容	占比
考科一：資訊安全管理概論	資訊安全管理概念	1.1 資訊安全管理系統	10%
		1.2 相關法規概論與遵循	10%
		1.3 隱私權保護與智慧財產權	5%
	資產與風險管理	2-1.資產分類分級與盤點	15%
		2-2.風險評鑑與風險處理	10%
	存取控制、加解密與金鑰管理	3-1.存取控制與身份認證	20%
		3-2.加解密與金鑰生命週期	10%
	事故管理與營運持續	4-1.事件與事故管理	10%
		4-2.備援與營運持續	10%

第二章. 參考書目

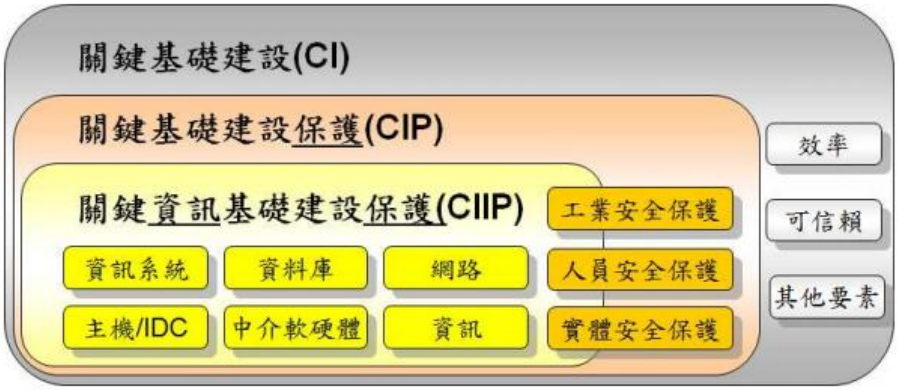
參考書	作者	出版社
資訊安全概論（第三版）	林祝興、張明信	旗標
資訊與網路安全：基礎系統資訊安全技術與實務（修訂版）	賈蓉生、許世豪、林金池、賈敏原	博碩
資訊安全概論與實務（第三版）	潘天佑	碁峰

第三章. 考科內容

本指引將說明 「資訊安全工程師」之考科一「資訊安全管理概論」考試內容，包含評鑑主題「資訊安全管理概念」、「資產與風險管理」、「存取控制、加解密與金鑰管理」與「事故管理與營運持續」，並在章節後面添加練習評量供讀者練習。

第四章. 資訊安全管理系統

關鍵基礎建設（Critical Infrastructure, CI），泛指一個國家為了維持民生、經濟與政府等相關運作而提供之基本設施與服務，包括實體以及以資訊電子為基礎之系統。如果是保護這些關鍵基礎建設的措施，不論是整體性的資產盤點、風險評估或是安全防護，都可以視為關鍵基礎建設保護（Critical Infrastructure Protection, CIP）；而保護這些關鍵資訊基礎建設的措施，就是關鍵資訊基礎建設保護（Critical Information Infrastructure Protection, CIIP），不僅僅是領域內各機構的協同保護，亦牽涉到跨領域的協同合作，其與 CI、CIP 之關係如下圖所示。



資料來源：資策會 MIC 委外研究報告

資訊安全管理系統（Information Security Management System, ISMS）是一套有系統地分析和管理資訊安全風險的方法，依據我國政府相關規定行政院及所屬各機關資訊安全管理要點，訂定「行政院及所屬各機關資訊安全管理規範」，供全國政府機關（構）參考施行。

第一節　資訊安全管理概念

由於資訊安全層面相當廣泛，本節將著重在「機密性、完整性與可用性」定義及「資訊安全管理系統」的名詞解釋及技術說明。

一、機密性、完整性與可用性定義

（一）資訊安全的基本功能及目的不外在提供資料和資源的機密性（Confidentiality）、完整性（Integrity）、可用性（Availability），即保護資訊之 C.I.A.。依據 ISO/IEC 27000 條款中針對資訊安全的解釋：

- 資訊安全是指對資訊機密性、完整性、可用性的保護。
- 另外亦可包含其他如驗證性（Authenticity）、可歸責性（Accountability）、不可否認性（Non-Repudiation）及可靠性 （Reliability）等性質。

（二）組織為落實這些重要的資訊安全原則：

- 企業應了解 CIA 原則的含義。
- 藉由那些機制提供 CIA 原則。
- 當原則有缺失時對企業造成些負面影響。

（三）CIA 原則的含義：

- 機密性：確認資訊不會提供或洩露給未經授權的個人、組織或流程。

- ✧ 確保資料傳遞與儲存的私密性，避免未經授權的使用者有意或無意的揭露資料內涵。例如：資料於網路傳送時被攔截竊取，或公司不小心公佈不該公佈的訊息，均是違反資料的機密性。

- 完整性：保護資產或資訊的準確性和完整性。
  - ✧ 應防止人為不慎的操作、惡意的竄改，或是自然雜訊的干擾，確保資訊或系統之正確性。
  - ✧ 防止假冒或未授權方式存取系統資源，進行資料之處理或更改。
- 可用性：確認被授權者在需要的時候，資訊與相關資產是可以存取與可以使用的。
  - ✧ 資訊與資訊處理的可用性，應避免因系統的故障、或是人為惡意的阻斷服務而受影響。
  - ✧ 企業資料必需即時並可靠的提供給企業內部各個層級的使用需求。

（四）保護資訊 C.I.A.不同的技術與方法：

- 機密性保護
  - ✧ 加密技術：機密性資料傳遞和儲存時務必加密處理。
  - ✧ 採用安全性協定，例如：SSL、IPSec。
  - ✧ 嚴格的認證程序與存取控制。

- ✧ 保護資料避免遺失的軟硬體等。

- 完整性保護
  - ✧ 對系統與資料的變更經過授權與確認。
  - ✧ 採取嚴謹的驗證程序或存取控制來減少不慎或意外地操作。
  - ✧ 使用者的活動都被記錄，以便確定誰對資訊作了變更。
  - ✧ 資料的完整性可以藉由加密技術來確保等。
- 可用性保護
  - ✧ 資料的管理與儲存應將資料的遺失機會降到最低，例如：資料庫的高可用性作法（多副本等技術）。
  - ✧ 建立備份程序，將資料儲存時間的相關規定納入考量。
  - ✧ 系統或網路的容錯備援。
  - ✧ 容量規劃及負載平衡等。

二、資訊安全管理系統

國際 IT 治理學會（IT Governance Institute, ITGI）針對資訊安全治理有提到：

（一）資訊安全必須是公司治理的一部分，應整合到公司的策略、理念、規劃、實施與營運中。

- 有效的資訊安全治理，需要企業經營管理階層的承諾，藉此建立企業在資訊安全的文化。

- 管理階層宜設定一個明確且與營運目標一致的政策方向，並經由發布與維護，涵蓋整個組織的資訊安全政策，以展現對資訊安全的支援與承諾。

（二）資訊安全是一個自上而下（Top-Down）的流程，需要一個周詳且能夠連結企業業務流程與目標的資訊安全性原則。

- 為確保與所有資訊安全相關的要求，能包含在組織的資訊安全性原則中，相關組織發展了好幾個國際標準，例如：ISO/IEC 27000 系列的安全標準、ISACA COBIT 等。

三、何謂 ISO/IEC 27000？

（一）由 ISO（國際標準化組織）及 IEC（國際電工委員會）所發表的一個資訊安全規範標準，提供企業資訊安全管理的框架。

（二）內容包含發展資訊安全管理系統（Information Security Management System, ISMS）所需的要求與指引。

（三）ISO/IEC 27000 包含一系列的標準，例如：

- ISO/IEC 27000：資訊安全管理系統（ISMS）- 概述和詞彙（Overview and vocabulary）
- ISO/IEC 27001：ISMS 要求（Requirements）
- ISO/IEC 27002：ISMS 作業規範（Code of Practice）
- ISO/IEC 27003：ISMS 實施指引（Implementation Guidance）

- ISO/IEC 27004：資訊安全管理量測（Measurement）
- ISO/IEC 27005：資訊安全風險管理（Risk Management）
- ISO/IEC 27007：稽核指導綱要（Guidelines for Information Security Management Systems Auditing）
- ISO/IEC 27017：雲服務資訊安全管理
- ISO/IEC 27018：雲服務個人資料保護管理

四、何謂 ISMS（資訊安全管理系統）

（一）資訊安全管理系統（Information Security Management System, ISMS）是一套有系統地分析和管理資訊安全風險的方法，為國際現行五大管理系統之一。

- 是整體管理系統的一部分，以業務風險的管理為基礎，用以建立、實施、運行、監控、檢視、維護和改善資訊安全。

（二）ISMS 為針對組織內部所使用之資訊，實施全面性之管理，以妥善保護資訊之機密性（Confidentiality），完整性（Integrity）與可用性（Availability ），並降低資安事件之衝擊至可承受之範圍。

（三）組織應識別並評估所有的風險、威脅和弱點，並實施相關的資訊安全控制措施，以及保障機制，以協助企業有效發現問題並評估最適當的解決方案：

- 資產（Asset）：指一種實體或邏輯的資源，對組織而言是有價值的（包含：軟體、人員、設施、服務及信譽等）。
- 弱點（Vulnerability）：資產本身具備的脆弱性，若被揭露會造成資訊機密性、完整性及可用性的損害；弱點本身不會產生損害，而是因為威脅出現。
- 威脅（Threat）：一個意料外的事件，成為導致系統或組織損害的潛在原因；威脅必須利用資產的弱點才能對資產造成傷害。
- 風險（Risk）：某種威脅利用資訊、資產等的脆弱性，導致對組織傷害的潛在可能性。

五、在 ISO/IEC 27000 一系列的標準中，ISO/IEC 27001 為 ISMS 主要驗證標準，而 ISO/IEC 27002 為指導綱要，明確地建議應有哪些資訊安全控制措施：

（一）ISO/IEC 27001：

- 目的在於要求組織應在其整體營運活動與其所面臨風險的狀況下，建立、實施、維持及持續改進 ISMS 文件化的要求，確保符合由風險評鑑、適用法規及其他要求所決定之資安要求，並確保選擇適切及相稱的安全控制措施，保護資訊資產，並提高利害相關者信心。

- 控制措施 （Control、Safeguards 或 Countermeasure）：用來降低風險發生的措施或防護機制。

（二）ISO/IEC 27001 對組織內部效益為：

- 提高員工資安意識，增進知識累積與經驗傳承，進而提升企業資訊安全管理能力。
- 降低資安風險，減少損失。
- 強化資安控制，減少客戶抱怨。
- 可為企業找到落實標準化、制度化之捷徑， 減少作業偏差。

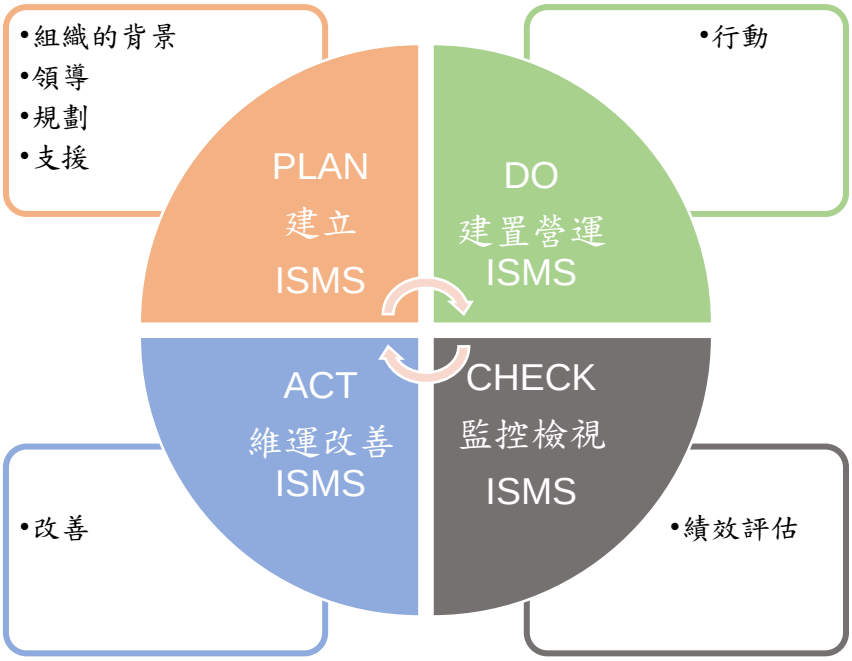
（三）ISO/IEC 27001 之外部效益為：

- 增加供應商、客戶及消費者之信心，有效提升競爭力，進而拓展行銷市場。
- 減少不同客戶對公司之重複資安稽核，避免人力、物力等浪費。
- 可經由完整而客觀之外部評鑑，評估公司 ISMS 運作方向是否符合國際標準規定。
- 符合國家政策要求。

六、資訊安全管理制度：

（一）資訊安全管理制度可分為 PDCA（Plan-Do-Check-Act）四大部份，針對品質工作按規劃、執行、查核與行動來進行活動，循環執行，

以確保可靠度目標之達成，並進而促使品質持續改善，如下圖所示：



（二）ISO/IEC 27001 PDCA 方法論是企業界普遍運用的一套「目標管理」流程，透過規劃（Plan）、執行（Do）、查核（Check）、行動（Act）四階段，確保每次的目標都能達成：

- Plan：按照企業的總體政策和目標，建立 ISMS 政策、目標、流程和程序，以管理風險，改善資訊安全。
- Do：實施和運行 ISMS 的政策、控制、流程和程序。
- Check：對 ISMS 政策、目標與實作經驗，評估衡量流程的績效，並向管理階層報告結果以做檢討。
- Act：依據內部 ISMS 稽核與檢核的結果，採取糾正和預防措施，達到 ISMS 的持續改善。

模擬考題

（一）關於機密性（Confidentiality），下列敘述何者「不」正確？

(A) 資訊不得在未授權的情況下對外揭露

(B) 資訊於儲存、傳輸過程中應採取加密措施

(C) 個人資料如帳號、密碼、信用卡卡號等資訊外洩為機敏性可能面臨之風險

(D) 機敏性資料僅有在駭客攻擊時才會面臨的風險

- 答案：(D)
- 解析：機密性係確保資料傳遞與儲存的私密性，避免未經授權的使用者有意或無意的揭露資料內涵；除駭客攻擊外，公司不小心公佈不該公佈的訊息也是。

（二）下列何者屬於資料完整性受影響？

(A) 機密資料外洩

(B) 檔案遭毀損而無法存取

(C) 系統無法正常提供服務

(D) 以明文方式傳輸

- 答案：(B)
- 解析：完整性應防止人為不慎的操作、惡意的竄改，或是自然雜訊的干擾，確保資訊或系統之正確性；檔案遭毀損而無法存取即為完整性遭影響。

（三）某系統的重要資料被駭客入侵，置換成含有惡意程式的檔案，此為下列何種資訊安全特性被破壞了？

(A) 機密性（Confidentiality）

(B) 完整性（Integrity）

(C) 可用性（Availability）

(D) 不可否認性（Non-repudiation）

- 答案：（B）
- 解析：完整性應防止人為不慎的操作、惡意的竄改，或是自然雜訊的干擾，確保資訊或系統之正確性；被駭客入侵，置換成含有惡意程式的檔係為遭受惡意的竄改。

（四）關於將檔案設定密碼保護之目的，下列敘述何者正確？

(A) 是為了確保資料之機密性

(B) 是為了確保資料之可用性

(C) 是為了確保資料之完整性

(D) 是為了確保資料之可讀性

- 答案：（A）
- 解析：機密性係確保資料傳遞與儲存的私密性，避免未經授權的使用者有意或無意的揭露資料內涵；設定密碼即是為了機密性。

（五）下列何者為「公司網路系統必須 24 小時運作」的主要原因？

(A) 機密性

(B) 可用性

(C) 完整性

(D) 不可否認性

- 答案：(B)
- 解析：可用性：確認被授權者在需要的時候，資訊與相關資產是可以存取與可以使用的。
  - ✧ 資訊與資訊處理的可用性，應避免因系統的故障、或是人為惡意的阻斷服務而受影響。
  - ✧ 企業資料必需即時並可靠的提供給企業內部各個層級的使用需求。

（六）下列何者為資訊安全的「可用性」之定義？

(A) 確保資訊的正確和完全性

(B) 確保資訊在需要時可被存取和使用

(C) 確保資訊在傳輸過程中已確認兩方的身分和合法性

(D) 確保資訊不會被揭露或被未經授權的個人、實體和流程所取得

- 答案：(B)
- 解析：可用性：確認被授權者在需要的時候，資訊與相關資產是可以存取與可以使用的。
  - ✧ 資訊與資訊處理的可用性，應避免因系統的故障、或是人為惡意的阻斷服務而受影響。
  - ✧ 企業資料必需即時並可靠的提供給企業內部各個層級的使用需求。

（七）關於資訊安全管理系統（Information Security Management System, ISMS），下列敘述何者較「不」正確？

(A) 導入資訊安全管理系統可以保護組織資訊資產的安全

(B) 要建立良好的資訊安全管理系統，需要制度面與技術面互相配合

(C) 最高管理階層的參與及支持是成功建立資訊安全管理系統的重點之一

(D) 在建立組織資訊安全管理系統的活動中，識別弱點會優先於識別資訊資產

- 答案：(D)
- 解析：在建立組織資訊安全管理系統的活動中，識別資訊資產會優先於識別弱點。

（八）資訊安全管理系統（Information Security Management System, ISMS）是在於管理面的要求，藉由審查機制、事件的回應及內部稽核來預防資訊安全事件或是降低其損失的風險，下列敘述何者不正確？

(A) 需要管理階層的承諾及提供相關支援，表達對資訊安全管理系統的支持

(B) 採用計畫(Plan)、執行(Do)、檢查(Check)及行動(Act)等四個階段的改進流程進行

(C) 資訊安全目標無需具體量化，導入解決方案，強化資訊安全防護為指導方針

(D) 內部稽核的成果報告需要在管理審查會議中進行檢討

- 答案：(C)
- 解析：資訊安全目標「需」具體量化，導入解決方案，強化資訊安全防護為指導方針。

（九）請問在資訊安全管理系統中的風險評鑑（Risk Assessment）作業，是在 Plan（規劃）、Do（執行）、Check（檢查）、Act（改善）循環中的那一部分？

(A) Plan（規劃）

(B) Do（執行）

(C) Check（檢查）

(D) Act（改善）

- 答案：(B)
- 解析：風險評鑑屬執行之一部份。

（十）在建置與運作資安系統時，常用戴明循環（Deming Cycle）協助管理，下列何項是戴明循環（Deming Cycle）正確的順序？

(A) Plan–Act–Do–Check

(B) Do–Check–Plan–Act

(C) Plan–Do–Check–Act

(D) Act–Check–Do–Plan

- 答案：(C)
- 解析：資訊安全管理制度可分為 PDCA （Plan-Do-Check-Act） 四大部份，針對品質工作按規劃、執行、查核與行動來進行活動，循環執行，以確保可靠度目標之達成，並進而促使品質持續改善。

第二節　相關法規概論與遵循

一、何謂資訊倫理

資訊倫理是在討論人們對資訊的態度以及行為，應用於電腦的使用、資訊科技、資訊系統、資訊網路的倫理規範。

資訊倫理不同於一般的法律，資訊倫理是屬於一種自律，以自己做起，做好自我的約束態度，不侵犯社會道德的一種規範。

資訊倫理的基本觀念就是要遵守國家法律，以不做出違法的事情為原則，並且尊重個人隱私權，給予每人的最基本權益，不盜用他人之智慧財產，達到資訊倫理的目的。

1986 年由美國管理信息科學專家梅森提出 PAPA 理論，包含了隱私權（Privacy）、正確性（Accuracy）、財產權（Property）及使用權（Accessibility），成為了資訊倫理重要的主軸。

二、何謂法規的遵循

資訊科技的發展越來越快，對企業或一般使用者的影響也越來越大，這些影響有些是正面的，但也有一些會對企業營運與個人權益產生重大的損失，特別是一些和資訊安全或隱私權相關的議題。

各地區政府或產業監管團體在近幾年來提出各項法規或要求，包含個人資料保護法、支付卡產業資料安全標準（Payment Card Industry Data Security Standard, PCI DSS）、健康保險可攜性與責任性法案

（Health Insurance Portability and Accountability Act, HIPAA）等。這些法規要求定期的報告與稽核，因此組織或業者都應適當地遵循這些規定。企業為符合法規規範與相關的要求，所進行的各項防範與控制措施，可稱為法規的遵循。

三、何謂稽核

資訊安全的稽核可以評估組織在資訊科技所實施的政策是否適當：協助偵測是否發生安全的違規事件、幫助判斷是否有誤用資源、並且可以阻止企圖入侵或危害系統的攻擊。

（一）稽核的類型：

- 第一方稽核（1st party audit）
  - ✧ 內部稽核。
- 第二方稽核（2nd party audit）
  - ✧ 外部提供者稽核。
  - ✧ 主管機關對所屬機構之稽核。
  - ✧ 其他外部利益方稽核。
- 第三方稽核（3rd party audit）
  - ✧ 驗證（Certification）或認證（Accreditation）稽核。
  - ✧ 法令（Statutory）、法規（Regulatory）和類似的稽核。

（二）稽核的角色與職責

- 主導稽核員（Lead Auditor）

1. 準備稽核計劃與通知

1-1 規劃稽核活動、準備工作文件，並向稽核小組說明。

1-2 與相關部門主管協調稽核時程。

2. 帶領內部稽核活動

2-1 匯整所有的稽核結果與意見，並編制內部稽核報告。

2-2 立即向受稽核方報告重大的缺失。

2-3 立即且明確地向受稽核方報告稽核結果。

3. 辦理啟動與結案會議

- 稽核小組成員（Audit Team Member）

✧ 支援主導稽核員的活動

✧ 依據稽核檢查清單執行稽核

✧ 報告缺失與改善的建議

✧ 確保稽核結果的機密性

✧ 確認一切行為符合道德與規範標準

- 受稽核方（Auditee）

✧ 負責保護資訊、資產與個人資料。

✧ 接受稽核報告，並檢視與討論。

✧ 依需要決定矯正措施，並安排資源按時完成。

（三）稽核人員應具備的能力

- 執行稽核的人員應保持其專業能力與獨立性，確保業務和營運上的職責分離（segregation of duties）。
- 資訊安全的稽核人員應擁有合格的專業能力，並具備進行稽核工作的相應知識和技能。
- 資訊安全稽核人員應對被稽核單位及其環境有所瞭解。
- 資訊安全稽核人員應取得充分且適當的稽核證據。
- 如果資訊安全稽核人員確認了重大的違規或非法行為，或可能存在的資訊，其應及時向適當的管理階層通報。

（四）稽核的執行

- 稽核證據 （Audit Evidence）

稽核證據與稽核準則（一組政策、程序或要求）有關，並且可查證的紀錄、事實陳述或其他資訊，應對所有的存取進行監控和紀錄，以提供日後稽核軌跡之參考。(稽核軌跡係指事件發生的過程中留下可供稽核的文件或紀錄，如系統日誌、申請表單、核准單據或公文及相關文件等。）

個人資料保護法規實施以後，對於個資的存取記錄、相關事證的保留與查核等，有更嚴格的規定。如果缺乏有效或是不足的使用紀錄與證據，無法佐證組織有提供適當的保護措施。不幸發生個資外洩事件時，也難以找出發生原因及攻擊者或肇

事者，不易預防未來事件的再次發生。

- 稽核發現（Audit Findings）

即將所蒐集的稽核證據對照稽核準則進行評估的結果。執行稽核時，藉由訪談、文件檢查、活動觀察或控制措施的測試來收集稽核發現。稽核人員在執行稽核的過程中，所獲得的各項證據都必須留下記錄，例如：所審查的文件名稱、版本，或是所訪談對象的職稱、回答的內容等。

稽核人員在執行稽核時應維持客觀與公正，對於各項查核作業均應以稽核軌跡、工作日誌或系統日誌、申請或授權表單等為基礎，進行客觀合理的分析與判斷。

模擬考題

（一）在資訊倫理領域中，常提到的四大議題（PAPA，學者 Mason 所提出），下列何者「不」在其中？

(A) 隱私權（Privacy）

(B) 正確性（Accuracy）

(C) 所有權/財產權（Property）

(D) 可用性（Availability）

- 答案：（D）
- 解析：PAPA 理論，包含了隱私權（Privacy）、正確性（Accuracy）、財產權（Property）及使用權（Accessibility）。

（二）請問資訊倫理常探討的四大議題（PAPA，學者 Mason 所提出）中，個人可保護自有資訊，具有決定是否公開或保密的權利，所指的是下列何者？

(A) 隱私權

(B) 正確性

(C) 存取權

(D) 廣泛性

- 答案：（A）
- 解析：個人可保護自有資訊，具有決定是否公開或保密的權利為隱私權。

（三）為保障持卡人的資料安全，制定統一的資料安全標準，提供資料安全的技術與作業要求之基準，此行為屬下列何者？

(A) PCI DSS

(B) HIPAA

(C) Sarbanes-Oxley Act

(D) Basel II

- 答案：（A）
- 解析：支付卡產業資料安全標準 Payment Card Industry Data Security Standard （PCI DSS）。

（四）由獨立的驗證單位所執行之稽核，稱為下列何者？

(A) 第一方（First Party）稽核

(B) 第二方（Second Party）稽核

(C) 第三方（Third Party）稽核

(D) 聯合/合併（Joint）稽核

- 答案：（C）
- 解析：驗證 （Certification）或認證（Accreditation）稽核屬第三方稽核。

（五）請問主管機關對所屬機構（如：金管會對銀行）執行之稽核，稱為下列何者？

(A) 第一方（First Party）稽核

(B) 第二方（Second Party）稽核

(C) 第三方（Third Party）稽核

(D) 聯合/合併（Joint）稽核

- 答案：(B)
- 解析：主管機關對所屬機構屬於第二方（Second Party）稽核。

（六）下列何種稽核可做出建議 ISO 27001 通過驗證發出證書？

(A) 第一方（First Party）稽核

(B) 第二方（Second Party）稽核

(C) 第三方（Third Party）稽核

(D) 第四方（Fourth party）稽核

- 答案：(C)
- 解析：驗證（Certification）或認證（Accreditation）稽核屬第三方稽核。

（七）請問目前國際上可做為取得認證與資訊安全相關的國際標準為何？

(A) ISO 27001

(B) ISO 27002

(C) ISO 27005

(D) ISO 27006

- 答案：(A)
- 解析：ISO 27001 可做為取得認證與資訊安全相關的國際標準。

（八）實施資訊安全管理系統（Information Security Management System, ISMS），第三方驗證公司是依據下列何種 ISO 標準進行驗證？

(A) ISO/IEC 27000 :2013

(B) ISO/IEC 27001 :2013

(C) ISO/IEC 27002 :2013

(D) ISO/IEC 27003 :2013

- 答案：（B）
- 解析：ISO/IEC 27001 :2013 為第三方驗證公司是進行驗證之標準。

（九）在進行資安內部稽核時，下列何者「不」是組織應該採取的做法？

(A) 由稽核小組規劃和建立內部稽核的計畫

(B) 在稽核計畫中定義稽核的範圍和準則

(C) 為確保稽核專業度，由資訊人員稽核其所負責的資訊系統

(D) 在完成稽核之後，將稽核結果報告給相關管理階層

- 答案：（C）
- 解析：為確保稽核專業度，由資訊人員「不得」稽核其所負責的資訊系統。

（十）下列那一項標準是針對雲端服務個人隱私資料的保護？

(A) ISO/IEC 27001

(B) ISO/IEC 27002

(C) ISO/IEC 27017

(D) ISO/IEC 27018

- 答案：(A)
- 解析：SO/IEC 27018 是針對雲端服務個人隱私資料的保護。

第三節　隱私權保護與智慧財產權

企業為符合法規規範與相關的要求，所進行的各項防範與控制措施，可稱為法規的遵循。

一、何謂個人資料保護法

（一）個人資料的保護也就是隱私權（Privacy）的保護與保障，隱私權的解釋：

- 隱私權是指個人具備法定的權利，可以選擇性地披露有關自己的資料，並進一步限制他人使用這些資料的方式。
- 個人在人格權上的利益不受不法僭用或侵害，個人與大眾無合法關聯的私事，亦不得妄予發布公開。

（二）企業藉由一套流程和程序來落實個人資料保護的規定，以及隱私權保護的原則，並成立一個因應小組來推動。在建立流程和程序之前必須先執行隱私權的風險評估，以保證完全符合法規規範。

二、我國的個人資料保護法規範行為

（一）蒐集：指以任何方式取得個人資料。

（二）處理：指為了建立或利用個人資料檔案 （包括備份檔案） 所執行的記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

（三）利用：指將蒐集之個人資料做為處理以外之使用。

三、個資法的相關規定

（一）個人資料

- 『個人資料保護法』第二條

1. 姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動，暨其他得以直接或間接方式識別該個人之資料。

- 『個人資料保護法』第六條

1. 特殊或具敏感性個資：醫療、基因、性生活、健康檢查及犯罪前科，105 年修訂新增加入「病歷」。

（二）告知的規定

- 個資法第八條提到，公務機關或非公務機關向當事人蒐集個人資料時，應明確告知當事人下列事項：

1. 公務機關或非公務機關名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依第三條規定得行使之權利及方式。

6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

（三）當事人權利

- 當事人就其個人資料依個資法第三條規定行使下列權利，不得預先拋棄或以特約來限制。針對當事者的權利行使，需在規定時限內回應處理。

1. 查詢或請求閱覽。
2. 請求製給複製本。
3. 請求補充或更正。
4. 請求停止蒐集、處理或利用。
5. 請求刪除。

（四）公務機關的要求

- 依個資法第十八條規定，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

（五）非公務機關的要求

- 依個資法第二十七條規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫，或業務終止後個人

資料處理方法。

（六）施行細則第十二條

- 個資法所稱適當安全維護措施、安全維護事項或適當之安全措施,指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。
- 前項措施得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善個資保護計畫的流程與施行。

（七）為防範個資的遺失、誤用、未經授權的存取、破壞等，組織應依據法規制定（個資法第 27 條）：

- 個人資料檔案安全維護計畫。
- 業務終止後個人資料處理方法。

（八）法務部提到上述標準等相關事項之辦法，得包括下列參考事項，同時宜審酌非公務機關規模、特性、保有個人資料之性質及數量等事項，並參酌施行細則第 12 條規定之適當安全措施事項訂定之，酌予調整：

- 個人資料保護之規劃。
- 個人資料之管理程序。
- 個人資料之管理措施。
- 個人資料之安全稽核、紀錄保存及改善機制。

管理階層對上述之計劃與處理方法的實施，每年應對人員、預算和其他資源的分配等進行審查。

四、智慧財產權（Intellectual property rights）

（一）組織應實施適當的程序，以確保符合與智慧財產權相關的法律、法規和合約要求，包含專有軟體產品的使用。僅能安裝與使用具有授權的軟體或產品，同時不超過授權內所允許的使用人數上限。且不得於著作權法所允許的範圍外進行：

- 複製或轉換成另一格式。
- 摘錄商業錄製品，如影片、聲音。
- 複製全部或部分之書籍、文章、報告等。

（二）智慧財產權的項目包含有：著作權、商標權、工業設計、專利、積體電路之電路布局等。

五、著作權協議（Copyright Agreements）

著作權是指法律所賦予著作人對於其所創作的著作的所有權利保護，包括著作人格權及著作財產權。著作人於著作完成時即享有著作權。

模擬考題

（一）資訊安全管理系統之法規遵循與適法性要求，旨在降低公司單位違反法律的風險，請問若公司要避免違反智慧財產權的相關法律，下列何者「不」包含在智慧財產權中？

(A) 著作權（Literary Property）

(B) 商標權（Trademark）

(C) 電子簽章法（Electronic Signature）

(D) 營業秘密（Trade Secret）

- 答案：(C)
- 解析：智慧財產權的項目包含有：著作權、商標權、工業設計、專利、積體電路之電路布局等。

（二）下列何者與保護「個人資訊隱私」有關？

(A) 個人資料保護法

(B) 專利法

(C) 商標法

(D) 著作權法

- 答案：(A)
- 解析：個人資料的保護也就是隱私權（Privacy）的保護與保障。

（三）為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。上述之法規為何？

(A) 電子簽章法

(B) 妨害電腦使用罪

(C) 著作權法

(D) 個人資料保護法

- 答案：(D)
- 解析：個人資料保護法之第 1 條：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用」。

（四）畢業後返校申請在校成績單，是行使個資法的哪一項權利？

(A) 請求刪除

(B) 請求製給複製本

(C) 請求補充

(D) 請求停止處理

- 答案：(B)
- 解析：畢業後返校申請在校成績單為請求製給複製本權利。

（五）關於智慧財產權（Intellectual Property Right, IPR），下列敘述何者「不」正確？

(A) 商標權是使用文字、標語和標誌的權利，註冊商標後，註冊人即享有商標專用權

(B) 專利權是對發明授予的權利，對專利權人之發明予以保護

(C) 著作權是為保護著讀者的權益，不被非授權複製與使用

(D) 營業秘密是指不爲公衆所知悉，能爲權利人帶來經濟利益，具有實用性並對權利人採取保密措施的技術資訊和經營資訊

- 答案：(C)
- 解析：著作權是指法律所賦予著作人對於其所創作的著作的所有權利保護。

（六）所有權（Property）是資訊倫理常探討的四大議題之一，請問關於所有權，下列敘述何者較為正確？

(A) 誰擁有資訊？

(B) 誰負責資訊的真實性與正確性？

(C) 在何種狀況保護措施下，可向他人揭露那些個人資料？

(D) 在何種條件下，個人與組織有權利來獲取所需資料？

- 答案：(A)
- 解析：(B) 資訊精確性、(C) 隱私權、(D) 資訊存取權

（七）公務或非公務機關在進行個人資料蒐集時，應明確告知當事人事項，請問其告知內容「不」包含下列何者？

(A) 個人資料蒐集的目的

(B) 個人資料的類別

(C) 個人資料儲存方式

(D) 個人資料利用的期間與地區

- 答案：(C)
- 解析：個人資料儲存方式不為個資法第八條所規定之應

告知事項。

（八）下列何者是我國個人資料保護法與歐盟一般資料保護規範（General Data Protection Regulation, GDPR）有較相同的規定？

(A) 資料刪除權

(B) 資料可攜權

(C) 引進新科技之個資處理方式時需進行資料保護影響評估

(D) 資料保護長制度

- 答案：(A)
- 解析：相較於其他三選項，我國個資法第三條第五款規定當事人具有請求刪除之權利。

（九）下列何者違反 GDPR（General Data Protection Regulation）的規範要求？

(A) GDPR 為歐盟一般資料保護法規

(B) 任何使用與歐盟公民相關資訊的公司都必須遵循

(C) 雲端處理者與控制者目前不納入 GDPR 強制實施範圍

(D) 要求持有個人可識別資訊的組織，需實施適切的安全控制措施，以防止個人資料遺失

- 答案：(C)
- 解析：GDPR 係規定所有資料處理者及控制者，並未將雲端除外。

（十）下列何者「不」是經濟合作及發展組織（Organization for Economic Cooperation and Development, OECD）之個人資料保護原則？

(A) 限制蒐集原則（Collection Limitation Principle）

(B) 分享原則（Share Principle）

(C) 公開原則（Openness Principle）

(D) 個人參與原則（Individual Participation Principle）

- 答案：（B）
- 解析：分享原則不為 OECD 之個人資料保護原則。

第五章. 資產與風險管理

一、 ISO/IEC 27002：2013 條款針對資訊對組織的價值有如下的詮釋與要求：

- 資訊的價值超越了書面文字、數字與影像，如知識、概念、思想與品牌等，都是資訊以無形的型式來呈現。
- 企業應像組織內其他重要的資產一樣來保護資訊，防止各種危害，範圍涵蓋與資訊有關之流程、系統、網路和人員。
- 資產的價值以及其風險可能會在任何時期發生變化，在各個階段中資訊安全都是重要的。
- 資訊宜依其對法律要求、組織價值、以及未經授權的披露或修改的重要性與敏感性來加以分類。
- 資訊安全的要求與控制應反應所涉及資訊的企業價值，以及由於缺乏足夠的安全性所導致潛在的負面業務影響。

二、風險管理 （Risk Management）

藉由協調各項活動以指導與控管組織的相關風險，通常包括：

（一）風險評鑑（Risk Assessment）

（二）風險處理（Risk Treatment）

（三）風險接受（Risk Acceptance）

（四）風險溝通 （Risk Communication）

第一節　資產分類分級與盤點

一、 資產的管理：

（一）識別與資訊及資訊處理設施相關聯之資產，並製作與維護此等資產清冊

（二）清冊中所紀錄之資產宜有擁有者：識別每項資產或資訊的擁有者，以提供該資產之責任與可歸責性。

- 每項資產（包含資料）必須指派擁有者，同時應被登記。
- 資產擁有者也是資產有關風險的擁有者。
- 資產擁有者可能不具資產之財產權，但對資產之生產、開發、維護、使用及安全有適當的責任。
- 可歸責性：確保使用者執行任何動作均有適當的軌跡可追蹤至執行者。

二、資訊的分類與分級：

（一）目標在確保資訊依據對組織的重要性受到適當等級的保護

- 資訊的敏感與重要程度可能各不相同。
- 在處理資訊時，資訊的分類可以表明保護措施之需要性、優先順序與預期程度。
- 只有擁有者可以調降等級。

資料類別	標準	範例
Public	公開不會造成傷害	您在公共網站上的資料
Internal	如果公開不會造成重大損害	在您的內部網站上的資料
Confidential	公開曝光可能會損害企業	專有的商業秘密
Private	公開曝光可能會損害他人隱私	政府的身分證號碼、信用卡號碼等個人資料

三、個人資料的盤點：

（一）對企業所有的業務與流程進行盤點，識別有使用或擁有個人資料的系統、檔案與活動。

（二）盤點流程中宜針對個人資料生命週期的各項處理活動細節予以檢視與紀錄，例如：人、事、時、地、物等。

（三）藉由個資盤點讓組織確認所蒐集個資的敏感性、影響程度、與相應的個資保護等級。如果員工不知道公司的機密或敏感資訊是什麼、在哪裡、以及如何保護這些資料，則很可能向未經授權的人士洩露此資訊。

（四）盤點組織所蒐集與擁有的個人資料項目與內容，例如：

- 個人資料檔案名稱。
- 個人資料檔案保有單位、負責人、維護人員與其他利害關係者。

- 保有之特定目的。
- 個資之類別，例如：識別類、特徵類等。
- 個資之範圍，例如:「專案小組聯絡名單」的範圍可能包含姓名、身分證統一編號、單位、職稱、住址、電話號碼、電子郵件信箱等。
- 個人資料檔案之保有期限。
- 個資之蒐集方法與來源。
- 個資生命週期的處理活動。
- 個人資料檔案之利用對象與範圍。
- 國際傳遞個資之直接收受者。

模擬考題

（一）以下關於資產清冊的敘述，何者較「不」正確？

(A) 在進行資產管理時，應優先建立資產清冊

(B) 將可移除式媒體載於資產清冊上，可減少資料遺失的機會

(C) 資產清冊需要識別與資訊及資訊處理設施有關的資產，並應予文件化

(D) 組織所有的資產，都應明列在資訊資產清冊上，也都需要標示購置時的成本和費用

- 答案：(D)
- 解析：組織所有的資產，都應明列在資訊資產清冊上，但毋需標示資產購置時的成本和費用。

（二）關於資訊資產分級的目的，下列敘述何者正確？

(A) 確保組織之相關安全責任

(B) 限制對資訊的存取

(C) 確保資產依組織之重要性，受到適切等級的保護

(D) 確保系統運作的完整性

- 答案：(C)
- 解析：資訊資產分級之目標在確保資訊依據對組織的重要性受到適當等級的保護。

（三）在資訊安全管理系統（Information Security Management System, ISMS）中定義並進行資訊資產分級，下列何者最適合納入評估

面向？

(A) 資訊資產的變現金額

(B) 資訊資產的折舊

(C) 資訊資產的流動性

(D) 資訊資產的機敏性

- 答案：(D)
- 解析：其他選項皆為財會等考量，非屬資訊資產的評量依據。

（四）對於資訊資產分級，以下敘述何者適當？

(A) 資訊資產分級之主要目的是方便組織進行資產登記與報廢

(B) 資訊資產分級之主要目的是協助組織定義資訊資產對組織的重要性

(C) 資訊資產的採購金額愈高，對組織的重要性一定愈高

(D) 人員非屬資訊資產應評估之象限之一

- 答案：(B)
- 解析：資訊資產分級之目標在確保資訊依據對組織的重要性受到適當等級的保護。

（五）請問下列對於資訊資產擁有者（Owner）在資產管理的工作描述何者為非？

(A) 確保資產已盤點與造冊

(B) 確保資產已適切分級並受保護

(C) 當資產刪除或銷毀資產時，確保已適當清除與處理

(D) 例行工作應親自執行，不可指派他人執行

- 答案：(D)
- 解析：資產擁有者可能不具資產之財產權，但對資產之生產、開發、維護、使用及安全有適當的責任。

(六)在資安管理中，關於資訊資產清冊，下列敘述何者「不」正確？

(A) 資產的重要性應與所支援的業務有關

(B) 運用資產管理軟體掃描可省去確認程序

(C) 資訊資產應依據依其類型進行分類

(D) 資產的重要性依其支援業務的重要性而有差異

- 答案：(B)
- 解析：大多數的資訊資產無法由軟體掃描取得，且掃描的結果需要進行確認以確保正確性。

(七) 關於資訊資產，下列敘述何者「不」正確？

(A) 資產指的是任何對組織有價值的事物

(B) 資產包含有型的事物，資訊包含無形的事物

(C) 資訊也是資產的一種

(D) 資訊可以以很多不同的形式存在

- 答案：(B)
- 解析：資訊的價值超越了書面文字、數字與影像：知識、概念、思想與品牌等，都是資訊以無形的型式來呈現。

（八）資訊資產價值需考量資訊資產的機密性、完整性及可用性，下列資訊資產何者的機密性價值更高？

(A) 人事資料

(B) 公司官網

(C) 線上學習系統

(D) 外部訓練申請單

- 答案：（A）
- 解析：人事資料屬於員工個人資料，更可能包含特種個人資料。

（九）關於電力供應，較符合資訊安全管理系統（Information Security Management System, ISMS）的何種資產類型？

(A) 軟體資產

(B) 資訊資產

(C) 硬體資產

(D) 服務資產

- 答案：（D）
- 解析：電力供應於 ISMS 中歸類為服務資產。

（十）若要保護機敏資料，針可移除式媒體（如：USB 隨身碟）的管理，下列敘述何者較「不」適當？

(A) 將可移除式媒體儲存於安全的環境

(B) 將可移除式媒體上的敏感資料進行加密

(C) 不將可移除式媒體登載於資產清冊上

(D) 不需使用的可移除式媒體，應將所儲存的資料徹底移除

- 答案：(C)
- 解析：移除式媒體應登載於資產清冊上。

第二節　風險評鑑與風險處理

一、風險評鑑（Risk Assessment）

包括風險分析與風險評估的整體流程：

（一）風險分析（Risk Analysis） 估計風險大小的系統性作法

- 系統化的使用資訊以鑑別資源與估計風險，以定性或定量之方式計算風險值。

（二）風險評估（Risk Evaluation）

- 將估計的風險與所訂的風險準則加以比較，以決定風險重要性的流程。

二、風險分析將風險進行定量或定性的描述

讓管理者能依據他們所認知的嚴重程度，或其他已確定的準則來對風險進行排序

（一）定性式風險分析（Qualitative Risk Analysis）：

- 採用尺度分級（如低、中、高）來描述後果的嚴重性，以及後果發生的可能性，以下為風險等級的範例：
  1. 事故情境之可能性分成如下等級：經常（4）、可能（3）、有可能（2）、不可能（1）、非常不可能（0）。
  2. 營運的衝擊分成如下等級：非常高（4）、高（3）、中（2）、低（1）、非常低（0）。

3. 風險等級：低風險（0-2）、中風險（3-5）、高風險（6-8）。

（二）定量式風險分析（Quantitative Risk Analysis）：

- 依據經濟上的損失，以及威脅可能成為一個事件的機率，來計算風險價值在定量式分析過程中可使用兩個指標作為參考：

  1. 事件發生的機率。
  2. 事件造成的損失。

- 定量式風險分析方式有兩種，即單一預期損失（Single Loss Expectancy, SLE）和年預期損失（Annual Loss Expectancy, ALE）。

  1. 單一預期損失（Single Loss Expectancy, SLE）：某項資產因某一風險所造成的損害。單一預期損失（SLE）可以用資產價值（Asset Value, AV）與曝光係數（Exposure Factor, EF）的乘積計算而得：

     SLE = AV * EF

     ＊曝光係數（Exposure Factor, EF）：代表資產因風險的影響，或是因風險對資產所產生的受損程度（比率），可能是一主觀的值。例如：資產價值減少 2/3，代表曝光係數是 0.66；如果資產完全失去，曝光係數就是 1.0 。

     範例：假設某一套系統的價值是 100 萬元（AV），因為

遭受拒絕服務（Denial of Service）攻擊，造成該系統有30% 的時間無法提供服務（EF = 30%）

SLE = 100 萬元 * 30% = 30 萬元

2. 年預期損失（Annual Loss Expectancy, ALE）：一年內從一個事件所造成損害，以貨幣形式表示。ALE 的計算是年發生率（Annual Rate of Occurrence, ARO）和單一預期損失（SLE）的乘積：

ALE = ARO * SLE

三、風險處理 （Risk Treatment）

選擇與實施各項控制措施，以修正風險的流程。ISO/IEC 27005 針對資訊安全的風險處理提出了四種選擇：

（一）風險修改（Modify Risk）：經由施行、移除或改變控制措施以管理風險等級，使殘餘風險可以被重新評定為可接受的，可能是解決風險（去除風險來源）或減輕風險（改變可能性）。

（二）風險保留（Retain Risk）或風險接受：無進一步的行動而保留風險的決策，例如：明顯符合組織的政策，或是風險等級滿足風險接受準則，則不需實施額外的控制措施，知悉並客觀地接受風險。

（三）風險避免（Avoid Risk）：停止產生風險的活動來避免風險，例如：從既有活動退出，或變更活動的運作狀況，像是在成本效

益下重新設計以避免風險。

（四）風險分攤（Share Risk）或風險轉移：將風險分攤到其他可以更有效管理該風險的另一方，例如：分攤的作法可藉由支援後果的保險 （保險公司），或是藉由外包給合作夥伴 （資訊服務業者）。

（五）風險處理的控制措施宜考量下列因素，確保風險降低到可接受的程度：

- 國家國際法律與法規的要求與限制
- 組織之目標
- 營運要求與限制條件
- 降低與風險相關的實施與營運成本，並保持和組織的要求與限制條件相稱
- 控制措施之實施與營運的投資，以及因安全失效可能導致的傷害，兩者需相稱

模擬考題

（一）在資訊安全管理系統（Information Security Management System, ISMS）中，風險識別「不」含下列何者？

(A) 識別各項資產的脆弱性

(B) 分析資安事故或事件對組織帶來的衝擊程度

(C) 評估環境或新技術帶來的威脅

(D) 建議購買軟硬體設備清單

- 答案：（D）
- 解析：風險識別不包含建議購買軟硬體設備清單。

（二）風險分析所使用的方法，除了「定量法（Quantitative）」之外，還可以採用下列何種方法？

(A) 定性法

(B) 類比法

(C) 平均法

(D) 參數法

- 答案：（A）
- 解析：系統化的使用資訊以鑑別資源與估計風險，以定性或定量之方式計算風險值。

（三）若公司為資訊資產購買保險，當資訊安全事件發生時，所造成的損失由保險公司理賠，此種風險處置策略屬於下列何者？

(A) 風險接受

(B) 風險降低

(C) 風險移轉

(D) 風險避免

- 答案：(C)
- 解析：風險分攤（Share Risk）或風險轉移：將風險分攤到其他可以更有效管理該風險的另一方，例如：分攤的作法可藉由支援後果的保險（保險公司）。

（四）關於風險改善計畫，下列敘述何者較「不」正確？

(A) 風險改善計畫不可變更

(B) 風險改善計畫應有期限

(C) 風險改善計畫完成後，應評估成效

(D) 風險改善計畫應針對超過可接受風險項目進行處置

- 答案：(A)
- 解析：風險改善計畫得視實際狀況討論後進行變更。

（五）某公司之風險評鑑發現，公司全球網站設置於內部網路，將增加外部入侵內部網路的風險，下列何者是「迴避」(Avoid）上述風險的作法？

(A) 將網站改設置於公司內防火牆的非交戰區（Demilitarized zone, DMZ）

(B) 將網站改設置於外部租用空間

(C) 增設網路監控設施，加強入侵監控機制

(D) 將網站設置於內部獨立網段

- 答案：(B)
- 解析：將網站設置於外部空間，透過網站入侵內網的風險即不存在。其他選項皆為風險控制的方法。

（六）關於風險規避（Risk Avoidance），下列敘述何者「不」正確？

(A) 決定不涉入風險處境

(B) 決定退出風險處境

(C) 通常不考量主管機關的影響，而會有躲避風險的傾向

(D) 會造成不願面對風險或淡化處理風險所需要的成本

- 答案：(C)
- 解析：停止產生風險的活動來避免風險，例如：從既有活動退出，或變更活動的運作狀況，像是在成本效益下重新設計以避免風險。

（七）關於風險評鑑管理程序，下列敘述何者不正確？

(A) 建立全景係界定風險評鑑範圍

(B) 詳細風險評鑑包括風險識別、風險分析與風險評估

(C) 風險處理若合意，則進入風險接受階段

(D) 風險評鑑若不合意，則進入風險溝通階段

- 答案：(D)
- 解析：風險評鑑若不合意，則回到建立全景階段。

（八）公司機房重地購買地震保險或者火險，是下列哪一個風險處理措施？

(A) 接受風險

(B) 規避風險

(C) 降低風險

(D) 轉移風險

- 答案：(D)
- 解析：風險分攤（Share Risk）或風險轉移：將風險分攤到其他可以更有效管理該風險的另一方，例如：分攤的作法可藉由支援後果的保險（保險公司）。

（九）關於風險評鑑與風險處理，下列敘述何者正確？

(A) 經過風險評鑑，低風險或處理成本過高的風險項目，可能會被組織選擇接受

(B) 風險評鑑可以百分百找出可能的風險項目，並且進行風險處置

(C) 風險處理可以百分百消除風險項目，確保資訊安全

(D) 風險處理後，組織就不再需要進行風險評鑑作業

- 答案：(A)
- 解析：經過風險評鑑，低風險或處理成本過高的風險項目，可能會被組織選擇接受。

（十）某公司的派工系統，原先未在高風險資產項目中，但近一年來接連遇到幾次服務中斷事件，造成極大的損失，若要重新檢視

該公司資產風險評鑑要素，下列何者「不」是適當的考量項目？

(A) 資訊資產重要性

(B) 資訊資產威脅

(C) 資訊資產殘值

(D) 資訊資產脆弱點

- 答案：(C)
- 解析：資訊資產殘值不為資產風險評鑑考量項目。

第六章. 存取控制、加解密與金鑰管理

第一節　存取控制與身分認證

一、存取控制的範疇（由外而內）大致上可以區分如下：

（一）實體的存取控制

（二）網路的存取控制

（三）系統的存取控制

（四）資料的存取控制

二、存取控制對於組織在營運要求的目標：

依據企業在營運與企業流程上的資訊安全要求，控制資訊與資訊處理設施的存取。

三、資訊科技中有若干不同的概念來實現資料的存取控制：

（一）存取控制類型

- 強制存取控制（Mandatory Access Control）
- 自由存取控制（Discretionary Access Control）
- 規則基準存取控制（Rule Based Access Control）
- 角色基準存取控制（Role Based Access Control）
- 宣告基準存取控制（Claim Based Access Control）

（二）組織的資訊適用於哪種類型的存取控制，應先了解其運作方式與特性，例如：「強制存取控制」以管理者授權為基礎，所有的資訊需經過管理者的授權，使用者才能存取資訊；「自由存取控制」由資訊擁有者決定哪些使用者對於資訊的存取權限，不需要經過管理者的授權。

（三）在實作存取控制的過程中，不必要的存取會增加資訊的風險，不論是有意或無意。因此，宜在職務與責任範圍這兩個領域中加以區隔（避免球員兼裁判），來降低資訊發生風險的機會，這種作法稱為職責分離或職務區隔（Segregation of duties）。

（四）授予存取權限包含下列項目：

- 身分（Identification）：代表人或系統的一個 token，例如：使用者名稱或密碼。
- 認證（Authentication）：系統確定使用者的身分是否真實和正確，且哪些資源的存取可能被授予。
- 授權（Authorization）：經適當授權而獲得存取的能力。

  最小權限（Least Privilege）：使用者應該基於最小權限原則，只能存取該業務所需工作的資料與權限。
- 紀錄（Accounting）：內容項目包含量測（Measuring）、監控（Monitoring）、報告（Reporting）與紀錄檔案(Logging)，以便提供未來作為稽核（Auditing）、計費（Billing）、分析

（Analysis）與管理之用，主要精神在於收集使用者與系統之間互動的資料，並留下軌跡紀錄。

四、使用者身分的認證：

（一）企業應採取適當的管理認證功能與技術，來做人員身分的管理與存取控制的驗證。

（二）身分的認證或驗證以身分提供者而言，可能包含下列幾項：

- 主機作業系統的認證

  Windows 或 LINUX 作業系統的本機認證。

- 組織人員身分的集中管理

  使用者帳戶、驗證、安全性原則與組織資源（例如，電腦、印表機與伺服器） 的集中式管理。例如，Active Directory 網域服務以及群組原則功能的運用。

- 聯邦式身分的識別

  將原本在企業內的單一登入（SSO）功能擴充至網際網路應用程式。例如：企業如果有些服務架構在公有雲的環境，需考慮應用程式部署在雲端運算平台上對使用者認證的限制。

（三）對於使用者身分的管理，可以藉由多因素驗證（多因子認證、Multi-factor Authentication），讓使用者身分被偷竊的風險得以降低。所謂的多因素驗證是利用多種獨立的方法來建立身分和

權限，包括：

- 您所知道的事，例如典型的使用者帳號與密碼。
- 您所擁有的事，例如代表您身分的 IC 卡或 smart card。
- 您所代表的事，例如指紋或虹膜掃描等生物特徵。

五、使用者密碼的管理：

（一）組織在密碼的管理上可參考下列指引

- 強制使用單獨的使用者 ID 和密碼，以維護可歸責性
  - ✧ 除使用密碼外，宜考慮多因素驗證等技術。
- 允許使用者選擇和更改自己的密碼，包括確認的程序
  - ✧ 有 X 次機會輸入正確的密碼，超過後密碼被鎖定（鎖定特定的時間後自動解除 or 經管理者重置）。
- 加強密碼的品質：使用高強度密碼（strong password）。
- 強制密碼的變更：密碼應定期變更。
- 帳號建立後，強制使用者在第一次登入系統時立即變更密碼。
- 密碼應避免舊密碼的重覆使用，密碼的歷程（History）需記錄。
- 在輸入或顯示密碼資訊時予以遮罩（Mask）。
- 密碼不可用無保護的型式（如 encrypted or hashed）儲存在電腦系統，也不能在網路上以明碼型式傳送。

（六）除了資料的存取控制外，組織也應對實體、網路或系統等進行存取控制：

- 實體進入控制措施
  - ✧ 根據業務需求等建立實體進入工作場所、建築物和區域的控制措施,措施應適用所有人員,包括正職/約聘員工、廠商、訪客等。
  - ✧ 確認只有經過授權的人員才允許進出。
- 網路控制措施
  - ✧ 對連接至網路的系統宜設限：使用網路存取控制來管控連結網路的設備，主要目的是要求設備必須要經過驗證與授權，才能存取網路上的服務或資料。
  - ✧ 網路存取保護：積極主動地保護企業網路安全，確保用戶端電腦必須以所設定的安全狀態才能連上企業網路。

模擬考題

（一）關於最小權限原則，下列敘述何者「不」正確？

(A) 最小權限原則指的是使用者的權限，不包含系統程序的權限

(B) 最小權限原則的核心是，僅提供執行任務所需的最小權限

(C) 最小權限原則可以避免被濫用或是盜用時造成的破壞

(D) 最小權限原則為計算機領域專有名詞之一

- 答案：(A)
- 解析：最小權限原則指的是使用者的權限，包含系統程序的權限。

（二）關於驗證（Authentication）與授權（Authorization），下列敘述何者正確？

(A) 輸入帳號密碼是屬於 Authorization

(B) CEO 可調閱資料是屬於 Authorization

(C) 使用者輸入 MFA Token 是屬於 Authorization

(D) 警察將嫌犯扣留 72 小時是屬於 Authentication

- 答案：(B)
- 解析：授權 (Authorization)：經適當授權而獲得存取的能力

（三）下列何者「不」是 AAA？

(A) Authentication

(B) Authorization

(C) Availability

(D) Accounting

- 答案：(C)
- 解析：AAA 包含「Authentication」、「Authorization」、「Accounting」

（四）關於存取控制需求的申請及審核，下列敘述何者「不」正確？

(A) 需要申請及審核機制

(B) 應定期檢視申請內容與當前需求是否一致

(C) 申請人主管審核通過即可逕行設定

(D) 組織應制定政策規範，使管理人員有所依循

- 答案：(C)
- 解析：存取控制需求的申請及審核需依照公司申請及審核機制。

（五）關於存取控制，下列敘述何者較「不」適當？

(A) 使用防火牆區隔內外網路，將公司對外全球網站放置於 DMZ 區（Demilitarized zone），並關閉非必要的連接埠

(B) 使用網段區隔技術，隔離敏感系統、重要機密的工作群組以及各類別的職務群組，但為了通聯及工作的便利性，內部網路各網段應直接互相通聯

(C) 機密檔案加密系統的使用者依不同的工作性質設定群組權限，非該群組成員無法開啟其加密檔案

(D) 重要系統設定其使用者超過一段時間未動作即會自動登出

- 答案：(B)
- 解析：使用網段區隔技術，隔離敏感系統、重要機密的工作群組以及各類別的職務群組，但為了通聯及工作的便利性，內部網路各網段「不」應直接互相通聯

（六）關於自然人憑證，下列敘述何者「不」正確？

(A) 自然人憑證是基於 PKI（Public Key Infrastructure）架構下之應用

(B) 自然人憑證在網路上使用時，其代表申請人之身分識別上具有法律效力

(C) 自然人憑證申請一次永久有效，無需換發

(D) 自然人憑證於網路上的相關應用具有不可否認性

- 答案：(C)
- 解析：自然人憑證需定期換發。

（七）下列何者「不」是單一登入（Single Sign-On, SSO）的優點？

(A) 集中權限控管

(B) 降低不同的帳號密碼記憶的困擾

(C) 減少重新輸入密碼的程序

(D) 簡訊認證

- 答案：(D)
- 解析：SSO 優點不包含簡訊認證。

（八）關於特權管理，下列敘述何者較正確？

(A) 管理者登入主機應該使用 Administrator or Root 帳號，以利管理權限之使用

(B) 資料庫管理員可利用管理者帳號備份資料外，還可以讀取資料及調校資料庫效能

(C) 基於代理人機制，系統管理員除了網路管理帳號外，也需主機管理者權限

(D) 應該定期審查特權帳號，若有人員離職也須立即審查相關系統帳號之使用

- 答案：(D)
- 解析：應該定期審查特權帳號，若有人員離職也須立即審查相關系統帳號之使用。

（九）如果運用「生物特徵」來做身分認證時，儀器的最佳靈敏度必須調整在「誤殺」與「誤放」兩條曲線的交叉點，這個點的錯誤率被稱為？

(A) 位元錯誤率（Bit Error Rate）

(B) 封包錯誤率（Packet Error Rate）

(C) 測試錯誤率（Test Error Rate）

(D) 交點錯誤率（Crossover Error Rate）

- 答案：(D)
- 解析：生物特徵來做身分認證時，儀器的最佳靈敏度在「誤殺」與「誤放」兩條曲線的交叉點稱為交點錯誤率。

（十）下列關於身分認證及權限管理的敘述，何者較「不」恰當？

(A) 使用者應妥善保管 IC 卡，不可任意外借他人使用

(B) 不定期清查帳號與權限

(C) 任何使用者均需輸入帳號及密碼，以進行使用者身分鑑別

(D) 專案或工作結束時，應刪除與系統營運或維護無關之帳號

- 答案：(B)
- 解析：需定期及不定期清查帳號與權限。

第二節　加解密與金鑰生命週期

行動式設備的使用可以提升員工的生產力，然而，行動式設備的遺失或被竊，可能讓企業的機密資料外洩。另外，網路服務上的檔案或資料傳送也因為使用不安全的方式來傳輸，容易造成重要資料的外洩。因此，我們需要以加密的方式來保護各種狀態下的資料。

一、何謂加密

加密是一種加強檔案或資料安全性的方式，它會打亂其中的內容，只有具備正確加密金鑰的人員才能還原及閱讀其內容；使用加密與完整性檢查，協助保護所儲存與傳送的資料，例如網站購物的交易資訊（如地址、電話號碼、信用卡號碼等）通常都會加密，以維護其安全。

（一）加密強度可以衡量攻擊者破解加密資料的難易度，一般而言影響加密強度的高低，有下列幾項因素：

- 演算法的強度
- 金鑰的長度：以相同技術而言，長度越長，越具機密性
- 金鑰保護機制

（二）加密的類型：

- 對稱性加密（Symmetric Encryption）
  - ✧ 加密與解密使用相同但逆向的演算法，所以其解密（decryption）演算法等同於加密演算法，也就是加密

與解密使用相同的金鑰，常見的對稱加密演算法有：DES、3DES、AES 等

- 非對稱性加密（Asymmetric Encryption）
  - ✧ 又稱為公開金鑰加密（Public Key Cryptography）。使用一對數學相關的金鑰：私密金鑰（Private Key）與公開金鑰 （Public Key），當用一把金鑰加密，就必須用相對應的另一把金鑰來解密。
  - ✧ 非對稱加密的特性，除了可以確保資訊的機密性外，因為只有發送端具備私密金鑰，因此可以確認資訊的來源，支援「不可否認性」。
  - ✧ 非對稱加密的應用：數位簽章（Digital Signatures）
  - ✧ 使用非對稱加密的技術（公鑰加密技術）來產生數位簽章，「數位簽章」可用於確認數位資訊由何人所產生或發送，如同簽署紙質文件與書面簽名的方法。
  - ✧ 常見的公鑰加密演算法有：RSA、Diffie-Hellman（D-H）密鑰交換協議中的公鑰加密演算法、橢圓曲線加密演算法（Elliptic Curve Cryptography, ECC）等。
- 雜湊（Hashing）
  - ✧ Hash Function（雜湊函數） 可以將輸入的資料打亂或壓縮，重新建立一個輸出的雜湊值。

- ✧ 雜湊函數屬於單方向的函數，輸出的雜湊值具有一定程度的獨特性，原則上無法從雜湊值反推回原始資料，常見的雜湊演算法有：SHA256 等。

（三）加密相關的標準與技術：

- Transport Layer Security（TLS、傳輸層安全）與 Secure Sockets Layer（SSL）
  - ✧ IETF（www.ietf.org）將 SSL 作了標準化，即 RFC2246，並將其稱為 TLS。從技術上而言，TLS1.1 與 SSL3.2 的差異非常微小。
  - ✧ TLS 與 SSL 在傳輸層對網路連接進行加密，與應用層協議獨立無關。SSL 採用公開密鑰技術，保證兩個應用間通信的保密性和可靠性，使客戶與伺服器應用之間的通信不被攻擊者竊聽。
  - ✧ 目前已為網際網路上保密通訊的工業標準，現行 Web 瀏覽器亦普遍將 Http 和 SSL 相結合，從而實現安全通信。
- IPSec（網際網路通訊協定安全性）
  - ✧ IPsec 是一套開放式標準的架構，它利用加密和認證來保護 IP 網路上的通訊安全，支援網路層級的對等驗證、資料來源驗證、資料完整性、資料機密性（加密）等功能。

- 憑證服務
  - ✧ 是種識別身分、存取控制與資訊保護的技術，可讓您建立與管理數位憑證，這些憑證用來保護敏感的個人資料。
  - ✧ 憑證（公開金鑰憑證）是數位式簽章的敘述，它會將公開金鑰連結到有相應私密金鑰的使用者。
  - ✧ 在公開金鑰加密中，會使用兩種不同的金鑰進行資訊的加密和解密，其中私密金鑰是只有擁有者知道的金鑰，公開金鑰則可公開給網路中的其他實體，這兩個金鑰各不相同，但在功能上是互補的。

二、金鑰生命週期的管理（Key management）

金鑰/密鑰（Key）是用來完成加密、解密、完整性驗證等密碼學應用的機密資訊。管理是制定和實施加密金鑰（cryptographic keys）在使用、保護和其生命週期的政策。

（一）金鑰的管理在支援加密技術的使用上，注意事項如下：

- 金鑰的產生、儲存與歸檔的設備，宜有實體的保護。
- 金鑰宜有明確的啟動與終止的日期，只能在有限期間內使用，降低被破解的機會。
- 保護所有的加密金鑰不被修改、遺失與破壞。
- 私鑰不會未經授權的揭露。

- 訂定金鑰被破解的處理程序。
- 避免在不同的系統使用相同的密鑰。

模擬考題

（一）關於金鑰與憑證管理，下列敘述何者「不」正確？

(A) 金鑰都應受保護不被修改和破壞，並應使用實體安全來保護用於產生、儲存和歸檔金鑰的設備，以避免金鑰遭受不當修改、不慎遺失或銷毀等情況

(B) 基於業務需要，須自行建置、委託建置或選用憑證機構（Certificate Authority）時，應綜合考量憑證機構之技術、管理、人員及財務的安全風險等

(C) 憑證機構資訊系統（含應用系統、密碼模組等）之安全驗證，應遵照權責主管機關訂定之規範作業，以確保其安全性

(D) 憑證機構使用之電子簽章或加密金鑰長度，視系統的安全需求，由組織自行決定

- 答案：（D）
- 解析：憑證機構使用之電子簽章或加密金鑰長度，視系統的安全需求，由組織決定使用之加密技術而定。

（二）密碼學常被認為是提供數位身分認證的基礎，請問一套加密系統「不」包含下列何者？

(A) 明文

(B) 暴力破解機制

(C) 加密演算法

(D) 密文

- 答案：(B)
- 解析：加密系統包含明文、密文、加密演算法。

（三）某銀行近日疑似遭遇駭客以彩虹表（Rainbow Table）攻擊法破解內部伺服器的密碼系統，為了能夠抵擋類似的攻擊手法再度發生，請問銀行的內部密碼系統該如何因應？

(A) 更換加密雜湊演算法

(B) 制定更嚴謹的密碼政策

(C) 啟用密碼鎖定原則

(D) 使用加鹽的金鑰延伸函式（Key Derivation Function with a Salt）

- 答案：(D)
- 解析：使用加鹽的金鑰延伸函式可避免彩虹表（Rainbow Table）攻擊法。

（四）下列何種加密技術，屬於「非對稱式金鑰加密技術」？

(A) 國際資料加密演算法（International Data Encryption Algorithm, IDEA）

(B) 進階加密標準（Advanced Encryption Standard, AES）

(C) 資料加密標準（Data Encryption Standard, DES）

(D) 橢圓曲線密碼學（Elliptic Curve Cryptography, ECC）

- 答案：(D)
- 解析：橢圓曲線密碼學屬於非對稱式金鑰加密技術。

（五）關於數位簽章（Digital Signature）及數位信封（Digital Envelop），下列敘述何者正確？

(A) 數位簽章與數位信箱皆運用雜湊函式（Hash Function）達成效果

(B) 數位簽章主要是將訊息摘要加密後運用對稱金鑰加密

(C) 數位信封將資料以對稱金鑰加密，再將金鑰透過公開金鑰加密技術傳輸供收訊方解密

(D) 數位簽章及數位信封技術在訊息傳遞時皆已加密訊息

- 答案：（C）
- 解析：數位信封將資料以對稱金鑰加密，再將金鑰透過公開金鑰加密技術傳輸供收訊方解密。

（六）請問下列何者「不是」對稱式加密？

(A) DES（Data Encryption Standard）

(B) 3DES （Triple DES）

(C) ECC（Elliptic Curve Cryptography）

(D) RC6（Rivest cipher 6）

- 答案：（C）
- 解析：橢圓曲線密碼學（ECC）屬於非對稱式金鑰加密技術

（七）關於「對稱式金鑰加密」與「非對稱金鑰加密」，下列敘述何者「不」正確？

(A) 「非對稱金鑰加密」在加解密使用不同金鑰

(B)「對稱金鑰加密」在金鑰洩露後，其加密效果即時失效

(C)「非對稱金鑰加密」的特性，可以實作數位簽章（Digital Signature）

(D)「非對稱金鑰加密」的計算，效能比「對稱金鑰加密」佳

- 答案：(D)
- 解析：對稱式效能較佳

（八）關於數位簽章（Digital Signature），下列敘述何者「不」正確？

(A) 使用了公開金鑰基礎建設（Public Key Infrastructure, PKI）

(B) 簽章時用公鑰（Public Key）加密

(C) 公鑰（Public key）必須向接受者信任的數位憑證認證機構（Certificate Authority, CA）註冊

(D) 可以用 EIGamal 演算法來實做數位簽章

- 答案：(B)
- 解析：通常會使用公鑰加密，用私鑰解密。而在數位簽章中，會使用私鑰加密(相當於生成簽名)，公鑰解密(相當於驗證簽名)。

（九）若明文為「WE ARE DISCOVERED FLEE AT ONCE」，使用凱撒密碼偏移量為 6，請問密文為下列何者？

(A) CKGXK JOYIU BKXKJ LRKKG ZUTIK

(B) IQMDQ PUEOA HQDQP RXQQM FAZOQ

(C) OWSJW VAKUG NWJWV XDWWS LGFUW

(D) UCYPC BGQAM TCPCB DJCCY RMLAC

- 答案：(A)
- 解析：CKGXK JOYIU BKXKJ LRKKG ZUTIK

（十）下列敘述何者「不」正確？

(A) 公私鑰加解密演算法使用「公鑰加密」與「私鑰解密」

(B) 數位簽章的時候，傳送端使用自己的公鑰製作簽章，接收端使用傳送端的私鑰驗證簽章

(C) 公鑰加密系統是多人都可以拿公鑰加密，但是只有一個人可以拿私鑰解密

(D) 數位簽章系統是只有一個人可以拿私鑰製作簽章，但是多人都可以拿公鑰驗證簽章

- 答案：(B)
- 解析：通常會使用公鑰加密，用私鑰解密。而在數位簽章中，會使用私鑰加密(相當於生成簽名)，公鑰解密(相當於驗證簽名)。

第七章. 事故管理與營運持續

第一節　事件與事故管理

一、我國個人資料管理法事件與事故管理相關規定

（一）組織為因應使用者或消費者個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定相關應變、通報及預防機制：

- 事故發生後應採取之應變措施，包括降低、控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。
- 事故發生後應受通報之對象及其通報方式。
- 事故發生後研議其矯正預防措施之機制。
- 業者遇到個人資料安全事故，將危及其正常營運或大量當事人權益者，應立即通報主管機關或直轄市、縣（市）政府。

二、資通安全事件通報及應變辦法

（一）針對各級政府機關（構）的通報作業也有相關規定：

- 各級政府機關（構）發現資安事件後除應循內部程序上報外，並須於 1 小時內，至國家資通安全通報應變網站（https://www.ncert.nat.gov.tw）通報登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政

府機關（構）或重要民生設施運作，需橫向通知相關應變分組。

- 進行資安事件處理，「4」、「3」級事件須於 36 小時內損害控制或復原作業；「2」、「1」級事件須於 72 小時內損害控制或復原作業。資安事件影響等級分為 4 個級別，由重至輕如下：

✧ 1.「4 級」：

1.1、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

1.2、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

1.3、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

✧ 2.「3 級」：

2.1、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

2.2、未涉及關鍵基礎設施維運之核心業務資訊或核心

資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

2.3、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

✧ 3.「2 級」:

3.1、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

3.2、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

3.3、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

✧ 4.「1 級」:

4.1、非核心業務資訊遭輕微洩漏。

4.2、非核心業務資訊或非核心資通系統遭輕微竄改。

4.3、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

三、歐盟一般資料保護規則

（一）歐盟於 2018 年 5 月 25 日生效，全面施行新版的個人資料保護規範「一般資料保護規則」（General Data Protection Regulation, GDPR） 針對個人資料外洩的通報也有嚴格的規定。如果發生資料外洩的事件，資料控制者通常必須在 72 小時內通知適當的主管機關。

四、ISO/IEC 27002 針對資訊安全事故及改善之管理包含下列控制措施：

（一）建立管理的職責和程序，以確保對資訊安全事故有快速、有效與有序的回應。

（二）資訊安全事件的通報：資訊安全事故應透過適當的管理管道盡快通報。

（三）資訊安全弱點的通報：資訊系統和服務的使用者，應注意任何發現或懷疑的資訊安全弱點，並且通報。

（四）資訊安全事件的評估與決策：資訊安全事件（events）如果要

被歸類為資訊安全事故（incidents）應進行評估後決定。

- 何謂資訊安全事件（Information Security Event）：

  系統、服務或網路狀態被識別出狀態變化的現象，指出可能是資訊安全政策的漏洞、安全措施的失效、或先前不知可能與安全相關的情況。

- 何謂資訊安全事故 （Information Security Incident）：

  有顯著機率危害營運及威脅資訊安全之單一或一連串非所欲或非所預期的資訊安全事件。

（五）資訊安全事故的回應：組織針對資訊安全事故，宜依據文件化的程序予以回應。

（六）由資訊安全事故中學習：從分析和解決資訊安全事故所獲得的知識應該用來減少未來事故的可能性或影響。

（七）證據之蒐集：組織應制定程序以識別、收集、採集與保存可以作為證據的資訊。

五、資訊技術基礎架構庫的事故管理流程（Incident Management Process）

（一）事故的確認（Incident identification）：只有當確認發生了事故，才能啟動相對應的工作。

（二）事故的記錄（Incident logging）：所有與事故相關的資訊都需進

行記錄，以便產生完整的歷史紀錄。

（三）事故的分類（Incident categorization）：在進行初次紀錄時，必須分配一個正確的事故分類編碼，以便記錄正確的類型。

（四）事故的優先等級（Incident prioritization）：事故的優先等級決定事故的影響程度和緊急性。

（五）初始的診斷（Initial diagnosis）：服務台分析人員進行初期的診斷。

（六）事故的提升（Incident escalation）：如服務台本身無法解決事故或者已超出一線解決的目標時間，應立即提升事故以獲得進一步的支援。

（七）調查與診斷（Investigation and Diagnosis）：事故處裡的每個支援人員都應將調查與診斷的活動完整紀錄。

（八）解決與復原（Resolution and Recovery）

（九）事故的關閉（Incident Closure）

模擬考題

（一）關於資安事件發生時的應變，下列敘述何者較「不」正確？

(A) 疑似病毒入侵時，應優先拔除網路線，避免病毒擴散

(B) 遭受天然災害時（如：地震、火災），應在有限範圍內攜帶重要資料離開現場

(C) 事件發生的第一時間，不需浪費時間進行判斷，應立刻採取行動

(D) 應保留事件發生的所有證據，以利後續分析

- 答案：(C)
- 解析：事件發生的第一時間，需進行判斷後立刻採取行動。

（二）若公司電腦檔案被勒索軟體加密，下列何者「不」是正常應變處置程序？

(A) 斷網降低網路擴散之風險，並且進行鑑識追蹤感染來源

(B) 清查是否有相關版本的備份，或是從受保護安全區取回檔案

(C) 交付比特幣贖金以加速檔案解密

(D) 必須依據資安通報流程進行通報

- 答案：(C)
- 解析：相關檔案無備份，私自交付比特幣贖金進行檔案解密。

（三）關於資安事故（Security Incident），下列敘述何者「不」正確？

(A) 指已經造成服務或營運中斷之資安事件（Security Event）

(B) 指極可能造成服務或營運中斷之資安事件（Security Event）

(C) 當造成中斷過久時，需啟動營運持續計畫

(D) 通常會先觀察，暫不處理

- 答案：（D）
- 解析：通常會先觀察後處理。

（四）某公司遭駭客針對網站伺服器傳送大量特定封包而導致網站癱瘓，造成資訊系統部分功能降低或喪失，此稱為下列何者？

(A) 資訊安全事件（Event）

(B) 資訊安全事故（Incident）

(C) 資訊安全風險（Risk）

(D) 資訊安全分析（Analysis）

- 答案：（B）
- 解析：ISO 27001:2013 A.16 資訊安全事故管理

（五）「為了分析資安事件的根本原因，會利用有價值的網路、資料、電腦系統，故意設置了脆弱性的伺服主機，用來吸引駭客攻擊，用來瞭解其入侵技術及行為模式」，此稱為下列何者？

(A) 多層次防禦（Layered Defense）

(B) 蜜罐（Honypot）

(C) 滲透測試（Penetration Test）

(D) 黑箱測試（Black-Box Testing）

- 答案：(B)
- 解析：蜜罐（Honypot)：通常偽裝成看似有利用價值的網路、資料、電腦系統，並故意設定了 bug，用來吸引駭客攻擊。由於蜜罐事實上並未對網路提供任何有價值的服務，所以任何對蜜罐的嘗試都是可疑的。蜜罐中還可能裝有監控軟體，用以監視駭客入侵後的舉動。

（六）下列何者可從多種資料來源中即時收集或從歷史資安事件分析而產生的威脅偵測及資安事故應變，同時也提供合適的報表以及歷史資安事故的分析？

(A) 安全資訊與事件管理（Security Information & Event Management, SIEM）

(B) 入侵偵測系統（Intrusion Detection Systems, IDS）

(C) 入侵預防系統（Intrusion Prevention Systems, IPS）

(D) 網頁應用防火牆（Web Application Firewall, WAF）

- 答案：(A)
- 解析：安全資訊與事件管理即時收集或從歷史資安事件分析而產生的威脅偵測及資安事故應變，同時也提供合適的報表以及歷史資安事故的分析。

（七）關於資安事件發生時的緊急應變措施，下列敘述何者不正確？

(A) 依訂定之緊急應變計畫，實施緊急應變處置，並持續監控與追蹤管制

(B) 一定要緊急關閉電腦防止資安事件發生

(C) 視資安事件損壞程度啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大

(D) 評估資安事件對業務運作造成之衝擊，並進行損害管制

- 答案：(B)
- 解析：緊急關閉電腦防止資安事件發生，可能造成證據遺失。

（八）某公司規定重要系統與資料，在發生重大災難時，也不能發生過長營運中斷或是資料的遺失，當該公司建置異地備援中心時，下列何者「最」能符合上述要求？

(A) 熱備援（Hot Backup Site）

(B) 暖備援（Warm Backup Site）

(C) 冷備援（Cold Backup Site）

(D) 無需建置備援中心

- 答案：(A)
- 解析：熱備援指在異地的備援中心擁有專屬的電腦設備，除了將關鍵業務系統建立完整的備援（mirroring）外，資料也有即時的同步或備份。當日常運作環境發生災難事件時，備援系統可以立即接管、銜接，同時資料不會有遺失的現象。

（九）資安事件緊急應變處置最重要目的為下列何者？

(A) 用防火牆或 WAF 做偵測跟阻擋

(B) 採用弱掃工具或滲透測試服務驗證是否完成修補

(C) 控制受害範圍

(D) 立即使用資料復原即可

- 答案：(C)
- 解析：緊急應變處置最重要目的為控制受害範圍，避免擴散。

（十）公司收到主管機關要求，必須每年進行網路資安健檢，下列何種處理較「不」符合？

(A) 遠端網路弱點掃描（Network Vulnerability Assessment）

(B) 遠端滲透測試（Penetration Testing）

(C) 到場網頁應用程式弱點掃描（Web Vulnerability Assessment）

(D) 到場網路安全備援服務

- 答案：(D)
- 解析：到場網路安全備援服務不為資安健診項目。

第二節　備援與營運持續

組織的營運或業務的持續性，若被破壞，將產生嚴重的影響。例如：無法持續提供使用者的交易或服務、企業利潤減少或虧損增加、對組織形象有負面的宣傳、或更甚者對公司的生存也產生危機。

因此，為對抗營運活動可能的中斷，保護重要企業流程免受重大資訊系統失效或災害的影響，並確保流程的及時恢復，組織應將資訊安全的持續性，整合到組織的企業持續性管理系統中。

一、復原方案

重大的災難事件，可能導致關鍵的系統，無法在日常運作的資料中心或系統中繼續運行，組織必須藉由異地的備援中心來復原系統，持續營運。異地的備援中心會依據所配備的環境、設施或服務等級分成下列：

（一）備份系統的準備程度

- Hot Site：在異地的備援中心擁有專屬的電腦設備，除了將關鍵業務系統建立完整的備援（mirroring）外，資料也有即時的同步或備份。當日常運作環境發生災難事件時，備援系統可以立即接管、銜接，同時資料不會有遺失的現象。Hot Site 的服務等級比較高，但所需成本也比較高。
- Warm Site：在異地的備援中心擁有合適的電腦設備，準備用來復原服務。另外，備份的資料可能有時間差，復原系

統後，部分資料會有遺失的現象。

- Cold Site：異地的備援中心只配備必要的環境或設施 ，像是電力、空調、網路等，在發生災難時可能需要將所需的相關設備搬移過來，執行安裝、 設定、還原等工作後，才能復原服務。Cold Site 的服務等級比較低，但所需成本也比較低。

（二）備份方式

- 全部備份(Full Backup): 即把硬碟或資料庫內的所有檔案、資料夾或資料作一次性的複製。
- 增量備份（Incremental Backup）: 指對上一次全部備份或增量備份後更新的資料進行備份。
- 差異備份（Differential Backup）: 差異備份提供執行完整備份後變更的檔案的備份。
- 選擇式備份(Selective Backup): 對系統的一部分進行備份。

二、組織在規劃關鍵系統或服務的可用性與持續性指標

（一）Availability（可用性）

一個服務、元件或組態項目（Configuration Item）在需要的時候，執行其所同意的功能的能力。通常 Availability 藉由一個百分比來予以量測及報告。

$$Availability\ (\%)$$

$$= \frac{Agreed\ Service\ Time(AST) - Downtime}{Agreed\ Service\ Time(AST)}\ X\ 100\%$$

（二）回復時間目標（Recovery Time Objective, RTO）

- 當發生服務中斷時，可以接受的當機時間。
- 當災難發生後，服務恢復的時間點。
- RTO 越低，所使用的復原策略的成本會越高。

（三）回復點目標（Recovery Point Objective, RPO）

- 當發生服務中斷時，資料可能產生遺失，RPO 代表可以接受的資料遺失狀況。
- 代表要復原資料的起始時間點。
- 範例：

  RPO=兩小時, 代表服務中斷所遺失的資料，最多是兩小時內的資料，也就是 backup 的間隔時間不能超過兩小時。

（四）復原服務的平均時間（Mean Time to Restore Service, MTRS）

- MTRS 所涵蓋的 downtime 包含全部有助於復原的項目，像是 record、respond、resolve、physically repair or replace 以及 recover 的時間。

（五）最大可容忍中斷時間（Maximum Tolerable Period of Disruption , MTPD）

- 不利的衝擊導致不被接受之結果所需的時間，此期間可能

無法提供產品服務或執行活動。

三、規劃策略的決定因素

（一）服務對企業營運的重要性

（二）營運持續與風險評鑑：營運持續管理宜識別可能導致營運流程中斷的事件，與這些事件的機率和衝擊，並瞭解其對資訊安全的影響。

（三）復原時間

（四）復原成本

（五）安全性

模擬考題

（一）關於災難復原計畫之目的，下列敘述何者「不」正確？

(A) 將災難造成的影響減少至最小程度

(B) 分析災難、安全缺失和服務損失的後果

(C) 採取必要的措施來確保業務能正常執行

(D) 回復資訊的完整，並確保資訊系統正常運作

- 答案：(B)
- 解析：災難復原計畫之目的包含將災難造成的影響減少至最小程度、採取必要的措施來確保業務能正常執行及回復資訊的完整，並確保資訊系統正常運作。

（二）關於營運測試計畫，下列敘述何者正確？

(A) 平行測試：在實際作業環境中進行測試

(B) 完全中斷測試：於備援平台上進行測試

(C) 模擬測試：建立模擬環境並於其中測試

(D) 結構化排練測試：權責單位各自討論處理方式與可行性

- 答案：(C)
- 解析：模擬測試：建立模擬環境並於其中測試。

（三）下列何者「不」屬於復原程序之項目？

(A) 於備援設備中安裝作業系統與應用程式

(B) 於復原系統重新載入備份資料

(C) 復原系統上線後重新評估災害發生風險

(D) 測試復原系統之功能是否正常

- 答案：(C)
- 解析：復原系統上線後重新評估災害發生風險不屬於復原程序。

（四）關於營運持續計畫之目的，下列敘述何者「不」正確？

(A) 營運持續計畫一套基於業務運行規律的管理要求和規範流程

(B) 業務持續性是指企業有應對風險、自動調整和快速反應的能力

(C) 將災難造成的影響減少至最小程度，確保業務流程能及時地繼續運行

(D) 制訂和實施應變計畫，確保在要求的時間內恢復業務流程

- 答案：(C)
- 解析：營運持續計畫為對抗營運活動可能的中斷，保護重要企業流程免受重大資訊系統失效或災害的影響，並確保流程的及時恢復，組織持續性。

（五）關於 RPO，下列敘述何者正確？

(A) 可以忍受多久的業務中斷

(B) 資料回復的時間點與資料量無關

(C) 以可容許資料資料損失時間與資料量，進行備份計畫評估

(D) RPO 投入資源越多，恢復越慢

- 答案：(C)

- 解析：當發生服務中斷時，資料可能產生遺失，RPO 代表可以接受的資料遺失狀況。

（六）若固定每星期日執行一次完整備份（Full Backup），之後每天會備份從上次完整備份到目前所異動的內容，此現象稱為下列何者？

(A) 差異備份（Differential Backup）

(B) 增量備份（Incremental Backup）

(C) 循環備份（Circulatory Backup）

(D) 緊急備份（Emergency Backup）

- 答案：（A）
- 解析：差異備份（Differential Backup）：差異備份提供執行完整備份後變更的檔案的備份。

（七）在進行營運持續規劃時，若評估發現公司資料遺失之最大可接受程度為 10 分鐘內，應考慮下列何者？

(A) 恢復點目標（Recovery Point Objective, RPO）

(B) 恢復時間目標（Recovery Time Objective, RTO）

(C) 工作恢復時間（Work Recovery Time, WRT）

(D) 最大可容忍中斷時間（Maximum Tolerable Period of Disruption, MTPD）

- 答案：（A）
- 解析：當發生服務中斷時，資料可能產生遺失，RPO 代表可以接受的資料遺失狀況。

（八）您是資安專家，希望能估計營運可承受之最長中斷時間（Maximum Tolerable Period of Disruption），而您最有可能從下列何者取得？

(A) 平衡計分卡（Balanced Score Card）

(B) 風險評鑑（Risk Assessment）

(C) 恢復點目標（Recovery Point Objective）

(D) 營運衝擊分析（Business Impact Analysis）

- 答案：（D）
- 解析：營運衝擊分析包含營運可承受之最長中斷時間（Maximum Tolerable Period of Disruption）。

（九）關於資料復原點的目標（Recovery Point Objective），下列敘述何者正確？

(A) 系統硬碟所儲存的資料量

(B) 系統進行備份所需要的時間

(C) 在災害發生之後，預計要將資料復原到特定的某一時間

(D) 在災害發生之後，預計資料無法回復的時間

- 答案：（C）
- 解析：當發生服務中斷時，資料可能產生遺失，RPO 代表可以接受的資料遺失狀況。

（十）組織要如何確認營運持續計畫的有效性？

(A) 以文件化方式呈現

(B) 進行營運持續演練

(C) 指派一位同仁負責計畫的撰寫

(D) 指派一組同仁負責計畫的撰寫

- 答案：(B)
- 解析：進行營運持續演練確認營運持續計畫的有效性。