《資訊安全實務》

一、請完整寫出下列名詞的全名，並說明其功能。（每小題5分，共25分）

(一) ISAC

(二) SOC

(三) CERT

(四) CI

(五) CII

命題意旨	資安組織名詞解釋。
答題關鍵	本題在考學生對於資安組織架構與層級的認識，尤其英文全名偏長，有一定難度；名詞解釋要詳細說明並區分各個名詞的不同，課堂上已練習多次，班內生可以穩穩地收下此題分數。

【擬答】

(一)ISAC：Information Sharing and Analysis Center，資安資訊分享與分析中心：

ISAC 的主要工作職掌有二：

1.資安維護：情資的蒐集與技術處理，掌握各類型威脅與弱點，提供分析結果與對策，進行有效預防措施，為事前預防階段。

2.事件分享：與各領域 ISAC 進行交流，強化情資分享與事件報告，以利資安人員快速與有效反應資安事件，為事後分享階段。

(二) SOC：Security Operation Center，資訊安全監控中心：提供連續不間斷的監控服務，於資訊系統生命週期間，提供事前威脅的辨別預防、事中威脅的即時監控，以及事後威脅的分析回顧，確保組織資訊安全。

(三) CERT：Computer Emergency Response Team，電腦緊急應變團隊：對於資安事件提供緊急應變，降低資安事件的系統或財產損害與系統回線時間，並儘速恢復正常營運；同時，建立跨體系整合運作模式，提供通報機制與紅藍軍攻防演練，防範未來類似的資安事件。

(四) CI：Critical Infrastructure，關鍵基礎設施：根據行政院國土安全政策會報定義，係指公有或私有、實體或虛擬的資產、生產系統以及網絡，因遭破壞進而影響政府及社會功能運作，造成人民傷亡或財產損失，引發經濟衰退或社會動盪，導致國家與個人安全、利益和隱私遭受損害者。

(五) CII：Critical Information Infrastructure，國家關鍵資訊基礎設施：資通安全管理法中，關鍵基礎設施所需的資訊網路、調度控制和監控系統等等，涵蓋營運和核心業務的範疇，是關鍵基礎設施不可或缺的元件，應配合對應之國家關鍵基礎設施列為重點管理項目。

二、資安的核心概念是風險管理，請說明資安的三個要素及風險處理之四個對策。（25分）

命題意旨	資訊安全的核心與風險處理。
答題關鍵	屬於資訊安全概要基本題型，資安 C.I.A 基本三大要素；風險處理屬於企業永續經營篇，可參考正課 ISMS 章節風險管控部分，此題拿高分不難。

【擬答】

(一) 資訊安全三要素：

1.機密性：保護資訊資產，獲得授權的人才可以得知資訊內容，保護資訊不被未授權第三方得知。

2.完整性：確保資訊內容的正確與完整，內容未被偽造、竄改與刪除。

3.可用性：確保資訊資產能提供合法授權使用者隨時存取。

(二) 風險處理：

風險處理是組織依據其政策、目標、文化與企業形象所定義能接受的風險等級所採取的應對方法，等級愈低，產生的資訊損失愈高；等級愈高，導入控管成本愈高。

1. 控制與降低：選擇適當的控制方法降低風險等級，如：資訊實體控管、禁止連外網。

2. 避免：避免因使用該項資產而造成的風險，如：不使用與採購國外弱點或是有後門的軟體程式。

3. 轉移：轉嫁可能的風險損失由外部其他單位承受，如：保險、SLA 服務級別。

4.接受：由於導入的成本遠高過於系統風險的損害，接受資訊系統產生的風險，由組織接受。

三、請說明識別（identification）與認證（authentication）之差異。另請舉例說明多因子認證中，所知之事、所持之物、與所具之形之意義，並舉例說明一個雙因子認證之作法。（25分）

命題意旨	本題在考資訊系統身分鑑別的組成與流程。
答題關鍵	此題應說明身份鑑別的分別定義細項，多因子認證是正課中多次強調的重點，講義上舉了不少最新生活科技的應用，班內生對此類題目掌握度相當高。

【擬答】

(一)識別（identification）與認證（authentication）之差異：

1.識別：系統能識別使用者是否合法，如：商品條碼。

2.鑑別：系統能確認其身分是否如其所稱，如：確認密碼是否正確。

(二)所知之事、所持之物與所具之形之意義：

1.所知之事：利用使用者知道的事情進行確認，如：密碼。

2.所持之物：利用使用者所持有的物品進行確認，如：門禁 RFID。

3.所具之形：利用使用者具有的生物特徵進行確認，如：指紋解鎖。

(三)雙因子認證之作法：

ATM 提款，除了需有該銀行核發的金融卡外，提款者須輸入金融卡內儲存的密碼，才可以正確合法地使用各項服務，避免金融卡遺失即被盜用的問題，與被破解、被知悉密碼後可能造成的損失。

四、依據資通安全事件通報及應變辦法之規定，公務機關知悉發生資通安全事件時，最遲應於多久時間內通報？通報內容應包括那七個項目？（25分）

命題意旨	此題在考「資通安全事件通報及應變辦法」，屬於資訊法規題目類型
答題關鍵	此題相當靈活，難度也高，準備資安考試鮮少會去閱讀相關資訊法規章節，第一小題則是 0 或 1 的考法；但是第二題算在範圍內，可以參考資訊安全正課補充講義之「資通安全事件應變」和「資安事件等級」，應該也可以拿到不少分數。

【擬答】

(一)

根據資通安全事件通報及應變辦法第四條：

公務機關知悉資通安全事件後，應於「一小時」內依主管機關指定之方式及對象，進行資通安全事件之通報。

(二)

根據資通安全事件通報及應變辦法第三條：

資通安全事件之通報內容，應包括下列項目：

一、發生機關。

二、發生或知悉時間。

三、狀況之描述。

四、等級之評估。

五、因應事件所採取之措施。

六、外部支援需求評估。

七、其他相關事項。