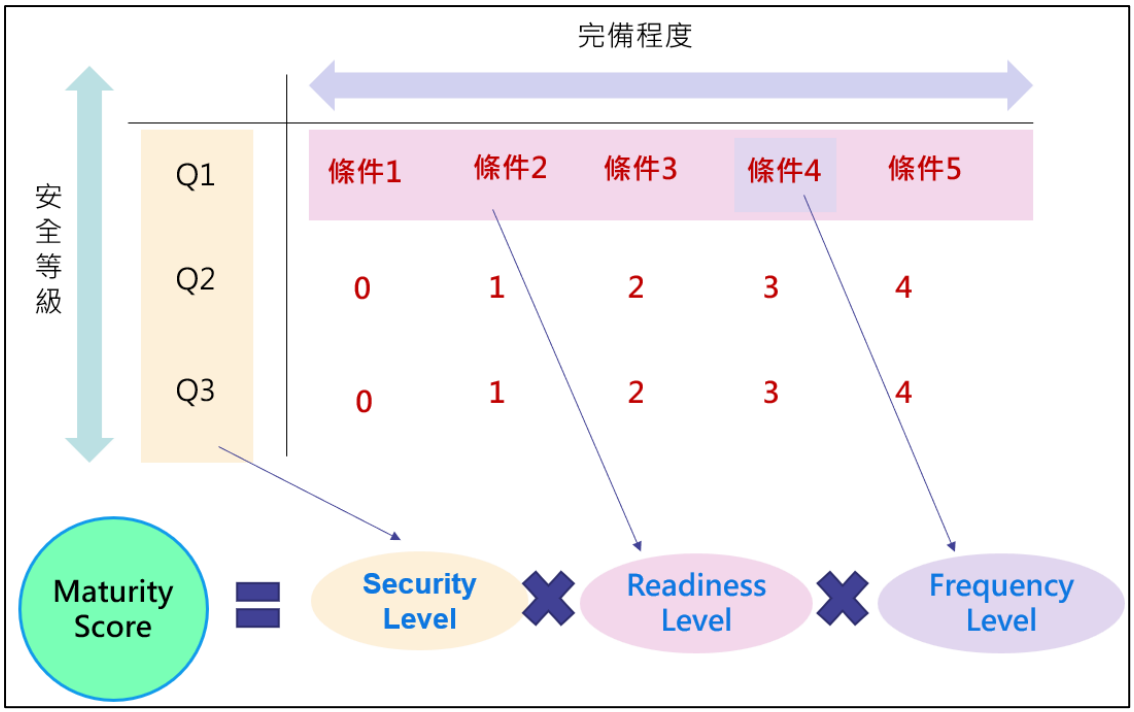
評級系統評分標準



題目配分以及說明：

題號	分類	題目敘述	總分
IT001	防護能力	組織可透過授權帳戶或程式來限制使用者、設備(包含其他資訊系統)存取系統	10
IT002	防護能力	在適用的受管制的資料規則中，提供一致的隱私和安全聲明。	8
IT003	防護能力	限制在外部系統上使用可攜帶式儲存裝置。	8
IT004	防護能力	組織可限制被授權的使用者只能存取他們授權範圍內的程式或資訊系統	10
IT005	防護能力	組織控制內部系統存取可對各種類型帳戶的權限，應採用最小權限原則(分配其業務功能所需的最少權限)	8

IT006	防護能力	組織存取非安全功能時，會使用非特權帳戶或角色	8
IT007	防護能力	限制登入失敗嘗試次數	8
IT008	防護能力	為了防止閒置一段時間的系統資訊洩漏，請使用資訊隱藏並將 session 鎖定	8
IT009	防護能力	在允許進行此類連線之前，請先授權無線存取權限	8
IT010	防護能力	將人員的職責分開，以減少共謀的惡意活動風險	6
IT011	防護能力	防止使用者執行超出權限範圍內的功能，並在審核日誌中捕捉此類的執行記錄	6
IT012	防護能力	在定義的條件後終止（自動）使用者 session	6
IT013	防護能力	使用身份驗證和加密保護無線存取 (wireless access)	6
IT014	防護能力	組識有使用行動設備管理機制，進行設備存取管控	6
IT015	防護能力	控制安全網域與系統連結時的資訊流動	4
IT016	防護能力	定期檢查和更新受管制的資料程式存取的權限	4
IT017	防護能力	識別並減輕與未識別的無線存取點 (wireless access points)連接的網路相關風險。	2
IT018	防護能力	對遠端存取 session 進行監控與控制	8
IT019	防護能力	透過受管理的存取控制點進行路由遠端存取	8
IT020	防護能力	採用加密機制來保護遠端存取 session 的機密性	6

IT021	防護能力	應記錄哪些帳戶和功能是允許被遠端操作與執行的	6
IT022	防護能力	根據組織定義的風險因素，來限制遠端網路存取。例如一天中的時間、存取位置、實體位置、網路連線狀態，以及當前已測量屬性的使用者和角色身份	4
IT023	防護能力	組織可驗證並控制/限制授權的使用者與程式與外部資訊系統的連接和使用	10
IT024	防護能力	組織可控管在公開的資訊平台上發佈的資訊內容	10
IT025	防護能力	組織可根據合法的授權控制，對授權的使用者與程式進行資料存取限制，管制資訊的流程	8
IT026	防護能力	在行動裝置和行動運算平台上請使用加密的受管制資料	6
IT027	識別能力	定義處理受管制的非機密資訊(controlled unclassified information, CUI)的處理過程	6
IT028	識別能力	利用某些特性（例如，韌體等級，作業系統類型）來識別庫存中的元件屬性，以便在發生漏洞時快速識別並找出問題發生點，如此可將修補程式快速部署或進行網路隔離	4
IT029	偵測能力	確保可以追溯單一系統操作的使用者，以便他們對其操作負責	8
IT030	偵測能力	應定期檢查已記錄的事件，並識別可能的安全事件，並且應根據組織需要更新記錄的事件列表	6
IT031	偵測能力	審核資訊紀錄失敗時，應發出警報	6

IT032	偵測能力	組織可確保系統建立並保留稽核記錄，並且稽核記錄內應包含足夠的資訊，以識別和調查非法或未經授權的系統活動	8
IT033	偵測能力	組織可提供可以同步標準時間與內部系統時間的時間同步系統，以生成稽核紀錄的時間戳記	8
IT034	偵測能力	將審核資訊（例如 log）收集到一個或多個集中儲存點	6
IT035	偵測能力	識別未回報的資產稽核紀錄，並確保組織定義的系統有被適當的記錄下來	2
IT036	偵測能力	保護未經授權的存取、修改和刪除審核資訊和審核記錄工具	6
IT037	偵測能力	將稽核記錄功能的管理權限，限縮給特定的特權帳戶	6
IT038	偵測能力	組織可查看稽核記錄	8
IT039	偵測能力	審查相關審核記錄，以調查和通報非法、未經授權、可疑或異常活動的跡象	6
IT040	偵測能力	應過濾並提取有意義且相關的審核紀錄，以建立簡潔有力的分報告，提升檢閱的效率	6
IT041	偵測能力	自動分析審核記錄，並識別關鍵指標（TTP; tools, techniques, procedures），或組織定義的可疑活動並對其採取對應措施	4
IT042	偵測能力	查看審核資訊以了解每台機器的活動，以及大範圍的機器活動	4
IT043	防護能力	組織可確保管理者、系統管理員和組織系統使用者，了解與其操作相關的安全風險，包含系統安全性相關的規範，標準和流程	8

IT044	防護能力	提供人員識別和回報潛在內部威脅指標的安全意識訓練	8
IT045	防護能力	提供人員安全意識訓練課程，將重點放在如何識別和應對社交工程的威脅(social engineering)、進階持續性威脅(advanced persistent threat actors)、安全漏洞以及可疑的行為; 並且至少每年一次或威脅發生重大變化時更新訓練課程內容	4
IT046	防護能力	在安全意識訓練中，應進行與現有威脅情境相似的實際演練，並且提供回饋給參與訓練的人員	4
IT047	防護能力	組織可確保受訓人員接受其所分配的資訊安全相關職責訓練內容	8
IT048	防護能力	組織可在各個系統開發生命週期中，建立和維護組織系統的基本配置和清單（包括硬體，軟體，韌體和文件）	8
IT049	防護能力	組織系統配置應採用最少功能性原則	8
IT050	防護能力	應監控使用者所安裝的軟體	8
IT051	防護能力	組織系統中所使用的資訊技術產品應建立和實施安全配置設定	8
IT052	防護能力	追蹤、查看、核准或不核准等配置變更記錄皆應記錄在組織系統中	8
IT053	防護能力	在實際變更配置前，應分析變更後會帶來的安全性影響	8
IT054	防護能力	系統配置應定義、記錄、核准和實施與組織系統變更相關的實體和邏輯存取限制	6
IT055	防護能力	組織可限制、解除或禁止使用不必要的程式功能、通訊埠(port)、協定(protocols)和服務	6

IT056	防護能力	組織可使用黑名單防止未經授權的軟體執行，或者使用白名單來允許授權軟體執行	6
IT057	防護能力	組織認可的系統，應採用應用程式白名單和應用程式審查保護	4
IT058	防護能力	配置時，應驗證組織所定義的安全關鍵評估或必要軟體的完整性和正確性（例如，信任基礎(roots of trust)、正式驗證(formal verification)或加密簽章(cryptographic signatures)）	2
IT059	防護能力	組織可識別資訊系統使用者和使用者所執行的程式或設備	10
IT060	防護能力	組織可允許存取組織系統前，應驗證帳戶、程式或設備的身份	10
IT061	防護能力	組織可建立新密碼時，應強制規定新密碼需符合一定的複雜度	8
IT062	防護能力	禁止在規定的時間內設定重複的密碼	8
IT063	防護能力	允許使用臨時密碼登錄系統，並立即將此密碼更改為永久密碼	8
IT064	防護能力	所有密碼在儲存和傳遞時，都必須以加密方式進行保護	8
IT065	防護能力	將身份驗證資訊時的反饋資訊模糊化	8
IT066	防護能力	本地端與網路連線時，應使用多因子身份驗證(multifactor authentication)	6
IT067	防護能力	任何帳戶權限在進行網路連線存取時，皆應採用可以對抗重送的身份驗證機制(replay-resistant authentication mechanisms)	6
IT068	防護能力	應防止在規定的時間之外重複使用相同的認證資訊	6

IT069	防護能力	在超過組織規定之閒置時間後，應禁止閒置標識符號(如：員編、email 帳號等)認證資訊繼續使用	6
IT070	回應能力	組織可建立組織系統內事件處理的能力，包括準備、檢測、分析、遏制、修復和回報	8
IT071	回應能力	運用駭客的技術和手法等相關背景知識，規劃事件通報執行作法	4
IT072	回應能力	網路事件發生時，應收集系統上的事件證據，並確保鑑識資料的安全	2
IT073	回應能力	組織可偵測和回報事件	8
IT074	回應能力	組織可分析與分類資安事件，以便於支持事件宣告和提供通報方案	8
IT075	回應能力	組織可根據事先定義好的程序，建立並實施應變措施	8
IT076	回應能力	應追蹤和記錄事件，並向組織內部和外部的指定人員或當局報告事件內容	6
IT077	回應能力	建立和維護有 24/7 安全性監視功能的安全中心	4
IT078	回應能力	需要建立手動的、自動的或是混合模式的即時惡意行為偵測模型	2
IT079	回應能力	建立並維護一個可以在 24 小時內，並且在任何地點進行實體或虛擬調查的網路事件通報團隊	2
IT080	回應能力	組織可對異常事件進行分析，以確定事件發生的根本原因	8
IT081	回應能力	測試組織事件通報的能力	2
IT082	回應能力	應進行演習訓練，以確保技術和流程上的通報反應	2

IT083	防護能力	在組織系統上執行維護管理	8
IT084	防護能力	會對用來進行系統維護的工具、技術、機制和人員進行管制	8
IT085	防護能力	透過外部網路連接時，需要使用多重要素驗證(multifactor authentication)來建立非本地端維護連線，並在非本地端維護完成時終止此類連接。	8
IT086	防護能力	應監督執行維護活動的每個人員	8
IT087	防護能力	確保清除用於非現場維護的設備中存在任何受管制資料。	6
IT088	防護能力	在組織系統使用某個媒體前，須先通過惡意程式的診斷和測試	6
IT089	防護能力	所有媒體（例如 USB、CD、DVD、硬體驅動程式或文件）皆應標記是否含有受管制的資料	6
IT090	防護能力	保護含有受管制的資料，包含：紙本與數位版本的受管制資料。	8
IT091	防護能力	將受管制資訊的存取權限，限制為僅允許授權用戶	8
IT092	防護能力	追蹤並管制可移動媒體的使用，並確保其正確地使用和拋棄	8
IT093	防護能力	若無法識別擁有者，則禁止使用可攜式儲存設備	6
IT094	防護能力	在進行報廢或重複使用之前，得先清除含有的受管制資料	10
IT095	防護能力	管制存取含有受管制資料的媒體，並且在受控區域外傳輸的過程中應建立有效機制，以防止對受管制資料的未授權存取	6

IT096	防護能力	使用加密機制以保護在傳輸過程中儲存在數位媒體上的受管制資料的機密性，除非另外有其他物理保護措施的保護。	6
IT097	防護能力	在授權存取包含受管制資料的組織系統之前，先進行人員篩選。	8
IT098	防護能力	確保在人員操作期間和操作之後（例如：離職和轉職），皆應保護含有受管制資料的系統。	8
IT099	防護能力	限制授權人員對組織資訊系統、設備和相應操作環境的實體存取。	10
IT100	防護能力	護送訪客和監控訪客的活動	10
IT101	防護能力	維護實體存取的審核記錄	10
IT102	防護能力	控管實體存取設備	10
IT103	防護能力	保護和監控實體設施，並確保設施內部的基礎結構（例如電源和網路電纜）受到保護，以使訪客和員工無法任意存取它	8
IT104	防護能力	在備用工作現場(員工家裡、第二辦公室)需執行受管制資料的保護措施。	6
IT105	復原能力	組織有定期執行資料備份及資料回復驗證程序	8
IT106	復原能力	組織有針對儲存主機進行資訊備份保護，確保資料機密性	8
IT107	復原能力	定期執行組織定義的完整、全面和靈活資料備份。	6
IT108	復原能力	確保資訊處理設施滿足組織定義的資訊安全連續性，備援性和可用性要求。	2
IT109	識別能力	組織可定期對組織營運（包含：任務，職能，形像或聲譽），組織資產和個人進行風險評估。特別是涉及企業資料處理、儲	8

		存或傳輸，以及組織營運的系統、資產與個人	
IT110	識別能力	組織可定期掃描組織系統和應用程式中的漏洞，並且也會在發現影響這些系統和應用程式的新漏洞時進行掃描	8
IT111	識別能力	定期執行風險評估，以根據定義的風險類別、風險來源和風險衡量標準確定風險，以及優先等級。	6
IT112	識別能力	分類並定期更新威脅剖繪(Profiles)和駭客的戰術、技術、流程(TTP)。	4
IT113	識別能力	將威脅情資整合到整個系統開發生命週期(包含：定義系統安全要求、開發系統和安全架構、選擇安全解決方案、監控和修補工作)的風險管理流程之中，並為系統提供資訊。	4
IT114	識別能力	對組織的 Internet 或其他網路連線的跨網閘道器上執行掃描，以發現可存取的「未授權」網路端口。	4
IT115	識別能力	組織可根據風險評估補救漏洞	8
IT116	識別能力	制定並實施風險緩解計劃。	6
IT117	識別能力	分開管理不受供應商支持的產品（例如，壽命終止），並根據需要進行限制以降低風險。	6
IT118	識別能力	針對非白名單的軟體採用例外處理，該處理方法還包含緩解措施。	2
IT119	識別能力	至少每年一次分析資安解決方案的有效性，並且基於當前和累積的威脅情資來解決對系統和組織的預期風險。	2

IT120	識別能力	根據企業需要制定和更新供應鏈風險管理計劃，以管理與 IT 供應鏈相關的資安風險。	4
IT121	識別能力	組織可制定、記錄並定期更新系統安全計劃，這些計劃描述系統邊界、系統運行環境、安全要求的實現方式，以及與其他系統的關係，或與其他系統的連接	8
IT122	識別能力	建立、維護和利用資安策略和藍圖來改善組織的資通安全。	4
IT123	識別能力	組織可定期評估組織系統中的安全控制，以確定這些控制在其應用中是否有效。(註：安全控制如：防火牆、網段隔離、防毒…等)	8
IT124	識別能力	組織可制定並實施行動計劃，以糾正資安缺陷，並減少或消除組織系統中漏洞	8
IT125	識別能力	持續監控安全控制措施，以確保控制措施的持續有效性。	2
IT126	識別能力	定期進行滲透測試，並利用自動掃描工具和專人測試。	4
IT127	識別能力	定期對組織資產進行紅隊演練，以驗證防禦能力。	4
IT128	識別能力	針對內部開發、內部使用的企業軟體進行資安評估，並在組織上將其定義為風險領域。	6
IT129	偵測能力	組織會接收，並回應網路威脅情資(如：駭客情資共享論壇，或特定威脅情資來源等)，並與利益相關人進行溝通。	6
IT130	偵測能力	建立並維護網路威脅獵捕功能，以搜尋組織系統中的威脅入侵指標(indicators of compromise)，並偵測、追蹤和破壞那些可逃避現有控制措施的威脅。	4

IT131	偵測能力	設計網路和系統安全功能，以利用、整合和共享威脅入侵指標(indicators of compromise)。	4
IT132	防護能力	禁止協作式設備(如：電腦鏡頭、麥克風、視訊會議系統等)的遠端控制功能啟用，並向當前在該設備上的使用者提供設備使用的指示。	8
IT133	防護能力	使用加密的連線(sessions)來管理網路設備。	8
IT134	防護能力	當要確保公司資料的機密性時，會使用FIPS驗證過的加密技術。	6
IT135	防護能力	採用資安架構設計、軟體安全開發技術和系統安全工程原理，來促進組織系統資安的有效性。	6
IT136	防護能力	將使用者功能與系統管理功能分開。	6
IT137	防護能力	防止透過共享系統資源進行未經授權和意料之外的資訊傳輸。	6
IT138	防護能力	預設情況下拒絕網路通訊流量，並在例外情況下允許網路通訊流量（即：預設全部拒絕、例外情況允許）。	6
IT139	防護能力	防止遠端設備同時與組織系統建立非遠端連接，以及透過其他連接與外部網路中的資源進行通訊（即：分割通道方法）。	6
IT140	防護能力	實施加密機制，以防止在傳輸過程中未經授權洩露公司資料，除非另有其他實體保護措施保護。	6
IT141	防護能力	在連線(sessions)結束時或在公司定義的不活動時間之後，須終止與通訊連線(sessions)關聯的網路連接。	6
IT142	防護能力	建立和管理加密金鑰，以用於組織系統中的加密部署。	6

IT143	防護能力	控制和監控行動碼(Mobile code)的使用。	6
IT144	防護能力	控制和監控網路語音（VoIP）技術的使用。	6
IT145	防護能力	保護通訊連線(communications sessions)的真實性。	6
IT146	防護能力	保護靜態資料的機密性。	6
IT147	防護能力	在系統和資安架構中，或在組織認為適當的地方，採用實體和虛擬隔離技術。	4
IT148	防護能力	隔離管理組織定義的高價值關鍵網路基礎架構設備和伺服器系統。	4
IT149	防護能力	配置監視系統，以記錄通過組織的Internet 網路邊界和組織定義的其他網路邊界的網路封包。	2
IT150	防護能力	強制執行 Port 網路埠和網路協議合規。	2
IT151	防護能力	組織可在資訊系統的外部邊界和關鍵內部邊界監視、控制和保護組織通訊（即組織資訊系統發送或接收的資訊）	10
IT152	防護能力	組織可部署子網路以供公共存取系統元件，且該子網路採用實體或邏輯上的分割，並滿足與內部網路分離	10
IT153	防護能力	實施域名系統（DNS）過濾服務。	6
IT154	防護能力	實施一項政策以限制資料被外部所擁有、被公開存取的網站（例如：論壇、LinkedIn、Facebook、Twitter）上發布。	6
IT155	防護能力	利用威脅情資主動阻止 DNS 請求轉址到惡意網域。	4

IT156	防護能力	採用機制來分析跨 Internet 網路邊界，或組織定義的其他邊界的可執行程式碼和腳本（例如：沙箱）。	4
IT157	防護能力	利用 URL 分類服務，並利用技術來對未經組織批准的網站實施 URL 過濾。	4
IT158	防護能力	除市售解決方案外，還採用組織定義和量身訂做的邊界保護。	2
IT159	防護能力	組織可即時辨識、報告和糾正資訊和資訊系統漏洞	10
IT160	防護能力	持續監視組織系統的外部情資，包含：安全告警和建議等，並採取相應措施。	8
IT161	防護能力	使用與受保護資訊和系統相關的威脅指標資訊，以及從外部組織獲得的有效緩解措施來為入侵偵測和威脅狩獵提供資訊。	4
IT162	防護能力	可在組織資訊系統內的適當位置，提供針對惡意程式保護	10
IT163	防護能力	當有新版本發佈時，更新惡意程式保護機制	10
IT164	防護能力	在下載、打開或執行檔案時，對資訊系統進行定期掃描，並對來自外部的檔案進行即時掃描	10
IT165	防護能力	分析系統行為來偵測和減輕，潛在惡意行為的指令和腳本於正常系統上執行。	2
IT166	防護能力	監視組織系統，包括入站和出站通訊流量，以偵測攻擊和潛在攻擊的指令。	8
IT167	防護能力	辨識未經授權使用組織系統的情況。	8
IT168	防護能力	在資訊系統存取入口和出口點採用垃圾郵件保護機制。	6
IT169	防護能力	持續監控個人和系統元件的異常或可疑行為。	2

IT170	防護能力	實施電子郵件偽造保護。	6
IT171	防護能力	利用沙箱來偵測或阻止潛在的惡意電子郵件。	6