金融業導入資安國際標準的發展與探討－上

陳瑩瑄

第壹章　緒論

第一節、研究背景與動機

隨著資訊科技不斷創新與演進，為能加速數位轉型，金融機構紛紛運用新興科技來發展數位金融業務，伴隨而來的是層出不窮的駭客攻擊，於2024年世界經濟論壇的《2024年全球風險報告》，於報告開頭即提醒全球領導人，世界局勢正受氣候變遷與地緣政治衝突兩大危機嚴重影響，全球的前景仍充滿著不確定性，全球面臨地緣、人口與科技以及氣候變遷等四結構的系統性轉變。

依報告內容顯示，對影響嚴重程度評估之未來兩年的十大風險，科技面向佔據第一名（假訊息與錯誤訊息）及第四名（網路犯罪與安全危機），未來十年的十大風險中，科技面向佔據第五名（假訊息與錯誤訊息）、第六名（AI技術的不良反應）及第八名（網路犯罪與安全危機），因此科技發展所帶來的風險，成為企業的重要議題之一。

臺灣行政院國家資通安全會報對於資訊安全防範及網路威脅等議題，依序不同階段發展的推動目標，分別提出「國家資通安全發展方案（106年至109年）」及「國家資通安全發展方案（110年至113年）」，作為我國推動資安防護策略與計畫之依循目標。加上金管會於年2020年提出之「金融資安行動方案」，以「強化資安監理」、「深化資安治理」、「精實金融韌性」及「發揮資安聯防」四大推動主軸，其中，「深化資安治理」鼓勵金融機構導入國際資安管理標準，「精實金融韌性」鼓勵金融機構導入國際營運持續管理標準，期許金融機構可依循主管機關的推動政策，並導入資安國際標準，建構完善的資訊安全防護架構及管理制度，強化本國金融業的資安量能。

因此，本行於2007年開始規劃導入國際標準資訊安全管理系統（ISO 27001），於2008年取得驗證，依循著主管機關的資安推展動向，以及國際標準發展歷程，為強化本行資訊安全與營運持續管理，2017年導入國際標準營運持續管理系統，於2018年取得驗證，透過持續滾動調整相關資安規範、強化資安防護設備，及借助第三方驗證機構找出執行盲點驗證有效性。

第二節、研究目的

本研究以「金融業導入資安國際標準的發展與探討」為研究目標，透過探討近年來主管機關推動金融業資訊安全的趨勢、近期發布之資安法規動向、國際標準組織及其發布與資安國際標準條款，以及公股銀行資安國際標準的導入與驗證情況後，並以本行導入及驗證國際標準資訊安全管理系統及營運持續管理系統為範例，建構出金融業導入資安國際標準的方式，期望可提供金融業透過本研究作為導入資安國際標準，甚至是未來推動導入雲端安全或人工智慧國際標準之參考依據，並達到主管機關持續精進與強化資安管理制度與落實新興科技資安風險控管之要求。

第貳章　技術文獻

第一節、國內發展動向

壹、主管機關動向

在全球數位金融科技不斷發展與推動下，區塊鏈、物聯網（Internet of Things，IoT）、雲端運用、人工智慧科技等新興科技層出不窮，帶來的資安風險越來越多元變化，駭客技術手法不斷創新，考量資通訊服務應用廣泛，且應用層面包含社會、經濟、環境等，因此，為能因應新型態資安攻擊與威脅，行政院國家資通安全會報依序不同階段發展的推動目標，分別提出「國家資通安全發展方案（106年至109年）」及「國家資通安全發展方案（110年至113年）」，作為我國推動資安防護策略與計畫之依循目標。

貳、主管機關近期發布法規

配合行政院推動國家資通安全發展方案，金管會對於金融機構的資安推動也陸續推展出許多法規，配合新興科技的運用，於2020年4月17日發布新版「金融機構運用新興科技作業規範」，強化金融機構運用新興科技的風險與控管，並鑒於資安威脅日益嚴峻與國際金融資安監理趨勢，2020年8月6日發布「金融資安行動方案」，且因應物聯網設備廣泛使用，於2021年4月30日發布新版「金融機構使用物聯網設備安全控管規範」，強化人員對於物聯網議題的認知意識要求。

於「金融資安行動方案」推動兩年期間，歷經新冠疫情驅動數位轉型、資安情勢加劇、重大災害及地緣政治等風險，提升金融資安韌性的重要性，於2022年12月27日發布「金融資安行動方案2.0」，2023年2月1日發布「金融機構資通安全防護基準」及2023年3月29日發布新版「金融機構資通系統與服務供應鏈風險管理規範」，修訂資通系統的安全控管及對供應鏈風險管理要求。

此外，中華民國銀行商業同業公會全國聯合會（下稱銀行公會）分別於2024年5月6日發布「金融機構運用人工智慧技術作業規範」、5月17日檢送「金融機構國際資安管理標準驗證範圍」建議及5月30日發布「金融機構資訊作業韌性規範」，金管會更於2024年6月20日發布「金融業運用人工智慧（AI）指引」，此四份規範發布主要係配合「金融資安行動方案」及近期新興科技發展運用推出，主管機關透過發布與國際標準驗證有關之規範及驗證建議之法令法規，要求企業建立資安管理基礎，持續不斷加速法規更新，強化控管措施之要求，展現主管機關對於資安控管與韌性作業的重視，並因應人工智慧科技（AI）科技運用日漸廣泛，且部分銀行已將ChatGPT導入相關作業流程，為強化金融機構運用人工智慧（AI）技術辦理銀行業務的客戶資料保護及銀行風險控管，也接續發布人工智慧相關的規範，以供金融機構遵循。

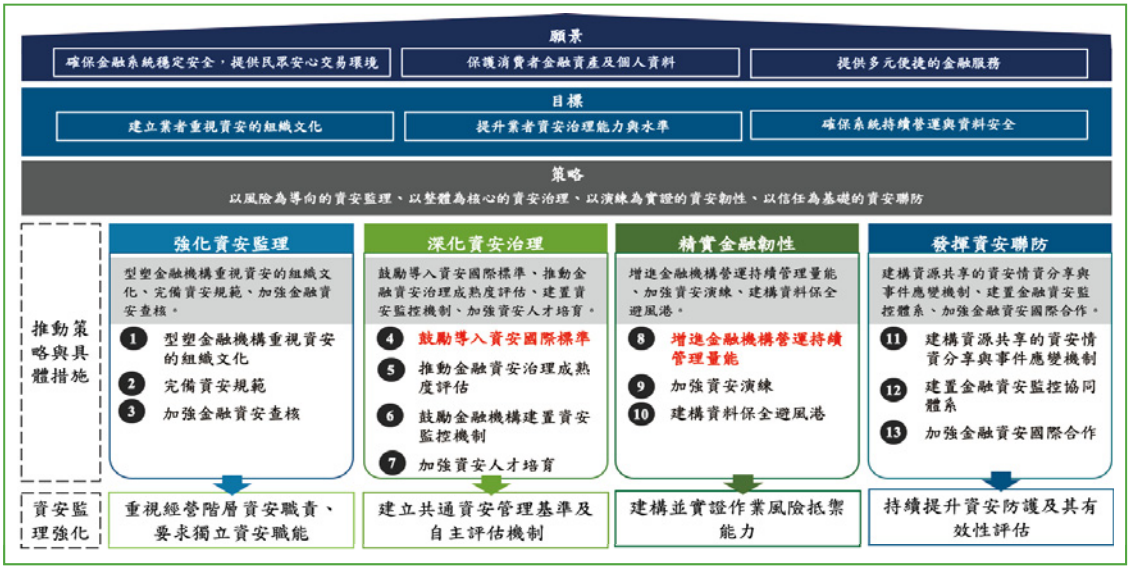
為探討金融機構導入資安國際標準與驗證，將以金管會「金融資安行動方案」及銀行公會檢送「金融機構國際資安管理標準驗證範圍」建議與「金融機構資訊作業韌性規範」進行說明。

圖貳-1法規發布歷程

資料來源：本研究整理

「金融資安行動方案」推動內容有四大執行措施，分別為「強化資安監理」、「深化資安治理」、「精實金融韌性」及「發揮資安聯防」，其中「深化資安治理」提及鼓勵金融機構導入國際資安管理標準，「精實金融韌性」增進金融機構營運持續管理量能涵蓋鼓勵金融機構導入國際營運持續管理標準之建議，「金融資安行動方案2.0」推動措施可詳圖貳-2。

圖貳-2金管會金融資安行動方案



資料來源：金管會、勤業眾信

主管機關鼓勵金融機構導入國際標準資訊安全管理標準主要目的係期望金融機構依循國際標準組織所訂定之資訊安全管理系統的條款要求，並透過公正第三方驗證資訊安全管理的有效性，完備資訊安全管理制度。因為導入國際標準資訊安全管理系統過程中，金融機構會重新檢視既有的資安管理制度規範與資安控管機制是否符合國際標準條款，且公正第三方驗證機構進行驗證時，如有提出執行面上的盲點或執行有效性，也可促進金融機構持續改善，建立良性改善循環。在此良善循環模式的架構下，依據金管會統計結果，截至2022年第三季，已有32家銀行、17家證券商及38家保險公司取得資訊安全管理標準驗證。

主管機關鼓勵金融機構導入營運持續管理標準的精神與上述的導入資訊安全管理標準其實相近，也是希望金融機構可依循國際標準組織所訂定之營運持續管理系統的條款要求，並透過公正第三方驗證營運持續管理的有效性，向利害關係人溝通其面臨衝擊之準備。同樣在導入國際標準營運持續管理系統過程中，重新檢視營運持續管理規範與程序、營運中斷的復原機制、資料回存測試及異地備援環境的資源充足性等，增進金融機構的營運持續能力。故依據金管會統計結果，截至2022年第三季，已有10家銀行、3家證券商及7家保險公司取得營運持續管理標準驗證。

表貳-1截至2022年第三季金融機構通過驗證家數

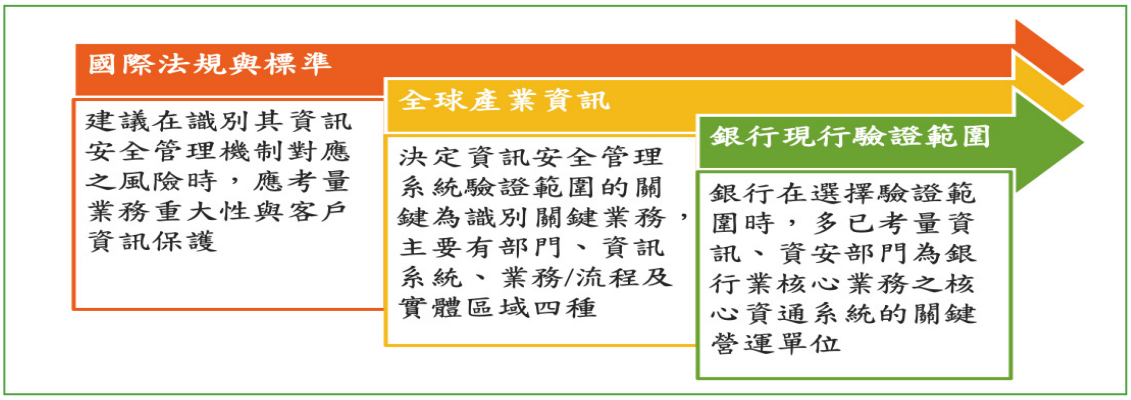
國際標準 \ 行業別	銀行	證券商	保險公司
國際資訊安全管理標準驗證	32	17	38
國際營運持續管理標準驗證	10	3	7

資料來源：金融資安行動方案

銀行公會於2024年5月17日檢送「金融機構國際資安管理標準驗證範圍」建議，主要依據金管會2024年5月3日金管銀國字第1130200953號函示原則同意辦理。緣由係金管會於「金融資安行動方案2.0」金融資安精進方向之「擴大導入國際資安管理標準及建置資安監控機制」中，為確保金融機構導入國際資安標準且有效運作，請銀行公會依據業別特性訂定「金融機構國際資安管理標準驗證範圍」供銀行同業參考，而驗證範圍如資訊基礎設施、全部核心資通系統、核心業務流程、網路金融服務及相關人員資產等構面。

因此，銀行公會透過研究國際相關法規、蒐集全球產業資訊與調查銀行業驗證範圍現況，作為研擬「金融機構國際資安管理標準驗證範圍」基礎，於研究國際相關法規要求，歸納業務重大性與客戶資訊保護為資安風險因應的兩大考量重點；於蒐集全球產業資訊，歸納出部門、資訊系統、業務/流程及實體區域為常見驗證範圍；於調查銀行業驗證範圍，歸納出銀行業多已考量資訊、資安部門為銀行業核心業務之核心資通系統的關鍵營運單位。

圖貳-3銀行公會研究調查方法



資料來源：銀行公會

綜合上述調查研究結果，銀行公會建議以「部門」別或「業務/流程」別的方式選擇驗證範圍，並期許銀行業者於建議公告實施後，針對未符合或為優於銀行公會建議之驗證範圍者，於公告實施日後兩年內完成擴大範圍之驗證。其中「部門」別或「業務/流程」別的方式說明如下：

一、驗證範圍選擇「部門」：至少應包含全資訊部門及資安部門，如果有非資訊部門亦有專屬的資訊單位負責資訊系統的開發、維運等作業，則應將該部門與重要業務資訊系統納入驗證範圍中。

二、驗證範圍選擇「業務/流程」：以銀行業的核心業務流程為優先。

三、驗證範圍選擇「部門」及「業務/流程」：兩種方式組合成驗證範圍者，應同時滿足兩種方式之要求。

銀行公會所述之非資訊部門如數位銀行、數位金融、信用卡、人資等部門，而其管理、操作之資訊系統符合無涉及個人資料處理，且無對行外提供服務，且屬終端使用計算應用，並經銀行評估無重大資安風險者，可不納入驗證範圍中。

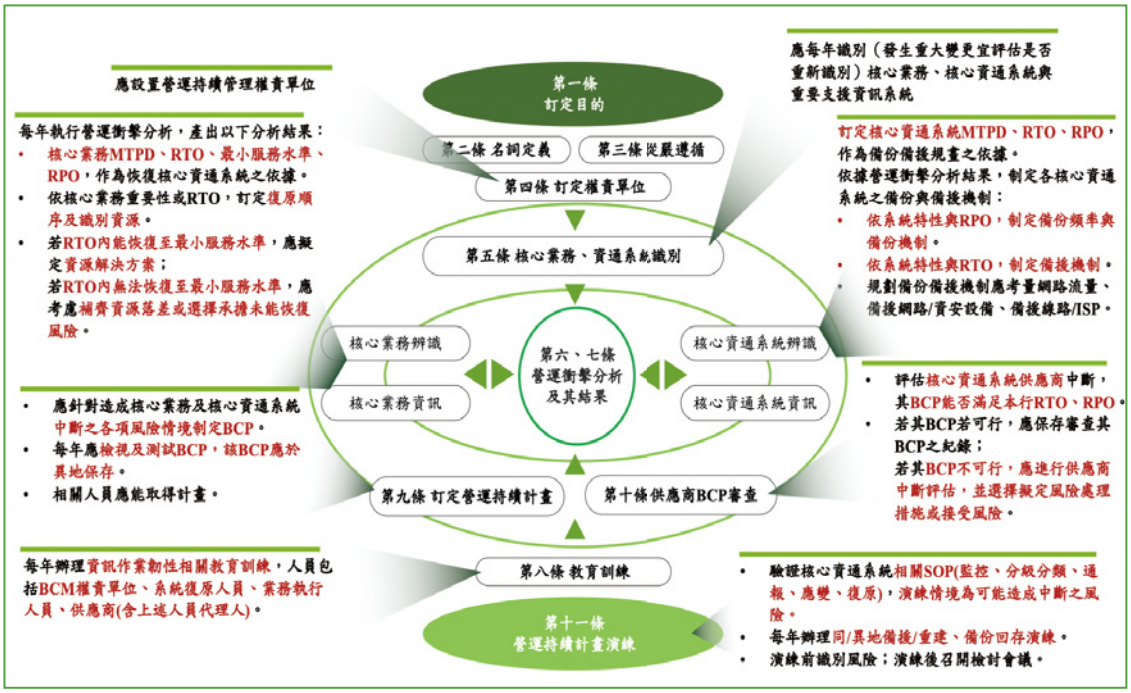
表貳-2銀行公會建議驗證範圍

建議驗證範圍	全資訊部門及資安部門	核心業務流程
說明	・以部門別的方式框列驗證範圍 ・資訊及資安部門通常負責全行所有資通系統的設計、開發、維運、網管、系統與資安管理等作業	・以業務別的方式框列驗證圍 ・維運銀行核心業務（如：存款、放款、匯款、外匯、財富管理、信用卡、信託等業務）相關部門的活動
保護標的	所有系統（包含核心資通系統）的資訊資產	核心業務流程所使用資通系統的資訊資產（包含核心資通系統與第一～三類系統）
特點	範圍界定明確	範圍涵蓋業務部門及資訊部門，可從流程的端點到端點（End to End）的方式檢視資安控管的設計
其他考量	範圍外支援性作業（如：人資、總務、法務）需額外討論其參與方式	・若流程間的作業複雜，恐有切割範圍不易之疑慮 ・共用型系統、資料、資通設備與人員需考量如何納入範圍

資料來源：銀行公會

此外，在資安驗證範圍建議的發布後，銀行公會接續於2024年5月30日發布「金融機構資訊作業韌性規範」，主要依據金管會2024年3月14日金管銀國字第1120236901號函辦理，此規範發布主因來自於金管會「金融資安行動方案」精實金融韌性，希望鼓勵金融機構參考國際營運持續管理標準，作為各金融機構提升作業效率與相關資訊作業韌性管控措施之依循，由此可見，主管機關期望金融機構可藉由導入國際標準，甚至是取得驗證之方式，強化資訊安全與營運持續的管理量能。

圖貳-4金融機構資訊作業韌性規範摘要說明



資料來源：勤業眾信

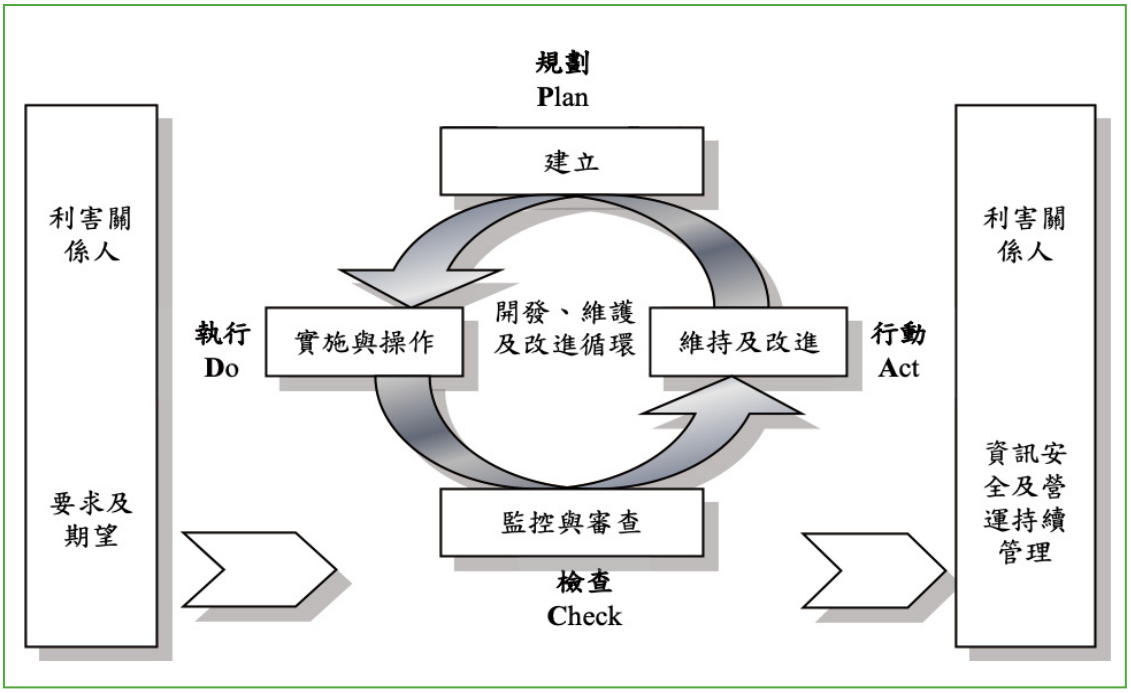
第二節、國際標準介紹

壹、國際標準組織與導入模式

國際標準組織（International Organization for Standardization，ISO）成立於1947年，總部位於瑞士日內瓦，目前已有164個成員國家，該組織致力於制定和推廣各種通用的國際標準，這些標準為各產業提供一套共同的基準，且可透過公正第三方進行驗證，因此，採行國際標準組織制定之標準，有助於企業提高競爭力、提升消費者信心，以及強化產品與服務的品質和安全。

導入國際標準時，通常採用“Plan-Do-Check-Act”（PDCA）之循環運作模式，來建立資訊安全管理系統及營運持續管理系統運作機制，並維繫其有效運作與持續改進。

圖貳-5 PDCA循環運作模式



資料來源：英國標準協會

PDCA於循環運作模式說明如下：

一、規劃（Plan）－建立：規劃並制定完善的資訊安全管理系統與營運持續管理系統，包含資訊安全與營運持續的政策、目標、風險評鑑程序及相關控制措施程序。

二、執行（Do）－實施與操作：將資訊安全管理系統與營運持續管理系統內容加以實施與執行。

三、檢查（Check）－監控與審查：持續追蹤資訊安全管理系統與營運持續管理系統實施情形，透過適當的量測方式評估績效，彙整執行結果並討論。

四、行動（Act）－維持及改進：依據資訊安全管理系統與營運持續管理系統內部稽核與管理審查結果進行相應的矯正處置，並持續改進。

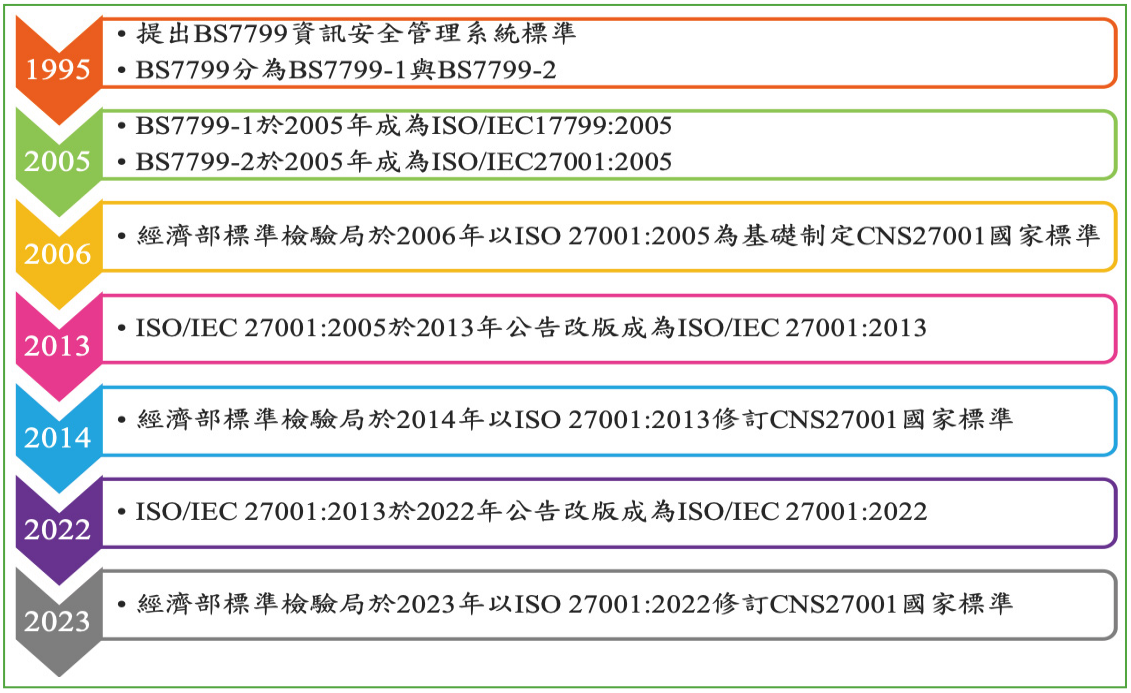
貳、資訊安全管理系統

目前業界用常採用的資安國際標準，主要為資訊安全管理系統（Information security management systems，ISMS），此標準為任何規模、各行各業的公司提供建立、實施、維護和持續改善資訊安全管理系統的指引。

ISO 27001中有許多內容是源自英國標準協會（The British Standards Institution，BSI）所制定之BS 7799，BS7799分為BS7799-1與BS7799-2，於2005年BS7799-1成為ISO/IEC17799：2005，BS7799-2內容主要為資訊安全相關規範、風險管控及使用指引，故2005年11月被國際標準組織修改為ISO/IEC27001：2005，且隨著科技創新運用，資安威脅樣態增加，分別於2013年及2022年進行標準條文更版，目前最新的版本為ISO 27001：2022。

我國經濟部標準檢驗局亦於2006年以ISO 27001：2005為基礎制定CNS 27001國家標準，配合國際標準組織2013年與2022年改版，經濟部標準檢驗局也同步於2014年及2023年修訂CNS 27001國家標準。

圖貳-6 ISO 27001與CNS27001國家標準發展歷程演進



資料來源：曹昱仁，2017、蔡伶宜，2018、英國標準協會、本研究整理

ISO 27001整份標準可拆分兩大部分，一部份為提供建立資訊安全管理系統的條款本文1至本文10，以及附錄A的資訊安全控制措施，因本文1至本文3為適用範圍、引用標準、用語及定義，依循PDCA的循環架構對應標準本文，摘要說明如下：

一、規劃（Plan）：對應本文4至本文7

（一）4組織全景：

1. 4.1瞭解組織及其全景，此項要求目的是組織應決定與目的有關且影響達成資訊安全管理系統預期成果能力之外部及內部議題。
2. 4.2瞭解關注方之需要及期望，此項要求目的是組織應決定與資訊安全管理系統有關的關注方、關注方相關要求事項，及哪些事項需透過資訊安全管理系統因應。
3. 4.3決定資訊安全管理系統之範圍，此項要求目的是組織應決定資訊安全管理系統之邊界及適用性，以建立範圍，且此範圍應以文件化資訊提供。
4. 4.4資訊安全管理系統，此項要求目的是組織應依ISO 27001國際標準要求事項，建立、實作、維持及持續改善資訊安全管理系統，且含所有過程與互動。

（二）5領導作為：

1. 5.1領導及承諾，此項要求目的是最高管理階層應依建立資訊安全政策、資訊安全目標、所需資源、人力等事項，展現對資訊安全管理系統之領導及承諾。
2. 5.2政策，此項要求目的是最高管理階層應建立資訊安全政策。
3. 5.3組織角色、責任及權限，此項要求目的是最高管理階層應確保資訊安全相關角色之責任及權限已於組織內指派並傳達。

（三）6規劃：

1. 6.1因應風險及機會之行動

（1）6.1.1一般要求規劃，此項要求目的是當規劃資訊安全管理系統時，組織應考量4.1所提及之議題及4.2所提及之要求事項，並決定需因應之風險及機會。

（2）6.1.2資訊安全風險評鑑，此項要求目的是組織應定義及應用資訊安全風險評鑑過程於下列事項：

a. 建立與維持風險接受及執行資訊安全風險評鑑之準則。

b.確保重複之資訊安全風險評鑑產生一致、有效及可比較的結果。

c.識別、分析及評估資訊安全風險。

（3）6.1.3資訊安全風險處理，此項要求目的是組織應定義並應用資訊安全風險處理過程，應考量風險評鑑結果，選擇適當之處理措施。

2. 6.2資訊安全目標及其達成之規劃，此項要求目的是組織應於各相關部門及層級建立資訊安全目標。
3. 6.3變更之規劃，此項要求目的是當組織決定需對資訊安全管理系統變更時，應以規劃之方式執行變更。

（四）7支援：

1. 7.1資源，此項要求目的是組織應決定並提供建立、實作、維持及持續改善資訊安全管理系統所需之資源。
2. 7.2能力，此項要求目的是組織應採取相應措施，包含：

（1）決定於組織控制下執行工作，影響其資訊安全績效人員之必要能力。

（2）確保人員於適當教育、訓練或經驗之基礎上能勝任。

（3）採取對現有員工提供訓練、指導或重新指派，或僱用或約聘勝任人員取得必要能力，並評估所採取行動之有效性。

（4）保存適切之文件化資訊，作為勝任之證據。

3. 7.3認知，此項要求目的是於組織控管下，執行工作之人員應有資訊安全相關認知。
4. 7.4溝通或傳達，此項要求目的是組織應建立資訊安全管理系統之內部及外部溝通或傳達的事項、時間、對象及方式。
5. 7.5文件化資訊，此項要求目的是組織應建立資訊安全管理系統相關要求有文件化，以確保需要時可用且適用。

二、執行（Do）：對應本文8

（一）8運作：

1. 8.1運作之規劃及控制，此項要求目的是組織應規劃、實作及控制符合要求事項所需之過程，並實作本文6所決定的所有行動。
2. 8.2資訊安全風險評鑑，此項要求目的是組織應依規劃之期間，或當提議或發生重大變更時，考量6.1.2（a）所建立之準則，執行資訊安全風險評鑑，且保存執行資訊安全風險評鑑相關文件。
3. 8.3資訊安全風險處理，此項要求目的是組織應實作資訊安全風險處理計畫，並保存資訊安全風險處理結果相關文件。

三、檢查（Check）：對應本文9

（一）9績效評估：

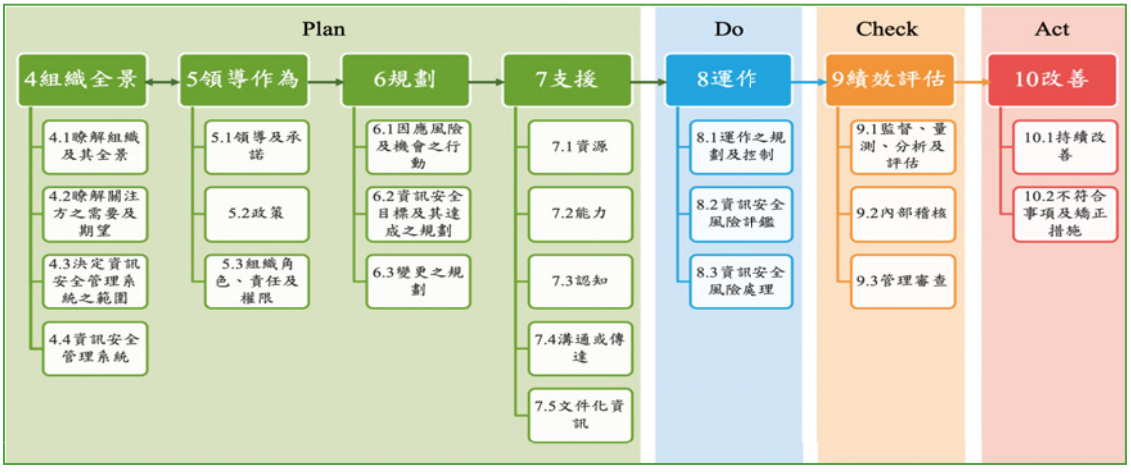
1. 9.1監督、量測、分析及評估，此項要求目的是組織應建立監督、量測、分析及評估的事項、時間、人員及方法，並確認其有效性。
2. 9.2內部稽核，此項要求目的是組織應規劃、建立、實作及維持稽核計畫，並依規劃之期間執行內部稽核。
3. 9.3管理審查，此項要求目的是最高管理階層應於規劃的期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性，並對管理審查討論事項及會議結果留存相關紀錄。

四、行動（Act）：對應本文10

（一）10改善：

1. 10.1持續改善，此項要求目的是組織應持續改善資訊安全管理系統之合宜性、適切性及有效性。
2. 10.2不符合事項及矯正措施，此項要求目的是組織如有不符合事項發生時，應對不符合事項採取適當處理措施，以控制並矯正之。

圖貳-7 ISO/IEC 27001：2022本文與PDCA對應



資料來源：英國標準協會，國際標準條文ISO 27001

於附錄A的資訊安全控制措施由組織、人員、實體及技術四大控制措施組成，組織控制措施共37項控制要求、人員控制措施共8項控制要求、實體控制措施共14項控制要求、技術控制措施共34項控制要求。

表貳-3附錄A的資訊安全控制措施

5	組織控制措施	5.31	確定法律、法規、監管和合約要求事項
5.1	資訊安全政策	5.32	智慧財產權
5.2	資訊安全之角色及責任	5.33	記錄之保護
5.3	職務區隔	5.34	PII 的隱私和保護
5.4	管理階層責任	5.35	資訊安全的獨立審查
5.5	與權責機關之聯繫	5.36	資訊安全政策、規則及標準之遵循性
5.6	與特殊利害關係團體之聯繫	5.37	文件化之運作程序
5.7	威脅情資	6	人員控制措施
5.8	專案管理中之資訊安全	6.1	篩選
5.9	資訊和其他相關資產的清單	6.2	聘用條款和條件
5.10	可接受使用的資訊和其他相關資產	6.3	資訊安全認知及教育訓練
5.11	資產之歸還	6.4	獎懲過程
5.12	資訊之分類分級	6.5	聘用終止或變更後的責任
5.13	資訊之標示	6.6	機密性或保密協議
5.14	資訊傳輸	6.7	遠距工作
5.15	存取控制	6.8	資訊安全事件通報
5.16	身分管理	7	實體控制措施
5.17	鑑別資訊	7.1	實體安全邊界
5.18	存取權限	7.2	實體進入控制
5.19	供應商關係中的資訊安全	7.3	保護辦公室、房間和設施
5.20	通過供應商協議解決資訊安全問題	7.4	實體安全監控
5.21	管理 ICT 供應鏈中的資訊安全	7.5	防範實體和環境威脅
5.22	供應商服務的監控、審查和變更管理	7.6	在安全區域工作
5.23	使用雲端服務的資訊安全	7.7	桌面淨空與螢幕淨空
5.24	資訊安全事件管理職責及準備	7.8	設備安置與保護
5.25	資訊安全事件評估與決策	7.9	場外資產之安全
5.26	對資訊安全事故之回應	7.10	儲存媒體
5.27	從資訊安全事件中學習	7.11	支持之公用服務事業
5.28	證據之蒐集	7.12	佈纜安全
5.29	中斷期間的資訊安全	7.13	設備維護
5.30	業務持續之 ICT 備妥性	7.14	設備汰除或再利用之安全

8	技術控制措施	8.18	具特殊權限公用程式之使用
8.1	使用者端點設備	8.19	運作中系統之軟體安裝
8.2	特權存取權限	8.20	網路安全
8.3	資訊存取限制	8.21	網路服務之安全
8.4	對原始碼之存取	8.22	網路區隔
8.5	安全鑑別	8.23	網頁過濾
8.6	容量管理	8.24	密碼技術的使用
8.7	防範惡意軟體	8.25	安全開發生命週期
8.8	技術脆弱性管理	8.26	應用系統安全要求事項
8.9	組態管理	8.27	安全系統架構和工程原則
8.10	資訊刪除	8.28	安全程式設計
8.11	資料遮蔽	8.29	開發和驗收中的安全測試
8.12	預防資料外洩	8.30	委外開發
8.13	資訊備份	8.31	開發、測試和運作環境的區隔
8.14	資訊處理設施的冗餘	8.32	變更管理
8.15	日誌記錄	8.33	測試資訊
8.16	監測活動	8.34	稽核測試期間資訊系統之保護
8.17	時鐘同步		

參、營運持續管理系統

營運持續管理系統（Business Continuity Management Systems，BCMS）為組織提供了一個框架，用於規劃、建立、實施、操作、監控、審查、維護和持續改進記錄的管理系統，以防止災害性事件、減少災害性事件的可能性並確保從災害性事件中恢復。

ISO 22301 的前身為英國標準協會所制定之BS 25999，2006年與2007年分別提出BS 25999社會安全－營運持續管理系統－指南（第一部分）及BS 25999社會安全－營運持續管理系統－要求（第二部分），是一套可衡量的準則與指導綱要，指導組織如何建立良好的防護機制，以確保營運持續能力，並於2012年5月由ISO國際標準組織正式公佈，轉換成ISO 22301營運持續管理系統標準，並於2019 年 10 月進行標準條文改版，目前最新的版本為ISO 22301：2019。

圖貳-8 ISO 22301發展歷程演進

資料來源：英國標準協會、本研究整理

ISO 22301是為提供建立營運持續管理系統提供相關要求，條文架構同ISO 27001標準，本文1至本文3為適用範圍、引用標準、用語及定義，依循PDCA的循環架構對應標準本文，摘要說明如下：

一、規劃（Plan）：對應本文4至本文7

（一）4組織全景：

1. 4.1瞭解組織及其全景，此項要求目的是組織應決定與目的有關且影響達成營運持續管理系統預期成果能力之外部及內部議題。
2. 4.2瞭解關注方之需要及期望，此項要求目的是組織應決定與營運持續管理系統有關的關注方及關注方相關要求事項。
3. 4.3決定營運持續管理系統之範圍，此項要求目的是組織應決定營運持續管理系統之邊界及適用性，以建立範圍，且此範圍應以文件化資訊提供。
4. 4.4營運持續管理系統，此項要求目的是組織應依ISO 22301國際標準要求事項，建立、實作、維持及持續改善營運持續管理系統，且含所有過程與互動。

（二）5領導力：

1. 5.1領導力與承諾，此項要求目的是最高管理階層應依營運持續管理系統的政策與目標、所需資源、人力等事項，展現對營運持續管理系統之領導力與承諾。
2. 5.2政策，此項要求目的是最高管理階層應建立營運持續政策，並將政策內容傳達給內部員工或外部關注方。
3. 5.3組織角色、責任及權限，此項要求目的是最高管理階層應確保營運持續相關角色之責任及權限已於組織內指派並傳達。

（三）6規劃：

1. 6.1因應風險及機會之行動
   （1）6.1.1決定風險及機會，此項要求目的是當規畫營運持續管理系統時，組織應考量4.1所提及之議題及4.2所提及之要求事項，並決定需因應之風險及機會。
   （2）6.1.2闡述風險及機會，此項要求目的是組織應規劃闡述這些風險與機會的活動，並規劃各項行動整合與實作於營運持續管理系統過程中。
2. 6.2營運持續目標及其達成之規劃，此項要求目的是組織應於各相關部門及層級建立營運持續目標。
3. 6.3規劃營運持續管理系統的變更，此項要求目的是當組織決定需變更調整營運持續管理系統，應以規劃之方式執行變更。

（四）7支援：

1. 7.1資源，此項要求目的是組織應決定並提供建立、實作、維持及持續改善營運持續管理系統所需之資源。
2. 7.2能力，此項要求目的是組織應採取相應措施，包含：

（1）決定於組織控制下執行工作，影響其營運持續績效人員之必要能力。
（2）確保人員於適當教育、訓練或經驗之基礎上能勝任。
（3）採取對現有員工提供訓練、指導或重新指派，或僱用或約聘勝任人員取得必要能力，並評估所採取行動之有效性。
（4）保存適切之文件化資訊，作為勝任之證據。

3. 7.3認知，此項要求目的是於組織控管下，執行工作之人員應有營運持續相關認知。
4. 7.4溝通或傳達，此項要求目的是組織應建立營運持續管理系統之內部及外部溝通或傳達的事項、時間、對象、方式及人員。
5. 7.5文件化資訊，此項要求目的是組織應建立營運持續管理系統相關要求有文件化，以確保需要時可用且適用。

二、執行（Do）：對應本文8

（一）8運作：

1. 8.1運作之規劃及控制，此項要求目的是組織應規劃、實作及控制符合要求事項所需之過程，並實作本文6.1中所決定的行動。
2. 8.2營運衝擊分析與風險評鑑

（1）8.2.1一般要求，此項要求目的是組織應實施並維護系統流程，以分析營運衝擊並評估中斷之風險，並定期或重大變更時，審查案營運衝擊分析與風險評鑑。
（2）8.2.2營運衝擊分析，此項要求目的是組織應透過流程來分析營運衝擊，以決定營運持續的優先順序及要求。
（3）8.2.3風險評鑑，此項要求目的是組織應實施與維持風險評鑑流程。

3. 8.3營運持續策略與解決方案

（1）8.3.1一般要求，此項要求目的是依據營運衝擊分析與風險評鑑的產出，組織應識別與選擇營運中斷前、中、後的營運策略。營運持續策略應包含一個或多個解決方案。
（2）8.3.2識別策略和解決方案，此項要求目的是依據營運中斷程度來識別策略和解決方案。
（3）8.3.3選擇策略和解決方案，此項要求目的是依據營運中斷程度來選擇策略和解決方案。
（4）8.3.4資源需求，此項要求目的是組織應決定資源需求來實施所選擇的營運持續策略。
（5）8.3.5解決方案的實施，此項要求目的是組織應實施和維持所選定的營運持續解決方案，以便在需要時能被啟用。

4. 8.4營運持續計劃和程序

（1）8.4.1一般要求，此項要求目的是組織應實施和維持一個回應架構，使能及時警告並與相關關注方進行溝通。組織應提供計劃及程序，以便在中斷時能夠管理組織，此計劃和程序是當需要啟動營運持續解決方案時使用。

（2）8.4.2回應架構，此項要求目的是組織應實施和維持一個架構，識別一個或多個當中斷時負責回應的團隊，並明訂每個團隊的角色與責任及各團隊間的關係。

（3）8.4.3警示與通報，此項要求目的是組織應與關注方於中斷前、中、後進行內部和外部溝通，且警示與通報程序應作為條款8.5，演練計劃的一部份。

（4）8.4.4營運持續計劃，此項要求目的是組織應文件化並維持營運持續計劃與程序，計劃與程序應提供引導資訊，以幫助團隊回應中斷及協助組織因應和回復，且於任何時間與地點皆可用。

（5）8.4.5復原，此項要求目的是組織應備有文件化流程，以在中斷發生後採取暫時措施，便於復原營運活動。

5. 8.5演練方案，此項要求目的是組織應進行建置與維護演練方案，測試以驗證其各期間之營運持續策略與解決方案的有效性。
6. 8.6評估營運持續文件資料與能力，此項要求目的是組織應評估營運衝擊分析、風險評鑑、策略、解決方案、計劃和程序的合宜性、適切性及有效性，對供應商的營運持續能力進行評估，以及評估是否符合適用的法令法規要求、組織自身營運持續政策與目標。

三、檢查（Check）：對應本文9

（一）9績效評估：

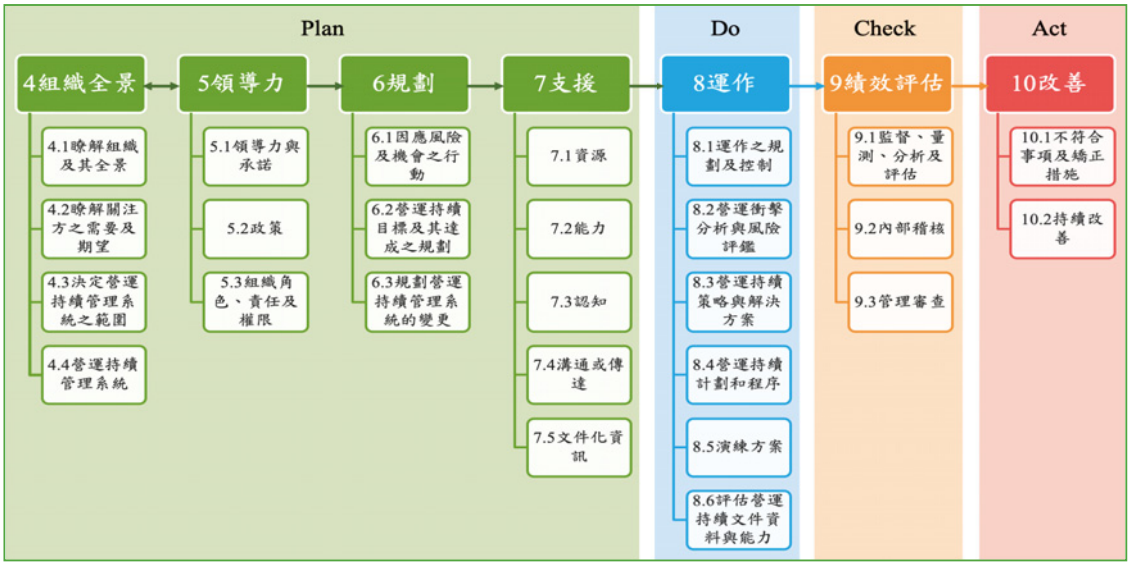
1. 9.1監督、量測、分析及評估，此項要求目的是組織應建立監督、量測、分析及評估的事項、時間、人員及方法，並確認其有效性。
2. 9.2內部稽核，此項要求目的是組織應規劃、建立、實作及維持稽核計畫，並依規劃之期間執行內部稽核。
3. 9.3管理審查，此項要求目的是最高管理階層應於規劃的期間，審查組織之營運持續管理系統，以確保其持續的合宜性、適切性及有效性，並對管理審查討論事項及會議結果留存相關紀錄。

四、行動（Act）：對應本文10

（一）10改善：

1. 10.1 不符合事項及矯正措施，此項要求目的是組織應決定改善的機會並採取必要的措施，以實現營運持續管理系統之預期結果，如有不符合事項發生時，應對不符合事項採取適當處理措施，以控制並矯正之，使其不再發生。
2. 10.2持續改善，此項要求目的是組織應透過定性與定量的量測，以持續改善營運持續管理系統之合宜性、適切性及有效性。

圖貳-9 ISO/IEC 22301：2019本文與PDCA對應



資料來源：英國標準協會，國際標準條文ISO 22301

綜上所述，透過國際標準資訊安全管理系統及營運持續管理系統介紹，可得知國際標準組織為使企業導入不同的國際標準於時，可快速與現有的國際標準整合，其條文架構皆依循PDCA的循環運作模式，包含國際標準組織推出與雲端安全或人工智慧相關之國際標準，皆為此模式。

另從國際標準資訊安全管理系統及營運持續管理系統的發展演進，可發現國際標準組織也隨著科技變遷，重新檢視既有的國際標準條文的合適性，並於近幾年進行國際標準改版公告，期望不論是否已有導入資安國際標準，期許會導入或參考國際標準內容之企業，可運用最新的資安國際標準，持續改進資安相關的管理制度與控管措施。

第三節、公股銀行國際標準的導入現況

經調查八家公股銀行導入國際標準資訊安全管理系統並通過第三方驗證之情形，截至2024年7月17日止，八家公股銀行皆已完成資訊安全管理系統導入及驗證作業，且驗證範圍與銀行公會建議之「部門」選項較相近。

表貳-4公股銀行資訊安全管理系統驗證情形

銀行名稱	驗證範圍
彰化銀行	資訊處與資訊安全處提供之業務資訊系統開發、操作及維護、網路設備、及機房和災害復原中心相關活動
臺灣銀行	資通安全處提供資訊安全管理活動
土地銀行	資訊處提供之資訊系統相關的設計、開發及維運，網路管理、機房管理及相關支援之資訊流程的資訊安全管理 資訊安全處提供之資訊安全管理活動

銀行名稱	驗證範圍
兆豐銀行	資訊處提供之資訊系統相關的設計、開發及維運，網路管理、機房管理及相關支援之資訊流程的資訊安全管理 資訊安全處提供之資訊安全管理活動
合作金庫	資訊處提供之資訊系統相關的設計、開發及維運，網路管理、機 房管理及相關支援之資訊流程的資訊安全管理
台企銀	資訊部所提供電子金融服務系統開發、操作及維護，網路設備管理、機房管理，及相關安全管理活動
第一銀行	資訊處與數位安全處提供 應用系統開發、維護及維運 處理與產出晶片卡 網路基礎設施、機房、備援中心的管理及所有支援資訊流程活動
華南銀行	資訊部門與資安部門提供之業務資訊系統開發、操作及維護、網路設備、及機房和災害復原中心相關活動

資料來源：本研究整理

經調查八家公股銀行導入國際標準營運持續管理系統並通過第三方驗證之情形，截至2024年7月17日止，六家公股銀行已完成營運持續管理系統導入及驗證作業，餘兩家公股銀行已於2024年進行營運持續管理系統的導入，預計於2025年進行驗證。

表貳-5公股銀行營運持續管理系統驗證情形

銀行名稱	取證時間	驗證範圍
彰化銀行	2017 年	個人網路銀行、企業網路銀行、行動網銀、淘金王
臺灣銀行	2008 年	電子金融服務 -e 企合成網、網路銀行暨網路 ATM、就學貸款入口網
土地銀行	2008 年	電子金融業務 - 個人網路銀行
兆豐銀行	2022 年	網路銀行、行動網銀、網路 ATM、EOI、海外網銀（蘇州）
合作金庫	2022 年	網路銀行（個銀與企銀）、行動銀行
台企銀	2021 年	電子金融業務、一般網路銀行、行動銀行、企業網路銀行
第一銀行	預計 2025 年	個路銀行、企業網路銀行、行動網銀
華南銀行	預計 2025 年	個路銀行與行動網銀

資料來源：本研究整理

綜上調查結果顯示，公股銀行皆已完成國際標準資訊安全管理系統導入與驗證，而國際標準營運持續管理系統主要於金管會2020年發布「金融資安行動方案」後，開始規劃導入，並於2021年起，半數以上的公股銀行成功導入並通過第三方驗證，可見公股銀行也是藉由導入國際標準來輔助組織資訊安全及營運持續管理制度的建立與實施，強化組織資訊安全防護與作業韌性相關措施，並透過第三方驗證機構來找出可持續改善或精進事項。

～待續～