金融業導入資安國際標準的發展與探討－下

陳瑩瑄

第參章　管理系統導入與驗證

本研究以「金融業導入資安國際標準的發展與探討」為主軸，依據前一章節介紹的國內發展動向、國際標準介紹及公股銀行國際標準的導入現況，為了確保本行資訊作業環境之安全控管書面制度與實際作業辦理之情形，均符合法令法規要求，透過檢視資訊安全資訊環境及作業流程，提出改善及強化措施，以維持資訊安全管理制度有效性，並藉由教育訓練課程與程序演練，提升本行同仁資安認知及事件應變能力，本行2007年開始規劃導入國際標準資訊安全管理系統（ISO 27001），依循條文內容要求，建立本行資訊安全管理制度。

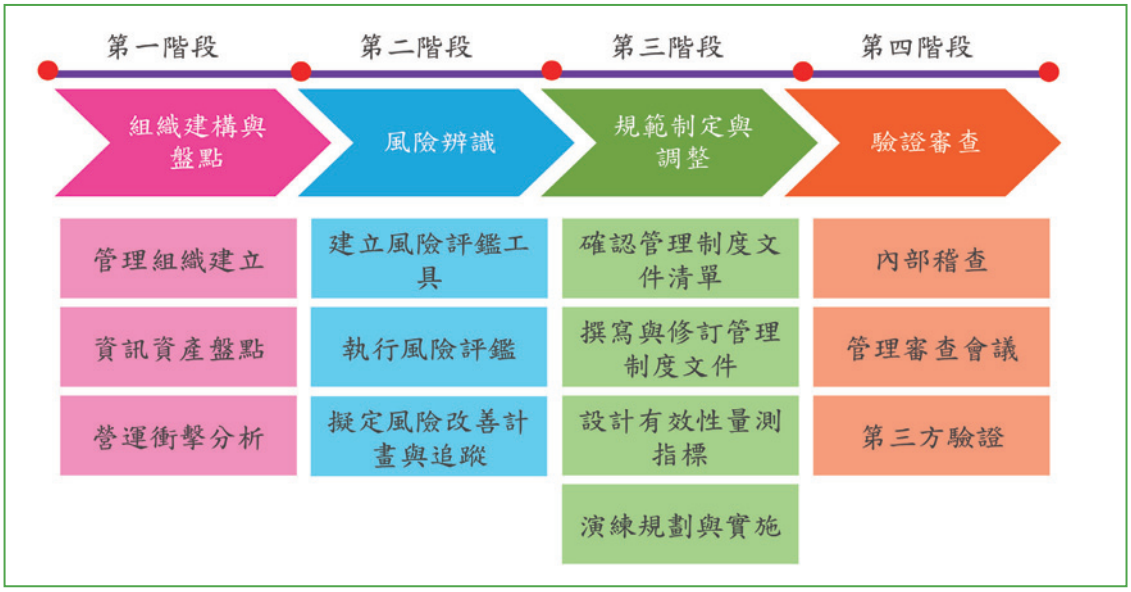
此外，因應外部威脅增加，除了採用資訊系統進行阻擋及防禦，採取適切且有效的應變計畫，已成為資安的趨勢，故為了強化電子化金融服務之品質，提供用戶安全，並透過教育訓練、演練等方式，提升人員認知，精進事故因應之意識與能力，本行於2017年導入國際標準營運持續管理系統（ISO 22301），依循國際標準條文要求，建立本行營運持續管理制度。

綜上所述，藉由導入國際標準，全面檢視資訊安全管理制度及營運持續管理制度的完整性及有效性，並取得國際標準驗證，亦可向客戶及主管機關彰顯本行對於資訊安全與持續營運的努力及證明，並符合主管機關期許。

第一節、整體架構

本研究整體架構依導入管理系統來建構管理制度分為四個階段，組織建立與盤點、風險辨識、規範制定與調整及驗證審查，流程如下圖：

圖參-1管理系統導入架構



資料來源：勤業眾信方法論

首先組織建構與盤點，主要包含管理組織建立，確認組織成員的角色與權責，以利進行管理制度的決策、推動與運行，並完成所有資訊及資安監控系統之資訊資產盤點及營運衝擊分析，並落實營運系統不中斷服務決心，提供客戶二十四小時全方位的服務。

第二階段為風險辨識，主要建立一套可供本行同仁針對資訊安全風險及營運持續風險進行評估的工具，採用量化分析方法，評估風險高中低之水準，並依據風險評鑑結果，擬定風險改善計畫與進行追蹤。

第三階段為規範制定與調整，主要撰寫與修訂管理制度相關文件、設定量測目標，並透過演練提升人員應變能力。

第四階段為驗證審查，透過內部稽查發現缺失並進行改善，報告現有的管理制度辦理情形，並透過第三方驗證衡量管理制度的有效性。

第二節、運作說明

壹、組織建構與盤點

一、管理組織建立

透過既有組織架構，規劃資訊安全及營運持續之日常管理組織，及發生資訊安全事件或資訊系統營運中斷因應之應變小組，並定義組織成員角色與權責。

二、資訊資產盤點

（一）資訊資產分類分級：

以資訊資產取得、處分之流程為基礎，訂定資訊資產分類分級法則及價值判斷標準，作為執行資訊資產分類時評估資產價值依據，並針對不同資產種類訂定其個別之保護措施，建立完整的資訊資產相關之取得、分類評估及處分程序。

（二）資訊資產分析與收集：

藉由分析資訊作業流程之方式瞭解現有控管，確認各資訊作業流程之輸入、處理及輸出程序是否正確，以協助收集資訊資產所涵蓋之範圍與項目。並配合工具程式之使用或利用現有的資產清單，有效收集並建立完整之資訊資產清冊。

（三）資訊資產彙整：

根據資訊資產清冊進行資訊資產群組分類方式，制訂資訊資產群組，做為管理資訊資產之基礎。資訊資產採用群組管理之方式，係在不改變風險程度之情況下，所採取為適度簡化風險評估作業之設計。

三、營運衝擊分析

基於本行業務項目，考量法令遵循、商譽、客戶、財務等面向，進行營運中斷衝擊調查，以評估營運持續要求。分析流程如下：

（一）決定衝擊因子：規劃衝擊因子及其判定分數準則，衝擊因子可包括財務影響、商譽影響、客戶流失、法規遵循等面向，並歸納出最大可容忍中斷時間。

（二）分析中斷影響以辨識系統相依性：依據業務特性及複雜度，設計營運衝擊分析問卷，辨識系統相依性，並歸納出最大可容忍中斷時間、復原時間目標、復原點目標與最小可接受服務水準。

（三）確認復原最小資源需求與利害關係團體：與各單位確認其所提供之資訊，並以此展開蒐集關鍵資訊系統復原所需之資源，資源需求調查範圍至少包含人員、資訊設備、資料文件、場地、網路基礎設施、外部供應等。利害關係團體則依據業務性質，可能涵蓋一般使用者、行內單位、金融同業等。

貳、風險辨識

一、建立風險評鑑工具

參考內部既有風險評鑑方法，設計符合ISO 27001及ISO 22301國際標準要求之評鑑方式，用以衡量資訊安全及營運持續之相關風險。

二、執行風險評鑑

（一）資訊安全風險評鑑：針對資訊資產之機密性、完整性及可用性評估其價值，同時依據現有之控管方式，權衡資產之弱點值與威脅值，歸納出資訊資產之風險值。同時配合ISO 27001國際標準要求，除針對已知風險進行風險評鑑作業外，針對未知的風險，亦應評估其發生機率與潛在衝擊程度，以提升組織對於未知風險的因應能力。

（二）營運持續風險評鑑：針對如天然災害、生物、人為災害、資訊科技等營運持續威脅類型，評估可能性及衝擊程度，歸納出營運持續之風險值。

三、擬定風險改善計畫與追蹤

依據風險評鑑結果，對高風險項目提出控管與改善建議。該控管與改善建議應包含資訊安全管理之短期、中期與長期之執行計畫，以提供強化資安保護機制之方向與目標。

參、規範制定與調整

一、確認管理制度文件清單

依據風險評鑑結果、資訊安全管理政策、適用性聲明等資訊，向下發展並調整現有資訊安全管理制度運行機制，包含資訊安全管理組織的角色權責、資訊資產分類及管理、風險評鑑、網路安全管理及資安事件管理等，藉由管理制度之調整，展出一階至四階文件。

二、撰寫與修訂管理制度文件

依據國際標準之要求，撰寫與修訂相關程序及管理規範，建立資訊安全政策、資訊安全暨營運持續一階至四階文件。

為符合ISO 27001及ISO 22301國際標準要求，並因應近期主管機關以及國際資安趨勢之重點，撰寫與修訂管理制度相關文件，以提升資訊安全管理控管於各項作業的落實程度，並建立符合國際標準要求之資訊安全管理制度。

三、設計有效性量測指標

依據資訊安全暨營運持續管理制度，設計符合資訊安全目標，擬定有效性量測指標，並將配合ISO 27001及ISO 22301國際標準對於監控、量測、分析及評估之要求，明訂各有效性量測指標之監控與量測的負責人員、時機，以及結果的分析及評估之方法、負責人員、時機。

四、演練規劃與實施

依據國內外法令法規、國際標準及風險評鑑結果，擬訂年度演練計畫表，辦理事件應變計畫桌面演練、人員疏散實地演練。

肆、驗證審查

一、內部稽查

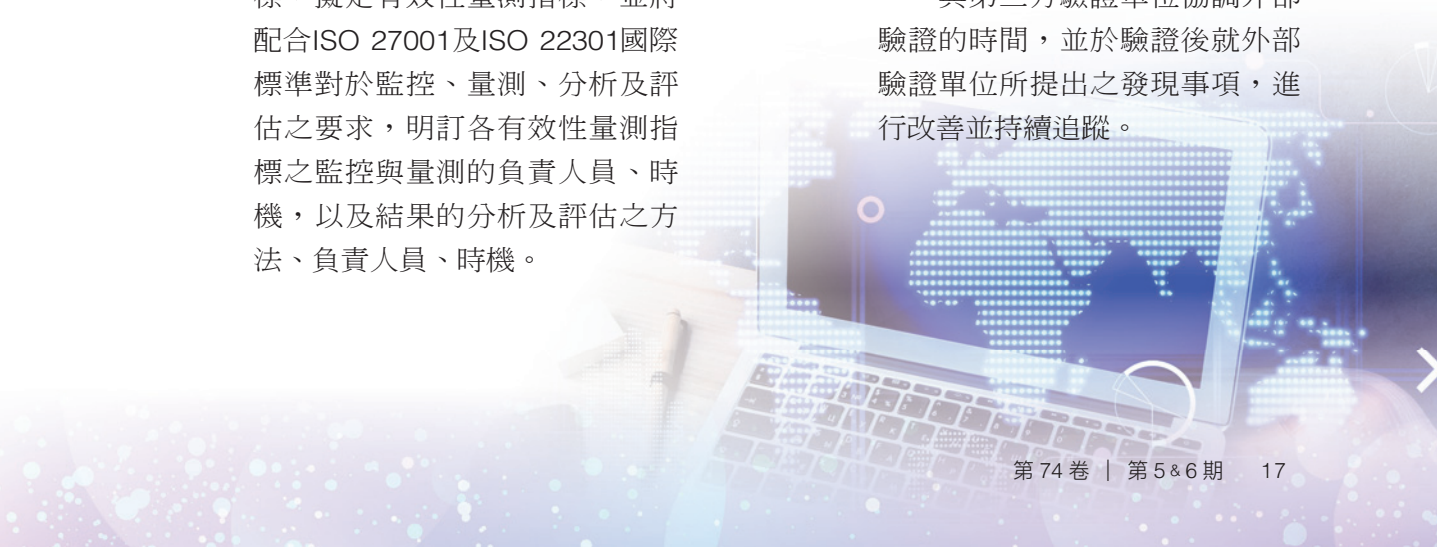
依據國際標準條文要求及資訊安全暨營運持續管理制度相關規範要求，擬定稽查工作底稿及稽查計畫，執行內部稽查活動並撰寫稽查工作底稿，如內部稽查有缺失項目，負責改善之單位應填寫矯正預防措施單，以利進行追蹤缺失改善之進度。

二、管理審查會議

依據ISO 27001及ISO 22301國際標準要求，準備資訊安全及營運持續管理審查會議之相關簡報資料，尤其針對不符合事項及矯正措施、監控及量測結果、稽查結果、資訊安全目標之落實等項目進行趨勢分析，邀集相關人員並召開管理審查會議，同時將管理審查會議之會議資料與紀錄留存書面化之證據。

三、第三方驗證

與第三方驗證單位協調外部驗證的時間，並於驗證後就外部驗證單位所提出之發現事項，進行改善並持續追蹤。



第肆章　導入實作－以彰化銀行為例

第一節、發展沿革

本行早期係由資訊處推動資訊安全管理系統導入，並以資訊處之業務資訊系統開發、操作及維護、網路設備、機房和災害復原中心相關活動為驗證範圍，於2008年10月通過ISO 27001：2005資訊安全管理制度認證，每年持續維運管理制度並透過第三方審查，維持證書有效性。然隨著業務拓展、資訊科技的環境變遷，為使強化本行資訊安全管理量能，以因應內外部的資安風險與挑戰，於2015年8月通過ISO 27001：2013轉版認證。

2017年底本行推動營運持續管理系統導入，初始導入與驗證範圍涵蓋網頁版與行動版個人網銀、企業網路銀行及淘金王系統開發、操作與維護，2018年7月通過ISO 22301：2012營運持續管理系統認證，為國內第一家將驗證範圍涵蓋至手機應用程式服務的銀行，並榮獲英國標準協會頒發「資安治理金盾獎」。

依據「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 38-1 條「銀行業應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。」，本行於2018年9月3日成立資訊安全處，資訊安全管理系統及營運持續管理制度推動權責單位移轉至資訊安全處，為使本行能因應環境改變的同時也能持落實資訊安全管理制度，將資訊安全處納入驗證範圍。且為因應主管機關對於營運持續管理查核之力道逐年加深，以及合乎海外金融法規的要求，於2020年將營運持續管理系統的推動範圍擴大至資訊處與資訊安全處所維護之資訊系統及海外分行系統。

本行自導入營運持續管理制度以來，遵循ISO 22301營運持續管理國際標準之要求，持續提升本行資訊系統對於災害之應變與復原能力，以提供穩定與高品質的資訊服務，以此回應主管機關於金融資安行動方案中所提及應精實金融韌性，增進營運持續管理量能，並識別核心業務與最大可容忍中斷時間。

國際標準組織於2019年10月發布ISO 22301：2019版本，於2022年12月發布ISO 27001：2022版本，本行為持續維護管理制度之有效性，分別2022年4月通過ISO 22301：2019轉版認證及2023年9月為國內第一家銀行通過英國標準協會ISO 27001：2022資訊安全管理制度轉版認證，並榮獲英國標準協會頒發「資訊韌性卓越獎」，持續至今，證書仍有效。

第二節、導入與驗證執行說明

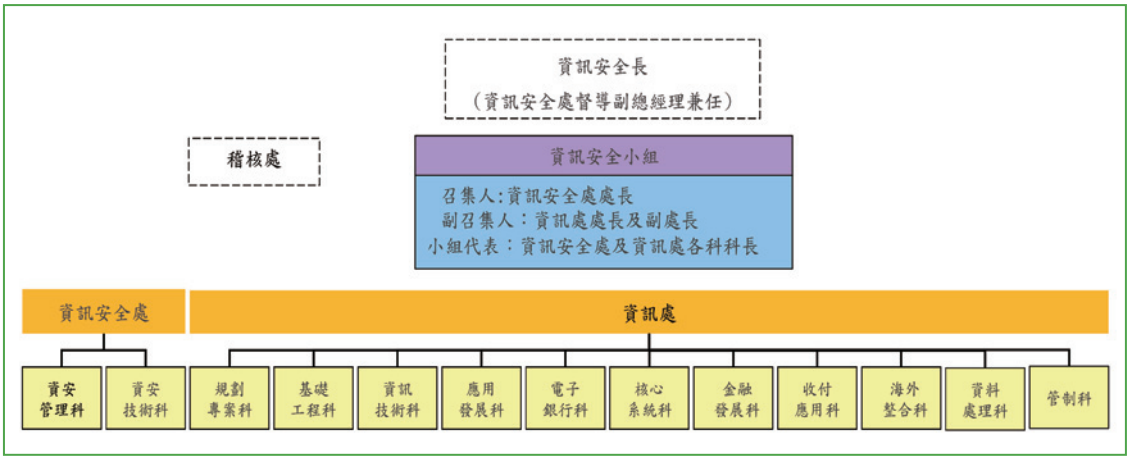
壹、組織建構與盤點

因應國際標準ISO 27001及ISO 22301條文要求，組織建構與盤點以本行資訊處與資訊安全處建構管理制度組織、進行資訊資產盤點及進行營運衝擊分析作業來說明。

於管理制度組織建立過程，主要為協調資安管理控制措施之落實情況，於2018年資訊安全處成立前，為資訊處單一部門內部的成員組成，資訊安全處成立後，組織架構變更為資訊安全處及資訊處組成一跨單位之資訊安全小組，由資訊安全處及資訊處相關處/科之管理代表參與，為常態任務編組。召集人由資訊安全處處長擔任，副召集人由資訊處處長及副處長擔任，資訊安全小組代表由資訊安全處資安管理科與資安技術科，以及資訊處應用發展科、資訊技術科、規劃專案科、基礎工程科、核心系統科、電子銀行科、資料處

理科、管制科、收付應用科、海外整合科及金融發展科等科長擔任，並訂定各角色在資訊安全暨營運持續管理制度之權責，現行資訊安全小組架構圖為下圖肆-1。

圖肆-1資訊安全小組架構圖

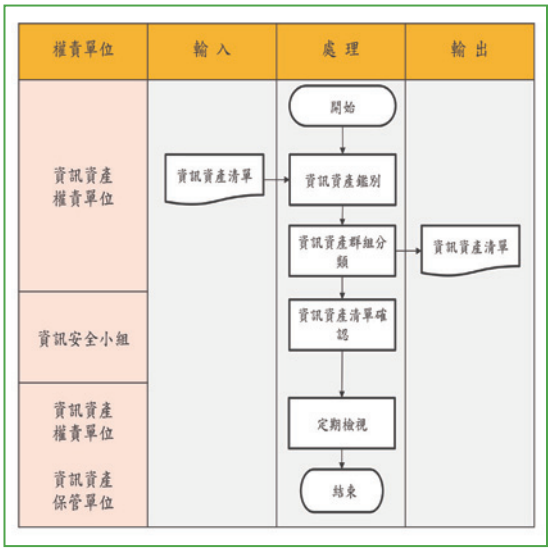


資料來源：本研究整理

除了資訊安全小組之成立，為使管理制度推展、運作及溝通順暢，兩處各科推派負責資訊安全管理制度及營運持續管理制度之文管窗口，有任何需傳達管理制度之遵循事項，或文件管制等皆由各科文管窗口負責協助相關事項。

為使充分盤點資訊處與資訊安全處所管轄之所有資訊資產，設計並規劃資訊資產盤點作業流程如下圖肆-2，並依資訊資產不同性質分為硬體、軟體、資料、文件及人員五大類。設計出資訊資產清單後，由各經辦就自身負責之資訊系統、設備或操作手冊等資產，每半年定期更新與維護其所管轄之資訊資產清單，陳報該科科長審核後，由負責資訊安全管理制度之文管窗口將最新的資訊資產清單上傳至內網，且每半年以「資訊資產清單清查表」確認資訊資產清單更新情形，並留存清查紀錄。若有新增、變更或移除資訊資產、系統有重大異動或作業環境改變時，則實施不定期的覆核，以更新及確保資訊資產清單的正確性及完整性。

圖肆-2資訊資產盤點作業流程



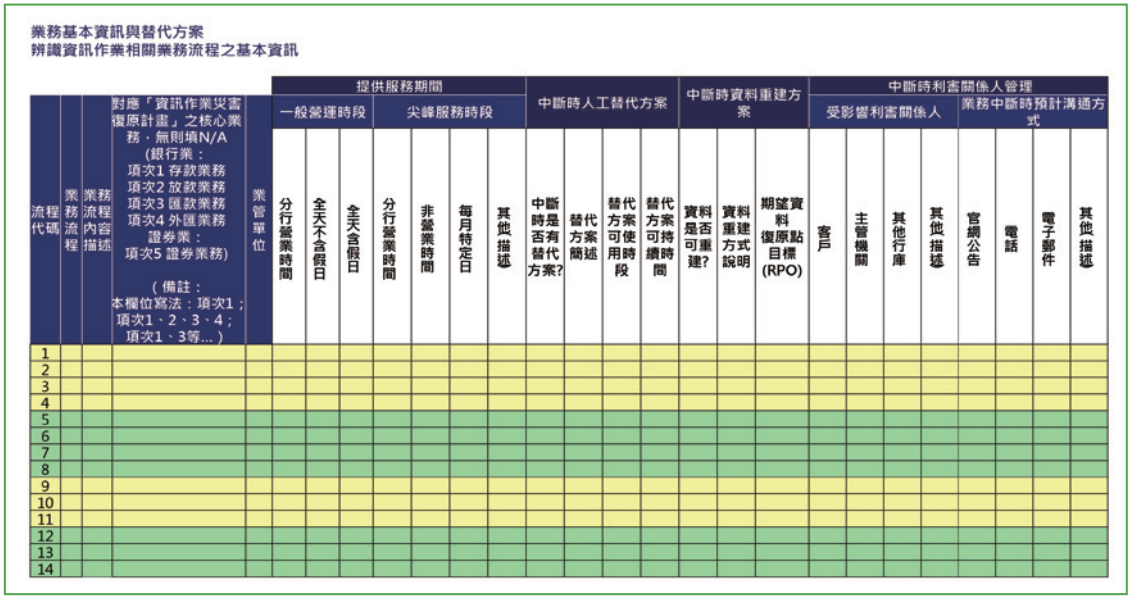
資料來源：本研究整理

為瞭解資訊安全處及資訊處所管理之應用系統復原相關之時間目標，及確保復原所需必要資源之充足程度，透過系統化的分析方法以釐清應用系統復原時間要求與復原水準，及所需使用的各項必要資源，藉以規劃適當之復原方案，因應可能之營運中斷風險。

依分析項目將營運衝擊分析問卷分為業務面以及系統面，業務面分析包含識別業務面資訊、替代方案、評估中斷影響程度、最小可接受服務水準、同異地資訊系統設備、網路設備、資安管理性設備、場地、基礎設施與供應商等。系統面分析依最小可接受服務水準，評估各項必要資源，包含相依應用系統項目、人員、工具、資料文件與供應商等。

資訊處及資訊安全處各科每半年以「營運衝擊分析問卷清查表」確認營運衝擊分析問卷更新情形，並留存清查紀錄，當範圍內有異動發生之時，則實施不定期的覆核，以更新及確保營運衝擊分析問卷的正確性及完整性。並由負責營運持續管理制度之文管窗口將最新版本之營運衝擊分析問卷上傳至內網。

圖肆-3營運衝擊分析問卷-業務面



業務基本資訊與替代方案
辨識資訊作業相關業務流程之基本資訊

流程代碼	業務流程	業務流程內容描述	對應「資訊作業災害復原計畫」之核心業務，無則填N/A (銀行業： 項次1 存款業務 項次2 放款業務 項次3 匯款業務 項次4 外匯業務 證券業： 項次5 證券業務) (備註： 本欄位寫法：項次1； 項次1、2、3、4； 項次1、3等...)	業管單位	提供服務期間							中斷時人工替代方案				中斷時資料重建方案			中斷時利害關係人管理							
					一般營運時段			尖峰服務時段													受影響利害關係人				業務中斷時預計溝通方式			
					分行營業時間	全天不含假日	全天含假日	分行營業時間	非營業時間	每月特定日	其他描述	中斷時是否替代方案?	替代案方案簡述	替代案方案可用時段	替代案方案可持續時間	資料是否可重建?	資料重建方式說明	期望資料復原點目標(RPO)	客戶	主管機關	其他行庫	其他描述	官網公告	電話	電子郵件	其他描述
1																									
2																									
3																									
4																									
5																									
6																									
7																									
8																									
9																									
10																									
11																									
12																									
13																									
14																									

資料來源：本研究整理

圖肆-4營運衝擊分析問卷-系統面

最小可接受服務水準復原所需資源 (人員/設備/文件表單)

No.	系統/設備類型	角色	人員能力需求	部門/科別	人數需求(位)	執行復原作業時所需設備	執行復原作業時所需軟體(軟體包)	執行復原作業時所需文件表單	文件表單儲存	
									儲存位址	更新頻率
INFRA	資料庫	主機DBA								
		開放系統DBA								
	網路設備	網管人員								
	系統主機	主機SE								
		開放系統SE								
		OP								

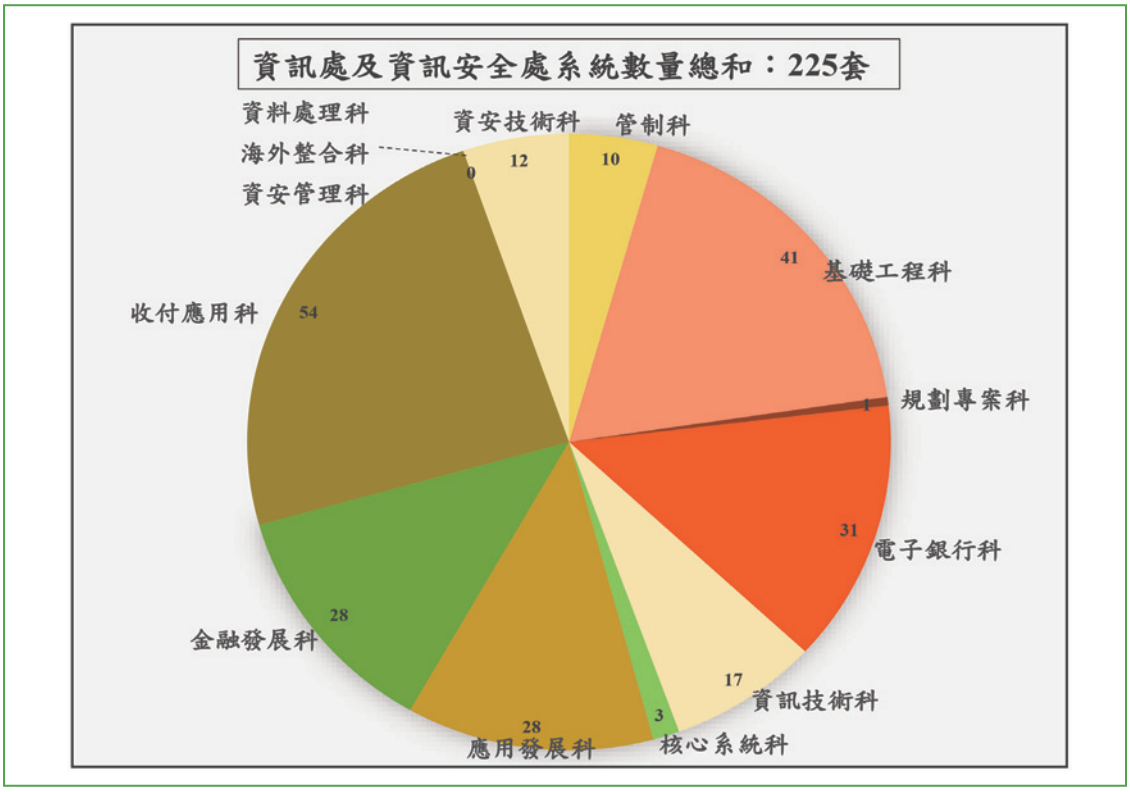
No.	應用系統名稱	角色	人員能力需求	部門/科別	人數需求(位)	執行復原作業時所需設備	執行復原作業時所需軟體(軟體包)	執行復原作業時所需文件表單	儲存位址	更新頻率
1		AP								
		業務單位								

資料來源：本研究整理

2020年將營運衝擊分析作業擴及海外分行時，依監視海外分行當地法規要求，討論並設計屬於海外分行專用的營運衝擊分析問卷，且為使海外分行同仁瞭解並進行分析活動，依海外分行地區時差安排多場教育訓練強化同仁意識，並請各海外分行對當地自行維護的資訊系統，如檔案伺服器系統、監視錄影系統等，完成營運衝擊分析問卷的填寫，並每年定期檢視更新。

資訊處與資訊安全處每年依據資訊系統新增、異動及廢止狀況統計各科維護之系統數，截至2025年4月底，資訊處與資訊安全處資訊系統總合為225套，分析如下圖肆-5。

圖肆-5資訊處與資訊安全處資訊系統維護分析圖



資料來源：本研究整理

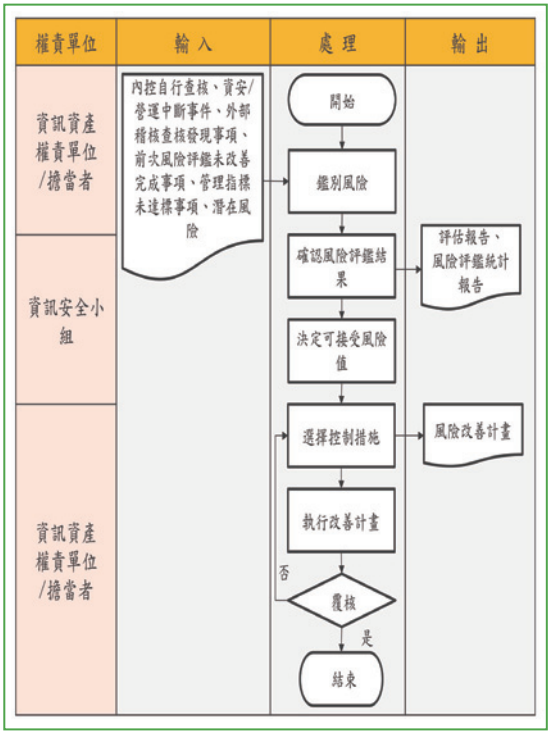
貳、風險辨識

依據國際標準要求，應規劃並執行風險評鑑作業，而進行風險評鑑就必須有一套執行的量測工具，故在建立資訊安全的風險評鑑工具過程，決定延續資訊資產清單的群組概念，並納入資訊資產的機密性、完整性及可用性三大特性，採資訊資產、外部資安威脅及內部控制強度三大維度加以量化並計算其分數之方式，產出風險值，並以80/20法則，定義出風險的高、中、低，以及設定可接受的風險水準，最後再將風險面向對應國際標準的控制要項，確認應改善或強化資安面向，以達到良好的循環改善管理。

建立營運持續的風險評鑑工具，雖然也採用量化方式設計，但分析的構面則有所不同，係考量造成資訊系統營運中斷面向發想，故採用天然災害、生物、人為災害及資訊科技四大構面，展開其向下可能會產生的風險面向，再依據其發生的可能性、造成的衝擊程度給予量化分數，計算其風險值，並針對高風險或高衝擊者採取對應的風險控制措施。

資訊處與資訊安全處建構好風險評鑑工具後，規劃並執行的風險評鑑作業，每半年會使用風險評鑑工具執行資訊安全管理風險評鑑及營運持續管理風險評鑑，如下說明：

圖肆-6資訊安全風險評鑑作業流程



資料來源：本研究整理

一、資訊安全管理風險評鑑

由資訊資產權責單位或擔當者鑑別風險，其內容包含：內控自行查核、資安/營運中斷事件、外部稽核查核發現事項（包含第三方查核及金管會查核）、前次風險評鑑未改善完成事項、管理指標未達標事項、潛在風險，並針對「已知風險」、「潛在風險」兩構面進行風險評鑑。經資訊安全處及資訊處共同召開風險評鑑會議，各科科長審核科內風險評鑑結果後，進行風險評鑑報告簽核作業。由資訊安全處將風險評鑑結果陳報風險管理委員會。

二、營運持續管理風險評鑑

依據營運持續威脅類型，將威脅類型區分四大類，如下說明：

（一）天然災害：災害型地震（含大樓結構損害或傾倒）、土石流、風災與水災（含極端氣候）、旱災。

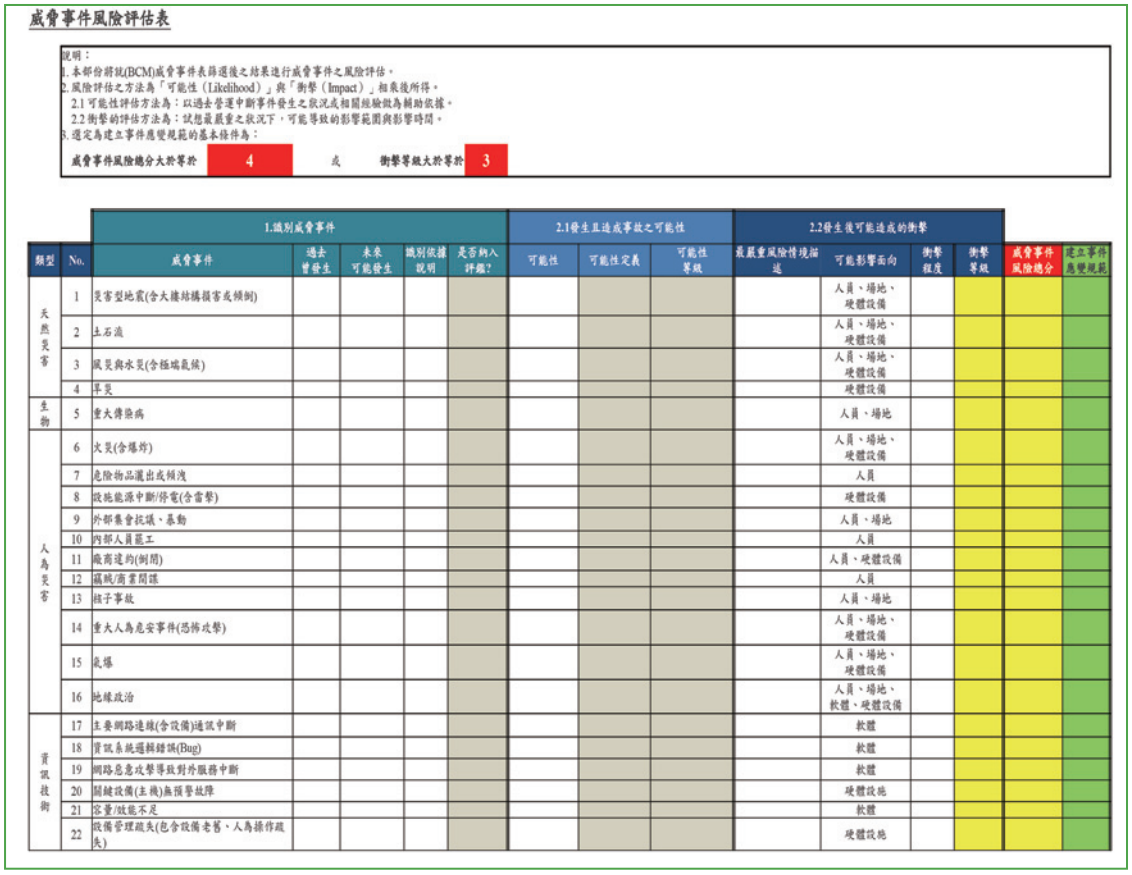
（二）生物：重大傳染病。

（三）人為災害：火災（含爆炸）、危險物品灑出或傾洩、設施能源中斷/停電（含雷擊）、外部集會抗議與暴動、內部人員罷工、廠商違約（倒閉）、竊賊/商業間諜、核子事故、重大人為危安事件（恐怖攻擊）、氣爆、地緣政治。

（四）資訊科技：主要網路連線（含設備）通訊中斷、資訊系統邏輯錯誤（Bug）、網路惡意攻擊導致對外服務中斷、關鍵設備（主機）無預警故障、容量/效能不足、設備管理疏失（包含設備老舊、人為操作疏失）。

就威脅類型進行內、外部議題蒐集，並評估其可能性及衝擊程度，評估營運持續威脅事件發生可能性時，考量過去曾發生之事件紀錄，評估衝擊程度時，考量現有管理制度及控管現狀，透過量化方式計算出風險權值後，經資訊安全處及資訊處召開風險評鑑會議，各科科長審核科內風險評鑑結果後，進行風險評鑑報告簽核作業。

圖肆-7營運持續管理風險評鑑



威脅事件風險評估表

說明：
1. 本部份將就(BCM)威脅事件表篩選後之結果進行威脅事件之風險評估。
2. 風險評估之方法為「可能性（Likelihood）」與「衝擊（Impact）」相乘後所得。
2.1 可能性評估方法為：以過去營運中斷事件發生之狀況或相關經驗做為輔助依據。
2.2 衝擊的評估方法為：試想最嚴重之狀況下，可能導致的影響範圍與影響時間。
3. 選定為建立事件應變規範的基本條件為：
威脅事件風險總分大於等於 4 或 衝擊等級大於等於 3

		1.識別威脅事件				2.1發生且造成事故之可能性			2.2發生後可能造成的衝擊					
類型	No.	威脅事件	過去曾發生	未來可能發生	識別依據說明	是否納入評鑑?	可能性	可能性定義	可能性等級	最嚴重風險情境描述	可能影響面向	衝擊程度	衝擊等級	威脅事件風險總分	建立事件應變規範
天然災害	1	災害型地震(含大規模橋樑毀損傾倒)									人員、場地、硬體設備				
	2	土石流									人員、場地、硬體設備				
	3	風災與水災(含極端氣候)									人員、場地、硬體設備				
	4	旱災									硬體設備				
生物	5	重大傳染病									人員、場地				
人為災害	6	火災(含爆炸)									人員、場地、硬體設備				
	7	危險物品溢出或傾洩									人員				
	8	設施能源中斷/停電(含雷擊)									硬體設備				
	9	外部集會抗爭、暴動									人員、場地				
	10	內部人員罷工									人員				
	11	廠商違約(倒閉)									人員、硬體設備				
	12	竊賊/商業間諜									人員				
	13	鈕子事故									人員、場地				
	14	重大人為意安事件(恐怖攻擊)									人員、場地、硬體設備				
	15	炸彈									人員、場地、硬體設備				
	16	地緣政治									人員、場地、軟體、硬體設備				
資訊技術	17	主要網路連線(含設備)通訊中斷									軟體				
	18	資訊系統邏輯錯誤(Bug)									軟體				
	19	網路惡意攻擊導致對外服務中斷									軟體				
	20	關鍵設備(主機)無預警故障									硬體設施				
	21	容量/效能不足									軟體				
	22	設備管理疏失(包含設備老舊、人為操作疏失)									硬體設施				

資料來源：本研究整理

完成資訊安全管理風險評鑑及營運持續管理風險評鑑，若風險評鑑結果之風險值超出可接受風險值，風險擁有者應填寫「風險改善計畫」（如圖肆-8），就此風險事項提出預計改善方式及預計完成日期，例如風險事項係屬缺乏作業程序之控管，其預計改善方式則應具體說明作業程序強化措施，包含但不限於作業手冊進行修訂、作業流程增設覆核人員、加強人員教育訓練等。

風險評鑑統籌單位應彙整風險改善計畫，並定期追蹤改善結果。於風險事項改善完成後，再次進行風險評估，並將風險評鑑與風險改善計畫提報管理審查會議（如圖肆-9），由資訊安全小組進行審查風險改善結果，以確認此風險改善措施是否有效，其風險值已降至可接受程度。

此外，如屬營運持續管理風險事項，除增修事件應變規範外，應依威脅事件類別，每年定期辦理系統備援演練、人員疏散演練及桌面程序演練，訓練同仁對於災害型威脅事件的應變能力。

圖肆-8風險改善計畫

序號		資產群組	資產群組類別	屬性（CIA）	值	弱點	值	威脅	值	風險值	高風險事項	預計改善方式	風險擁有者/改善負責人	預計完成日期	狀態	改善後風險值	是否符合風險可接受程度
ISMS-10903-IA-014	A科	S01	與交易直接相關軟體	I	3	缺乏作業程序之控管	2	損毀	3	18	經檢視AA系統之code review 報告，因負責單修改位未能於期限內完成中風險項目之修補，故有填寫資安檢測修補作業延長時限申請單，並註明預計完成日期為2019/11/30。後續詢問單位同仁是否有追蹤後續修改情況，同仁表示有透過電話確認修改狀況，惟未留存確認紀錄，建議後續可以透過email、請修改單位提出修改完成之證明(完成修改)或請修改單位再提一份資安檢測修補作業延長時限申請單(未能完成修改)的方式留存相關佐證資料，以茲證明有確實追蹤。	1. 追蹤該程式員後續修改進度。 2. 補填資安檢測修補作業延長時限申請單。 3. 完成中風險事項之修補，資安檢測修補作業延長時限申請單結案。	黃ＯＯ	2020/4/6	已完成	9	Y
ISMS-10903-IA-014	A科	S01	與交易直接相關軟體	A	3	缺乏作業程序之控管	2	延遲 失效 損毀	3	18	經檢視AA系統之code review 報告，因負責單修改位未能於期限內完成中風險項目之修補，故有填寫資安檢測修補作業延長時限申請單，並註明預計完成日期為2019/11/30。後續詢問單位同仁是否有追蹤後續修改情況，同仁表示有透過電話確認修改狀況，惟未留存確認紀錄，建議後續可以透過email、請修改單位提出修改完成之證明(完成修改)或請修改單位再提一份資安檢測修補作業延長時限申請單(未能完成修改)的方式留存相關佐證資料，以茲證明有確實追蹤。	1. 追蹤該程式員後續修改進度。 2. 補填資安檢測修補作業延長時限申請單。 3. 完成中風險事項之修補，資安檢測修補作業延長時限申請單結案。	謝ＯＯ	2020/4/6	已完成	9	Y
ISMS-11109-PT-011	B科	I01	資安管理體系	N/A	N/A	缺乏對相關政府法令的遵循制度	N/A	--	N/A	27	國家資通安全發展方案(110年至113年) 鑒於資通訊服務應用廣泛，以及我國重大科技創新政策，對於國家安全，甚至是社會經濟活動各種應用層面，資通安全皆扮演關鍵角色，為能因應國際趨勢與新型態資安攻擊與威脅，在既有的防禦基礎及面向上延續我國的資安防護能量與優勢，除持續落實第五期國家資通安全發展方案(106年至109年)，行政院國家資通安全會報為逐步提升我國資通安全防護能量，爰據以提出「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。	將根據法規的調整內容，進行文件修訂。	洪ＯＯ	2024/12/31	已完成	1	Y

資料來源：本研究整理

圖肆-9管理審查-風險評鑑與風險改善計畫提報內容

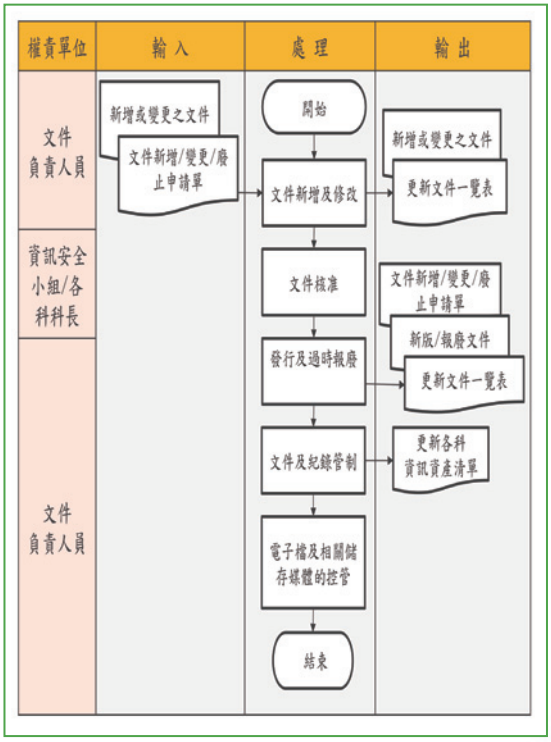
威脅事件	衝擊分數	風險分數	風險處理方式 風險控制 預防性措施	事件應變規範
災害型地震(含大樓結構損害或傾倒)	3	3	• 定期辦理人員疏散演練 • 預先發展事件應變與通報機制	• 資訊大樓災害應變程序 • 資安事故緊急通報及應變規範書
風災與水災(含極端氣候)	2	6	• 平時密切注意中央氣象局發布之陸上颱風警報、豪雨特報，並應依照警報內容預先進行相關預防措施。 • 預先發展事件應變與通報機制	• 資訊大樓災害應變程序 • 資訊作業災害復原計畫 • 資安事故緊急通報及應變規範書
重大傳染病	2	4	• 維持資訊處工作場所環境衛生，定期進行清潔消毒，提供充足衛生用品 • 預先規劃異地辦公室及人力配置原則 • 預先發展事件應變與通報機制	• 資訊大樓災害應變程序 • 彰化銀行因應疫情強制集體隔離緊急應變措施處理要點 • 資訊作業災害復原計畫
火災(含爆炸)	3	3	• 辦公室與機房內裝設滅火設備與定期檢查 • 定期辦理消防逃生演練 • 預先發展事件應變與通報機制	• 資訊大樓災害應變程序 • 資訊作業災害復原計畫 • 資安事故緊急通報及應變規範書
核子事故	3	3	• 預先發展事件應變與通報機制	• 資訊大樓災害應變程序

資料來源：本研究整理

參、規範制定與調整

依循國際標準制度的條款要求，將資訊安全暨營運持續相關文件分成第一階至第四階文件，並依據文件新增、修改、廢止及對應之文件階層，規劃並設計文件增修、核准、發行、報廢、紀錄保存及電子檔及媒體控管等機制，此外，將管理制度相關文件等級分為公開、一般、敏感及密四級，各階文件依序分類歸檔，依使用者職權賦予適當之文件存取權限，對於敏感或密等級資料及文件，加強管控以避免資料外洩，文件管理作業流程如下圖肆-10。

圖肆-10文件管理作業流程

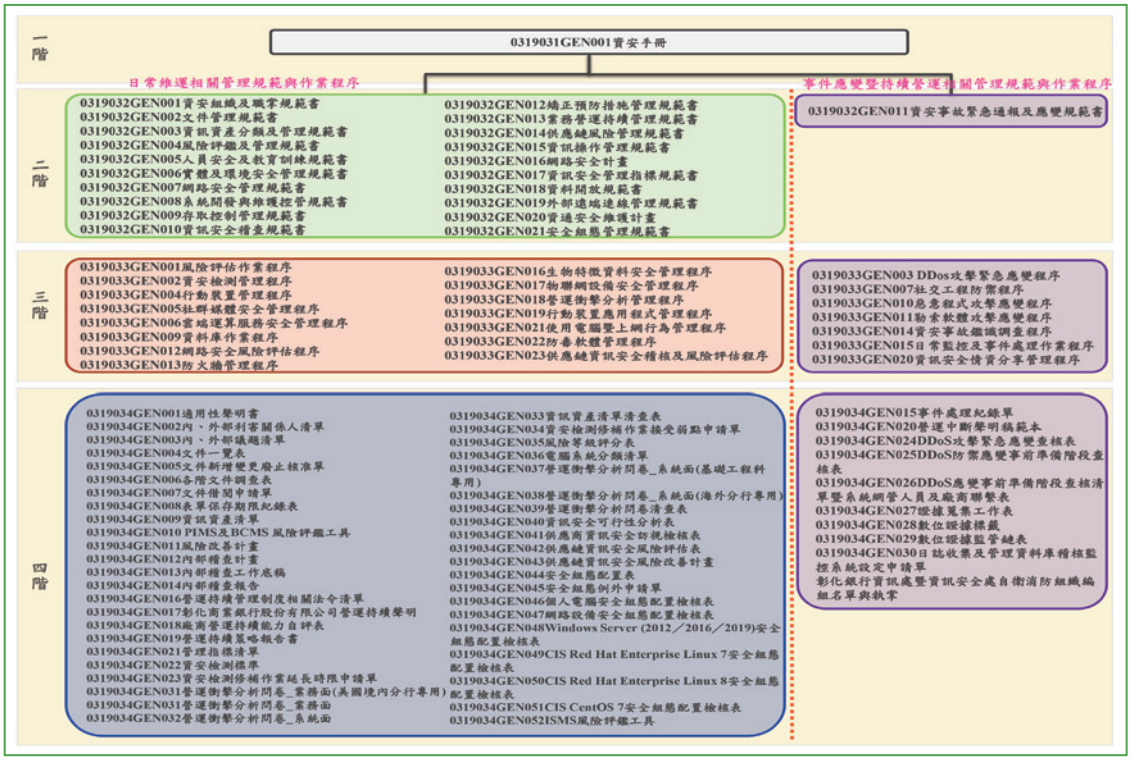


資料來源：本研究整理

針對不同階層文件設定不同的核准層級，第一階與第二階文件之增修應由資訊安全小組召集人或副召集人負責定期與不定期之評估與審核，第三階及四階文件應由資訊安全小組之召集人或副召集人或各科科長指派專人負責定期及不定期之增修，並由各管理制度組織召集人或副召集人或各科科長負責審核。且文件之增修應填寫「文件新增/變更/廢止核准單」，資訊安全處以資安管理科為審核單位，資訊處以基礎工程科為審核單位，且第一階、第二階文件須依「彰化銀行業務規章制定準則」業務規章之修正，另檢附條文對照表向資訊安全處主管提出申請。

為符合最新法令法規要求，配合監理機關及查核單位檢查建議，資訊安全處與資訊處各科每半年以「各階文件調查表」確認文件更新情形，並核對「文件一覽表」及彙總文件異動情形，以確保提供最新版本文件供同仁依循，目前資訊安全處訂定之共通資安暨營運持續共通遵循規範，一階至四階文件整理如圖肆-11，又可區分成日常維運相關管理規範與作業程序及事件應變暨營運持續相關管理規範與作業程序。

圖肆-11資安暨營運持續管理制度文件



資料來源：本研究整理

為測量資訊安全處及資訊處資訊安全管理及營運持續管理所選擇控制措施之有效性，擬定之管理指標依資安暨營運持續管理之規劃、建立、實施、運作、監督、查核、維護與改進各項作業控制項目一致，並涵蓋機密性、完整性及可用性三大面向。管理指標之新增、修訂及發佈須填寫「管理指標清單」，交由資訊安全小組核定，且依據各管理指標之衡量週期，定期量測並評估量測指標結果之有效性，每半年於管理審查會議中，針對管理指標之結果進行審查與檢討，以確認資訊安全處及資訊處資安暨營運持續管理目標之達成情形。

圖肆-12資安暨營運持續管理指標清單

管理系統管理目標	C	I	A	序號	量測指標	目標值	可量化方式	衡量週期	負責單位/科別
ISMS： 可靠(Reliability)。			V	1	維持DRP的12套核心業務相關系統正常運作時間之可使用率達99.90%以上。	99.90%	12套核心業務相關系統以「資安事故緊急通報及應變規範書定義之服務中斷時間填寫「資安事件處理紀錄單」統計。全年12套核心業務相關系統正常運作時間總和(分鐘) /核心業務相關系統全年總和(365x24x60x12)分鐘X100%=可使用率。	年	資訊處 基礎工程科
ISMS： 安全(Security)、可靠(Reliability)。 BCMS： 降低威脅事件導致資訊服務中斷之機率。	V		V	2	確保因資訊安全事故、資訊洩漏或其他安全事故，造成本行商業受損或營運服務暫停中斷達其常事件等級之情事，每年不得超過1次。	≦1	以「資安事故緊急通報及應變規範書」定義之服務中斷時間填寫「事件報告」統計，由管制科進行彙整，每年加以統計。	年	資訊處 管制科
ISMS： 穩定(Stability)、安全(Security)、可靠(Reliability)。	V	V	V	3	確保相關之資訊安全措施或規範符合國內及海外現行相關法令之要求(每年至少查核一次)，不得超過1項違反事件。	≦1	每年「遵守法令主管制度」查核之結果。	年	資訊處 規劃專業科 資訊安全處 資安管理科

資料來源：本研究整理

依據國際標準及法令法規要求，資訊處與資訊安全處每年定期辦理資安事故程序演練、資訊大樓災害應變桌面演練及資訊大樓人員疏散演練，演練情境說明如下：

一、資安事故程序演練

資安事故程序演練情境包含DDoS程序演練、ATM程序演練、勒索軟體及惡意程式重大資安事件情境演練、網頁應用服務系統之網頁安全進行進階防禦措施演練、SWIFT系統遭入侵攻擊程序演練，以及紐約分行資安事件演練，且演練內容應包含數位證據保全作業機制。

二、資訊大樓災害應變桌面演練

依據營運持續管理制度風險評鑑結果，選定高風險值或高衝擊值之情境，辦理資訊大樓災害應變桌面演練（如：風災與水災、重大傳染病、核子事故、地緣政治、資訊系統容量效能不足等情境）。

三、資訊大樓人員疏散演練

依據營運持續管理制度風險評鑑結果，選定高風險值或高衝擊值之情境，辦理資訊大樓人員疏散演練（如：火災、災害型地震等情境）。

辦理演練前皆會事先擬定演練計畫，確認演練的情境、演練範圍、演練日期、預期達成演練目標、各階段的參與人員與其角色職掌、演練所需文件等內容，並設計演練的腳本，於演練後進行檢討，留存相應的演練紀錄。資安事故程序演練過程會依循事故狀況發現與通報、事故判定、事故處理與資安通報、事故後續通報及事故檢討五個演練步驟如圖肆-13進行演練。

圖肆-13演練步驟

資料來源：本研究整理

資訊大樓災害應變桌面演練與資訊大樓人員疏散演練的演練成員皆係依演練情境所對應之自衛消防編組班別進行相應的演練。由於資訊大樓人員疏散演練主要以火災或災害型地震為演練主題，需要資訊處與資訊安全處全體同仁以及當日有到訪的廠商共同完成疏散，並到達指定的集合地點集合，完成人員清點作業後，才算完成演練，故演練前會先召開多場次的說明會，與所有同仁宣達演練注意事項、自衛消防編組成員的職掌，並與大樓中控室確認各階段廣播內容，以確保同仁於不同階段皆可依廣播指示做出相對應的演練動作。

而規劃逃生集合地點時，會先於資訊大樓周遭進行場勘，考量同仁逃生過程的安全性、集合地點的分流路線、地點空間大小等議題後，選出適當的集合地點，故綜上考量後，依資訊大樓的兩個逃生梯（A梯、B梯），將資訊大樓同仁應逃生路線進行分流如圖肆-14，並選定建興公園為逃生集合地點，且為使同仁可快速與自己單位同仁集合，完成人員清單作業，將公園劃分小區域，讓兩處同仁及廠商瞭解抵達公園後，集合區域的所在位置如圖肆-15。

圖肆-14資訊大樓疏散路線

資料來源：本研究整理

圖肆-15資訊大樓各單位於建興公園之集合位置

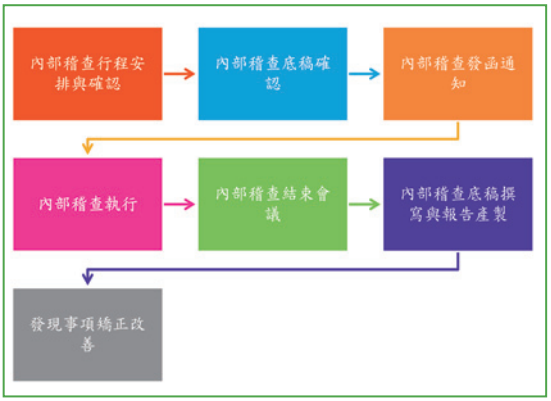
資料來源：本研究整理

肆、驗證審查

依據國際標準條文要求及資訊安全暨營運持續管理制度相關規範要求，資訊處與資訊安全處每半年會由持有資訊安全管理系統主導稽核員證照及營運持續管理系統主導稽核員證照的同仁進行內部稽查作業，安排內部稽查行程時，秉持稽核員不能查核自己自身業務、上下半年查核單位不得重複、同場次稽核員不可同單位等條件，完成當次的稽查行程安排，並確認是否有因當日必要會議、請假或差時/輪班上班等因素須調整稽查行程者，進行溝通確認。

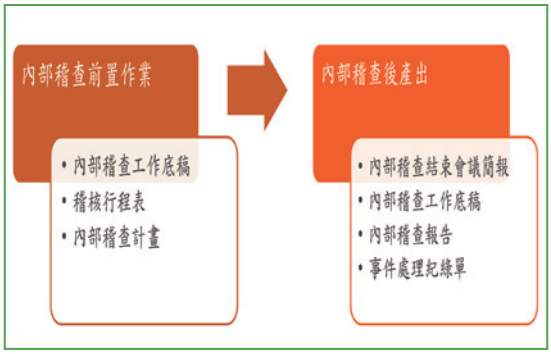
同時確認內部稽查工作底稿是否因應內外部規範變動進行調整，並產製「內部稽查計畫」闡明稽查範圍與項目，呈報資訊安全小組核定，完成相應工作後，正式發函通知受查單位於指定時程辦理內部稽查作業，稽核過程如有發現事項，應於內部稽查結束會議進行報告，與受查單位確認發現事項後，撰寫「內部稽查工作底稿」及「內部稽查報告」，缺失發生單位應針對異常原因於「事件處理紀錄單」上填寫矯正與預防措施，填具預計完成日期與實際完成日期，並由該當科負責人應對改善狀況進行改善對策有效性確認，並將「事件處理紀錄單」交於內部稽查單位覆核備查，內部稽查作業流程整理如下圖肆-16。

圖肆-16內部稽查作業流程



資料來源：本研究整理

圖肆-17內部稽查前後產製文件



資料來源：本研究整理

資訊處與資訊安全處每半年或不定期召開管理審查會議，以協助資訊安全處及資訊處資安暨營運持續管理制度之政策、目標、各階文件及適用性聲明書之審核，以及資訊安全及營運持續相關事項之研議，並確保矯正措施之有效運作，並於會議結束後產製會議紀錄留存備查，會議議題包含以下項目：

一、上次管理審查會議後結果之追蹤檢討。

二、可能影響資訊安全及營運持續管理系統之內、外部環境或議題之改變。

三、與資訊安全管理系統相關關注方之所需要及期望的變更。

四、資安暨營運持續管理風險評鑑與風險改善計畫結果。

五、營運持續管理前次風險評鑑中未闡述之風險或議題。

六、資安暨營運持續管理執行績效之回饋。

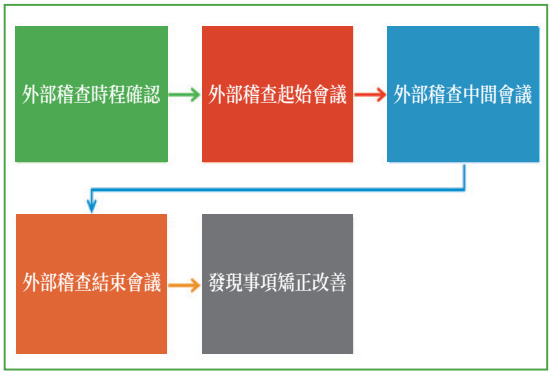
七、來自利害相關團體之回饋或要求事項。

八、從中斷事件，以及險成災害所得之經驗與改善措施。

九、其它持續改善之建議事項。

完成所有前述階段後，與第三方驗證機構確認外部稽核時程，通知受查單位應配合查核時間，提醒同仁受查注意事項，並事前確認內部作業是否皆已完成並符合內部規範，配合第三方驗證機構召開啟始會議，並於每天結束驗證召開中間會議，溝通當天的發現事項或待補資料，並於驗證查核最後一天召開結束會，與所有受機單位確認發現事項，並依驗證單位所提出之發現事項，填寫「事件處理紀錄單」進行改善並持續追蹤，外部稽查作業流程整理如下圖肆-18。

圖肆-18外部稽查作業流程



資料來源：本研究整理

另依據國際標準要求，取得證書後每年及每三年應進行驗證，以維持證書有效性。依英國標準協會（BSI）稽核發現定義及發現事項之後續作為（如表肆-1），稽核發現如為次要不符合事項，應於兩週內提出矯正措施計畫，並由稽核團隊進行審查；屬改善機會者，應依內部改善程序辦理矯正，並於下次複查時確認改善結果。

本行驗證審查頻率係每年進行兩次複審作業，每三年進行全面審查作業。自取得國際標準驗證迄今，本行驗證結果無主要不符合事項，少數為次要不符合事項，大多數為改善機會，且均依規於期限完成矯正，證書持續有效。

表肆-1英國標準協會稽核發現定義及發現事項之後續作為

稽核發現定義	說明	發現事項之後續作為
主要不符合事項	下列之情況可能被分類為重大的不符合： 如果對有效的流程控制是否到位，或者對產品或服務是否滿足特定的要求存有重大懷疑； 與同一要求或問題相關的大量次要不符合，可能會表現出系統性失效，因此構成重大不符合。	當次稽核將宣告管理系統或證書失效（可當場終止或繼續進行稽核），需再另外安排特別拜訪，現場確認改善之狀況符合要求。
次要不符合事項	不影響達成預期結果能力的不符合事項。	當次稽核將宣告建議發證或證書持續有效，但須在規定期限內提出矯正措施計畫（2 週內），由稽核團隊進行審查。
改善機會	表示該項目前已符合標準，如改善後，可達到更好的資訊安全水準。	非不符合事項，係稽核員在稽核中所作的事實陳述，並有客觀證據證實，指出弱點或潛在缺陷，若不改進就可能導致未來出現不符合。 改善機會事項將於下次複查時，確認改善結果。

資料來源：英國標準協會

第伍章　結論

資安國際標準已扮演金融業建構管理制度或資安控管的重要角色，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，探討目前主管機關的資安推動方針，以及資安國際標準演進與條文，可發現配合新興科技推陳出新，主管機關近期新增或修訂資安法規越來越頻繁，而國際標準組織也重新檢視既有的資安國際標準條文的合適性，近期也公告新版本的標準，推動既有導入資安國際標準的企業，可以運用最新的資安國際標準，重新檢視並精進資安管理制度。

同時，2024年5月銀行公會檢送的「金融機構國際資安管理標準驗證範圍」建議，提供金融業第一個新契機，已有進行國際標準驗證之銀行，正進行國際標準驗證範圍的重新檢視與評估，尚未導入國際資安管理標準驗證的銀行，依循銀行公會的驗證建議，選擇適合的驗證範圍，規劃導入資安國際標準的相關作業，而對於已導入國際資安管理標準驗證的金融業，目前正重新檢視現有驗證範圍是否符合銀行公會「部門」或「業務/流程」驗證範圍，並確認是否有其他非資訊相關單位有系統維運，評估是否將資訊系統集中資訊單位管理，或擴大驗證範圍，以符合主管機關的期許。

此外，因應2019年爆發的重大流行疾病Covid-19，作業韌性的議題被凸顯出來，故2024年5月銀行公會發布「金融機構資訊作業韌性規範」，也是金融業評估是否導入國際營運持續管理標準的第二個契機，營運持續管理系統強調企業應建立一套系統化的管理機制，以強化並管理組織內部資訊作業韌性相關作業，而銀行公會的規範內容也係參考國際標準營運持續管理系統的相關要求而制定，同時呼應金管會「金融資安行動方案」中「深化資安治理」鼓勵金融機構導入國際資安管理標準，及「精實金融韌性」鼓勵金融機構導入國際營運持續管理標準的方針。

因此，綜上所述，配合2024年主管機關的法令法規發展動向，目前金融業在資安治理與精實金融韌性方面，導入資安國際標準為現今重要的課題，透過本行導入並驗證國際標準資訊安全管理系統及營運持續管理系統的方法架構，可提供金融業在導入資安國際標準時的推動參考，以達到主管機關期望，另透過本次介紹得知國際標準組織所發展之國際標準之條文架構，已趨近依循PDCA循環運作模式，故雖本行已導入及驗證資訊安全管理系統及營運持續管理系統，但其各階段所要執行的工作，如組織建構、風險辨識、規範制定與調整及驗證審查等都是相同模式，故也可作為金融業導入雲端安全或人工智慧等其他國際標準之參考依據。

～完～

參考文獻

1. 王振鴻，2009年，全組織導入資訊安全管理系統的個案研究
2. 張正宏，2012年，探討銀行業ISOIEC 27001 2005資訊安全管理現況—以T 銀行為例
3. 蔡綺婷，2013年，檢政機關員工資訊安全認知之建立—從資訊安全管理系統的導入探討
4. 朱庭逸，2013年，營運持續管理成熟度之研究-以銀行業為例
5. 曹昱仁，2017年，探討醫療院所導入資訊安全管理系統對資訊安全成熟度影響之研究
6. 董鎬瑋，2017年，營建產業導入ISO 22301營運持續管理系統應用之研究
7. 蔡伶宜，2018年，基於ISO 27001：2013轉版建置資訊安全管理系統程序探討—以某大學為例
8. 金融監督管理委員會，2020年，金融資安行動方案1.0
9. 中華民國銀行商業同業公會全國聯合會，2020年，金融機構運用新興科技作業規範
10. 金融監督管理委員會，2021年，金融控股公司及銀行業內部控制及稽核制度實施辦法
11. 中華民國銀行商業同業公會全國聯合會，2021年，金融機構使用物聯網設備安全控管規範
12. 中華民國銀行商業同業公會全國聯合會，2021年，金融機構資通安全防護基準
13. 金融監督管理委員會，2022年，金融資安行動方案2.0

14. 中華民國銀行商業同業公會全國聯合會，2024年，金融機構資通系統與服務供應鏈風險管理規範
15. 中華民國銀行商業同業公會全國聯合會，2024年，金融機構運用人工智慧技術作業規範
16. 中華民國銀行商業同業公會全國聯合會，2024年，金融機構國際資安管理標準驗證範圍建議
17. 中華民國銀行商業同業公會全國聯合會，2024年，金融機構資訊作業韌性規範
18. 金融監督管理委員會，2024年，金融業運用人工智慧（AI）指引
19. 資訊安全管理系統，2022年，Information security, cybersecurity and privacy protection - Information security management systems - Requirements
20. 營運持續管理系統，2019年，Societal security - Business continuity management systems - Requirements
21. 金融監督管理委員會，2024年，https：//www.fsc.gov.tw/ch/index.jsp
22. 中華民國銀行商業同業公會全國聯合會，2024年，https：//www.ba.org.tw/Publicinformation/Index
23. 國際標準組織（ISO），2024年，https：//www.iso.org/home.html
24. 英國標準協會（BSI），2024年，https：//www.bsigroup.com/en-AU/
25. 世界經濟論壇，2024年，https：//www.weforum.org/
26. 數位發展部資通安全署，2024年，https：//moda.gov.tw/ACS/
27. ISO101，2024年，https：//iso101.com.tw/iso-introduction/
28. 風險社會與政策研究中心，2024年，https：//www.rsprc.ntu.edu.tw/zh-tw/m01-3/1863