（ISO 22301）」認證之重審／複審作業，四項制度均順利通過審查，維持國際標準證書之有效性，其中資訊安全管理制度（ISO 27001）配合金管會啟動「金融資安行動方案」計畫，亦已取得TAF驗證。

(2) 持續強化本行資訊安全之管控暨機敏性資料之防護，包括建置「網路閘道資料防護系統」、「網域工作站最高權限管理系統」、「電子郵件機敏性資料偵測防護系統」、「端點資料防護系統」、「資訊安全監控管理系統」及「資通安全威脅偵測管理系統」。

## 六、資通安全管理

### （一）資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源

1. 資通安全風險管理架構

（1）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 條規定，本行已指派副總經理擔任資通（訊）安全長，並設置資通安全處，專責辦理本行資通安全業務，負責規劃、監控及執行資通安全管理業務。

（2）設置「資訊安全推行小組」，由本行資通（訊）安全長擔任召集人，定期召開「電腦作業安全對策會報」（113 年度共召開 2 次），統籌全行資訊安全政策、計畫、資源調度等協調及研議事項。

（3）導入資訊安全管理相關制度，取得資訊安全管理制度（ISO 27001）、營運持續管理制度（ISO 22301）、個人資訊管理制度（BS 10012）等國際標準認證，每年通過公正第三方之驗證，持續維持本行國際標準證書之有效性，以符合國際資訊安全管理發展趨勢，並達國際管理水準之目標。

2. 資通安全政策

本行訂有資訊安全政策，闡明本行資訊安全目標、工作規劃、各角色應於資訊作業落實資安事項。本政策至少每年評估一次，以符合相關法令、技術及業務等最新發展現況。

3. 具體管理方案及投入資通安全管理之資源

（1）每年訂定及實施資通安全維護計畫，辦理核心及非核心業務盤點、導入資訊安全管理制度及通過外部機構驗證、資通系統分級及防護基準、業務持續運作演練、安全檢測、防範惡意電子郵件社交工程演練等作業。

（2）建構「多層次縱深防禦機制」，利用多層次的防禦技術來阻絕不同類型的攻擊，降低來自網際網路及內部網路的安全威脅風險，維護重要資產的機密性、完整性及可用性。

（3）建置資安威脅偵測及資安情資管理機制，及時識別並處理風險，以達防範未然之效。

(4) 定期執行弱點掃描、滲透測試及電腦系統資訊安全評估作業，藉以發現潛在之資訊安全威脅與弱點，此外，辦理紅隊演練，透過持續辦理上述各項資安檢測作業，以發掘本行可能之資安風險，強化本行資安防禦量能。

(5) 辦理企業外部資安風險評級，透過外部視角評估本行資安風險，以確認組織對外服務曝險程度，並就評級結果進行改善作業，以提升本行資訊安全。

(6) 賡續辦理電子郵件社交工程演練作業，演練樣本更貼近公務與生活，以提升同仁對資安防護之警覺心，降低電子郵件社交工程攻擊之風險。

(7) 每年透過教育訓練、內部會議、張貼公告等方式，向全體同仁宣導資通安全事件及資安趨勢相關資訊，並定期開設「資訊安全管理訓練班」、「資訊設備暨資安防護研習班」、「資訊系統安全基準與資安防護研習班」及「金融科技應用與資安防護研習班」等研習課程，深化同仁資安意識；另本行資訊安全專責人員每年需參與15小時以上之資訊安全專業課程訓練或職能訓練，以加強資安專業能力。

(8) 本行已訂有資安事件通報機制及制定相關緊急應變處理程序，並透過演練滾動式調整改善。如遭受重大資通安全事件，即由本行資通(訊)安全長召集跨部門之「資通安全事件應變小組(CSIRT)」緊急應變處理。

### (二) 113年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施

無。

## 七、勞資關係

### (一) 各項員工福利措施、退休制度與其實施情形，以及勞資間之協議與各項員工權益維護措施情形

本行為國營金融事業機構，亦屬適用勞動基準法之行業，員工勞動條件、各項福利措施，退撫制度等事項悉依勞動基準法及公務員等相關法令辦理，勞資權益均有明確規範保障。對員工所提具體主張訴求，行方除設置勞資會議定期進行協商溝通外，亦隨時透過員工座談或各級人事評議委員會等方式加強溝通，化解疑義，爭取共識，本行將在互信、互重前提下，謀取勞資雙方最大福祉。