台灣樂天信用卡(股)公司內部控制制度聲明書

謹代表台灣樂天信用卡股份有限公司聲明本公司於 110 年 1 月 1 日至 110 年12月31日確實遵循「信用卡業務機構內部控制及稽核制度應注意事項」，建立內部控制制度，實施風險管理，並由超然獨立之稽核部門執行查核，定期陳報董事會及監察人。經審慎評估，本年度各單位內部控制及法規遵循情形，除附表所列事項外，均能有效執行。

謹 致

金融監督管理委員會

聲明人

董事長：（簽章）

總經理：（簽章）

稽核主管：錢郁芬（簽章）

法令遵循主管：周祐存（簽章）

中　華　民　國　111　年　3　月　23　日

台灣樂天信用卡(股)公司內部控制制度應加強事項及改善計畫

（基準日：110 年 12 月 31 日）

應加強事項	改善措施	預定完成改善時間
內部查核檢查及資訊安全評估檢測意見，列入內部控制制度應改善事項：	擬具改善措施如下：	
一、未持續定期執行作業系統(Windows and Linux)安全參數檢核及規則設定維護程序，截至查核期間 110 年 12 月 31 日，尚未執行 110 年之定期檢視包括: 主機目錄或檔案之存取權限、密碼及帳戶鎖定原則、定期變更密碼、系統軌跡紀錄等之妥適性及完整性，有未依公司內部規定落實辦理定期控管檢視。	一、擬依規每季進行作業系統安全參數檢核及規則設定檢視，預計 111/03/18 前完成今年第一季確認作業，並取得系統部主管簽核。	一、已於 111 年 3 月 18 日完成改善
二、未執行資訊資產盤點風險評估，截至內部稽核查核期間 12 月，始依 109 (2020)年金融檢查之面請改善意見進行 2021 年下半年資訊資產盤點及風險評估作業，惟至 12 月 31 日尚未完成。	二、擬重新檢視並制訂系統資產分類盤點及風險評估準則，並於取得核准後，於 111 年 2 月底前完成資訊資產分類盤點及風險評估。	二、已於 111 年 2 月 28 日完成改善。
三、未落實執行員工上網行為管理作業，雖已建置員工上網行為管理準則，各部門使用網路權限依黑白名單管理。惟因負責人員有未盡職責依規執行檢視控管設定之妥適性，截至查核結束尚未辦理完成該項檢視。	三、擬重新檢視黑白名單之網路連結，擬定第一版的黑白名單使用之標準清單列表，將依據此列表進行控管，若有變動申請，經核准後始得變動列表內容，並留存申請及異動文件版本控管。	三、已於 111 年 3 月 9 日完成改善。
四、未執行網路弱點掃描及滲透測試作業，截至查核期間 12 月 31 日止，雖已執行 2021 Q1 ~ Q3(主機及設備、網路)網路弱點掃描，惟因所使用網路弱點掃描軟體授權期滿而續約作業尚未完成，無法匯出執行後存放於軟體資料庫之弱點掃描報告資料及發現問題之修補；滲透測試作業亦因此未依進度每年至少執行一次。。	四、擬進行掃描軟體續約後，依規每季執行一次弱點掃描(包括網站弱點掃描、伺服器主機弱點掃描、網路弱點掃描)，及每年執行一次滲透測試，已於 111 年 2 月 14 日完成測試，預計於 111(2022)/03/31 前將發現之問題修復完成。	四、已於 111 年 3 月 22 日完成改善。

五、未定期辦理 2021(110)年物聯網設備安全評估作業，截至查核期間 2021(110)年 12 月底，仍未依法規”金融機構使用物聯網設備安全控管規範第三條應建立物聯網設備管理清冊並至少每年更新一次，以識別設備用途、網段、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制” 執行 110 年度清冊管理及評估作業。	五、擬清查並更新所有 TRC 物聯網設備清單，重新進行物聯網設備評估，預計於 111 年 3 月底前完成改善。	五、持續辦理中，預計於 111 年 3 月底前完成改善。
六、未妥適之人力配置管理，人員異動頻繁，但未有完善之工作交接執行，雖設有人員職務代理工作表，但未落實施行，致現有人員轉職或離職之工作未能有人員銜接完成，或人員休假之工作未有代理人員確實代理執行，應改善之控管作業被延宕或無法依公司規定及時程完成。	六、擬招募符合工作需求人員以補足人力缺口，重新就人員工作分配、訓練計畫、工作交接控管、職務代理等項目落實控管，並每月與人員進行面談，確實了解人員工作狀態以降低人員流動頻率。	六、持續辦理中，預計於 111 年 4 月底前完成改善。
七、110(2021)年辦理第三季一般自行查核之系統資訊相關查核作業無法完成，系統資訊部因人力工作配置及管理欠妥，應有之管控工作未定期或即時辦理，截至 111(2022)年 2 月第三季一般自行查核結束，尚無法提供完整第三季自行查核資料，致系統資訊相關之自行查核作業無法完成。	七、擬補足人力缺口，妥適工作分配管理，依時程完成應有之控管作業，以配合 111 年辦理第二次自行查核(第一季一般查核)時，提供完整之查核資料。	七、持續辦理中，預計於 111 年 5 月底前完成改善。
八、宜加強預防資料傳輸外洩功能，內部網路存取雖已嚴格限制，惟部分系統仍為 Http 機制，需加強防止資料在傳輸中外洩之功能。	八、檢視計有 CTI、eJCIC 及 AutoFlow 等服務系統僅為公司內部使用，未連結外網之服務仍維持 Http 機制，擬就該等系統接洽廠商排定時程完成 SSL 憑證安裝，將 Http 強化為 Https，以加強防止資料在傳輸中外洩之功能。	九、持續辦理中，預計於 111 年 5 月底前完成改善。
九、宜建置 DDos 攻擊監控應變機制，目前官方網站伺服器委由外部供應商維運，經檢視 2021/06 之相關報告已具有入侵防護功能，惟尚需建立 DDoS 攻擊監控與事故應變機制，並每年進行程序演練。	九、擬接洽廠商就網站伺服器進行評估，並提供 DDoS 攻擊防禦內容適配程度方案，預計於 111(2022)/6/30 前導入 DDOS 攻擊防禦服務，完成監控及程序演練。	九、持續辦理中，預計於 111 年 6 月底前完成改善。