

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 111 年 1 月 1 日至 111 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，均能確實有效執行。

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 112 年 3 月 29 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：111 年 12 月 31 日)

應 加 強 事 項	改 善 措 施	預 定 完 成 改 善 時 間
受主管機關專案檢查及內部查核檢查意見，列入內部控制制度應改善事項：	擬具改善措施如下：	
一、 各業務單位負責公司日常風險之監控、衡量及評估等執行層面之事務，並定期提出風險管理相關報告，惟未設置專責風險控管單位或指定一管理單位替代。	已於 2022 年 12 月第三屆第二十九次董事會陳報成立風險管理單位，並就風險管理單位組織架構及職責功能，修訂敘明於組織規程，一併陳報 12 月董事會核准。 風險管理單位與各部門已依各業務性質檢視風險性質並建立完成風險管理監控機制，將負責每半年定期檢核評估整風險承擔能力，自 112 年開始辦理每半年完成評估檢視後，於董事會提出風險控管報告。	一、 已於 111/12/30 完成改善。
二、 就每半年進行一次之防火牆規則檢查作業，有未明確規範檢視防火牆規則重點原則項目，如：重要連線採 SSH (Secure Shell) 遠端登入協定、FTP 資料連接埠及遠端桌面協定(RDP) 等高風險通訊埠，不利作業遵循及有效控管網路存取安全。	系統部門將修改「SYS-P-009 網路安全管理程序準則-V5」明確規範檢視防火牆規則重點原則項目如：重要連線採 SSH (Secure Shell)遠端登入協定、FTP 資料連接埠及遠端桌面協定(RDP)等高風險通訊埠，以符合檢查作業之妥適性及需要性，並於 112 年上半年防火牆檢查作業時執行。	二、 持續辦理中，預計於 112/6/30 前完成。
三、 對所收到資安情資有未評估及處理並留存相關作業紀錄者，不利提昇網路資訊安全，如:110.7.21 之後各期 F-ISAC 情資週報及月報所通報之勒索軟體防護、DDOS 安全防護措施、中繼	系統部門將修改「SYS-S-038 接獲資安訊息警訊處理流程 V2」，將情資週報及月報所通報之勒索軟體防護、DDOS 安全防護措施、中繼站 IP 與網域及惡意檔案清單納入目前作業程序，並將	三、 持續辦理中，預計於 112/5/31 前完成。

<p>站 IP 與網域及惡意檔案清單等資安情資皆未有相關評估處理。</p>	<p>指定專人進行教育訓練後自 112 年 1 月 1 日開始執行，並留存相關評估處理紀錄。</p>	
<p>四、 建置防火牆 Fortigate 100D 作為無線網路 WiFi 連線網際網路之控制器，查有部分資安防護軟體已逾期，未評估是否應予更新或採其他相關補強措施，如：管理介面顯示韌體及一般更新（如：網際網路服務資料庫版本：2.00662）、入侵防禦系統模組（IPS 定義版本：6.00741）皆於 108.7.21 逾期，不利資安防護作業。</p>	<p>擬就其防火牆及資安防護軟體重新進行評估後予以更新及補強。</p>	<p>四、 持續辦理中，預計於 112/5/31 前完成。</p>
<p>五、 於 google play 及 Apple Store 等平台所發布之「樂天信用卡」行動應用程式 (APP) 有下列事項欠妥 (1) 未於「樂天信用卡」行動應用程式 (APP) 發布前檢視應用程式所需權限與所提供服務是否相當，且未於首次發布或權限變動前經資安、法遵及風控等單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務； (2) 對於裝置遭破解之偵測有欠完善，啟動應用程式時，尚未偵測行動裝置是否啟用開發工作之偵錯功能 (USB debugging) 之疑似遭破解方式 (3) 未於官網及下載頁面提示使用者安裝防護軟體。</p>	<p>(1) 就 iOS 及 Android APP 所需權限與所提供服務進行整理，並比對 109 年及 111 年列表評估所有權限(110 年無權限異動)，有部份權限異動，已重新進行說明並列表後送資安、法遵及風管(風險管理委員會)簽核完成； (2) 除偵測行動裝置疑似遭破解方式 (root 及 jailbreak) 外，並加入行動裝置是否啟用開發工作之偵錯功能 (USB debugging) 之疑似遭破方式； (3) 已將 109 年即完成之下載公告「使用者於行動裝置上安裝防護軟體」提示文字，移至樂天信用卡官網首頁明顯位置。</p>	<p>五、 已於 111/12/30 完成改善。</p>
<p>六、 於 google play 及 Apple Store 等平台所發布之「樂天信用卡」行動應用程式 (APP) 有下列事項欠妥</p>	<p>依所訂 APP 開發及維護、測試、上線流程，明定獨立之程式碼控管人員才有程式碼更動權限，任何異動皆須程式碼控管人員檢視異動原因，經主管</p>	<p>六、 持續辦理中，預計於 112/5/31 前完成。</p>

<p>尚未建立偽冒應用程式偵測、下架或告警機制，不利預先辨識偽冒 APP 及評估後續相關處理事宜。</p>	<p>核可始得異動，並需留存異動申請、檢視及核准文件另列重要程式碼檢查表，定期檢視重要相關程式碼有否異動，若有異動應找出原因並提出改善計畫以解決問題。</p>	
<p>七、 於 google play 及 Apple Store 等平台所發布之「樂天信用卡」行動應用程式 (APP) 有下列事項欠妥： (1) APP 檢測範圍尚未將 OWASP 公布之 Mobile APP Security Checklist L2 納入檢測，並由資安專責單位確認完成改善；(2) 開啟行動應用程式採用間接驗證生物特徵技術，由使用者端行動裝置驗證指紋及臉部辨識生物特徵，僅讀取身分確認機制驗證結果，惟未事先評估使用者身分驗證機制之有效性。</p>	<p>(1) 已將 OWASP 公布之 Moblie APP Security Checklist L2 項目納入 111 年度與鑒真實實驗室進行中之檢測項目，並已開始進行檢測； (2) 將於建立使用者開啟行動應用程式採用間接驗證生物特徵技術時，評估使用者身分驗證機制之有效性，以符合「金融機構辦理電子銀行業務安全控管作業基準」第 9 條第 1 項第 4 款第 2 目規定並提供相關證明文件。</p>	<p>七、 (1) 111 年鑒真實實驗室已在進行中，預計於 112/5/31 完成； (2) 就間接驗證生物特徵技術有效性評估已於 112/2/24 完成。</p>
<p>八、 辦理法令遵循自評作業，法令宣導內容及查核事項有(1)援引過時法令或已廢止函令；(2)對「法令遵循自評檢核表」所列「遵循事項條文(查核事項)」未妥為設計評估內容，致各單位對檢核表所列查核事項多未辦理查核；(3)對抽樣查核業務有未註明抽測項目、抽測件數及抽查個案名稱備查者，致法令遵循自行評估作業有流於形式等情事。</p>	<p>(1). 將修訂條文更新至 111 年下半年度法遵自評查核內容程序並加強法遵自評內容法規更新檢查作業以避免未援引最新版條文之情事發生， (2). 依各單位「業務相關性」及「查核必要性」等原則，重新檢視自評檢核表所列遵循事項條文(查核事項)內容， (3). 重新設計統一之標準檢核結果報告格式，報告並列示應檢測項目，檢核條文、抽查個案名稱及檢核結果…等。</p>	<p>八、 已於 111/12/30 完成改善。</p>
<p>九、 未妥適之人力配置管理</p>	<p>就系統部人員管理重新進行：</p>	<p>九、 持續辦理中，預計於 112/6/30 前完</p>

<p>系統部負責之經辦未能充分掌握工作職能之知識技術，主管亦未有追蹤管理，致有：(1)未完整(Windows and Linux)系統安全參數檢核及規則設定維護檢核程序、(2)未持續辦理資訊資產盤點風險評估、(3)未完成員工上網行為管理、(4)未完成網路弱點掃描及滲透測試作業、(5)未落實每月檢視追蹤委外廠商(DXC)之服務作業、(6)未辦理系統復原營運持續演練及演練報告以檢視是否符合可接受之復原時間目標(RTO)及資料復原點目標(RPO)等工作，多未能及時辦理完成。</p>	<p>1. 工作分配及訓練計畫</p> <ol style="list-style-type: none"> 1) 根據目前系統部之 SOP 及準則，列出所有工作項目 2) 評估現有人力及個人專業，調整工作分配及工作內容 3) 制定工作訓練計畫，提供新人及在職人員訓練 <p>2. 職務代理</p> <p>設定代理人及職務代理項目並制定人員代理管控，以利因輪班或休假之因素，工作仍能正常進行。</p>	<p>成。</p>
--	---	-----------