

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 109 年 1 月 1 日至 109 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 110 年 3 月 15 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：109 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列入內部控制制度應改善事項：	擬具改善措施如下：	
一、新卡戶之利率定價制度設計欠合理，致有利率定價集中於高利率(>=11.88%)級距情事。	一、已配合差別利率之年度定期檢視，重新分析檢視新卡戶評分基準表之各評分項目與風險配分，就評估結果修改新卡戶評分基準表，並於 110 年 2 月 28 日前實施結果檢驗，適用循環利率 11.88%以上者占比已從 89.5%調整為 74.4%。	一、已於 110 年 2 月底前完成改善。
二、應檢視「應收帳款減損評估作業準則」所訂預期信用損失有關前瞻性資訊參數因子訂定及違約損失率設定參數之回收率計算規範是否妥適。	二、已重新檢視並修訂「應收帳款減損評估作業準則」納入違約機率計算之前瞻性資訊參數調整原則及各年度回收率之計算規範，於 110 年 1 月底前依新調整之規範進行每年例行前瞻性資訊參數更新及回收率計算作業，並於 110 年 2 月 28 日前提交實施結果。	二、已於 110 年 2 月底前完成改善。
三、應依「金融機構辦理電腦系統資訊安全評估辦法」規定擬定資訊安全計畫提報董事會核定，依系統類別重要性由獨立於電腦系統開發與維護等相關部門或外部專業機構定期或分階段辦理資訊安全評估作業，提交報告由稽核單位進行缺失改善事項追蹤覆查；並每年至少一次辦理電子郵件之社交工程演練。	三、已接洽符合資格之專業機構，就各系統審視評估並研擬評估計畫，並依經董事會核准之評估計畫為專案辦理，並將電子郵件社交工程演練納入本次委託辦理事項，預估於 110/8/31 前完成並提交專案評估報告。	三、持續辦理中，預計於 110 年 8 月底前完成改善。

四、就行動裝置應用程式(APP)作業之開發及維護作業，應每年委由合格檢測實驗室辦理檢測，訂定相關管理規範及上架前安全檢測程序，應於發布前經法遵及風控單位同意系統權限，並於啟動時自動偵測是否遭破解(root)提示使用者，及建立 APP 問題回報及處理控管程序等節。	四、已洽尋合格之專業實驗室進行 APP 基本資安檢測，預計於 110/6/30 前完成；並訂於 110/2/28 前就各項作業特性，訂定相關權責及規範，調整需求開發管理系統之權責及流程控管機制；就已開啟之 11 項相關系統權限，評估與提供之服務相當，送由法遵及風控等單位同意，並修改程式偵測是否遭破解及是否於虛擬環境運行，顯示提示使用者相關風險之訊息；及應用程式 APP 問題回報及處理程序納入作業程序(SOP)，並就客戶反應之問題列表管理。	四、持續辦理中，預計於 110 年 6 月底前完成 APP 基本資安檢測，並已於 110 年 2 月底前完成各項作業及控管機制等相關作業。
五、開放式伺服器主機之最高權限使用者帳號應設簿登記控管，建立事前申請與事後覆核機制，對各項主機作業系統參數辦理定期檢核，定期清理伺服器系統檔案、評估主機目錄或檔案之存取權限等之妥適性。	五、將就各主機設立帳號權限使用管控流程表，載明各項變更事由及事前、事後紀錄留存；就 Linux 及 Windows 系統主機已著手於伺服器主機、系統檔案等各項設定之檢視並評估調整方式；並進行帳戶、密碼參數清查，於清查後進行檢視及調整安全設定，對未有防毒保護之伺服器安裝防毒軟體。預計於 110 年 3 月底前完成改善。	五、持續辦理中，預計於 110 年 3 月底前完成改善。
六、防火牆系統最高權限使用者帳號之權責應符合最小授權原則；對異動與已無流量之防火牆規則應評估其必要性與風險，檢視是否有開啟安全性風險之通訊或非必要通訊埠之規則等情事。	六、已完成就所有防火牆系統帳號及權限設定清查列表並訂定控管辦法，系統部成員僅預設唯讀權限，任何權限變更須依需求經申請核准始得變更設定，針對最高權限使用者帳號密碼，則由獨立單位保管人員保管密碼，以符合最小授權控管原則。 另已進行防火牆規則評估清查，就已無使用服務需求之防火牆安全性風險納入進行相關清理。	六、已於 109/11/30 完成改善。

七、緊急應變管理，未訂定各系統合理之復原時間目標(RTO)及系統復原點目標(RPO)、亦未針對資訊系統訂定每年定期演練之持續營運計畫。 就委由易思資訊公司管理之重要主機，尚未評估該受委託廠商對於系統維護之合格復原時間及異地備援機制之妥適性等情事。	七、於 110 年 2 月 28 日前已彙整各部門系統合理之復原時間目標(RTO)及系統復原點目標(RPO)，制訂本公司營運持續性計畫，並依計畫就維護業務營運之重要主機檢視評估，並制訂 110 年營運持續性實地演練計畫及執行演練報告。	七、已於 110/2/28 完成復原時間目標(RTO)及系統復原點目標(RPO)彙整、年度營運持續性計畫及實地演練。
八、資訊部門技術長除具有行動裝置應用程式開發人員權限，並綜理主機設備管理及資訊安全相關作業，且持有各主機高權限之系統使用帳號，不符職權分工及內部牽制原則。	八、已就系統開發流程各作業階段負責之角色定義職掌，區分各職掌工作內容、責任及帳號權限配置，述明職權分工管控，並於工作管理系統就現行系統部人員依此職掌分工設定完成不同角色權責以為職權分工牽制管控之落實。	八、已於 109/12/31 前完成系統部人力清點並以工作管理系統建立職務職掌分配完成。