日商三井住友銀行台北分行內部控制制度聲明書

SMBC Taipei Branch

Statement of Internal Control

謹代表日商三井住友銀行台北分行聲明本銀行於110年1月1日至110年12月31日確實遵循「金融控股公司及銀行業內部控制及稽核制度實施辦法」、外國銀行在臺分行適用「金融控股公司及銀行業內部控制及稽核制度實施辦法」說明對照表（*暨金融監督管理委員會備查之風險導向稽核及內部控制制度*）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，定期陳報總行、區域中心，並確實遵循前開辦法第三十八條第五款及第三十八條之一規定，與同業公會所定資訊安全自律規範。經審慎評估，本年度各單位內部控制、法規遵循制度及資訊安全整體執行情形，除附表所列事項外，均能確實有效執行。

On behalf of SMBC Taipei Branch, we herebycertify that from January 01 to December 31, 2021, the Bank has duly complied with the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries" , and the Comparison Table of "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries" for Foreign Bank Branches (*and the risk-based approach approved by the Financial Supervisory Commission*) in establishing the internal control system and implementing risk management procedures. The Bank has duly complied with the subparagraph 5, Article 38 and Article 38-1 of above Implementation Rules, and the information security self-disciplinary regulations specified by the Banks Association of the ROC. The Bank has been audited by independent auditors who submit reports to headquarter and regional office. After prudent evaluation, except for the items listed in the attached schedule, the Bank's each department has implemented effective

internal control, compliance systems and overall information security implementation during the year to which this statement relates.

謹致

金融監督管理委員會

The Statement is submitted to the Financial Supervisory Commission

聲明人

Statement by

在臺負責人：加藤芳郎 加藤芳郎 （簽章）

Responsible Person in Taiwan

臺灣區法令遵循主管：游雨鈴 游雨鈴 （簽章）

Head of Compliance in Taiwan

總稽核／或負責臺灣區稽核業務之主管：蒲贊如 蒲贊如 （簽章）

Auditor in charge of auditing on Taiwan branch(es)

負責臺灣區資訊安全主管：岩崎好晃 岩崎好晃 （簽章）

Officer in charge of information security on Taiwan branch(es)

中　　華　　民　　國　111　年　03　月　21　日

日商三井住友銀行台北分行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
1. (內部稽核缺失) **行銷資料之法律遵循檢查** a) 分行行銷資料之法遵檢查表未定期更新、未納入總行檢查表中適用分行之檢查要點。 b) 環球貿易融資部使用於與客戶開會的行銷資料，並未準備分行檢查表供法務部檢查，再者，環球貿易融資部並未留存當時使用之行銷資料供稽核檢查。	a) 分行將重新評估分行檢查表，以確保總行檢查表當中適用之要求有納入分行檢查表。分行檢查表將併入台北分行法遵手冊，每年定期審核。 b) 環球貿易融資部已將有缺失的文件與相對應之分行檢查表送交法務部門檢查完成。環球貿易融資部將保存相關資料。	a) 項目之分行檢查表評估，預計於2022年2月28日以前完成；台北分行法遵手冊修改預計於2022年4月30日完成。 b) 已於2021年11月30日完成。
2. (內部稽核缺失) **授信業務之相關法規遵循** 應加強分行對於授信業務檢核的控管機制。經查核發現以下缺失： a) 風力發電相關的授信條件已變更，但敏感性分析並未納入最新條件與購電量情境。 b) 若干相關的法規要求未納入授信檢核表中；兩份授信申請案漏未檢附檢核表。 惟本次稽核未發現上述抽樣案件有違反法規之事實。	a) 風險管理部將提醒業務人員且更新檢核表。業務人員會準備檢核表以確認相關要求有涵蓋在敏感性分析中，或是確實留存不需敏感性分析之理由，風險管理部會確認檢核表與授信申請的一致性。 b) 風險管理部會更新檢核表，研討會已於2021年11月舉辦。 c) 業務部門人員及外匯資金部人員應負責執行檢核表確認，並再交由風險管理部檢查檢核表。	已於2022年1月31日完成。
3. (內部稽核缺失) **「客戶交易指示自動化傳輸服務（以下簡稱SMAR&TS）」客戶文件控管應加強** 本次進行抽樣檢查，發現以下缺失： a) SMAR&TS相關合約遺失，未留存於文件清單中及金庫內；本次遺失之合約已由客戶重新簽署，銀行並未承受損失。 b) 定期維護的文件清單內容不正確。	a) 台北分行已與客戶溝通並重新簽署SMAR&TS合約。 b) 台北分行正規畫改善計畫，檢視目前的SMAR&TS金庫內文件，並比對實際提供的客戶服務；主要措施將包括： i.檢討過後，將簽報內部簽呈，內容涵蓋：歸檔規則、遞送規則、年度盤點範圍。 ii.在上述簽呈被核准後，將進行SMAR&TS服務紀錄及文件清單的比對，SMAR&TS文件將被重新檢視。	a) 已於2021年12月15日完成。 b)i 預計於2022年3月11日完成。 b)ii 預計於2022年9月30前完成。

4. (內部稽核缺失) **對於作業系統層級之特權使用者帳號(Privileged User IDs)之管控，應予強化** 經查核發現以下缺失： a) 預防性控制措施：未有效控管執行特權使用者帳號之取得。 b) 預防性控制措施：未遵循特權使用者帳號之緊急登入程序。 c) 預防性控制措施：未及時更新高特權帳號控管簿之資訊。 d) 偵測性控制措施：對於特權使用者帳號缺乏足夠監控、範圍不足亦無建立紀錄簿。	分行將會採取兩階段方法。 特權帳號將會被區分為高特權帳號及一般特權作業用帳號，且應有相對應的管控方式： 於第一階段，為減低密碼洩漏及特權帳號未授權使用之風險，將採取立即性風險降低措施。第一階段將會於特權帳號管理之新控制架構正式建立前完成。 於第二階段，將會修訂特權帳號管控架構。若實際管控作業與內規不符且有困難執行，將提出說明並以例外申請方式尋求系統風險監督部門之核准。 ai) 管理所有已登記系統帳號之使用。 aii)將對於syop0344升級權限進行相關作業軌跡之調查，並將報告呈送分行管理階層。 aiii) 對所有相關人員及主管舉辦特權管理相關之教育訓練。 aiv) 進行以下流程，以正式適用符合內部規定之控制架構： ➢ 對於特權帳號之作業軌跡的流程與架構審查。 ➢ 特權帳號管理之流程(包含使用者權限之申請核准、定期密碼變更及使用監督之提供、取消、新增、修改及刪除)。 ➢ 每年將舉辦之教育訓練。 b) 修正系統帳號緊急使用之流程(包含申請核准、登入活動審查、密碼變更、紀錄保存及活動檢查)； c) 執行特權帳號之庫存審查。 d) 加強密碼信封使用紀錄本，並納入帳號使用資訊。 e) 每半年檢查帳號控制分類、系統帳號控管簿及伺服器所蒐集之帳號名單的一致性。	ai) 2022年1月31日已改善 aii) 2021年12月10日已改善 aiii) 2021年12月31日已改善 aiv) 預計於2022年5月31日前完成 b) 預計於2022年5月31日前完成 c) 2022年2月28日已改善 d) 2022年1月31日已改善 e) 預計於2022年5月31日前完成
5. (內部稽核缺失) **對於系統開發及系統變更之控制應**	分行會以風險降低方法(risk mitigation approaches)強化現行	a), b) 已於2022年1月28日完成 c) 預計於2022年3月25日完成

當強化 本次抽樣系統開發及系統變更案件，發現以下缺失： a) 機器人作業流程(Robotic Process Automation, 以下簡稱RPA)之系統開發，其測試筆數不足。資訊系統部(Information Technology Department, 以下簡稱ITD)未就系統測試之影響，向系統風險監督部門(System Risk Supervisory Department)進行諮詢。 b) ITD未保留系統測試(使用者測試除外)及建置後覆查之文件。此外，分行並未全面評估系統上線之影響。	系統開發方法： a) 關於測試方法： ➢ 評估未來業務成長量後，壓力測試會以足夠的個數執行。 ➢ 於使用者測試(UAT)之前，確認程式品質及相關系統缺失，且建置後覆查會以制式文件方式保留以供追蹤。 關於RPA之測試安排 於系統測試之前，會實施相關風險評估。若諮詢總行部門後，得知該測試會在測試環境下影響生產數據(production data)，會參考相關全球指引使用測試數據(test data)，並在完成後移除該測試資訊。 b) 關於建置後覆查 將會以文件形式保留所有系統狀況之評估結果。於蒐集所有使用者部門之意見且完成建置後覆查制式文件後，將會以郵件將系統上線資訊通知相關人員。 c) 分行作業手冊應依上述措施，予以更新。	
6. (內部稽核缺失) **復原時間目標(RTO)與復原點目標(RPO)之管理應加強** 檢視分行所使用系統之復原時間目標(RTO)與復原點目標(RPO)，發現以下缺失： a) 系統的RTOs和RPOs在不同手冊間規定不一致。 b) 分行未確認總行報告未涵蓋之系統，其RTOs和RPOs也能符合分行所設目標。	a) 企劃部會修改分行BCP手冊並設定核心業務的RTO，該手冊之系統清單將只會留下核心業務系統；企劃部會負責確保有經手核心業務之部門的BCP 手冊的系統，都有涵蓋在分行層級BCP手冊的系統清單內。 b) 企劃部會追蹤資訊部的復原時間/復原點和分行的RTO/RPO間的不一致，若有不一致，企劃部會記錄該部門可否接受此不一致，或額外的修正措施。前述措施至少每年執行一次。	預計於2022年3月31日完成
7. (外部查核缺失) 對員工使用電子郵件傳遞涉及個人資料之控管機制有欠周延，未以系統方式篩檢，無法事先防範個人資料之安全控管，並進行個人資料之有效保護，不利落實個人資料保護作業。	有關採用系統篩檢電子郵件加強個人資料保護之事，台北分行已與日本總行商討導入電子郵件個人資料篩檢系統(DLP)之可行性及時程。總行正研擬亞太區行內電子郵件安全管控（含個資篩檢系統）改善計畫，預計2023年底前完成導入。台北分行會持續密切與總	預計於2023年12月31日前完成