兆豐金融控股股份有限公司
內部控制制度聲明書

謹代表兆豐金融控股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「金融控股公司及銀行業內部控制及稽核制度實施辦法」，建立內部控制制度，實施風險管理，由超然獨立之稽核部門執行查核，定期陳報董事會及審計委員會。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；本聲明書將成為本公司年報及公開說明書之主要內容，並對外公開。上述公開之內容如有虛偽、隱匿等不法情事，將涉及證券交易法第二十條、第三十二條、第一百七十一條及第一百七十四條等之法律責任。

謹 致

金融監督管理委員會

聲明人

董事長：張兆順

總經理：胡光華

總稽核：蔡瑞瑛

總機構法令遵循主管：鄔翌琳

中　華　民　國　111　年　3　月　15　日

兆豐金融控股股份有限公司
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
兆豐銀行		
一、辦理授信業務核貸時之徵授信作業及貸後管理等缺失。	(一) 對徵信人員加強宣導善用各類資料庫，以利分析產業景氣及產品價格波動情形，並應參酌借戶過往營運實績及同業營運情形，評估其未來償還計畫之可行性，詳實反映借戶中長期償債能力。 (二) 彙總各項授信函文規範及法令規定制定「辦理授信業務補充注意事項」，提供辦理授信業務人員注意遵循。 (三) 對聯貸小組同仁加強宣導辦理類此授信聯貸案規劃應注意事項，降低承做風險；另於授信覆審及自行查核項目加強檢視承諾條件執行情形。 (四) 建立報表加強對聯貸變更條件案之控管，並於 e-loan 授信系統建置「貸後管理追蹤平台」，強化貸後管理機制。 (五) 針對授信集中產業、特殊產業或景氣大幅波動等產業，審慎評估情境及參數設定辦理壓力測試，以利適時採取因應措施。	已依改善措施完成改善。
二、辦理房屋貸款業務未能完善建立內部控制制度及未確實執行內部控制制度之情事。	(一) 加強貸前徵審及檢核作業： 1. 以系統檢核可量化之人頭戶態樣，加強消金徵審作業之教育訓練。 2. 針對相同進件來源之房貸案，建立輪流分派辦理之控管機制。 3. 建立地政士黑名單查詢比對機制，審慎辦理高風險代書引介案件。 (二) 強化擔保品鑑估作業控管： 1. 建置不動產「自動化執行同	已依改善措施完成改善。

應加強事項	改善措施	預定完成改善時間
	質性物件訪價查詢系統」，並修訂營業單位估價授權及應移送總處單位覆核之標準。 2. 以系統控管估價人員及授信簽報人員不得為同一人。 (三) 加強貸後管理追蹤作業： 1. 強化「國內消金警示戶明細表」檢核管理功能。 2. 增訂「不動產實價登錄回查機制」之控管措施。 3. 增訂「房貸動撥後6個月內需調閱擔保品謄本」之貸後追蹤事項。 4. 建立以風險為本之消金覆審制度。 5. 加強覆查分行自行查核之落實情形。 (四) 其他管控措施： 1. 增訂行員資金流向異常疑似舞弊或違法違規情事之後續調查及陳報辦法。 2. 針對查有疑似人頭戶缺失態樣且不具合理性之個案加強追蹤控管。	
三、未落實辦理ATM補鈔、排障及盤點程序與委外保全運送現金作業流程之管控。	(一) 辦理ATM補鈔及收取存款作業，確實由ATM主管及經辦二人全程會同辦理，並禁止以差額加鈔方式補鈔。 (二) 辦理ATM排障或補鈔作業時，主管須先查證ATM機台於系統之狀態顯示，確認實際情況後再會同開啟ATM金庫，並列印查詢紀錄留存備查。 (三) 加強二道防線督導力道，新增辦理實地抽點分行ATM庫存現金，及不定期抽查分行ATM補鈔及排障作業之監視錄影紀錄。 (四) 委外保全收回現金確實交由銀行主管及經辦人員於錄影系統	除第(八)項加強ATM監控系統檢核功能及第(九)項建置分行錄影系統傳輸即時監控，預計111年3月底前完成外，其餘各項已依改善措施完成改善。

應加強事項	改善措施	預定完成改善時間
	下共同拆封點收及雙簽，並由主管確認當日委由保全收取之款項已確實入帳。 (五) 列舉常見交友軟體投資詐騙手法，對行員加強宣導並注意防範。 (六) 銀行內部詐欺防制系統新增行員國內異常交易偵測風險模型。 (七) 調高自行查核執行情形之考核比重，及增訂未落實辦理之懲處機制，督促營業單位確實辦理自行查核作業。 (八) ATM 監控管理系統增加餘鈔異常之檢核功能，並產製 ATM 金庫開關紀錄報表供分行加強檢視。 (九) 建置分行錄影系統傳輸，俾利總處業管單位不定時以數位化監看鏡頭方式抽點監控，掌握分行 ATM 補鈔作業即時訊息。	
四、辦理保險商品招攬作業，未遵循不得有以其他名目收取報酬等不合營業常規交易之規定。	(一) 已清查類似情形案件，終止與該等保險公司之保戶再行銷合作方案。 (二) 按月蒐集並檢視主管機關對同業之裁罰案件及法規異動情形，確認相關內控措施符合規定，以防範類似缺失情事再次發生。	已依改善措施完成改善。
五、銀行「行動裝置管理要點」針對自攜裝置之定義範圍相較不足，且未就公司配發及員工自攜裝置予以區隔，對允許使用之自攜裝置類型、作業系統、應用系統或服務亦未予以詳列。	依據「運用新興科技作業準則」之自攜裝置適用範圍修訂「行動裝置管理要點」，將公司配發及員工自攜裝置予以區隔，並詳列對允許使用之自攜裝置類型(如手機、平板及筆電等)、作業系統、應用系統或服務。	預計 111 年 3 月底前完成改善。

應加強事項	改善措施	預定完成改善時間
兆豐產險 金管會 109 年度辦理電子商務系統專案檢查，核處新臺幣 120 萬元及 2 項糾正：		
一、資訊安全專責單位應配置適當人力資源及設備，負責規劃、監控及執行資訊安全管理作業，惟本次檢查發現有系統弱點修補管控欠妥，造成多項嚴重風險未能及時修補、防火牆規則設定審核欠落實，造成設定寬鬆，及未建立重要日誌監控及告警機制等資安防護作業欠妥事項，顯示資安專責單位未能妥適行使職權及有效發揮監督功能，核有未落實執行保險法之規定，核處新台幣 60 萬元罰鍰。	(一) 111 年 1 月 3 日已招募新進資訊安全專責人員，並將委外聘請資安顧問服務，以加強資安控管。 (二) 已持續採購系統，增加科技輔助，以加強資訊系統維運管理。 (三) 已持續加強內外、部法規遵循檢視，並建置「應用系統開發與維護管理檢查表」，以利各單位遵循。 (四) 已委由資安監控中心協助辦理每天 24 小時資安監控服務。	委外聘請資安顧問服務預計於 111 年 3 月底完成外，其餘均已依改善措施完成改善。
二、所訂「應用系統開發與維護管理作業須知」未明訂新系統開發應辦理技術與安全性可行性評估，以致辦理 B2B 平台整合全險種系統(含團險、火險、車險)及意外險核心系統委外開發，有對其採用之容器(Container)技術公司內部技術管控能力不足、未取得程式原始碼卻未辦理風險評估及擬定配套補償措施、未建置網頁程式及檔案防置換或防竄改機制等缺失，不利資訊安全；另提供保經代使用之應用系統，其使用者登入密碼原則設定與所訂「應用系統開發與維護管理作業須知」不符，且使用者帳號清查欠完整，查有未落實執行內部控制制度情事，核處新台幣 60 萬元罰鍰。	(一) 已於 110 年 3 月完成容器管理平台移轉作業，並已加強技術管控能力。 (二) 已訂定相關規範要求未取得程式原始碼之系統應辦理風險評估及擬定配套補償措施。 (三) 已修正相關系統之密碼原則以符合「應用系統開發與維護管理作業須知」。 (四) 已辦理相關系統帳號清查並新增檢核機制。 (五) 將建置對外服務之網頁應用系統網頁程式及檔案防置換或防竄改機制。	(一)~(四)已依改善措施完成改善。 (五)網頁程式及檔案防置換或防竄改機制，已於 111 年 1 月底更新。
三、就資訊安全管理，有專責單	(一) 109 年度整體資訊安全執行情	除第(七)項弱點掃

應加強事項	改善措施	預定完成改善時間
位提報董事會內容欠缺整體資安防護及緊急應變辦理情形、未制定憑證(金鑰)管理規範並請廠商落實檢視是否符合內控文件之要求、未建立容器化伺服器叢聚環境(cluster)之安全管理規範及相關作業程序、未訂定重要性主機監控管理規範及作業系統(資料庫)修補與安全性更新之標準作業程序、未建立特權帳號管控規範並清查納管、未訂定網頁應用程式防火牆管理規範、未積極辦理弱點掃描結果所發現弱點之後續修補作業並追蹤管理、對滲透測試結果所發現弱點之後續修補作業欠妥等缺失，不利資訊安全，經核有礙健全經營之虞，爰依保險法規定予以糾正。	形已依規定納入相關項目，並提報110年1月27日第23屆董事會第17次會議在案。 (二) 已修正憑證管理規範並與廠商組成之檢測小組、顧問確認電腦系統資訊安全評估報告之正確性。 (三) 已訂定應用程式容器化管理作業規範及相關作業程序。 (四) 已訂定重要性主機監控管理規範及作業系統(資料庫)修補與安全性更新之標準作業程序。 (五) 已建立特權帳號管控規範並清查納管。 (六) 已訂定網頁應用程式防火牆管理規範。 (七) 已持續辦理弱點掃描，修補後續弱點之作業，並追蹤管理。 (八) 已完成滲透測試並修補後續弱點之作業。	描結果之後續修補作業預計於111年6月底完成外，其餘均已依改善措施完成改善。
四、就委外廠商管理，雖訂有通案適用之「緊急應變計畫須知」，惟未能於個別委外契約中連結該須知之規定，要求廠商落實相關緊急應變計畫，無法有效降低服務中斷風險；另就未取得程式原始碼之系統，雖於契約約定風險發生之補償措施，惟未積極強化委外作業期間之風險管控，不利資訊安全，經核有礙健全經營之虞，爰依保險法規定予以糾正。	(一) 為維護保戶權益及服務不中斷，已依主管機關要求訂定電子保單認存證平台、簡訊發送系統平台及電子商務交易機制服務平台緊急應變計畫，若個別服務平台發生緊急事件時，則立即啟動緊急應變措施。 (二) 已修訂規範：納入未取得程式原始碼之資訊系統必須辦理風險評估及擬定相關配套補償措施之規定。	已依改善措施完成改善。

應加強事項	改善措施	預定完成改善時間
兆豐證券 一、辦理客戶與忠孝分公司業務人員之投資糾紛案件，有未落實執行內部控制制度，核已違反證券商管理規則規定，遭金管會核予糾正及核處新臺幣24萬元罰鍰，以及命令公司解除營業員李○軒職務，缺失摘述如下： (一)李姓營業員有誘騙客戶將投資股款匯至其個人帳戶、或未經受託而賣出客戶帳上股票及以偽造之股票庫存截圖欺騙客戶等情事，違反證券商負責人與業務人員管理規則第18條第1項、第2項第10款及第11款規定。 (二)忠孝分公司經理人及櫃檯主管對客戶之陳情，經調查發現李員涉有違反法令情事時，未即時主動通報，違反內部控制制度標準規範CA-11420「對客戶申訴或檢舉案件之處理作業」(六)規定。	就違規事項已採行以下措施： (一) 業於109年6月對李員予以免職處分，櫃檯主管核處三次警告，分公司經理人核處乙次警告。 (二) 已陸續採取下列配套措施： 1.主管落實走動式管理，加強關懷員工，善盡督導管理責任。 2.營業據點經理人於營業時間須在營業櫃檯內辦公，以觀察業務人員有無異常行為，俾利落實走動式管理。 3.營業據點實施善意關懷客戶訪談作業，使主管藉此了解營業員與客戶往來情形有無異常行為。 4.如發現業務人員與客戶往來異常行為，將透過金控母公司洽請兆豐銀行提供金流或其他資料以協助公司防堵營業員不正行為機制，進一步了解業務人員資金往來情形，俾利強化業務人員管控措施。	已依改善措施完成改善。
二、辦理資訊作業，有下列事項欠妥： (一)未建置妥適網路連線監控及防護機制，不利資訊安全，如： 1.未建立資通安全事件威脅偵測管理平台。 2.未建置防火牆控管內	1.將建置資通安全事件威脅偵測管理平台(SOC)。 2.將建置實體防火牆設備，用以取代	1.預計111年12月底完成。 2.預計111年9月底完成。

應加強事項	改善措施	預定完成改善時間
部伺服器區、分公司及總公司 OA 網段間之存取。	現行網段群組區隔管控方式。	
3.置於分公司內部網路之精誠報價系統相關設備，有以專線與外部廠商直接連線取得報價資訊，未建立妥適防護機制。	3.將建置實體防火牆設備，以強化現行與外部廠商專線連結方式。	3.預計 111 年 9 月底完成。
(二)109 年及 110 年委外辦理滲透測試，有下列事項欠妥，如：		
1.未明訂滲透測試受託機構及執行人員應具備資格，不利確保作業品質。	1.將於 111 年與資訊廠商簽訂合約前，除要求具備相關能力技術資格及證明，並於簽訂合約時，納入相關資格條文並要求檢附相關證明文件做為合約附件。	1.預訂 111 年 3 月底簽訂完成。
2.僅將兆豐 e 網通納入滲透測試範圍，其他連線至 Internet 之對外服務系統則未納入。	2.爾後每年(至少一次)辦理滲透測試作業時，納入所有正式對外服務系統，以完整評估對外服務資訊安全。	2.預計 111 年 6 月底完成。
3.發現對外網站存有資安弱點。	3.爾後辦理官網弱點掃描作業，除委由現行資訊廠商執行弱點掃描作業外，再增加另一資訊廠商並採用不同掃描工具，以減少未發現之弱點。	3.預計 111 年 6 月底完成。
(三)辦理個人資料安全維護作業，有下列事項欠妥，如：		
1.尚未建立疑似滴漏式資料外洩告警資訊及後續追蹤機制。	1.已委請資訊廠商協助建立滴漏式規則及告警追蹤機制。	1.預計 111 年 3 月底完成。
2.對寫出檔案至 USB 而觸發過濾各級風險控管規則者，未由觸發人員填寫理由並建立定期覆核機制。	2.已委請資訊廠商協助設定，對寫出檔案至 USB 裝置時，觸發人員須填寫理由，並建立覆核機制之功能。	2.預計 111 年 3 月底完成。

應加強事項	改善措施	預定完成改善時間
3.使用個人手機或其他行動裝置收取公司電子郵件，尚未建立過濾阻擋或其他控管機制。	3. 將依檢查意見，規劃建置相關控管系統。	3.預計111年6月底完成。
4.使用公司內部網路芳鄰功能，尚未制訂相關管理規範與控管措施，並定期辦理清查。	4. 已委請資訊廠商協助或尋求其他控管產品，以關閉個人電腦網路芳鄰功能。	4.預計111年3月底完成。
(四)網路下單系統及行動應用程式（APP）引用第三方函式庫，有未辦理風險評估即逕予引用，且未建立前揭函式庫清單及版本管控程序。	將請委外廠商提供所引用第三方函式庫清單及版本，另評估相關控管資訊產品，以便對前述清單及版本進行風險評估及後續改善作業，並制定相關管理規範。	預計111年6月底完成。
三、部分資訊系統（例如理財通），係使用微軟已不支援安全性更新之作業系統或資料庫系統，致未能定期修補相關安全漏洞。	該系統主機預定於111年3月底前完成系統更換作業。	預計111年3月底完成。