

富邦綜合證券股份有限公司
內部控制制度聲明書

日期：115年3月11日

本公司民國114年度之內部控制制度，依據自行評估的結果，謹聲明如下：

- 一、本公司確知建立、實施和維護內部控制制度係本公司董事會及經理人之責任，本公司業已建立此一制度。其目的係在對營運之效果及效率(含獲利、績效及保障資產安全等)、報導具可靠性、及時性、透明性及符合相關規範暨相關法令規章之遵循等目標的達成，提供合理的確保。
- 二、內部控制制度有其先天限制，不論設計如何完善，有效之內部控制制度亦僅能對上述三項目標之達成提供合理的確保；而且，由於環境、情況之改變，內部控制制度之有效性可能隨之改變。惟本公司之內部控制制度設有自我監督之機制，缺失一經辨認，本公司即採取更正之行動。
- 三、本公司係依據「證券暨期貨市場各服務事業建立內部控制制度處理準則」(以下簡稱「處理準則」)規定之內部控制制度有效性之判斷項目，判斷內部控制制度之設計及執行是否有效。該「處理準則」所採用之內部控制制度判斷項目，係為依管理控制之過程，將內部控制制度劃分為五個組成要素：1. 控制環境，2. 風險評估，3. 控制作業，4. 資訊與溝通，及5. 監督作業。每個組成要素又包括若干項目。前述項目請參見「處理準則」之規定。
- 四、本公司業已採用上述內部控制制度判斷項目，評估內部控制制度之設計及執行的有效性。
- 五、本公司基於前項評估結果，認為本公司於民國114年12月31日的內部控制制度(含對子公司之監督與管理、資訊安全整體執行情形)，包括瞭解營運之效果及效率目標達成之程度、報導係屬可靠、及時、透明及符合相關規範暨相關法令規章之遵循有關的內部控制制度等之設計及執行，除附件所列事項外，係屬有效，其能合理確保上述目標之達成。
- 六、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及期貨交易法第一百一十五條等之法律責任。
- 七、本聲明書業經本公司民國115年3月11日董事會通過，出席董事9人中，有0人持反對意見，餘均同意本聲明書之內容，併此聲明。

富邦綜合證券股份有限公司

董事長：程明乾 簽章

總經理：鄧永龍 簽章

稽核主管：林弘毅 簽章

資訊安全長：鍾學暉 簽章

(基準日 114年12月31日)

應 加 強 事 項	改 善 措 施	預 定 完 成 改 善 時 間
<p>一、金管會檢查局對公司進行「資通安全專案檢查」，有下列缺失情事：</p> <p>(一)辦理防火牆及網路設備管理作業，有部分防火牆未納入檢核之情事，以及防火牆重要安全參數檢視作業欠落實。</p> <p>(二)提供下單服務之行動應用系統更新上架前，有未執行源碼掃描，以及行動應用程式上架前有未就重大更新項目辦理OWASP MOBILE TOP 10檢測。</p> <p>(三)辦理委外開發程式管理，由供應商以電子郵件交付或自委外廠商網站下載後辦理上線作業，尚未建立完整性及來源辨識性驗證機制，以及委外開發系統更新上架前，委外廠商有未提供源碼檢測或弱點掃描等安全性檢測證明等情事。</p> <p>以上金管會於114.10.20對公司予以糾正併核處新臺幣30萬元罰鍰。</p>	<p>(一)</p> <ol style="list-style-type: none"> 1. 修訂「證券防火牆設定異動管理程序」，將各分公司與外部資訊源公司間之防火牆項目納入年度安全規則檢視作業。 2. 依據「網路設備上限檢核作業」所訂定之防火牆重要參數設定標準，重新檢視所有防火牆之安全參數設定，並產出檢視報告，檢視結果將簽報權責主管，以落實每年定期檢視之規定。 <p>(二)</p> <ol style="list-style-type: none"> 1. 本公司將修訂「證券行動應用程式上線階段標準作業程序」，將「源碼掃描」納入核心系統行動應用程式更新之必備流程，並明確定義執行時機與責任單位。 2. 針對無法取得原始程式碼之行動應用程式，將與委外廠商簽訂「源碼掃描安全檢測報告」合約，於每次更新上架前由廠商依約提供檢測報告，並由本公司資訊安全單位進行審查後，始得辦理更新上架作業。 3. 富邦 e+ APP 將導入 Fortify 源碼掃描工具進行安全檢測，檢測項目涵蓋 OWASP MOBILE TOP 10，以補強自動化檢測之完整性。 <p>(三)</p> <ol style="list-style-type: none"> 1. 委外開發程式之完整性驗證強化措施： <ol style="list-style-type: none"> (1) 委外廠商交付程式時，須一併提供程式檔案之檢核碼 (Checksum)，由本公司進行比對，確認檔案完整性後方可辦理上線。 (2) 若委由第三方驗證公司執行黑箱檢測，則由本公司另行提供檔案之檢核碼予第三方驗證公司，並要求其下載後進行檢核碼比對，確認檔案完整性後再執行資安檢測作業。上述作業方式將納入標準作業程序 (SOP) 以資遵循。 2. 委外開發系統安全性檢測強化措施： <ol style="list-style-type: none"> (1) 全面盤點委外開發系統是否提供安全性檢測證明，並彙整成清單。 (2) 對於清單中未提供安全性測試證明之委外系統，將逐案進行改善作業，包含合約條款之增修，以強化安全性控管(如：行動應用程式資安檢測、源碼檢測、弱點掃描等)。 	<p>(一)有關本項檢查意見預計於115.3.31日前完成改善。</p> <p>(二)有關本項檢查意見，因涉及委外廠商合約簽訂等因素，預計於115.6.30日前完成改善。</p> <p>(三)有關本項檢查意見，因涉及委外廠商合約簽訂等因素，預計於115.6.30日前完成改善。</p>
<p>二、金融監督管理委員會對公司未於114.7.10日以前公告申報114.6月份營運情形，於114.9.17對公司核處新臺幣30萬元罰鍰。</p>	<p>公司除重申應確切遵循證券交易法規定申報時效，於規定時程內完成相關申報事項，並對違失人員進行懲處以及落實內部檢核機制，以避免疏失再次發生。</p>	<p>已完成改善。</p>

註：請詳列遭主管機關處警告(含)以上或罰鍰新臺幣24萬元以上之處分；另併請詳列受主管機關、證券交易所、證券櫃檯買賣中心、期貨交易所查核發現資訊安全缺失之改善情形。