臺銀證券 112 年度核心營運評估報告

為強化核心資訊系統營運持續能力，本公司依據「公司治理實務守則」第8條之3「每年評估核心營運系統及設備，對評估結果採取適當措施，並提報董事會，以確保營運持續及作業韌性之能力」規定，就本公司推動營運持續管理與韌性執行辦理情形報告如下：

一、辨識核心系統風險因子與所採取之風險防範措施

本公司核心資訊系統以經紀業務相關系統為主，在證券市場交易時間內與交易所直接連線交易，各系統持續正常連線至為重要，為確保其可用性，本公司已就可能影響系統運作之風險因子進行辨識，茲就辨識結果、規劃防範措施及本(112)年度執行情形說明如下：

風險類型	營運中斷高風險事件	規劃防範措施	本年度執行情形
資訊系統異常	網路中斷	汰換原廠終止服務(EOS)網路設備	進行資訊處機房及分公司 Layer2 交換器汰換。
	外部網路攻擊	1. 建置資安防護、服務及安全性檢測 2. 人員監控異常 IP 登入 3. 辦理社交工程演練	1. 辦理應用程式防火牆維護、資安健診、網站應用系統弱點檢測及系統弱點掃描等作業。 2. 導入網路惡意行為偵測系統(DDI)。 3. 增加網路防護機制： (1)新購分公司防火牆 (2)SOC 中心即時監控惡意來源 IP/中繼站連線。 (3)全球資訊網導入 CDN 服務。 (4)建立遠端連線側錄機制。

			4. 系統每日產出異常登入 IP 清單，過濾後予以封阻。 5. 參加財政部及金控舉辦之社交工程演練。
	硬體設備故障	1. 建立核心營運系統雙主機異地熱備援機制 2. 汰換原廠終止服務(EOS)伺服器	1. 本公司核心電子交易系統皆有雙主機異地熱備援機制。 2. 汰換電子交易中樞系統主機。
	軟體邏輯錯誤	1. 建置測試環境，確認程式正常運作後方可過版上線 2. 程式過版前，應先進行弱點掃描等資安檢測，並擬訂上線復原計畫，若系統之邏輯錯誤，無法立即處理，則可依上線復原計畫進行程式退版程序 3. 核心營運系統異動、資料轉換及可能影響交易系統之作業前，應召開三方審查會議，由資訊單位、使用(測試)單位及廠商參加，依系統程式測試評核表審查測試程序之完整性及了解程式變更程序之妥適性	1. 程式換版前落實上線前進行弱點掃描，符合改善標準始得上線。 2. 可能影響交易之核心系統之程式上線前，召開三方審查會議及填寫測試評核表。 3. 電子交易系統換版前後，需填寫電子交易系統換版功能檢核表，確認換版後各項功能正常。
委外廠商	資安風險	1. 每年兩次對核心系統廠商進行實地資安查核，提升委外廠商資安意識及強化資安作業標準，避免成為資安漏洞 2. 依循行政院「資通系統籌獲各階段資安強化措施」，於資通系統籌獲之	1. 112 年度上半年至奇唯科技、下半年至中菲電腦進行委外廠商資安實地查核。 2. 依據金管會訂定「證券商作業委託他人處理應注

		需求階段、建置階段及維運階段，納入資安之管控項目，以選任適當之委外廠商，並監督其資通安全維護情形	意事項」，研議調整與委外廠商之契約。
	服務水準未達本公司要求標準	1. 設定資訊服務應有之服務水準及績效並訂定罰則 2. 採購文件規範廠商須指定負責專案管理人員，負責資通安全管理事項 3. 其他採購部份，需簽署廠商承諾書，在條款中納入完成日及違約條款等條件，並由採購人員及需求單位按時程追蹤納管	各資訊服務採購案均依規定辦理。
	委外廠商運作異常嚴重影響本公司營運	1. 客戶電子下單平台有三家以分散風險，倘發生其中某平台運作異常情形，客戶可洽營業員或另兩個下單平台交易 2. 盡可能採用與其他同業相同之公版，降低廠商漏誤更版風險	持續辦理
外部災害	地震、火災	1. 本公司於臺灣銀行資訊處設有備援機房，建置核心營運系統備援機制，每年辦理備援演練，使同仁熟悉備援切換步驟，以縮短備援切換所需時間。 2. 已於 103 年度進行耐震補強工程 3. 已投保火險及地震險，萬一災難發生時，得以進行風險轉移 4. 資訊機房建有環控系統，並委託專業廠商定期維護 5. 每半年進行一次自衛消防編組教育訓練	1. 本年度於 5 月 5 日、5 月 21 日、5 月 30 及 5 月 31 日進行核心營運系統備援演練，使同仁熟悉備援切換步驟，以縮短備援切換所需時間。 2. 投保火險及地震險將風險轉移。 3. 112 年 3 月 25 日結合防空疏散避難計畫，辦理上半年「臺銀綜合

		6. 每半年進行一次消防疏散演練 7. 建置總公司資訊機房防火門以阻隔火源 8. 建置總公司資訊機房自動滅火設備	證券股份有限公司自衛消防編組訓練計畫」；112年9月12日辦理下半年「臺銀綜合證券股份有限公司自衛消防編組訓練計畫」及消防疏散演練。 4. 建置總公司資訊機房防火門 5. 建置總公司資訊機房自動滅火系統
	電力供應異常	1. 短時間中斷或電壓異常：本公司資訊機房建有不斷電系統，並委託專業廠商定期維護 2. 長時間斷電：本公司建有柴油發電機，除定期維護外，每月進行兩次發電機測試	1. 不斷電系統正常運作 2. 依規定進行發電機測試

二、強化營運持續管理投入之實體資源規劃與預算編列

為強化資訊系統效能及資訊作業安全，本公司持續針對各核心資訊系統項目規劃補強改善方案，以提升營運不中斷的能力及提升本公司資安防護能力。簡述近3年及未來1年規劃辦理之核心營運設備及系統支出(例如含資本支出、維護費用及軟硬體設備)執行費用如下：

	110年度	111年度	112年度	113年度
建置內容說明	1. 汰換前後檯系統主機等軟硬體終止支援設備。 2. 提升營運不中斷的能力。 3. 強化網路設備及線路備援以	1. 汰換雙機房交易區外部防火牆等軟硬體終止支援設備。 2. 提升營運不中斷的能力。 3. 強化網路設備及線路備援以	1. 汰換資訊處機房L2 9200系列交換器等軟硬體終止支援設備。 2. 新購分公司防火牆。 3. 建置遠端測錄	1. 汰換總公司管道間L2 9200L系列交換器。 2. 總公司行動下單系統伺服器汰換。 3. ISO27001:2022轉版 。

	及不斷電系統、環控系統等維護。 1. 提升資安防護能力，採購安全性檢測及資安防護設備採購及維護及稽核軌跡留存。	及不斷電系統、環控系統等維護。 4. 提升資安防護能力，採購安全性檢測及資安防護設備採購及維護及稽核軌跡留存。	系統。 4. 交易中樞等已達使用年限伺服器汰換。 5. 總公司資訊機房環控系統升級。 6. 建置總公司資訊機房防火門及自動滅火系統。 7. 強化網路設備及線路備援以及不斷電系統等維護。 8. 提升資安防護能力，採購安全性檢測及資安防護設備採購及維護及稽核軌跡留存。	4. 證交所連線主機汰換。 5. 承德機房建置虛擬化平台。 6. 強化網路設備及線路備援以及不斷電系統。 7. 提升資安防護能力，採購安全性檢測及資安防護設備採購及維護及稽核軌跡留存。
預期效益	營運不中斷及強化資安防護	營運不中斷及強化資安防護	營運不中斷及強化資安防護	營運不中斷及強化資安防護
投入費用	36,942,573 元	14,095,085 元	暫估 13,186,894 元	預算 24,755,270 元

三、強化營運持續管理投入之人力資源規劃

本公司資訊單位為管理部資訊科，設有科長一人，科員八人，112 年 11 月將增補 1 名資訊人員，持有國際證照數量及教育訓練辦理規劃如下：

	法規要求	112 年度
國際證照	兩名資安專職人員，每人至少要有一張國際證照	ISO/ICE 27001:2022 Information Security Management System(ISMS) Lead Auditor ：3 人 Certified Ethical Hacker(CEH)：2 人 Certified Information Systems Security Professional (CISSP)：1 人 EC-Council Certified Incident

		Handler(ECIH) ：1人
教育訓練規劃	1. 資通安全專責人員至少二名人員各接受十二小時以上之資通安全專業課程訓練。 2. 資通安全專責人員以外之資訊人員每人每二年至少接受三小時以上之資通安全專業課程訓練。 3. 一般使用者及主管三小時以上資通安全通識教育訓練。	本年度已完成各類別教育訓練。