

康和綜合證券股份有限公司

內部控制制度聲明書

日期：113年2月27日

本公司民國112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112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、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113年2月27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。

康和綜合證券股份有限公司

董事長：鄭大宇

總經理：邱榮澄

稽核主管：施淑珍

負責資訊安全之最高主管：張志堅



簽章

簽章

簽章

簽章

附件



康和綜合證券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：112 年 12 月 31 日)

應加強事項	改善措施	預定完成改善時間
<p>證交所協同櫃買中心於 109 年 12 月 30 日及 31 日派員赴本公司進行查核，發現有下列缺失事項：</p> <p>(一) 本公司所轉投資之子公司康聯資產管理服務股份有限公司（下稱康聯公司）92 年及 93 年參與設立及現金增資華和資產股份有限公司（原名為康證資產管理股份有限公司，102 年度變更公司名稱，下稱華和公司）後，康聯公司 92 年至 108 年損益均以認列華和公司投資損益為主，且華和公司主要營業項目為不動產開發及買賣，核已違反前財政部證券暨期貨管理委員會核准本公司申請轉投資康聯公司時，所要求所投資資產管理服務公司之業務範圍應符合 91 年 3 月 7 日 (91) 台財證 (二) 字第 001501 號函，及已逾越金管會 107 年 6 月 1 日金管證券字第 1070320901 號令所允許證券商得轉投資國內事業範圍。</p> <p>(金融監督管理委員會 110 年 10 月 6 日金管證券字第 11003639491 號函、金管證券罰字第 1100363949 號裁處書，予以糾正、核處新臺幣 24 萬元罰鍰，並請本公司委託非簽證會計師出具專案審查報告)</p>	<p>子公司康聯公司所持有之華和公司股權，本公司已督促子公司康聯公司評估將所持有之華和公司股權進行出售之後續追蹤，為經本公司 111 年 11 月 8 日董事會決議通過進行解散及清算子公司康聯公司，經由清算程序，由清算人處分出售華和公司股權，本案現向金融監督管理委員會申請解散中。</p>	<p>持續追蹤。</p>



應加強事項	改善措施	預定完成改善時間
<p>本公司遭駭客攻擊發生客戶個資外洩，證交所於 111 年 8 月 17 日至 19 日對本公司進行查核，發現有下列缺失事項：</p> <p>(一)本公司遭駭客竊取個資，EMS 系統出現警示訊息，本公司卻未能即時知悉，致未於知悉事件 30 分鐘內至證券期貨市場資通安全通報系統通報。</p> <p>(二)本公司未對自行開發維護 CRM 系統、CRM App 及帳務中台系統進行原始碼檢測，僅由人工方式覆核原始碼，致未能發現程式漏洞；另 CRM 系統係提供公司內部人員使用，本公司卻將與其連線之 CRM App 置於 Google Play 平台供大眾下載，致駭客利用程式漏洞取得客戶個人資料。</p> <p>(三)CRM 系統之防毒軟體未設定排程掃描，且有未定期對電腦系統及資料儲存媒體進行病毒掃描情事。</p> <p>(四)CRM 系統使用者密碼變更期限未設定至少每三個月變更一次，且密碼長度僅為 5 碼，未使用優質密碼設定。</p> <p>(五)CRM 系統有未能定期辦理帳號盤點作業情事。</p> <p>(金融監督管理委員會 112 年 2 月 13 日金管證券字第 11203805321 號函、金管證券罰字第 1120380532 號裁處書，予以糾正、核處新臺幣 72 萬元罰鍰)</p>	<p>(一)本公司資訊部重新規劃並宣導通報流程，於 111 年 9 月 8 日資訊部月會對同仁進行宣導。</p> <p>(二)CRM APP 於 111 年 8 月即停止對外服務，並從 Google Store 下架完成。</p> <p>1.CRM 系統、帳務中台系統已透過防毒軟體檢查，完成改善。</p> <p>2.CRM 系統已使用雜湊比對、帳務中台系統使用程式比對，完成改善。</p> <p>3.CRM 系統、帳務中台系統在檔案名稱加入版號，完成改善。</p> <p>4.CRM 系統、帳務中台系統注入攻擊防護測試，完成改善。</p> <p>(三)CRM 系統已有掃毒紀錄與設定防毒軟體掃描排程，完成改善。</p> <p>(四)CRM 系統已設定密碼有效期期限為 90 天，密碼最小長度為 8 碼密碼中要包含小寫、大寫、數字，完成改善。</p> <p>(五)CRM 系統於 111 年下半年執行帳號盤點審查與簽核，完成改善。</p>	<p>左列缺失事項皆已完成改善。</p>

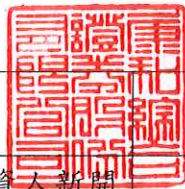
應加強事項	改善措施	預定完成改善時間
<p>檢查局於 110 年 12 月 6 日至 12 月 24 日對本公司進行一般業務檢查，發現下列缺失：</p> <p>(一)處理涉及負責人被檢舉案之程序，違反公司治理相關規定：</p> <ol style="list-style-type: none"> <li>1.本公司就檢舉案之檢舉事項，查核範圍未見完整，核有未當。</li> <li>2.本公司有將檢舉案調查結果先送被檢舉人簽核情事。</li> <li>3.該檢舉案調查結果未列審計委員會及董事會討論案。</li> <li>4.於董事會及審計委員會討論檢舉案相關議案，本公司未落實有利益衝突之人，應予迴避，且讓被檢舉人參與議案討論及表決。</li> </ol> <p>(二)非審計委員會或薪酬委員會之成員例行性列席會議，且未於討論及表決時離席。</p> <p>(三)公司內部未有對人員涉訟之墊付保釋金作業有明確規範下，以公司資金代墊保釋金。</p> <p>(四)辦理高風險股票控管作業，對客戶短期間多次申請放寬單一個股融資成數及額度，未依內部規定於控管開放申請單揭露客戶相關資訊。</p> <p>(五)辦理客戶受託買賣額度審核作業未落實歸戶控管，對總歸戶額度達 500 萬元以上之客戶，未徵提資力證明及未向票據交換所查詢票據退票資</p>	<p>(一)1.本公司另行調閱檢舉函指陳事項外其餘子公司交際費明細表，自各子公司交際費中，除被檢舉人於 107 年擔任子公司康和期貨之副董事長期間有核銷交際費外，並無在其它子公司核銷交際費。</p> <p>2.本公司日後受理檢舉案件及調查過程中，遇有利益衝突之人，應予迴避及出具「檢舉案調查報告表」不得經被檢舉當事人簽核及影響調查之獨立性，以符合本公司「檢舉制度」第 3 條之規定。</p> <p>3.本公司審計委員會及議事單位會加強注意關於列席人員利益迴避之要求，以符合證券暨期貨市場各服務事業建立內部控制制度處理準則第 28 條之 1 及本公司所訂「康和綜合證券股份有限公司檢舉制度」第 3 條規定之要求。</p> <p>4.本公司對於日後與董事有利害關係之案件，會詳加注意並以討論案方式提報審計委員會及董事會，以符合證券交易法第 14 條之 5 規定之要求。</p> <p>(二)1.本公司審計委員會議事進行方式係採取逐案進行，審計委員會主席會請相關單位及總經理、董事長列席會議說</p>	<p>左列缺失事項除(一)4.為檢查局歷次檢查未改善事項須持續追蹤外，餘皆已完成改善，並完成委託非簽證會計師出具專案審查報告。</p>



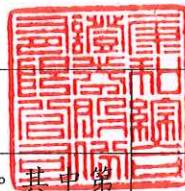


應加強事項	改善措施	預定完成改善時間
<p>料；歸戶額度達 1,000 萬元以上之客戶，未每年調查更新徵信資料。</p> <p>(六)辦理自訂槓桿股權選擇權業務，與客戶承作自訂槓桿股權選擇權，未提供最大風險情境分析、未適當揭露作業處理費、庫存費及應收付金額情事。另調整客戶作業處理費率未送權責主管准駁。</p> <p>(七)辦理黃豆 ETF 之買賣操作交易與買賣報告說明書所載操作策略不一致。</p> <p>(八)辦理法人客戶開戶審查作業，未將資本額資料建檔，且後續辦理定期審核作業，未即時辦理補正，致受託買賣額度達疑似洗錢或資恐交易態樣，未能於帳戶類洗錢態樣檢核表列示以供辦理檢核作業。</p> <p>(九)辦理受託買賣有價證券業務，客戶對帳單寄送內部業務人員電郵信箱。</p> <p>(金融監督管理委員會 112 年 3 月 2 日金管證券罰字第 1120380875 號裁處書，予以警告、核處新臺幣 144 萬元罰鍰，並請本公司委託非簽證會計師出具專案審查報告)</p>	<p>明，待所有議案說明完畢後，議事人員(司儀)再請列席主管、總經理、董事長迴避，再請審計委員會委員進行逐案討論及表決，本公司會更加注意審計委員會獨立董事獨立職權之行使。</p> <p>2.自 111 年 1 月 1 日起，非審計委員會之成員已未再列席審計委員會。</p> <p>3.本公司自 111 年 2 月 9 日第五屆第六次薪酬委員會起，業依「股票上市或於證券商營業處所買賣公司薪資報酬委員會設置及行使職權辦法」第 8 條第 4 項規定辦理。薪酬委員會除委員及議事人員外，其餘人員視召集人指示列席，惟於討論及表決時離席。</p> <p>(三)本公司已於 111 年 3 月 2 日增訂「預支管理辦法」，明確規範必須與本公司業務相關方得報支。</p> <p>(四)本公司已於 111 年 4 月 11 日加強高風險股票例外管理之審核作業及相關風險控管宣導，並增設分公司經理人於簽核「控管開放申請單」時務必於意見欄批註評估審核意見之功能，以落實審核作業及風險控管。</p> <p>(五)本公司已於 110 年 12 月 23 日公告分公司，重申</p>	

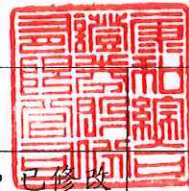
應加強事項	改善措施	預定完成改善時間
	<p>分公司辦理投資人新開戶及額度異動申請，務必進行歸戶查詢暨分配作業；另為利分公司執行總歸戶額度之控管，已於 111 年 2 月中旬新增控管程式，於投資人臨櫃開戶時得以其 ID 查詢該客戶於本公司已開立之所有帳戶及額度，以落實客戶總歸戶額度之管控。</p> <p>(六)1.本公司已依產品說明書之情境分析說明，於本公司官網公告專區，強化說明強制收回事務之情境分析。</p> <p>2.本公司已依產品說明書之說明，於本公司官網公告專區，公告各類型商品之相關費率。</p> <p>3.本公司已於每日交易對帳單增加揭露淨收支明細表，提升資訊完整度。</p> <p>4.系統已於 111 年 3 月 31 日完成修正，日後所有作業處理費之調整，均須填具「作業處理費折讓申請單」送權責主管准駁，且系統維護調整作業處理費均須經由權責主管覆核。</p> <p>5.修訂本公司「股權衍生性金融商品業務作業流程」第五條條文內容。</p> <p>(七)本公司已於 110 年 6 月 25 日修改「指數股票型基金策略交易風險管理</p>	







應加強事項	改善措施	預定完成改善時間
	<p>準則」並施行。其中第二條交易策略增訂業務合作交易策略乙項，在第三條交易策略定義新增業務合作交易策略並說明交易流程。</p> <p>(八)為避免人員於後台客戶徵信資料維護檔「資本額」欄位漏建檔，而導致參數來源為空值，致使態樣無法產出之情形，業已調整「資本額」參數來源資料，並將該欄位設定為必填欄，系統得以正確抓取該欄位資料進行比對，已於111年2月23日上線實施。</p> <p>(九)本公司「查詢證券電子信箱比對表」於111年7月1日上線，並同時公告相關規定。</p>	
<p>本公司就所報暗網疑似販售客戶個資一案，委託資誠聯合會計師事務所辦理自109年8月1日至112年8月15日有關個人資料保護之內部控制制度專案審查。</p> <p>本公司於「個人資料保護內部控制制度聲明書」所列重大應改進事項，除上述第二項有關遭駭客攻擊所列缺失及改善措施外，另有下列重大應改進事項：</p> <p>一、個人資料盤點及風險評估作業需予加強</p> <p>(一)未於個人資料檔案清冊表達出委外作業。</p> <p>(二)業務管理部有經手個人資料(複委託配息名單)，但未執行個資盤點及風險</p>	<p>一、(一)清冊內容未表達出委外作業部分，預計於113年3月底前完成個人資料檔案清冊暨風險評鑑管理辦法及附件之修正(增加委外作業盤點項目)，以利於113年4月辦理個人資料檔案清冊暨風險評鑑作業時有所依循。</p> <p>(二)將於113年1月底起，由結算部產出複委託配息名單資料，直接提供給海外上手。</p> <p>(三)已將員工體檢資料列入112年個資盤點清冊，並於113年1月5日將相關資料提交法遵部存查。</p> <p>二、(一)1.針對Web線上開</p>	<p>一、(一)預計113年3月底前完成改善。</p> <p>(二)截至113年1月底尚無發生，將俟後續發生時追蹤其改善情形。</p> <p>(三)已於113年1月5日完成改善。</p> <p>二、(一)1.已於113年1月12日完成改善。</p> <p>2.預計113年4月底前完成改善。</p> <p>(二)1.已完成改善。</p> <p>2.已於113年1月31日完成改善。</p> <p>(三)1.預計113年6月底前完成改善。</p> <p>2.預計113年6月底前完成改善。</p> <p>3.已完成改善。</p> <p>4.(1)預計113年3月</p>



應加強事項	改善措施	預定完成改善時間
<p>評估。</p> <p>(三)人力資源部未將員工體檢資料納入個人資料檔案清冊。</p> <p>二、系統存取功能及權限管理需予加強</p> <p>(一)對含個人資料內容下載之控管</p> <p>於Web線上開戶系統、臨櫃開戶系統之操作，未針對含個人資料內容之下載加以限制。</p> <p>(二)系統密碼原則設定</p> <p>1.CRM 作業系統密碼設定，未使用優質密碼設定。</p> <p>2.新電子交易系統之作業系統一般員工帳號已採與AD同步之方式進行控管，惟對於直接在作業系統層建立之帳號，尚未設定密碼原則。</p> <p>(三)帳號管理</p> <p>1.資訊部雖已每半年進行AD之最高權限帳號與特許帳號清查，惟尚未針對AD之一般帳號進行清查。</p> <p>2.未針對共用資料夾權限進行清查。</p> <p>3.資訊部目前已有執行CRM系統帳號權限清查；惟於109~111上半年未執行CRM應用系統、資料庫帳號權限定期清查。</p> <p>4.AD網域帳號存在</p>	<p>戶系統之部份，已修改程式於畫面欄位增加遮罩，然因作業所需滑鼠移到該筆資料會完整顯示，惟匯出時資料將一律進行遮罩，以降低資料大量外洩之風險。</p> <p>2.臨櫃開戶系統之部份，預計請委外廠商修改程式於點選「列印」按鈕時進行記錄，以留存資料轉出軌跡。</p> <p>(二)1.CRM 作業系統密碼已改善採用優質密碼設定，已設定密碼有效期期限為90天，密碼最小長度為8碼密碼中要包含小寫、大寫、數字，完成改善。</p> <p>2.將修改密碼原則設定。</p> <p>(三)1.考量一般權限帳號僅預設開放最低使用者權限且無個資相關疑慮，其他權限皆透過個應用程式進行控管風險相對較低。因此，過往集中資源針對風險較高的最高權限帳號與特許帳號每半年執行清查，未來將定期進行全面清查。</p> <p>2.將於系統帳號權限盤點時將共用資料夾權限列入盤點項目。</p> <p>3.CRM系統於111年下半年執行帳號盤點審查與簽核，完成改</p>	<p>底前完成改善。</p> <p>(2)已完成。</p> <p>三、(一)(二)已於113年1月31日完成改善。</p> <p>(三)預計113年4月底前完成改善。</p> <p>(四)已於113年1月3日完成改善。</p> <p>四、(一)已完成改善。</p> <p>(二)預計113年12月底前完成改善。</p> <p>五、已於113年1月8日完成改善。</p>





應加強事項	改善措施	預定完成改善時間
<p>共用帳號，且會計部之共用帳號已不需使用。</p> <p>三、電子郵件控管需予加強</p> <p>(一)電子郵件過濾系統無法判讀圖檔，可逕予以寄送。</p> <p>(二)未對未觸發攔截之郵件進行管控。</p> <p>(三)員工可透過個人行動裝置下載儲存電子郵件。</p> <p>(四)依電子郵件過濾條件，模擬寄送大量虛擬個人資料，發現有某一新部門未正確套用過濾條件之情事，致測試時可將資料寄出。</p> <p>四、網際網路控管需予加強</p> <p>資訊部使用 Fortinet 與 WinMatrix 工具限制員工無法登入部分網站，其餘未受限之部分網站(如 WordPress.com)可進行上傳檔案(圖片、word 檔案)。</p> <p>五、稽核軌跡留存年限需予加強</p> <p>下列軌跡資料未符「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第 14 條第 3 項規範之至少留存 5 年：</p> <p>(一)可攜式儲存媒體(USB、光碟機)之存取紀錄僅留存 3 年。</p> <p>(二)內部私有雲存取紀錄的留存期間僅設定為 1 年。</p> <p>(三)CRM 系統之資料庫</p>	<p>善。</p> <p>4.(1)共用帳號為各部門特殊業務需求專用帳號，因特殊應用系統權限問題需專用帳號執行相同應用供不同同仁可正常使用系統，將與使用者確認是否可改為群組權限的方式加入個別使用者帳號，如無解決方案還是需開放專用帳號供使用者使用，將確認以最小權限提供應用系統專用，不提供其他服務。</p> <p>(2)已將會計部之共用帳號進行移除。</p> <p>三、(一)目前先採只要有圖形檔案附件寄送外部時皆送主管稽核，待導入相關軟體可控制時再調整其他控管方式。</p> <p>(二)將透過設定將含有個資的郵件皆納入稽核，高風險郵件需由主管放行，系統每周寄送自動放行之稽核郵件清單供各單位主管覆核。</p> <p>(三)將停止員工透過行動裝置收信，並改以 VPN(資料不落地)的方式連回公司。</p> <p>(四)針對資安部成員寄送含虛擬個資之附件未進行攔阻之部份，經查因郵件稽核系統內過濾規則的成員是獨立設定的，新增資安部的時候未將此過濾條件</p>	

應加強事項	改善措施	預定完成改善時間
<p>未對使用者登入相關紀錄保存稽核軌跡。</p> <p>(四)新電子交易系統資料庫、作業系統之登入相關稽核軌跡未完整保存5年。</p> <p>(金融監督管理委員會112年9月11日金管證券字第1120353875號函，請本公司委託具資安查核能力之非簽證會計師出具專案審查報告)</p>	<p>加入，導致資安部的成員會未套到稽核政策，此部分系統管理員已完成改善。</p> <p>四、(一)已禁止同仁連接WordPress.com、Synology 與 Wix 網頁，降低風險。</p> <p>(二)考量網際網路上未來會持續有新網站或網頁，單靠黑名單阻擋方式難免有所疏漏，為避免類似問題發生，長期將評估並導入資料外洩防禦(DLP)解決方案深化整體控管機制。</p> <p>五、變更設定留存五年。</p>	

註：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。