資通安全管理：

---

113 年實作項目:

1.本公司每年不定期對全體員工實施釣魚郵件教育,已於實施日期: 7/1,7/19,7/29,8/22

2.於董事會會議上做資安報告:1.資安架構重新調整及建置:5/10

2.弱點測試及修補:10/29

3.資訊安全主管於 113 年 8-11 月參加相關專業資訊安全訓練共計 96 小時，並有完訓證書(CEH、CISSP)及通過考試取得資通安全署認可之證照(CEH).

(一) 敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等

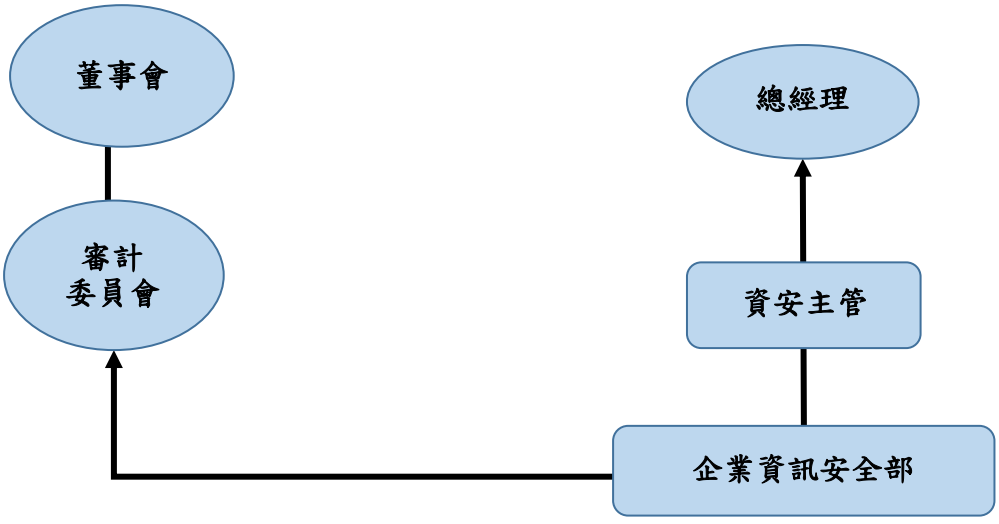
1、資通安全風險管理架構

(1) 企業資訊安全治理組織

本公司於民國 113 年 1 月設立「企業資訊安全部」,統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由企業資訊安全主管每半年向董事會彙報資安管理成效、資安相關議題及方向。

資安主管肩負監督治理企業資訊安全之責，督評核公司資訊與網路安全管理機制及方向並檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。

(2) 企業資訊安全組織架構



2、資通安全政策

（1）企業資訊安全管理策略與架構

企業資訊安全組織為有效落實資安管理，依據規畫、執行、查核與行動（Plan-DoCheck-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施，並定期與財務副總回報執行成效。

「規畫階段」著重資安風險管理，建立完整的資訊安全管理系統（Information Security Management System, ISMS)，從系統面、技術面、程序面降低企業資安威脅，建立符合最高規格的機密資訊保護服務。

「執行階段」則建構多層資安防護，持續導入將資安防禦創新技術，將資安控管機制整合內化於軟硬體維運等平日作業流程，系統化監控資訊安全，維護昶昕實業股份有限公司重要資產的機密性、完整性及可用性。

「查核階段」積極監控資安管理成效，依據查核結果進行資安指標衡量及量化分析，並預計透過定期模擬演練資安攻擊(先由內部資訊安全部執行)進行資訊安全成熟度評鑑。

「行動階段」則以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效；當員工違反相關規範及程序時，依據資安違規處理流程進行處置，並視違規情節進行人事處分（包括員工當年度考績或採取必要的法律行動）；此外，亦依據績效指標及成熟度評鑑結果，定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，確保昶昕實業股份有限公司重要系統作業正常運作及機密資訊不外洩。

（2）企業資訊安全風險管理與持續改善架構

檢討與持續改善

- 資訊安全措施檢討改善
- 資安威脅及技術掌握
- 資訊安全違規及處置
- 資訊安全教育訓練與宣導

資安風險管理

- 企業資訊安全風險評估
- 資訊安全風險管理與對策制定
- 客戶交易資訊安全保護機制

監控資安管理成效

- 資訊安全持續監控
- 資訊安全指標量化評估
- 資訊安全攻擊模擬演練
- 機密資訊保護
- 資安成熟度評鑑

多層資安防護

- 人員與實體安全
- 帳號與權限管理
- 資安監控與維運
- 資料安全保護技術強化

- 網路安全
- 裝置安全
- 異地主機備援機制

(3) 具體管理方案

網路安全

- 強化網路防火牆與網路控管，防止網路攻擊。
- 防火牆及防毒軟體自動更新。

裝置安全

- 電腦及主機建置防毒軟體和 MDR(端點防護託管服務)，強化惡意軟體行為偵測。

資料安全保護技術強化

- 應用具有一寫多讀(WORM)不可變技術之NAS來儲存系統備份及作業資料。
- 使用資料加密工具對於機密資料做加密保護。
- 郵件主機安裝第三方憑證加密,做往來信件內容保護。

資安威脅及技術掌握

- 每月研究新技術及使用弱點掃描系統漏洞及補漏洞。

資訊安全攻擊模擬演練

- 使用國際駭客常用之工具做模擬攻擊測試,以驗證設備之耐受度。

異地主機備援機制

- 使用離線備份(系統及資料)做異地主機復原作業。

檢討與持續改善-教育訓練與宣導

- 加強員工對社交工程攻擊的釣魚郵件警覺性和防禦心。
- 定期舉辦或 E-MAIL 通知釣魚郵件案例宣導教育。

(4) 投入資通安全管理之資源

- 防火牆(FortiGate-81F ,UTM:多合一,IPS:入侵防護)。
- 防毒軟體(WithSecure Business Suite)。
- MDR 端點防護託管服務(SentinelOne)。
- 舊電腦(XP、WIN 7)升級至 WIN 10、11。
- 一寫多讀(WORM)不可變技術之 NAS(DS224+)檔案伺服器。

(二) 列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施：

本公司於民國113年2月24日受到勒索病毒感染，感染過程中導致ERP主機硬體之基本系統檔損毀無法正常開機，備份資料被加密無法做復原作業，當時影響範圍如下:例行性人員系統作業改由人工作業因應。

改善措施如下：

(1) 因舊主機硬體已有無法修復之漏洞，故重新購買新款安全性較佳之主機硬體，且重新導入ERP系統和離線備份及異地主機備援機制。

(2) 導入主動防禦入侵之防火牆及防毒軟體及行為偵測之MDR。

(3) 重要系統及檔案儲存於不可變之檔案伺服器。

(4) 人員資安教育訓練和宣導。