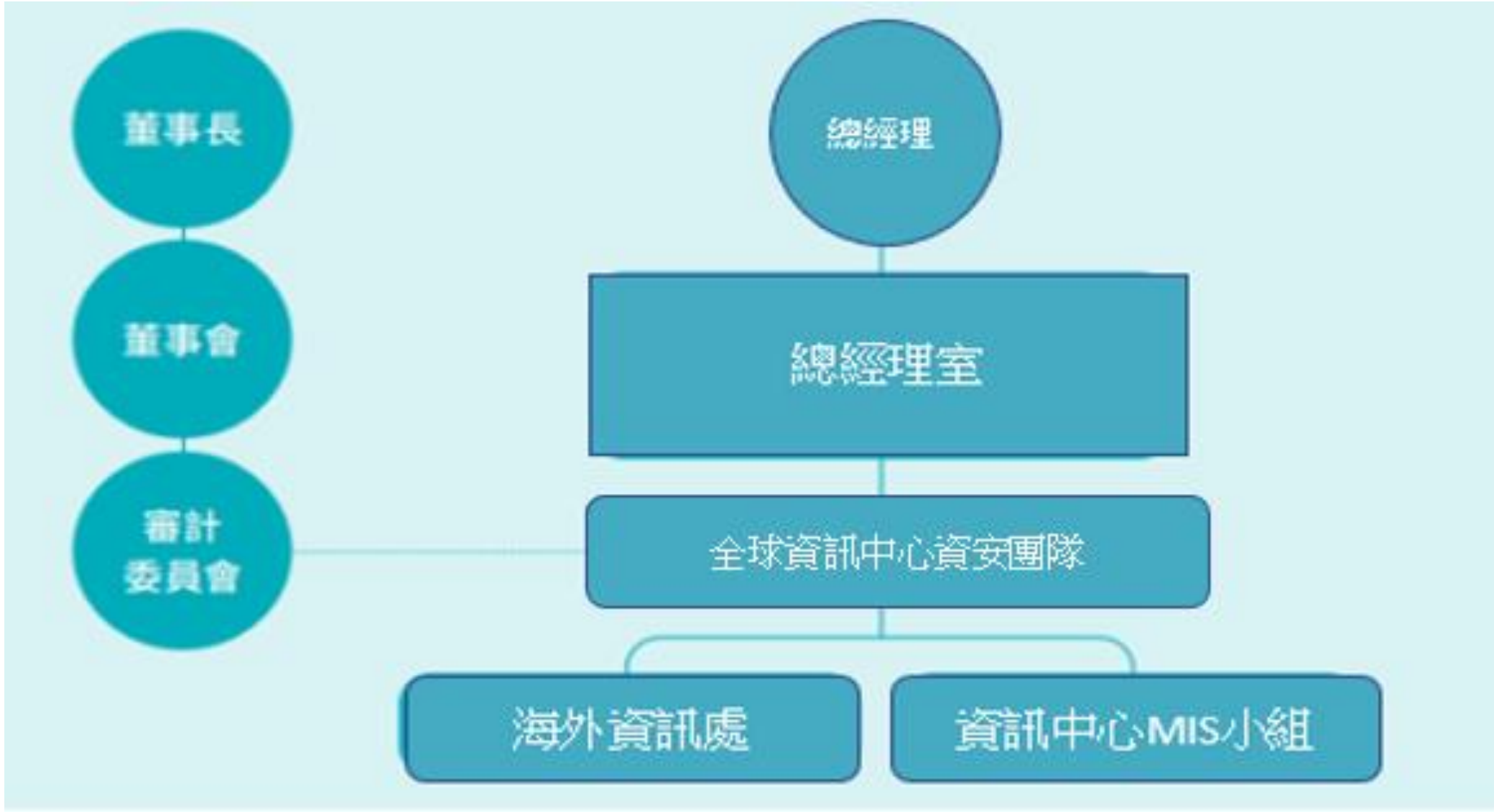
宏遠興業
資通安全管理之資訊揭露

資通安全風險管理架構

- 1.企業資訊安全治理組織宏遠興業民國 X 年設立「企業資訊安全組織」，下轄資訊 安全處與資訊保護處，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，由企業資訊安全組織最高 主管每半年向董事會審計委員會彙報資安管理成效、資安 相關議題及方向。宏遠興業審計委員會肩負監督治理企業 資訊安全之責，由具有資安領域相關背景的審計委員 A 監督評核宏遠興業資訊與網路安全管理機制及方向。宏遠興業為執行企業資訊安全組織訂定的資安策略，確保 內部遵循資安相關準則、程序與法規，特別成立「宏遠興業專屬資訊保護委員會」，由資訊技術及資材暨風險管理 資深副總經理擔任主席，法務、人力資源、研究發展、營運組織副總經理擔任委員會成員，並設置企業資訊安全組 織最高主管為執行秘書、內部稽核最高主管為觀察員，每 季召開會議，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。

宏遠興業公司企業資訊安全組織架構



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，透過涵蓋台灣廠區與海外子公司各單位的「資訊保護工作推動團隊」，每月召開例行會議，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，並定期與專屬資訊保護委員會回報執行成效。「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)，推動各廠區持續通過國際資安管理系統認證（ISO/IEC 27001、ISO/IEC 15408），從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求、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、供應商資安管理等平日作業流程，系統化監控資訊安全，維護宏遠興業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，並透過定期模擬演練資安攻擊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，確保宏遠興業公司重要機密資訊不外洩。

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
- 資訊保護問卷調查
- 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
- 遵循資安國際標準（ISO/IEC 27001, ISO/IEC 15408, SCF, NIST, SAFE）
- 客戶資訊安全保護機制

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
- 機密資訊保護遵循度查核
- 資安成熟度評鑑
- 通過資安國際稽核認證

多層資安防護

- 人員與實體安全
- 雲端安全
- 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
- 應用程式安全
- 供應鏈資訊安全
- 資料安全

多層資安防護

網路安全
- 導入先進技術執行電腦掃描及系統與軟體更新
- 強化網路防火牆與網路控管，防止電腦病毒跨機台及跨廠區擴散

裝置安全
- 建置機台入廠掃毒機制，防止內含惡意軟體的機台進入公司
- 依電腦類型建置端點防毒措施，強化惡意軟體行為偵測

應用程式安全
- 制定開發流程應用程式安全自檢表、評核標準及改善目標
- 持續強化應用程式安全控管機制，並整合於開發流程及平台

供應鏈資訊安全
- 建構供應商資安保護自我檢核機制
- 定期傳達　　公司最新的資安規定及注意事項

資料安全保護技術強化
- 開發先進資訊保護工具，藉由資料標籤加強文件機密分類及資料保護
- 文件及資料加密控管及有效追蹤
- 郵件外寄控管

檢討與持續改善

教育訓練與宣導
- 加強員工對郵件社交工程攻擊的警覺性，執行釣魚郵件防禦偵測
- 定期舉辦員工辨識能力演練，提升員工資安意識

資訊技術安全之風險及管理措施

宏遠興業已建立全面的網路與電腦相關資安防護措施，但無 法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻 擊。這些網路攻擊以非法方式入侵宏遠興業公司的內部網路系 統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴 重網路攻擊的情況下，宏遠興業公司的系統可能會失去公司重要 的資料，生產線也可能因此停擺。宏遠興業透過持續檢視和 評估其資訊安全規章及程序，以確保其適當性和有效性，但 不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新 的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業 8 祕密及其他機密資訊，例如客戶或其他利害關係人的專有資 訊以及公司員工的個資。 惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導 入宏遠興業公司的網路系統，以干擾公司的營運、對○○公司進行敲詐或勒索，取得電腦系統控制權，或窺探機密資訊。這 些攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司 的網路安全系統；也可能使○○公司因涉入公司對其有保密 義務之員工、客戶或第三方資訊外洩而導致的相關法律案件 或監管調查，而承擔重大法律責任。 ○○公司過去曾經因購買及安裝內含惡意軟體的設備而遭 受攻擊，未來也可能面臨類似的攻擊。為了預防及降低此類 攻擊所造成的傷害，宏遠興業公司落實相關改進措施並持續更 新，例如建置機台入廠掃毒機制以防止內含惡意軟體的機台 進入公司；強化網路防火牆與網路控管以防止電腦病毒跨機 台及跨廠區擴散；依電腦類型建置端點防毒措施；導入先進 的解決方案以偵測與處理惡意軟體；設計開發資安強化個人 電腦供員工使用；設計開發雲端應用安全政策；導入新技術加強資料保護；加強釣魚郵件偵測；建立一個整合的自動化 資安維運平台，並定期執行員工警覺性測試及委託外部專家 執行資安評鑑。雖然公司持續加強資訊安全防護措施， 但仍無法保證公司免於惡意軟體及駭客攻擊。 此外，宏遠興業公司需要分享高度敏感及機密的資訊給部分其雇 用提供宏遠興業及其全球關係企業服務的第三方廠商，以使 其能提供相關服務。儘管公司在和第三方服務廠商簽訂 之服務合約中，要求其遵守保密及／或網路安全規定，但不 能保證每個第三方服務廠商都將嚴守這些義務。由上述服務 廠商及／或其承攬商所維護的內部網路系統及外部雲端運算網路（例如伺服器），亦會有遭受網路攻擊的風險。若宏遠興業或其服務廠商無法及時解決這些網路攻擊所造成的 9 技術性問題，或確保宏遠興業（及屬於本公司客戶或其他第 三方）的數據完整性及可用性，或控制住公司或其服務廠商 的電腦系統，皆可能嚴重損及宏遠興業對客戶和其他利害關 係人的承諾，而公司營運成果、財務狀況、前景及聲譽亦可 能因此遭受重大不利影響。