編號	評鑑指標	資訊依據
2.24	公司是否建置資訊安全風險管理架構，訂定資訊安全政策及具體管理方案，並揭露於公司網站或年報？	公司網站或年報

需同時符合以下三項要件，始能於構面計分。

[要件一]建置資訊安全風險管理架構(如：成立資安委員會，定期檢討資安政策，並定期向董事會報告等)。

[要件二]訂定並揭露資訊安全政策。

[要件三]訂定並揭露資訊安全具體管理方案(包含是否投保資安險，若無，則詳述相關預防措施)。

[備註]公司揭露 110 年**仍在效期內之** ISO27001 或 CNS27001 認證，可直接於構面計分。

範例 1：

1. 資訊安全目的與範圍：

對象：包括員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。
範圍：為確保本公司資訊安全，制定相關規章制度，應用技術和數據安全標準制定，並納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護。

2. **【資訊安全風險架構】**:

- 由本公司總經理召集成立跨部門資訊安全管理小組，資訊部門與行政管理部門負責主導及規劃，各業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。
- 本小組負責制定資訊安全管理政策，定期檢討修正。
- 本小組定期召開會議檢討執行情形，並每年定期向董事會報告執行情形與檢討。

3. **【資訊安全政策目標】** ：

- 確保本公司營運業務持續運作，且本公司提供的資訊服務可穩定使用。
- 確保本公司所保管的資訊資產之機密性、完整性與可用性，並保障人員資料之隱私。

- 建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。
-

4. **【資訊安全控制措施】:**
   - 建立訂定期盤點資訊資產清單，依資安風險評鑑進行風險管理，落實各項管控措施。
   - 公司定期執行資訊安全宣導作業，每年辦理與資訊安全教育訓練，新進人員皆須簽定資訊保密協定。
   - 本公司所有員工、委外廠商暨其協力廠商須簽定保密聲明書，已確保使用本公司資訊以提供資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。
   - 重要資訊系統或設備應建置適當之備援或監控機制並定期演練，維持其可用性。
   - 個人電腦應安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權軟體。
   - 同仁帳號、密碼與權限應善盡保管與使用責任並定期換置。
   - 制定資訊安全事件的回應及通報標準程序，以適當對資訊安全事件做即時處理，避免傷害擴大。
   - 全體人員應遵守法律規範與資訊安全政策要求，主管人員應督導資安遵行制度落實情況，強化同仁資安認知及法令觀念。
   - 考量資訊安全之風險不確定性，110 年度(受評鑑年度)已購買資安險。

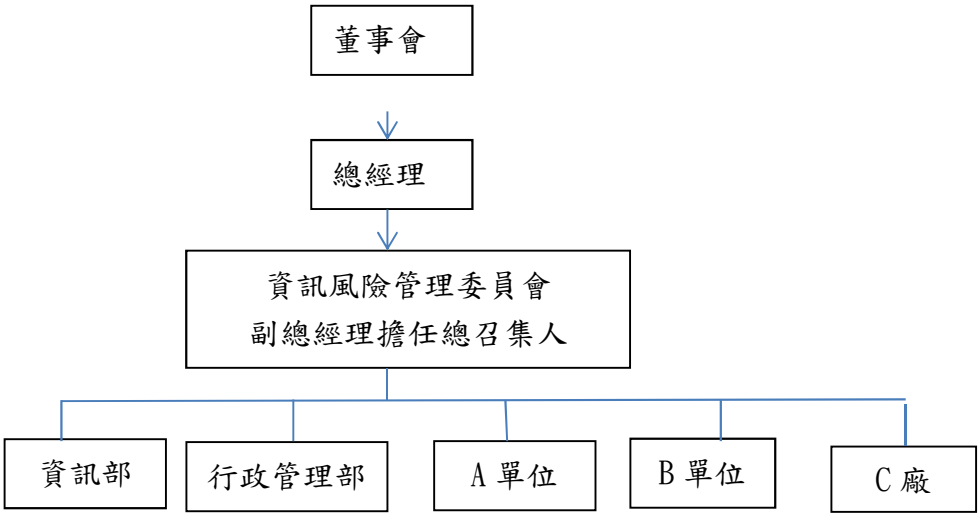
5. 110 年辦理資訊安全宣導執行情形：
   - 教育教練：

     本年度辦理兩梯次資訊安全教育訓練，3 小時「防範網路社交工程認知與技巧」及 3 小時「資訊安全管理與應用」，經理人及員工共計 255 人次參與。

範例 2：

本公司已於 110 年 X 月由副總經理擔任召集人成立【資訊安全風險管理委員會】，本委員會負責審視各業務單位之資訊安全政策之治理、規劃、督導及執行情形，以建構出資訊安全防衛能力及同仁良好的資訊安全意識，每年並定期向董事會報告當年度執行情形。

【資訊安全管理架構】如下：



【資訊安全政策】：

資安政策		
資安治理	控制風險加強防範 強化資訊安全架構	制定完整管理制度，強化教育訓練、資訊安全基礎架構設計及保護技術。確保資訊之系統可用性、限制權管及存取管理、抵抗外部威脅
法令遵循	建置合規機制 定期檢視/修訂	建立符合規範機制，定期檢視及修訂相關作業規範以符合資安標準。

【具體管理措施】：

資訊安全管理類型	相關作業
系統可用性	監控系統、網路可用狀態 資料異地備援系統，確保完整資訊可復原 定期演練災害發生，系統還原程序 中斷資訊服務應變措施

外部威脅	偵測病毒與惡性程式攻擊，防範資訊受損 電腦主機弱點檢測及更新
權限管理	人員帳號及權限之設定管理 定期檢查盤點帳號及必要業務之使用權限 重要機房出入權限管理
存取控管	管制資訊檔案存取 資料存取紀錄 重要資料依規定加密

110 年度執行情形：

- 本公司資訊安全本公司於 110 年度召開 4 次資訊安全管理委員會議，檢討各單位資安政策之執行情形，當年度並無危害本會資訊安全之事件。
- 本年度辦理 1 次異地備援演練及 3 次社交工程演練，加強員工對於資訊安全風險之應變與警覺性。
- 110 年 8 月投保【資訊安全責任險】

範例 3：

本公司資訊安全政策為「維護公司資訊之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，遭致資訊與資產遭致不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害」。本公司已於 105 年導入 ISO 27001 資訊管理系統，並**定期取得 ISO 27001 認證，目前證書之有效期為 110 年 1 月至 111 年 12 月**。透過 ISO27001 資訊安全管理系統之導入，強化資訊安全事件之應變處理能力，保護公司與客戶之資產安全。