巨大機械工業股份有限公司
資通安全與風險管理

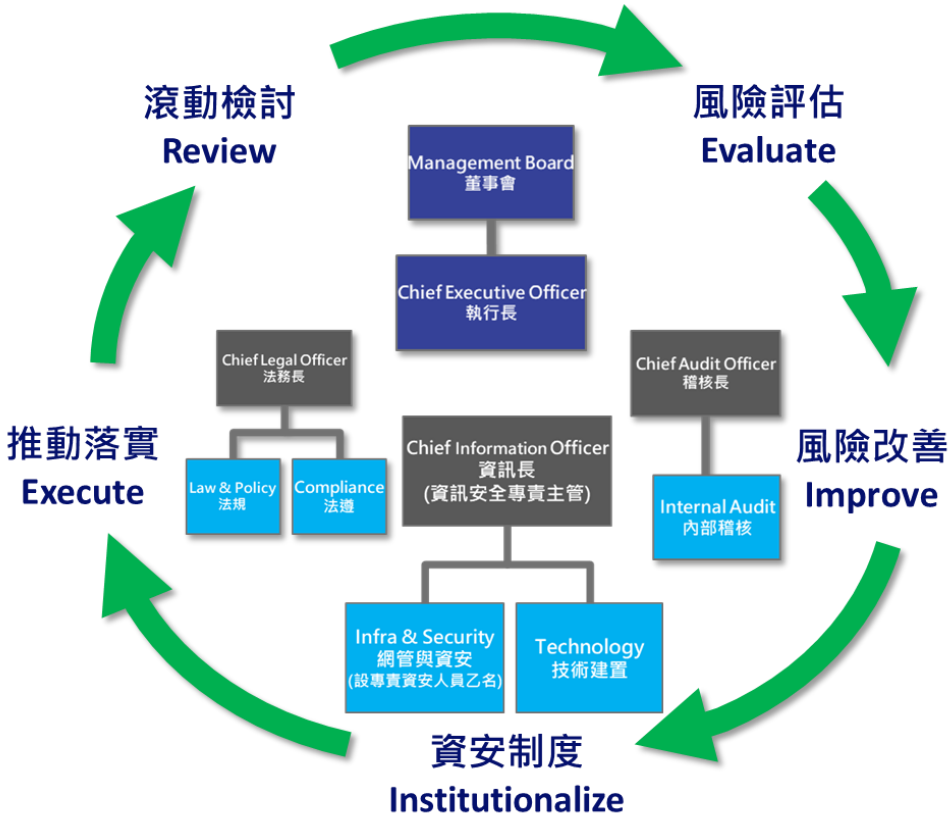
（一）敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

1、資訊安全管理架構：

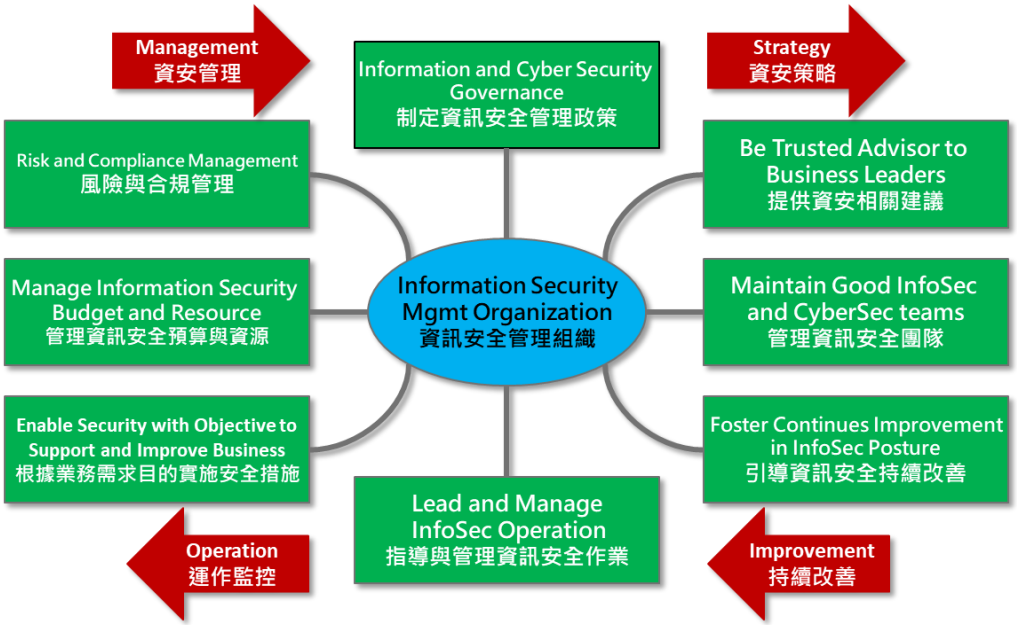
組織運作模式-採循環式管理，確保可靠度目標之達成且持續改善。

1-1. 本公司資訊安全之權責單位為全球資訊中心，設置資訊長乙名，與專責資安人員乙名，負責訂定內部資訊安全管理政策、規劃暨執行資訊安全作業、宣導與資安政策推動與落實。

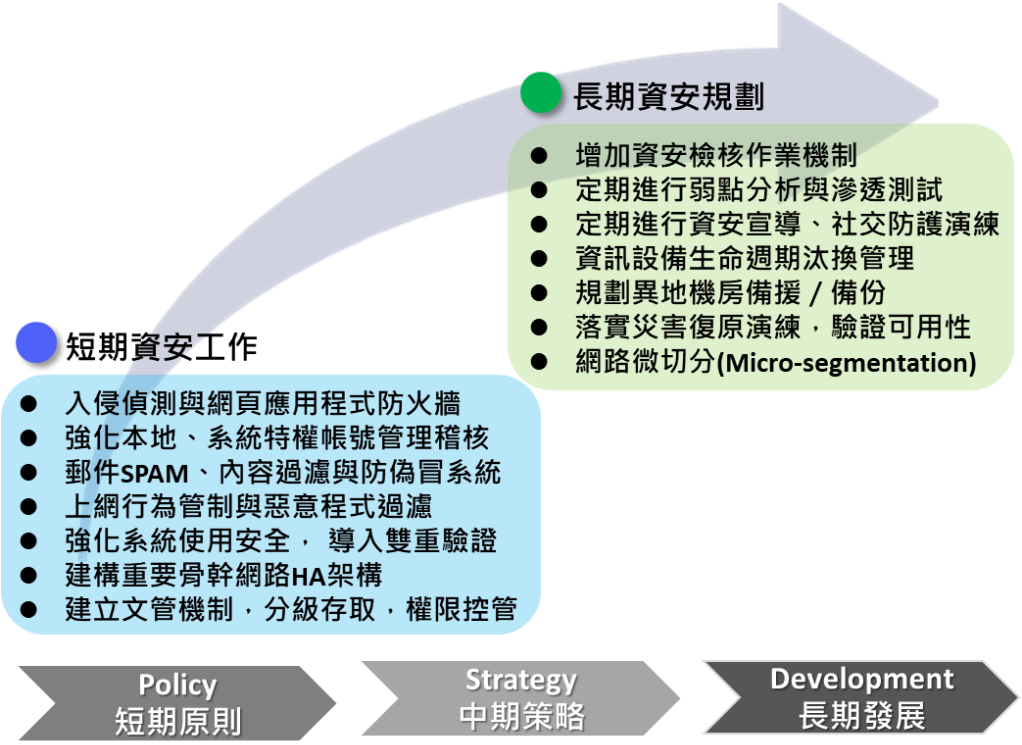
1-2. 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，與專職稽核人員數名，負責督導內部資安執行狀況，並定期向審計委員會報告公司資訊安全檢查情形，若查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。



2、資訊安全管理策略：



3、資訊安全管理計劃：



2024 年資安目標	2024 年績效
資通系統可用性達 99.99%以上（中斷時數/總運作時數≤ 0.1%）	SLA (Service Level Agreement)99.99 %達成，年度中斷時間需低於 8.76 小時, 2024 年度服務中斷事件累計 2 小時，達成目標。
重大資安事件（第三、四級資安事件）不得發生	未發第三、四級資安事件
關鍵核心系統備份成功率達 100%	核心系統備份
資安意識強化宣導	進行資安意識宣導，提升員工上網及郵件安全判讀觀念

4、資訊安全管理措施：

4-1. 成立資訊安全執行小組，訂定資訊安全管理政策及具體實施方案，以確保資訊安全。

4-2. 依據個人資料保護法審慎處理個人資訊。

4-3. 個人電腦、伺服器皆需設密碼，並安裝防毒軟體，密碼及病毒碼需定期更新。

4-4. 應遵守智慧財產權相關規定，確保安裝之電腦軟體皆有合法授權。

4-5. 重要資料進行備份、盤點，並定期確認備份有效性。

4-6. 依「資訊災難緊急應變計劃」定期演練，以利資安事件發生時快速恢復系統運作。

4-7. 定期執行資訊安全宣導作業，強化同仁資安認知及法令觀念。

4-8. 本公司目前正進行資安險評估。

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，如無法合理估計者，應說明其無法合理估計之事實：無此情形。

資安事件通報 0 件。同仁若有違反資安相關規定，將依相關懲戒程序處置違紀人員。

期程	措施	2024 年資訊安全措施推動執行成果
短期	● 成立資訊安全執行小組，訂定資訊安全管理政策及具體實施方案，以確保資訊安全。 ● 依據個人資料保護法審慎處理個人資訊。 ● 個人電腦、伺服器皆需設密碼，並安裝防毒軟體，密碼及病毒碼需定期更新。 ● 應遵守智慧財產權相關規定，確保安裝之電腦軟體皆有合法授權。 ● 重要資料進行備份、盤點，並定期確認備份有效性。 ● 定期執行資訊安全宣導作業，強化同仁資安認知及法令觀念。	● 參照 ISO27001 管理制度，成立資訊安全執行小組陳審後公告資訊安全政策與相關施行管理規章，並取得 SGS 驗證。 ● 對於個人資料或隱私均遵守相關法令規定辦理。 ● 個人電腦、伺服器設有通行碼與定期更新，並均裝設防毒軟體與病毒碼定期更新。 ● 電腦設備設有資產管理盤點軟體，確保合法軟體授權之安裝。 ● 每季盤點重要資料及定期執行核心備份、復原演練。 ● 每半年定期宣導資訊安全相關實事或法令要求事項，提升同仁安全意識觀念。