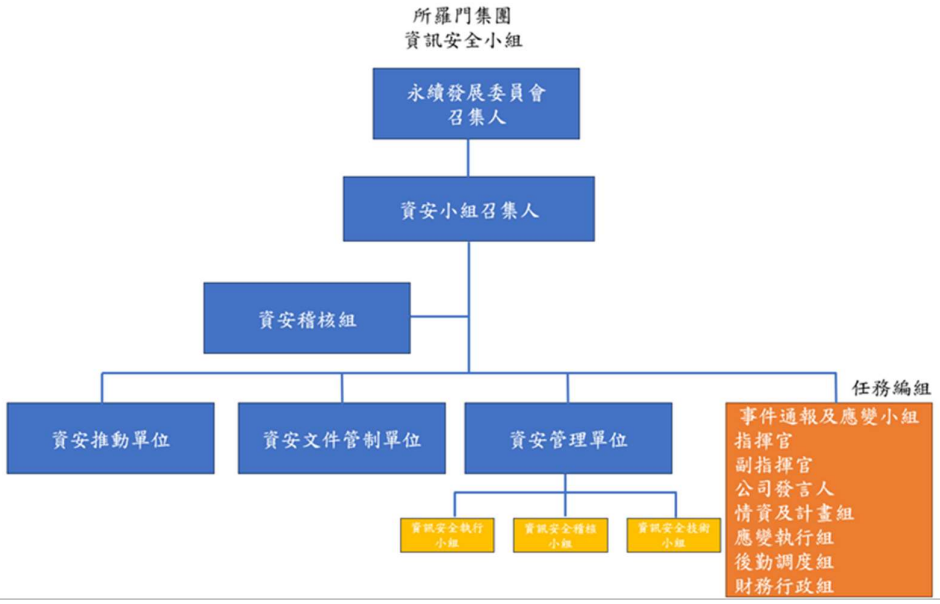
所羅門股份有限公司(集團)

資通安全管理(114 年度)

(一)資通安全風險管理架構：

- 本公司配合主管機關金管會對於資訊安全管理機制要求，將上市(櫃)公司分為三級，本公司已按所屬第二級標準規定已完成設置資訊安全專責單位、主管及資訊安全人員，專門負責資訊安全事務，進行資訊安全制度之規劃、監控及執行資訊安全管理作業，持續優化與改善可能發生之資安風險。
- 組織運作模式，於永續發展委員會下設立資安小組，負責制定與宣導公司資安政策及資訊安全作業程序，公司內部各單位為執行資通安全作業推度單位，資安管理單位負責程序及人員教育訓練，落實資安政策的導入及實施，本公司由稽核室擔任資通安全監理之督導單位，負責督導內部資安執行狀況，並由稽核室進行資安風險查核，如發現缺失，將要求受查單位提出相關具體改善作法，且定期追蹤改善成效，以降低內部資安風險，每年並就稽核結果定期呈報董事會。



(二)資通安全政策：

目的：為推動資訊管理系統，建立安全及可信賴之資訊作業環境，確保資料、 系統、設備及網路安全強化資訊安全管理，確保所屬資訊資產的機密性、完整性與可用性，及提：高相關人員資訊安全意識，以提供本公司資訊服務持續運作之環境，符合相關法規要求，避免遭受內、外部的蓄意或意外之威脅及提升服務品質，以達永續經營之目標。

範圍：

1.本公司之所有員工、合作夥伴或單位等，皆有責任遵循此一政策。

2.資通安全管理範疇涵蓋四個面向控制措施，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

2.1 組織面控制措施。

2.2 人員面控制措施。

2.3 實體面控制措施。

2.4 技術面管理。

(三)具體管理方案：

隨科技日新月異本公司持續建置與更新資訊安全管理系統，不斷落實相關管理措施，防範外部資安威脅，並建立內部人員之作業行為規範，藉以提昇公司整體資訊環境之安全性，及將低內部人員資安風險。

類別	說明	相關作業
權限管理	人員帳號、權限管理、與系統操作行為之管理措施	人員帳號權限管理及審核
		人員帳號權限定期盤點
存取管控	人員存取內外部系統及資料傳輸管道之控制措施	內/外部存取管控措施
		資料外洩管道之控制措施
外部威脅	內部系統潛存弱點、中毒管道與防護措施	主機/電腦定期更新措施
		定期執行網路安全檢測及修補
		病毒防護與惡意程式偵測
系統可用性	系統可用狀態與服務中斷時之處置措施	系統/網路可用狀態監控
		服務中斷之應變措施
		資料備份備援措施、本/異地備援機制
		定期災害還原演練

(四)投入資通安全管理的資源：

1.進行資訊安全教育訓練，提昇全體同仁資安知識與專業技能，本公司於新人報到時實施新進人員資訊安全教育訓練實務課程，藉以提昇公司同仁資訊安全認知，並針對專職人員進行相關專業技能訓練。

2.落實營運持續管理程序，訂定營運持續演練計畫（Business Continuity Plan, BCP)，每年執行營運持續演練以確保公司業務持續運作，在關鍵時刻發揮應變能力並提高資訊服務水準。

3.加入資安聯防機制，為強化主動防禦策略，本公司已加入TWCERT/CC 資安聯盟，藉由 TWCERT/CC 資安聯防機制，不定期取得資安及網駭情資，進行威脅情資共享，掌握業界經驗並及時提出內部資安告警訊，檢視內部設備及系統更新並持續強化防禦量能，提升重要合作廠商對我司商譽及資訊安全信任度。

4.113 年導入 ISO/IEC 27001:2022 資訊安全管理制度：已於114.3.25 被 SGS 通知為符合 ISO/IEC 27001:2022 要求之組織。

5.113 年導入 IEC 62443 4-1 產品安全開發：業已於同年 11 月通過認證。

6.設置之員工人數：

本公司採集團方式管理：

(1)資安人員：設置 2 名，含集團共 4 名

(2)資訊人員(輔助資安):設置 5 名

7. 114 年度會議討論次數：討論 ISO 27001 等議案計召開 8 次會議。

8.外部訓練：

序號	課程名稱	時數	參與人次
1	CYBERSEC 2025 臺灣資安大會	24 小時	2 人
2	奧義 AI 資安年會	8 小時	2 人
3	恆逸 CEH Master 總複習課程	14 小時	1 人

(五)重大資通安全事件所遭受之損失、可能影響及因應措施：

時段：最近年度及截至年報刊印日止

本公司於民國 114 年度發生一次重大資安事件發生，營運一切正常，經評估對公司財務及業務無影響。本公司已建構一套完整的多層次防禦措施，由外而內包含防火牆、入侵偵測、防毒系統、弱點掃描及修補程式管理等，以確保持續提升公司資安防禦能力。但面對不斷翻新的攻擊手法與防禦體系有時間差的固有風險，因此過去的防禦成果無法保證未來不會發生，因此本公司對於資訊安全的要求也將與時俱進持續優化。善盡資訊安全應當之注意事項及盡責之管理責任，降低公司的營運風險，維護客戶權益與回饋股東最大的投資價值與利益。