2023 年壓力測試

- 依 2020 年 12 月南亞科技董事會通過之「風險管理辦法」，各部門應依業務性質辨識作業流程風險、評估風險因子、建立風險指標與防範機制，針對高風險項目建立風險胃納及承受度或壓力測試，以有效控制及管理風險。

- 本公司 2023 年針對財務風險及非財務風險進行敏感性分析或壓力測試結果如下：

A.財務風險壓力測試-匯率

DRAM 銷售是以美金為主，假設 2023 年台幣兌美金匯率由 2022 年底的 30.71 升值到 29.50，預估最大可能的兌損約新台幣 3.5 億元。

B.非財務風險壓力測試: 如水資源風險-可用水量壓力測試，營運風險-電力供應，市場風險–均價及銷售量，營運策略風險-損益預測敏感度，法遵風險-反托拉斯、資訊安全風險-駭侵事件等。

a.水資源風險–可用水量壓力測試

- 檢視公司內、外部水源供應及蓄水系統，模擬各階段限水狀況，以自有備用水井(7 口)可供 5,500 CMD、蓄水池 43,000 噸，及調度長庚高爾夫球場井水(4 口)可供 3,600 CMD，在原水完全停水狀況下可維持工廠 47 天正常生產；
- 模擬一、二階限水及三階限水可能狀況：原水供五停二、供四停三、供三停四、供二停五，均不影響生產。

b.營運風險-電力供應

- 電力中斷會嚴重影響本公司生產製造，公司重要生產系統與設備，均與廠內 DUPS 系統及緊急發電機連結，可避免突發性電力壓降或台電計劃性限電所造成影響。
- 經檢視公司內、外部電力供應系統，模擬台電依契約容量減少 5%、10%、15%、20%電力供應時，以廠內緊急發電機及 DUPS 支援，仍可維持工廠正常生產；若外部供電完全中斷，則會造成停產的損失。以 2022 年營業額 562 億元計算，衝擊營業損失約 47 億元/月。

c.市場風險–均價及銷售量

- 公司定期對銷售量與售價兩因子進行敏感性分析，以確認業務目標的可實現性，並制定應變策略和計劃。
- 於 2023 年分析中可看出：

(1)預期價格較 2022 減少 33%，若年變動在-38%~-29%時的 EPS 變化

(2)預期銷售量較 2022 成長 13%，若年變動在+1%~+25%時的 EPS 變化。

d.營運策略風險-損益預測敏感度

制定銷售暨生產策略時，進行損益敏感度分析，從分析中可看出在各項定義的銷售暨生產產品組合下，搭配目標價格，分別進行 90%, 110%及 120%售價的變動下，各產品組合的損益影響，進而選定有利的銷售暨生產策略。

e.法遵風險-違反美國托拉斯法

•涉及違反美國反托拉斯相關法規，進行風險評估壓力測試。

•評估結果說明如下：

(1)若交運至美國地區之伺服器用記憶體模組之實際獲利為 625 萬美元，假設被害人係依據我方實際獲利認定其損害額。

(2)上述實際利得未超過 1 億美元，無須加罰兩倍。故刑事罰金部分，公司最高可罰 1 億美元。民事賠償賠償部分，最高可加乘實際利得 3 倍作為懲罰性賠償金，即約 1,875 萬美元。依此計算，換算為新台幣，總計約為新台幣 35.6 億。

(3)另可能造成不同程度的負面影響(如：公司形象與股價波動等)。

•風險控管方向：

(1)針對配合調查程序、支付訴訟費用、公司形象與財務等面向衝擊：透過評估內部所有證據，判定是否應儘速達成和解，以取得和解談判較優勢的地位及條件，爭取及早脫離訴訟或減輕責任，有效控制訴訟成本來達到降低風險。

(2)針對高階與員工觸法衝擊：透過提供員工/高風險人員法遵教育訓練與定期內部稽核等方式，確保法遵計畫的落實，並配套規劃董、監事責任保險來達到轉移風險。

f.資訊安全風險- 駭侵事件

•因應近年駭侵事件層出不窮，企業面對駭客威脅，除了事前防護之外，針對駭侵事件的處理，更需透過定期演練，以達到程序驗證、工具驗證與提升熟練度之目的。

•企業一旦發生駭侵事件，從通報、應變與復原皆必須與時間賽跑，透過演練可實際評估或測試各階段的處理時效，並將作業標準化或自動化，以簡化並提升整體時效，降低駭客入侵之衝擊。

•根據駭侵事件演練，調整系統偵測與回報方式、修訂緊急應變程序，並依降低災損原則，擬定個人電腦復原與優先順序，以達到事前預防、事發偵測與損害控制各階段目標。

•依據資安專業調查，駭客團體最快 18 分 49 秒即能完成入侵；另依據 2022 iThome CIO 大調查發現，高科技製造業平均 74%時間處於駭客攻擊狀況，且平均 9.1 天才會發現駭客攻擊。

•若能在駭客入侵前即予阻止，即能有效防止危害發生，本次在無預警狀況下，能於 15 分鐘內發現駭侵活動，並於 2 小時內完成系統回復，確認目前入侵偵測及應變時效符合目標。