腳踏實地
的資安風險控制策略

登豐數位科技
技術總監 黃建笙

他山之石，可以攻錯!!

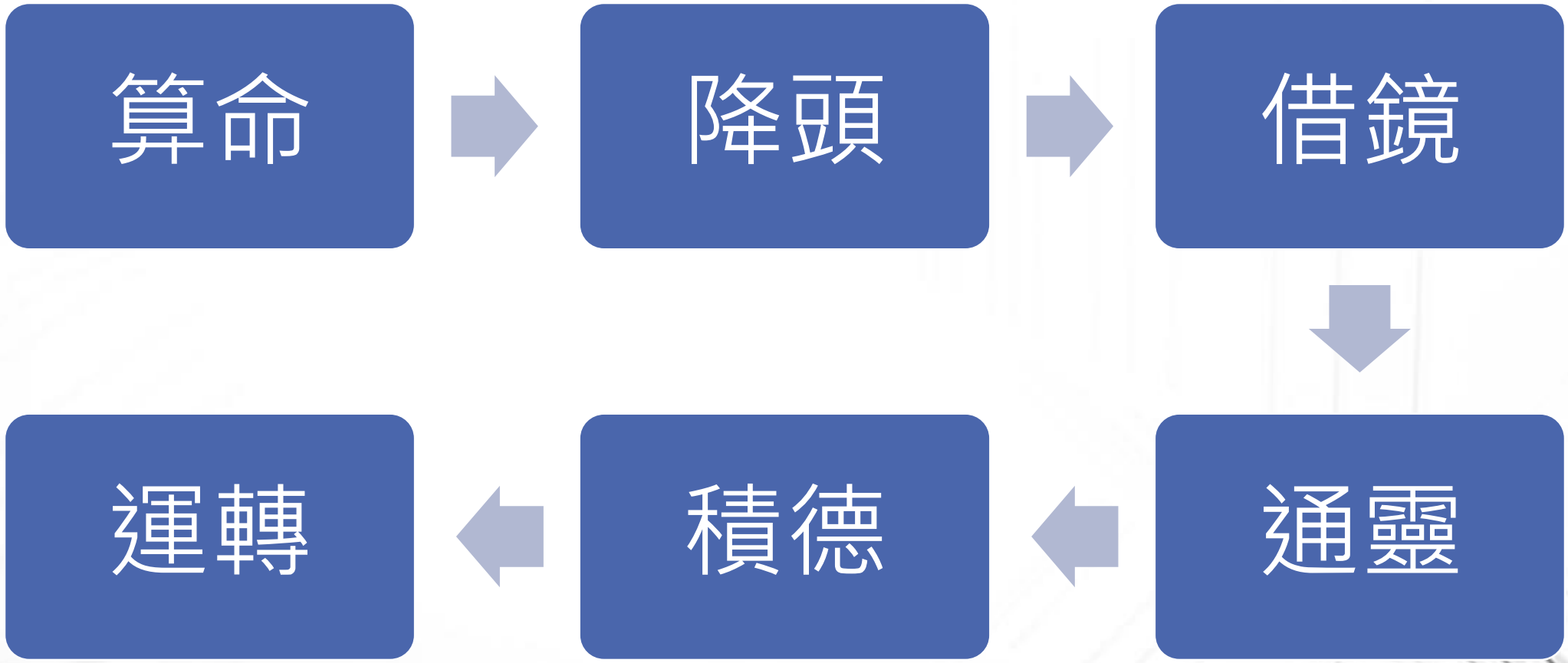
但是不能嘴!!!!!

風險管理的核心是：

損失降到

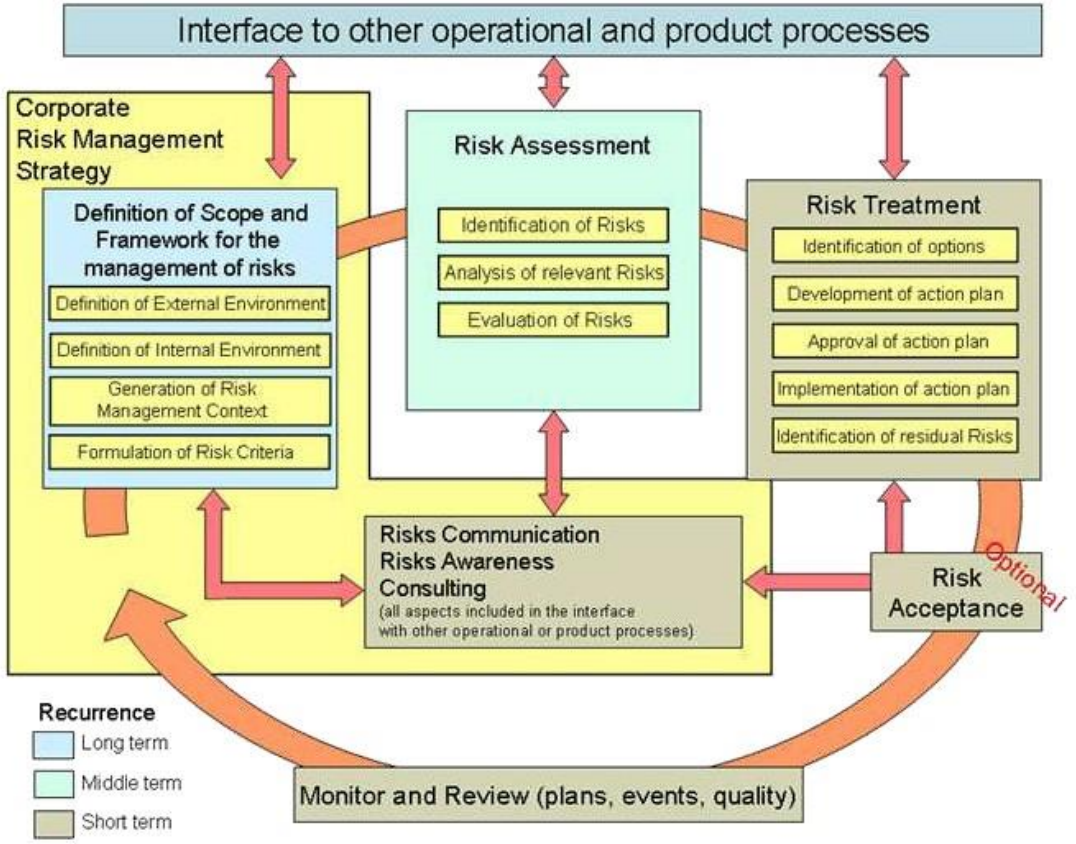
Owner可以接受就好!

風險不會乖乖待在表格上!



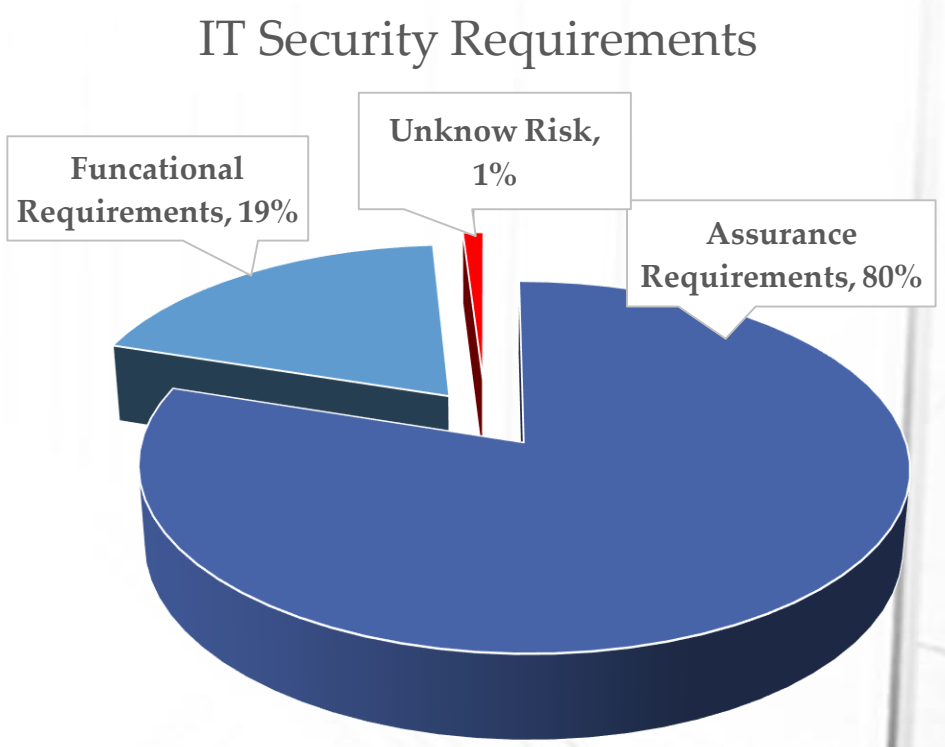
標準只是標準，別被框住!

- 快速幫你找出問題。
- 快速幫你算出數值。
- 快速幫你定出對策。
- 快速幫你...



別人家的事就是你的事

- 同條件下的企業80%是相同的。
- 另外的19%，是經驗!
- 1%是自以為是的安全
- 而產生的差異在於...
  你們沒有**妄想症**的員工!!



就控制處理流程上來說：

風險=不良率?

計算的方式差異

- 不良率=(不良品)/產出總數
- 單一因子損失=(資產價值*曝露因子)

但是...產線不是只有一關

風險也不是個別只有一個

不良率 VS 風險

流程

負面

輕重

品質

人力

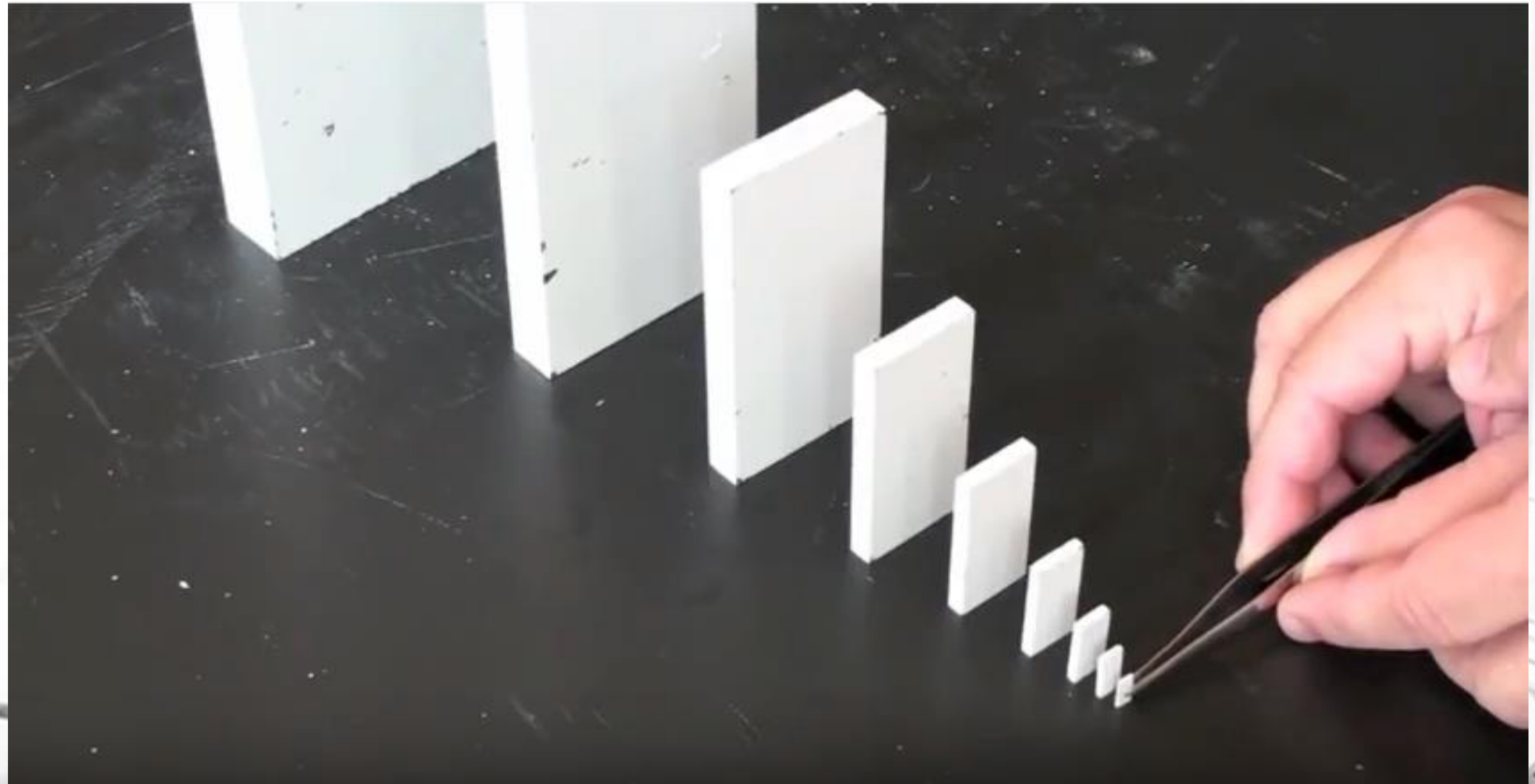
影響

$ $

流程是加倍影響

- 每一個關卡上的風險未受控，到下一個關卡影響就會加倍。
- 出現第二個互伴因子，影響會更大。
- 流程上不應該排除任何影響小的風險。
- 令你意想不到，昨天吃的感冒藥是死因。

連鎖效應都和莫菲定理一起來



風險和不良率一樣

都和錢有關!

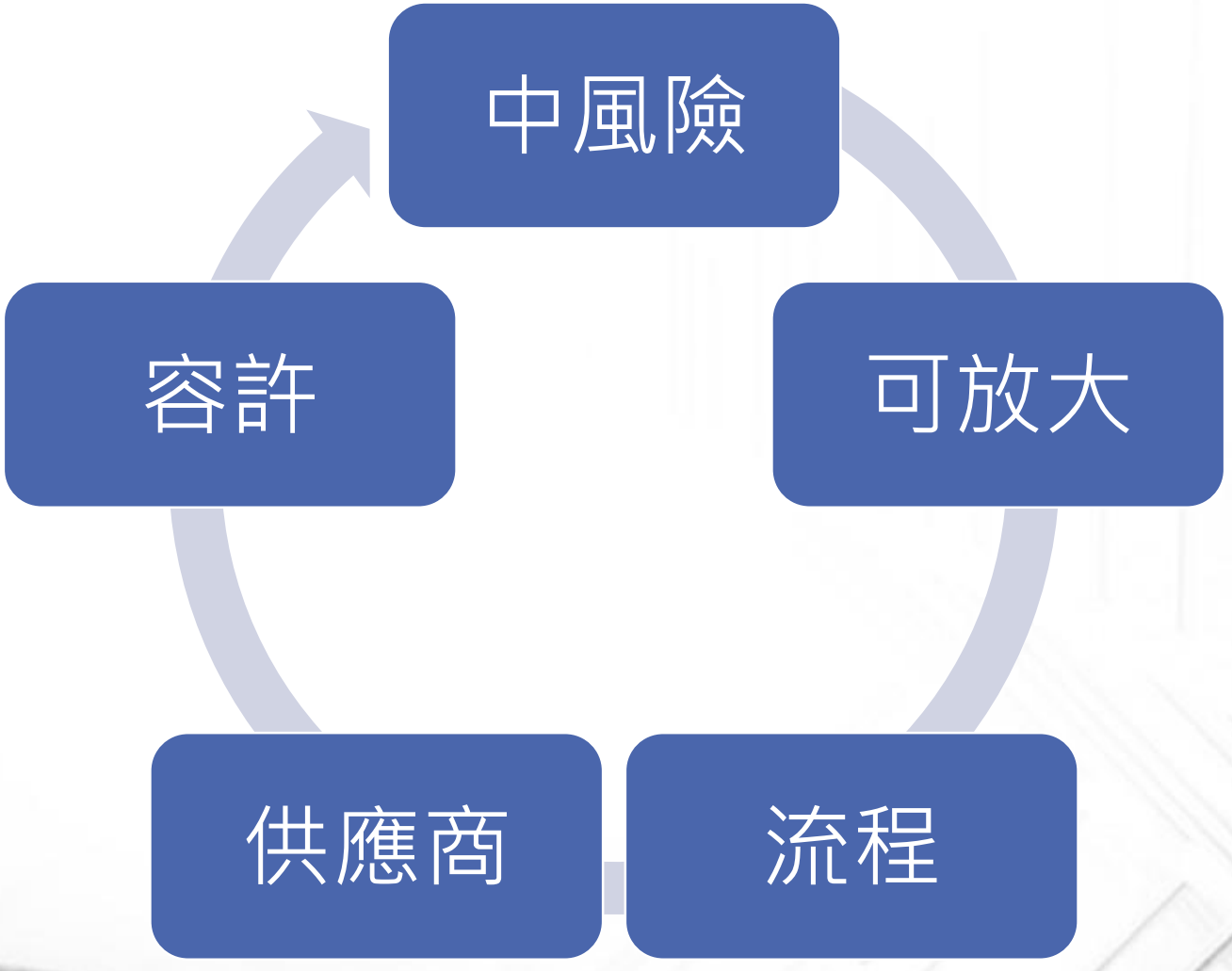
沒道理風險只在表上

不良率在刀口上

攻守互換才知道難

- 懂得攻擊，才更懂得防守!
- 守方：損失一分就全輸。
- 攻方：打下一分就贏。
- 該讓自已走出去，讓社群更活躍
- 別人出包別只是笑，要更努力的看!
- 肝臟如同鐘無豔，努力的付出要看見!

如果資源是有限的!



這個世界上

沒有任何一種解決方案

是終生有效的!!

有連結就有風險

- 網路是基本款。
- USB儲存裝置是常見的。
- 麥克風和喇叭讓電腦病毒講話也不是新聞。
- 連利用2G GSM 打War Walking，對岸都發生了。
- WannaCry能打進台積電，還有什麼不可能的!!
- Edward A. Murphy在天上看著你!!!


Murphy's Law means whatever can happen will happen.

墨菲定律告訴我們!!

資安負責人想到的事後一定會發生!!

解決方案是...

叫資安負責人別亂想!!

面對未知風險應該要

有錢人：

- 顧問、專家、導入各項解決80%以上問題的方案。

自行手工打造

- 胡思亂想是必要的、最好有一點妄想症。
- 參加社群維持身體健康、思想健全!!

任何一個問題的解決方案

都能涵蓋80%以上的需求

剩下的Owner能接受嗎?

唯有滾動的石頭不會生苔!

風險要時時Review!!

Thanks
Q&A