

BS 25999 - BCM 營運持續管理新趨勢

撰文◎林俊男

怡和保險經紀人股份有限公司 副總經理

Jardine Lloyd Thompson Ltd.

一、前言

有鑒於營運持續管理(Business Continuity Management, BCM)對企業發展的重要性，英國標準協會 BSI 已分別在 2006 年下半年及 2007 年 11 月公佈了營運持續管理系統標準推行指引 BS 25999-1:2006 Code of practice for business continuity management 及系統驗證標準 BS 25999-2:2006 Specification for business continuity management。企業對營運持續管理愈來愈重視之際，此標準的制定提供了良好的參考指引。

經歷過 921 大地震、SARS 等重大災害事件，台灣很多企業都已規劃了營運持續計劃 (Business Continuity Plan, BCP)，以因應未來可能的重大災害事故。企業不只要能管理短期性的重大災害，為提升企業長期競爭力，企業組織運作必須結合風險管理，以彈性策略強化企業恢復力(Enterprise Resilience)；以營運持續計劃為基礎，從而建立、推行、運作、監督、檢討、維持及持續改善的營運持續管理系統(Business Continuity Management, BCM)。

二、BS 25999 營運持續管理系統標準架構

英國標準協會 BSI 所制定的營運持續管理系統標準 BS 25999，基本上是以建立、推行與運作、監督與檢討、維持與持續改善(Plan, Do, Check and Act) PDCA 管理循環為架構，如圖 1 所示。

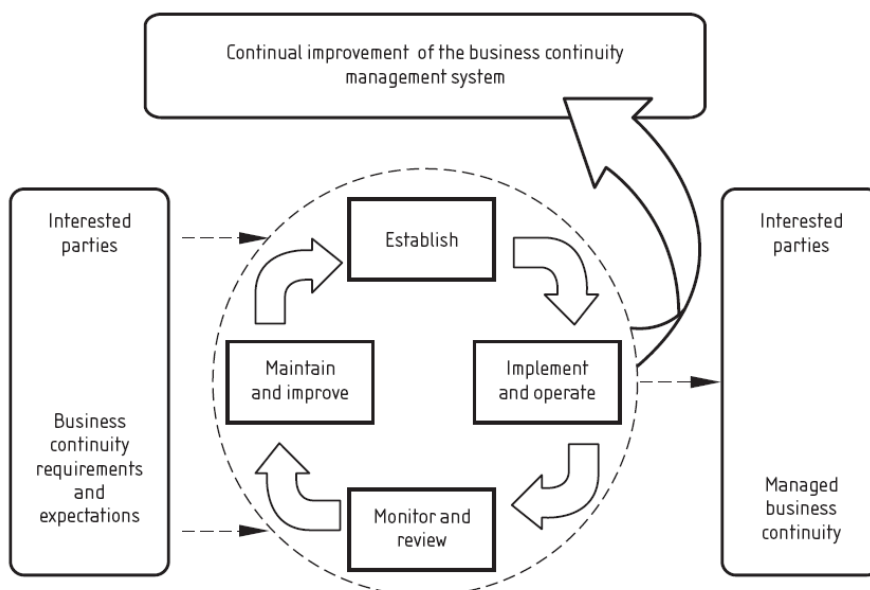


圖 1 BCM 管理系統 PDCA 管理循環 (摘自 BS 25999-2)

所謂 **BCM 管理系統的 PDCA 管理循環**是指：

1. 規劃 **Plan**：了解企業營運持續需求及必要性，據以建立企業營運持續政策、目標、標的、控制措施、流程與程序，以管理風險及改善營運持續性，得以符合組織全體之經營政策與目標；
2. 執行 **Do**：推動及運作營運持續政策、控制措施、流程與程序，以管理組織全部的營運持續風險；
3. 檢討 **Check**：根據所設定之營運持續目標及政策，監督與檢討 **BCM 管理系統**的績效及有效性，並將結果向管理階層報告，以檢討並決定補救及改善措施；
4. 改善 **Act**：根據管理階層審查結果，以及 **BCM 管理系統**的範圍、政策與目標之重新評價結果，採取預防及矯正措施，以維持與持續改善 **BCM 管理系統**。

PDCA 管理循環架構已在其他國際標準一再重複被運用，例如 **ISO 9001 品質管理系統標準**, **ISO 14001 環境管理系統標準**, **ISO 27001 資訊安全管理系統標準**, **ISO 20000 資訊技術服務管理系統標準**等。此趨勢有利於企業進行內部管理系統整合以減少重覆並提昇效率。

三、企業營運持續管理策略

在 **BS 25999-1** 推行指引中對提昇企業恢復力，明確的提出幾項參考做法，包括以下幾個方面：

- 人力、技巧及知識
- 工作場所設施
- 支援技術
- 資訊數據
- 設備與補給
- 人員救濟

茲分述如下：

1. 人力、技能及知識

對於企業運作關鍵的技能與知識，應採取適當的策略以確保能持續運作，可考慮的措施包括：

- 對員工及包商作多重技能訓練
- 關鍵技能須分散在不同員工身上，避免過度集中
- 由第三者提供關鍵技能
- 知識保存及管理

2. 工作場所設施

爲了降低重大意外事故的衝擊，可考慮以下替代措施：

- 在公司內設置替代工作場所設施

- 由關係企業提供替代工作場所設施
- 由第三者提供替代工作場所設施
- 在家或公司以外地點工作

3. 支援性技術

當重大意外事故發生時，支援性技術持續運作的策略隨企業型態不同，而有不同的方式，包括：

- 由公司內部支應
- 由外部單位提供服務給公司
- 由第三者在外部提供服務

例如，當企業資訊系統完全癱瘓，則可能需要全部改由人工維持運作直到資訊系統回復為止。

4. 資訊數據

公司運作重要的資訊，不管是電子式或書面資料，都應適當保護且維持可恢復性。異地備份資訊必須確保：

- 機密性
- 不同資訊來源間的一致性與完整性
- 須可重新安裝

另外，運作中資訊(亦即，尚未備份之資訊)如何確保不流失也應事先規劃。

5. 設備與補給

關鍵設備或零配件維持適當庫存可考慮的策略如下：

- 庫存在其他地點
- 由第三者隨時支應補給需求
- 分散及時供應系統至其他地點
- 暫存於外部倉庫或發貨地點
- 將次組裝作業移至替代地點
- 將舊設備作為緊急備用
- 對於獨特且前置期較長之設備須有額外的風險控管
- 關鍵製程須作地理上的分散

對於關鍵供應商可考慮的策略如下：

- 多重供應商
- 鼓勵或要求供應商建立營運持續之恢復力
- 與關鍵供應商訂定優先供貨合約
- 找尋替代供應商

6. 人員救濟

重大事故發生時，可考慮的人員救濟活動包括：

- 緊急疏散及人員清點
- 持續對員工/客戶溝通及安全提醒
- 安置因事故無居所之員工或包商
- 復健服務(物理及心理)
- 家庭照顧
- 交通協助
- 電話通知員工及家屬
- 協助無居所之員工及訪客暫時居住處所

另外，風險轉移也是必要考量的策略之一。保險是財務上最後一道防線，在規劃營運持續管理計劃時，企業保險承辦單位宜納入專案小組，搭配風險鑑別結果與復原策略，檢視公司產險保單是否有足夠的保障，例如：

- 是否購買營業中斷保險，且保障是否足夠
- 是否購買因供應商外包商所引起的間接營業中斷保險(contingent business interruption)，且保障是否足夠
- 附加保障條款保障範圍是否足夠，例如：ICOW (Increase Cost of Working)條款等
- 保單內容之排除條款與限制條件
- 是否考慮因事故造成第三者損害之相關責任保險

保險是企業在重大事故之後，得以重新恢復營業之重要財務支柱，而保險理賠程序也宜納入營運持續管理計劃的一部份。

以上復原策略的選擇需考慮下列三項因素：

- 最大可容忍期間 maximum tolerable period
- 成本 cost
- 後果嚴重程度 consequence

因此，建議以整合風險成本(total cost of risk)的觀念來管理企業營運持續策略。所謂整體風險成本包括，風險控制費用、保費、及事故自留損失等(參見圖 2)。這三項成本是互相關聯的，所以需要以長期的觀點整合管理以降低且穩定全成本。茲說明如下：

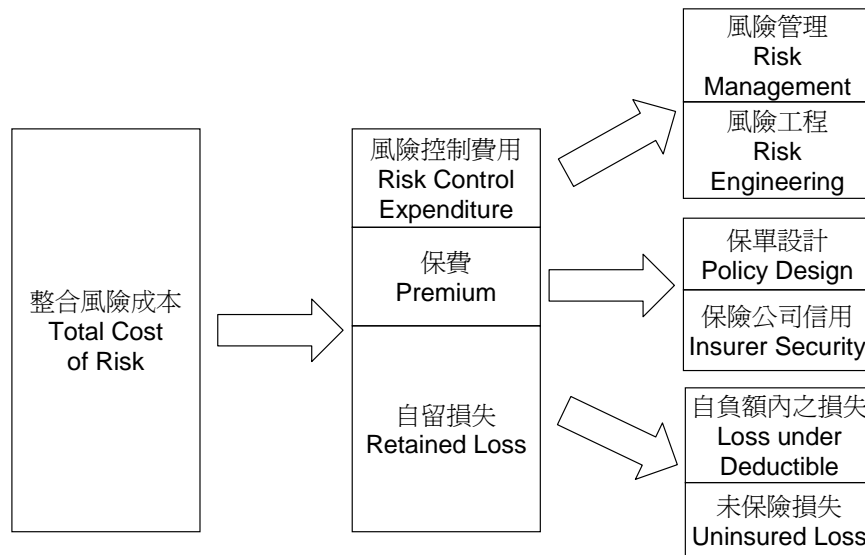


圖 2 整合風險成本之架構

一、風險控制費用

風險控制費用包含，企業內風險管理組織之行政費用、風險管理改善計劃推行費用、風險控制工程費用等。這部分的費用最不容易反映它的投資效益，因為，沒發生事故是否為風險控制改善的結果無法判定；而且，作了風險控制改善能反映多少保費的降低也沒有公式計算。然而，風險控制是降低風險損失的根本措施，保險只是彌補不確定性的風險損失。

二、保費

影響保費高低因素包括，保險市場供需行情、被保險人風險品質、保險單涵蓋範圍、保險及再保險公司之信用評等、及自負額高低等因素。保費一分錢一分貨，重要的是能根據企業本身的風險特性安排適切的保單結構，才能提供合宜的保障。

三、事故自留損失

提高自負額可降低保費，相對的也增加了自留損失的潛在風險。而且，保險並不能涵蓋所有可能的損失，除了自負額以內損失必須由企業自行負擔之外，還有很多潛在風險損失是保險不承保的項目。尤其，重大事故之後的商譽損失更是難以彌補。因此，唯有投入風險控制改善才能真正降低損失風險。至於自負額的決定，除了保險公司要求的額度以外，可以衡量公司財務狀況，包括獲利情況與淨流動資本(net working capital)等，以評估是否有足夠的財務能力負擔額外的自負額損失，以及其成本效益。

四、結語

營運持續管理的目的不只是建立營運持續計劃，企業更要透過營運策略結合風險考量，逐步調整生產或服務流程，以強化企業恢復力。建立企業恢復力，由於策略及內部程序的改變，讓企業運作更有彈性、更能有效因應市場需求驟變。因此，不僅讓企業能承受重大災害事故，同時也提昇了企業的可信賴度與競爭力。

英國標準協會 **BSI** 已開始接受企業申請 **BS 25999** 標準符合性驗證，透過第三者驗證證書的取得，企業也可以向客戶展示穩定供貨或提供服務的能力，以爭取長期穩定的訂單。對於購買營運中斷保險的企業，也可能據以向保險市場爭取較優惠的費率。

未來 **BS 25999** 也可能進一步被 **ISO** 國際標準組織所採用成為國際性標準，一旦一些國際性大廠也認同此標準，將有可能把它納入對供應商的要求，透過供應鏈影響整個產業。因此，有必要持續觀察此標準未來發展的趨勢，及早因應市場的變化。(完)