

國際最新營運持續標準甫發行，即引起全球企業高度重視

BCM 營運持續管理國際標準 BS 25999-1:2006
Code of practice for business continuity management
營運持續管理作業要點
已於 2006 年 11 月底由 BSI 英國標準協會正式發布



BCM 營運持續管理 (BCM, Business Continuity Management)

讓企業中斷機會減至最低- 營運持續能力增至最大
Minimizing disruptions – Maximizing recovery

蒲樹盛 (Peter Pu)

BSI 英國標準協會 協理

ISO 27001 資訊安全管理系統 產品經理

BS 25999 BCM 營運持續管理系統 產品經理

e-mail : peter.pu@bsi-global.com

壹、前言

組織經營過程中，充滿許多挑戰與變化，許多異常事件若無妥善制度管理，將迅速擴大為危機與災難，如何洞燭機先，善用預防制度來規劃這些無法預料的事，已是組織管理必備之管理技能。

近年來營運持續管理(BCM, Business Continuity Management)已受到國際高度重視，各組織無不積極導入與實施。營運持續管理(BCM)之目標係為防制營運活動的中斷，經由實施營運持續管理作業及營運持續計畫(BCP, Business Continuity Plan)，結合預防和復原控制措施及程序，將災難和管理缺失（可能是由於自然災害、意外、設備故障和蓄意行為等引起）造成的營運中斷情形降低到可接受的等級。

貳、營運與危機 - 如何預料無法預料的事(Expect the unexpected)

組織可能面臨營運中斷之風險十分複雜，經驗顯示其衝擊大多可歸納於來自下列一種或一種以上之情境：

- 內部服務失效
- 財務失效
- 營運成本增加

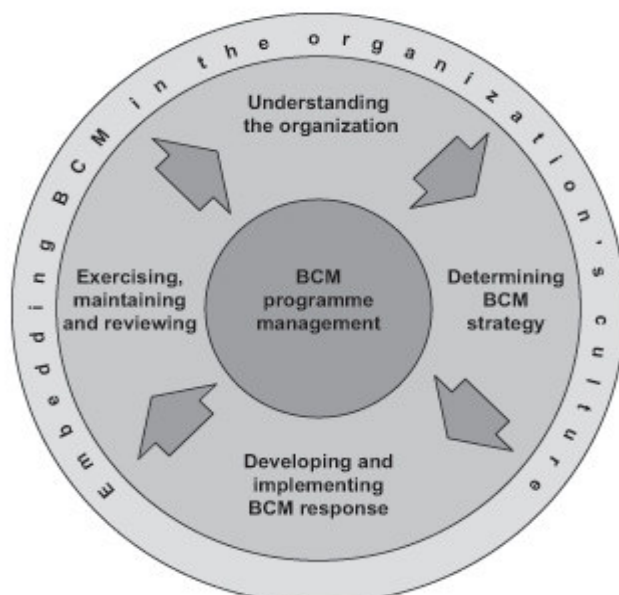
- 市場佔有率喪失
- 違反法律、法規或標準
- 人員安全風險
- 政治的、法人的或人員的困境
- 違反道德責任
- 信譽受損
- 喪失商譽及形象
- 喪失營運或環境控制能力

以上情境均可作為組織發展營運持續計畫(BCP)之參考劇情。更重要的是，組織應落實公司治理精神，妥善管理營運風險(business risk)及作業風險(operational risk)。

參、營運持續管理(BCM)架構

為使讀者能夠瞭解營運持續管理(BCM)之架構，將逐項說明營運持續管理(BCM)步驟及應採取之行動。

營運持續管理(BCM)之生命週期可包括下列幾個階段：



BCM 生命週期 (資料來源: BS 25999-1)

一、瞭解您的組織 (Understanding the Organization) :

每個組織應對其所處環境進行分析，可從可能引起營運過程中斷的事件開始，如設備故障、水災和火災，可採用下列兩種方法來分析營運中斷之衝擊與風險：

1. 風險評鑑(RA, Risk Assessment,)

RA 的目的在鑑別、定義與評估組織資產所面對的威脅、弱點及其風險值，以便確立可接受風險程度以及管理風險相關的行動計劃。這些風險可能歸屬於組織內部或外部，應仔細評估其發生機率及衝擊。

2. 營運衝擊分析(BIA, Business Impact Analysis)

BIA 的目的在鑑別：

- 關鍵營運流程 (Critical Business Processes) ；
- 關鍵營運流程中斷對組織造成之傷害或損失；
- 關鍵營運流程及其附屬項目復原至作業同意水準，所要求的可接受時間長短-復原目標時間(RTO, Recovery Time Objective)。

BIA 的鑑別過程中，應將下列方面納入考慮：

- 損害程度之等級-包括收入損失、附加成本、商譽損失、喪失競爭優勢等
- 最低營運程度所需之員工,技能,設施及服務
- 復原至最低營運程度所需之員工,技能,設施及服務所需之時間
- 完全復原至原服務水準所需之員工,技能,設施及服務所需之時間

以上兩項活動都應讓營運資源和作業的擁有者(owner)完全參與。重點在瞭解組織所面臨風險發生的可能性和衝擊，並鑑別出重要營運過程及排定優先順序。結合 BIA 與 RA 優先進行 BCM 與風險控制，將促使組織依成本及效益考量預先部署所需機制，及早建立緊急因應程序、備援方案及復原程序，傷害將可避免或減低！

二、決定營運持續管理策略 (Determining BCM strategy) :

組織瞭解了可能的風險（或災難）後，應針對風險之優先順序決定將採取之策略。

決定策略並不容易，須仔細考慮組織營運目標、資源、文化、流程及投入成本。一般來說，處理風險的策略可以從下列方向考慮：

- 1、 避免風險：當該風險影響極大時，便應設法極力阻隔風險。
- 2、 降低風險：採取適當控制措施，當風險發生時可因適當控制而將損失減

少。例如：建立災難應變的聯繫機制。

- 3、轉移風險：考慮購買適當的保險，作為持續營運過程的一部分。許多遭逢災變的災民，均因缺乏保險，而沒有任何理賠補償，加重了災後復原的負擔與痛苦！
- 4、接受風險：對於可接受之風險便可採取接受因應。

三、發展及實施營運持續管理回應 (Developing and implementing BCM response)

組織應發展 BCP 計畫以維護營運操作，或在關鍵營運過程中斷或故障後在必要的時間內恢復營運，營運持續管理計畫作業應考慮以下內容：

- (a) 計畫啟動條件（評鑑辦法、應參與人員等）應清楚說明各項計畫需遵守的啟動條件；
- (b) 職責說明：鑑別並協議所有權責，說明由誰負責執行計畫的那個部分，必要時應指定代理人
- (c) 緊急程序：在危急事件發生後，應採取那些行動，應包括公共關係管理的安排，及與適當有關機關（如警察、消防單位和當地政府）保持有效的聯繫；
- (d) 備援程序：必須在要求時間內完成最低營運水準復原工作，需特別注意與外部的營運依存要件（business dependency）與合約的適當性；
- (e) 復原程序：應採取那些行動以復原正常營運作業，包含鑑別必要的資源需求；
- (f) 程序文件化：確保所有計畫前後框架一致，並鑑別測試和維護的優先順序，如疏散計畫或任何現有的備援作業；
- (g) 維護時間表：應指定如何及何時測試該計畫，以說明及維護該計畫的程序；
- (h) 認知及教育訓練：旨在讓參與者瞭解營運持續過程，確保該過程持續有效；針對議定的緊急程序及過程進行適當的員工訓練，包括危機管理；

四、演練、維護及審查 (Exercising, maintaining and reviewing)

過去過度強調 IT 系統的演練，已被視為較狹隘的 BCM 演練，組織應嘗試對更廣泛之管理作為進行演練及測試。

1、對BCP計畫進行演練

營運持續計畫在演練階段時會面臨失敗的可能性，通常是由於假設錯誤、疏忽、或設備、人員之變動，因此應定期演練及測試，確保符合最新狀況及有效性，這類演練還應確保復原小組的所有成員以及其他相關人員瞭解計畫內容。

營運持續計畫的演練測試時間表，應指出各部分計畫的檢查方式和時間，建議經常對計畫各部分進行演練測試，應採用各種技術確保計畫能在實際狀況中運作，這些技術包括：

- (a) 針對各種情況進行沙盤推演（利用暫時停止營運，以狀況的範例討論營運復原程序）。
- (b) 狀況模擬（尤其在意外事件或危機範例後，用以訓練員工的定位管理）。

- (c) 復原測試（確保可有效復原）。
- (d) 測試異地復原（在主要營運場所外，同時執行營運作業和復原作業）。
- (e) 測試供應商的設施和服務（確保廠商提供的服務和產品符合合約中的規定）。
- (f) 完整演練（測試組織、人員、設備、設施和作業是否能夠妥善處理中斷情況）。

2、計畫的維護和重新審查

應透過定期審查和更新方式來維護營運持續計畫，確保其持續有效，應在組織的變更管理計畫中加入計畫的維護程序，以確保營運持續計畫的主要項目得到適當處理。

各個營運持續計畫的定期審查應分配責任；若發現營運持續計畫尚未反應營運作業的變更時，應對計畫作適當的更新，正式的變更管制應確保所公布的計畫都是最新版本，並且利用對整體計畫的定期審查來確保計畫處於最新狀況。

五、組織的BCM文化建立（Embedding BCM in the organization's culture）

僅建立計畫或程序是不夠的，建立文化是長期過程且可能遇見不可低估的抗拒，必須透過長期有計畫的教育訓練及宣導活動，讓參與者瞭解營運持續過程，確保過程持續有效，使組織建立BCM文化，使危機風險意識深入人心！

當任何事件發生時，若同仁對其管理能力均具有信心，則成功的 BCM 文化深化將已經開始。所有管理經驗均顯示並同意平時教育訓練是重要的，但往往流於形式或便宜行事，直到傷痛造成徒增遺憾！

肆、結語

未作準備是危機惡化的主因，BCM 管理程序的目的是提供不間斷的管理、協調與監督，以確定所有活動均以議定之方式執行與實施，以達成組織營運要求及危機管理目標。

從全球災難發生及災後復原過程中，有許多值得我們引以為戒的經驗，我們是否能改善現有缺失及訓練不足之處，將與未來災難後果有直接因果關係。台灣多屬中小組織，許多關鍵營運流程都必須依賴外部資源及產品服務，唯有前瞻卓越的管理視野，才能永續經營。我們是否已有完善因應方案，實應定期審查並及早準備！

營運持續管理(BCM)提供了很好的防護框架與指導，能否善用並確保您的營運持續，就考驗您的管理及執行力了！

未來 BCM 國際標準 BS 25999 將發行為兩部份：

- BS 25999-1:2006 Code of practice for business continuity management.
BS 25999-1:2006 營運持續管理作業要點
- BS 25999-2:2007 Specification for business continuity management.
BS 25999-2:2007 營運持續管理要求（即將發行）

BS 25999-2:2007 將明確規定有關 BCM 的驗證要求及流程，預計於 2007 年 8 月發行。屆時各企業及組織，可經由 BSI 之驗證取得 BCM 證書，證明其營運持續能力。BSI 將密切提供最新相關訊息及訓練課程，協助組織增加營運持續能力，提昇競爭力！

附錄：常見災難類型：

• **Natural Events 天然事件**

- Earthquake 地震
- Flood 水災
- Mudslide 山崩
- Hurricane 颶風
- Blizzard 暴風雪
- Tornado 龍捲風

• **Accidents 意外事故**

- Explosion 爆炸
- Fire 火災
- Power outages 電力中斷
- Broken pipes 管道破損
- Collisions from vehicles 車輛碰撞
- Hazardous material spill 危險物品散落
- Nuclear disaster 核災
- Terrorism, Sabotage and Acts of War 恐怖行動,破壞及戰爭
- Bombing 炸彈
- Kidnapping 綁架
- Mailing or spreading life-threatening bacteria or viruses 郵寄或散佈細菌或病毒

• **Miscellaneous events 各式事件**

- Explosion 爆炸
- Hardware, software failure 軟硬體失效
- Employee evacuation absence 員工離職
- Testing outage 測試中斷
- Human error and omission 人員錯誤及失職
- Disgruntled employee 員工不滿
- Malicious mischief 惡意破壞
- Riot 暴動