

## **BS25999:2007 之系統化展開**

**前言：**

BS25999 Business Continuity Management(BCM) 是英國標準協會繼 ISO9001(原 BS5750)與 ISO14001(原 BS7750)系統認證標準之後，又創造一波企業界反應高度熱切的一個新標準。它的目的是幫助組織鑑別威脅組織的潛在衝擊，建立彈性的框架，以保護股東、聲望、品牌與利益，有效因應能力之全面性管理程序。而所謂的全面性管理程序則是以利害關係者的需求為出發點，全面納入有關品質、物流、環境、工安、資安、風險管理等等管理系統要求，最終則能滿足利害關係者的要求並能持續不斷改善。而建置此套系統的難處就在於整合各項管理系統要求。主導人員與其 BCM 團隊需具備各方面的知識，方能統合協調各種矛盾。

**目的：**

之前 BSI 電子報已陸續介紹一些 BCM 的基本資料與概念。依最近 BSI 英國總部所傳回之 BS25999 認證最新訊息，全球 BSI 已認證發出證書的已超過十家，並陸續有更多知名全球性企業集團準備實施與認證。這些資料也彙集出企業實施 BCM 初期所稽核到的問題點，透露出非常值得深思的現象。其中第一名是組織並未讀過與瞭解 BS25999 標準，第二名是缺乏系統管理之觀念。簡言之即時在建置時不能建立一完整之系統架構，各項活動不能連接，缺乏一致性，就會產生許多資源浪費並且造成新的風險。

故本文章將依條文之架構，循序說明如何來系統化展開各項 BCM 要求，以利將來之維護與更新，並能和其他管理系統相容並進。

## 第一章：BCM 系統架構圖



上圖是 BS25999 Part-1 指導綱要所揭示的生命週期圖，各階段之說明如下：

**營運持續管理方案：**主要為建立 BCM 系統架構，指定角色、職掌與能力，並且做持續之維護與管控。它也是整個 BCM 生命週期的核心。

**瞭解組織：**主要包括 BIA 營運衝擊分析與 RA 風險評鑑。其目的是令組織能鑑別關鍵活動及所需資源來支持關鍵產品和服務，瞭解所受威脅以及選擇適當的風險處理方式。

**決定 BCM 策略：**依照前一階段所分析之風險與衝擊狀況決定適當的處理策略。

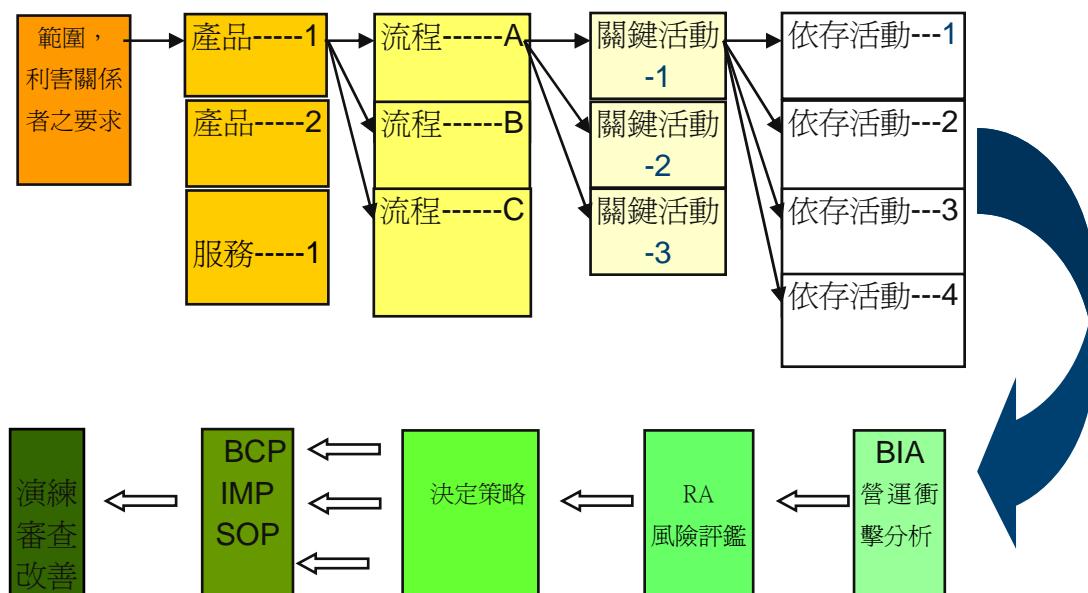
**發展和實行 BCM 因應：**其目的是令組織能發展與實施適當的 BCM 計劃與安排

來管理任何危急事件以及持續其關鍵活動，主要內容為 Incident Management Plan(IMP)危急事件管理計劃 與 Business Continuity Plan(BCP)。

**演練、維護與審查：**目的是驗證 BCM 安排的持續有效性以及較大的確保危急事件發生後，關鍵活動能依需求來恢復。

**將 BCM 植入組織的文化中：**目的為確保組織無論其規模或行業別能將營運持續植入其日常運作和管理流程，包括宣導與訓練，以及提昇人員對 BCM 的認知。

針對此生命週期圖我們的系統化展開架構為：



## 第二章：範圍與利害關係者

決定組織 BCM 範圍是架構 BCM 系統非常重要的第一件事，第一步就是要鑑別出所有相關利害關係者以及找出他們對組織的要求。下面這張簡單的表格可幫助組織做好這件事：

利害關係者	需求
客戶、潛在客戶	物料零件之供應，品質問題之處理，技術支援，樣品提供.....
消費者 (end users)	產品或服務品質之持續性...
代理商	.....
供應商	貨款...
職業公會	遵守公會決議....
老闆，董事會	利潤，公司治理....
管理階層	目標達成....
員工，工會	薪資，歸屬感....
員工的親屬	....
會計師，金融分析師	....
競爭者	競合協定....
股東	權益之確保，利潤分享....
媒體	及時之資訊提供....
技術母廠	權利金，技術保密....
政府，主管機關	法令法規之遵守，稅收....
特殊利益團體	....
附近居民	環境與噪音之保護，福利提供....
.....	.....

每個組織、不同行業其利害關係者的需求都會不同。表格中利害關係者與需求之內容只列舉其部份，組織應根據其產業別與市場特性深入並全面找出各種利害關係者與其需求。對利害關係者的分類愈細愈能充分鑑別出各類需求。

另外條文也列出需考慮：營運持續之要求，組織的目的與責任，風險的可接受水準以及法令，法規與合約上的責任。

考慮以上幾個因素以及參考組織之各地點的功能與職掌圖便能適當地鑑別出BCM範圍，不會漏掉高風險的部位。

### 第三章：關鍵產品與服務

瞭解利害關係者的需求與組織本身之需求即能明確鑑別出關鍵產品與服務，需注意的是不是每一個利害關係者的需求都會被鑑別成關鍵產品與服務，可以參考組織的主要責任與義務，主要營業收入，重要之法令法規以及客戶合約之要

求後，其重要性就能明確。另需注意”服務”的提供也是一種產品，服務業並不一定會提供實質性的產品給客戶，依ISO9001的定義，”產品”包括實質的硬體以及無實質的”服務”。

#### **第四章：流程**

此處所指之流程就是 ISO9001 所提之流程方法或過程方法。每一個流程即是以某個功能之六個面向的展開。如接單或採購功能，其包括輸入、輸出、資源、界面單位、方法以及衡量指標。前段流程的輸出會成為後段流程的輸入。系統就是由這些流程交互串聯所構成的。

每一個關鍵產品與服務都可展開其整個實現流程，一般是從產品規劃、接單一直到交貨，鑑別出所有主要流程與支持流程。每一個流程是由關連性較強的一連串活動所構成的。

#### **第五章：關鍵活動**

從上一章所鑑別之系統流程圖我們就可找出所有各種活動，但並非都是關鍵活動。依BS25999 part-2的定義指出，凡對於交付關鍵產品與服務有重要性與時間敏感性者。簡言之，當此種活動停止時對於交付關鍵產品與服務就會產生衝擊者即是關鍵活動。這個階段就要先做粗略的衝擊與風險的考慮，以明確鑑別出所有關鍵活動。

#### **第六章：依存活動**

支持關鍵活動的資產與資源都叫做依存活動。依存活動依BS25999 Part-1的說明可分成六大類：People人員、Premise地點、Technology技術、Information資訊、Supplies供應補給以及Stakeholder利害關係者。分成這六大類有利組織彙集所

有資產與資源，甚至在後面IMP危急事件管理計劃與BCP營運持續計劃所需的資源規劃也是劃分成此六大類。我們可以利用一個簡單的表格開始來鏈結關鍵活動與依存活動：

產品	齒輪軸		表 A
關鍵活動	關鍵活動之細部描述	依存活動	負責人
車削加工	生產線上各工作母機對原物料進行程序化的機械加工過程	CNC 車床	生產線組長
		合格校刀師傅	
		操作員	
		加工電腦程式	
		切削油	
		相關檢具	
		電力設施, 穩壓器	
		電力	
		加工工程圖	
		夾具與刀具	
		所浸漬之防銹油	
原料提供	提供鑄造粗坯	供應商	採購主管
		運貨商與卡車司機	

此範例僅供參考。企業組織可依其需要加入其他內容以充實之。

## 第七章：Business Impact Analysis (BIA) 營運衝擊分析

根據條文之要求，營運衝擊分析必須包括：

1. 鑑別關鍵活動
2. 鑑別這些活動中斷所造成之衝擊，並且決定出隨著中斷時間的增長，其衝擊程度的變動
3. 建立每一關鍵活動的最長可容忍中斷時間(MTPD)
4. 鑑別所有支持這些關鍵活動的依存活動
5. 在關鍵活動繼續的最長容忍中斷時間內設定復原目標時間(RTO)
6. 關鍵活動繼續執行的最低運作程度

7. 關鍵活動達到正常水準運作的最長時間

8. 依據復原之優先順序來分類這些活動

我們可以簡單地設計一張表格B來包含這些內容，並和表A做聯結：

									表B
時標 → 關鍵活動 ↓	1天	3天	7天	15天	最長容 忍中斷 時間 MTPD	最低運 作水準	復原目 標時間 RTO	復原優 先順序	回正常 水準運 作的最 長時間
車削加工	低	中	高	高	3天	50%	2天		4天

時標可依需要填入幾小時，幾天甚至幾週。而衝擊之大小可由組織自行分類，可分成高中低，也可評定分數。當關鍵活動下降至最低運作水準，隨者時間的增加其中斷的衝擊性也逐漸提高，直到不能忍受時則此時間段就是最長可容忍中斷時間 (Maximum Tolerable Period of Disruption)。

在此階段值得注意的有：

- 關鍵活動之中斷應該由下降到最低運作水準那點開始算起。
- RTO主要意義是一個點，不一定要很在乎其起算點，但一定要在MTPD那點之前，以保持安全距離，若是BCP(營運持續計劃)在操作時有產生意外，則仍有緩衝空間，以確保在MTPD那點之前能完成恢復。而BCP是需明確其實際操作時間，以令決策者知道在那個時限以前必須啟動BCP，以確保能於RTO那點之前能完成恢復行動。以表B範例來看，若BCP的時間是30小時，且其中斷是中斷時其營運水準直接降到0，則決策者只有18小時(48-30=18)的考慮時間來決定是否啟動BCP營運持續計劃，否則無法在RTO以前復原。
- MTPD與RTO會隨時間季節不同而有所變動，如市場的淡旺季，同業間之強弱變化與競合，人力資源組織，法令法規之更新等等變化。故需定期與不定期更新

BIA中的MTPD與RTO。

- d. 衝擊是針對關鍵活動中斷而非依存活動。
- e. 一個關關鍵活動的各項依存活動的RTO將會決定出關鍵活動的RTO。

## 第八章：Risk Assessment (RA) 風險評鑑

風險這詞的定義包括衝擊(嚴重性)與其可能性。風險評鑑主要目的是瞭解與評價造成關鍵活動與依存活動中斷之風險。依條文之規定此風險評鑑的內容應包括：威脅、弱點(原因)、衝擊(後果)、可能性與其風險控制方法。

風險控制方法一般可歸納成四種：

- 避免風險：當該風險影響極大時，便應設法極力阻隔風險。
- 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。
- 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！
- 接受風險：對於可接受之風險便可採取接受因應

我們可以再建立一張表 C，沿襲前幾章的 BIA 表 A 與表 B，展開此風險評鑑

							表 C
關鍵活動/依存活動	威脅	衝擊、後果	評 分	弱點	評 分	總 分	風險控制方法, IMP/BCP
車削加工/CNC 車床	設備故障	延誤交期 WIP 庫存增加 維修費用 停機期間無產 值		設備老舊			充足備品 成品安全庫存需 2 天 IMP-0325 BCP-0371

一般科學化管理都會將事情化成數字，以方便管理。組織應發展相關評分法則來

客觀地評價這些分數，並參考這些評定的風險分數進行策略的決定。

從圖表可看出威脅，弱點與依存活動相互排列組合就會產生多種風險組合。雖然數目會多，但我們以系統化展開與歸納就能有條不紊。

以上從第二章至第八章都屬於**瞭解組織**這階段的活動

## 第九章：決定策略

依風險評鑑所顯示之風險等級以及所決定之策略，在本章我們會將其展開成：

- SOP(植入日常作業)：如要求設置安全庫存水準，並列入日常監控。
- IMP(Incident Management Plan) 危急事件管理計劃：主要是在危急事件發生造成中斷時，當下的對應活動，包括：緊急救助與人員疏散、災害圍堵與損失評估。
- BCP(Business Continuity Plan) 營運持續計劃：在危急事件管理做到一個階段時，必須開始啟動營運持續計劃，以於 MTPD 之前將關鍵活動復原至最低運作水準。

IMP，BCP 與 SOP 都需要定期與不定期審查與更新，以確保符合 BCM 安排之所有相關要求，包括 BCM 政策與總體目標。

## 第十章：發展與實行 BCM 因應

主要工作是執行所決定之 BCM 策略，包括日常 SOP 之維持以及當危急事件發生時所需採取的 IMP 與 BCP。IMP 與 BCP 的內容在條文 4.3 有很具體的要求，但其編寫原則主要以時標(when)為順序，再詳述由誰來執行(who)，執行那些工作(what)，如何執行(how)以及所需參考之資訊。組織可設計一個標準格式來包括這些內容。而表 C 則在最後一欄提及相關 IMP 與 BCP 的計劃番號。負責人員在發生危急事件時能藉由 RA 表 C 很快找到 IMP 與 BCP 予以執行。

## 第十一章：演練，維護與審查

IMP 的有效性主要在於是否減少傷亡與損失，BCP 的有效性則在於 RTO 時間內復原關鍵活動。要確認 IMP 與 BCP 是否有效最好的方式就是演練。演練有各種不同規模與模式，組織應依適當性排出演練計劃並執行之，以確保 BCM 的安排符合 BCM 的目的與要求。

組織在日常也需注意各種會影響 BCM 安排的組織內外部變動，來更新 BCM 的相關安排。條文 4.4.3 所提必須建立一個審查與變更管制機制，可以考慮在定期經營會議中討論 BCM，並決定其變動與更新。

內部稽核與管理審查是一種全面與宏觀的審查制度，妥善使用可以見樹又見林的確認與更新 BCM 的實施成效。而所發現之問題可依條文 6.1.2 預防行動，6.1.3 矯正行動以及 6.2 持續改善的要求來做改進。整個 PDCA 的循環就可週而復始的轉動起來了。

### 結語：

前文所述之 BCM 生命週期之各階段工作，我們利用了三張表格(表 A，B，C)以及標準的 IMP 與 BCP 格式將之全部串聯起來，我們就容易來做系統化管理了。當這些表格全面發展完成以後，人員在碰到各種威脅與關鍵活動中斷時都能很快地循著這些表格找出相對應的 SOP，IMP 與 BCP 文件來予以執行。組織內外部有變動時，也能循著這些表格找出相對應的 SOP，IMP 與 BCP 文件來予以更新與審查。這就是所謂的 BCM 系統化展開。

### 附註：

本文所提之各種表格與其格式內容僅供參考，組織應依其 BCM 範圍與行業特性發展適合本身運用的表格與內容，並將這些表格予以串聯。同時也需透過訓練讓 BCM 團隊理解並能使用這些表格。