業務永續營運管理基礎課程

安侯企業管理股份公司
張祚豪　副理

99年09月09日

講師 – 張祚豪（Howard Chang）

現職：

安侯企管KPMG
資訊科技諮詢服務 副理

專業資格：

- 美國伊利諾大學香檳分校 會計碩士
- 美國愛荷華州立大學
  Information Assurance 碩士
- 國際電腦稽核協會（ISACA）會員
- 國際認證電腦稽核師（CISA）
- 資訊安全經理人（CISM）
- 國際資訊安全管理師（CISSP）
- 美國會計師（USCPA）
- ISO 27001 Lead Auditor 訓練合格
- ITSM Lead Auditor 訓練合格

資訊安全講授經驗 – 資訊安全訓練講師：

- 司法院
- 財政部臺北市國稅局
- 財政部北區國稅局
- 財政部中區國稅局
- 教育部
- 衛生署...

資訊安全實務經驗：

- 資訊安全管理制度（ISMS）輔導與維護
  司法院、教育部、晶元光電、台灣電力公司、衛生署
  財政部臺北市國稅局、財政部北區國稅局、財政部高雄市國稅局
- 金融保險業、製造業
  資訊環境一般控制（IT General Controls）查核
- 金融業 資訊安全委外廠商稽核
- Business Continuity Management review

簡報大綱

- 從「H1N1與氣候變遷」看「業務永續營運管理（BCM）」
- BCM基本概念
- 區網中心如何推動BCM
- 問題與討論

前言

- 本課程BCM名詞定義:

  BCM (Business Continuity Management)

  ＝業務永續營運管理

  ＝業務持續管理

  ＝營運持續管理

  ＝企業永續管理

  ＝業務持續運作管理

從「H1N1與氣候變遷」看「業務永續營運管理（BCM）」

引子-從SARS到H1N1

- 全球化的影響，地區性流行性疾病更易形成跨地區的大規模流行性疾病
- 大規模流行性疾病對組織業務持續運作(Business Continuity)的重大衝擊
- 大規模流行性疾病對人力資源安排的重大挑戰
  - 案例說明：大規模流行性疾病之BCM執行作為

引子-從氣候變遷到百年難遇一次的重大水災

- 氣候變遷=>氣候異常=>重大天災
- 重大天災對組織業務持續運作(Business Continuity)的重大衝擊
- 重大天災對基礎設施維運的重大挑戰
- 重大天災對人力資源安排的重大挑戰

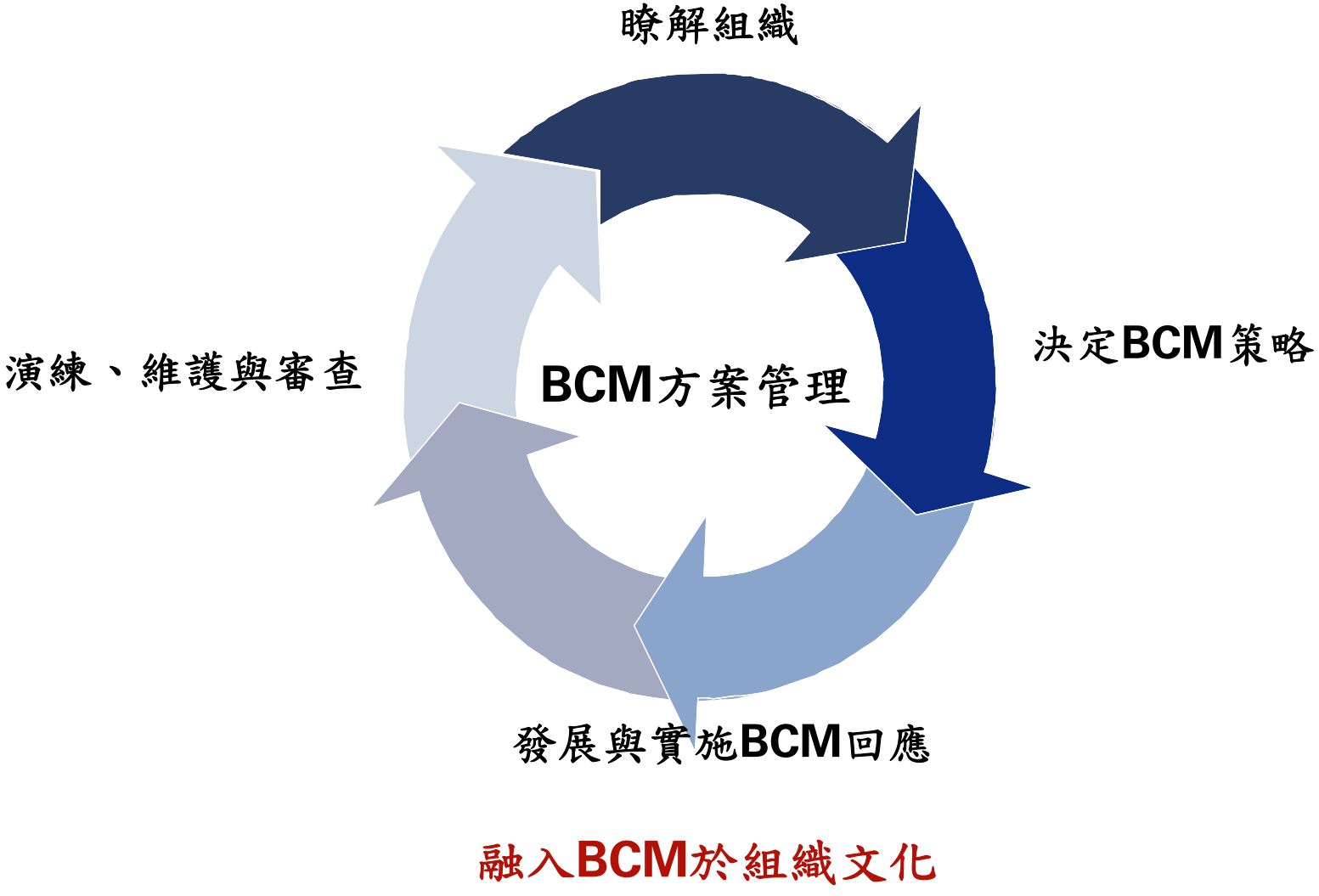
業務永續管理(BCM)之定義?

何謂營運持續管理?

是一個全面的管理過程。其鑑別出威脅組織的潛在衝擊，提供一具彈性的架構及有效反應能力之整體管理程序，以保護利害關係人、聲譽、品牌與價值。

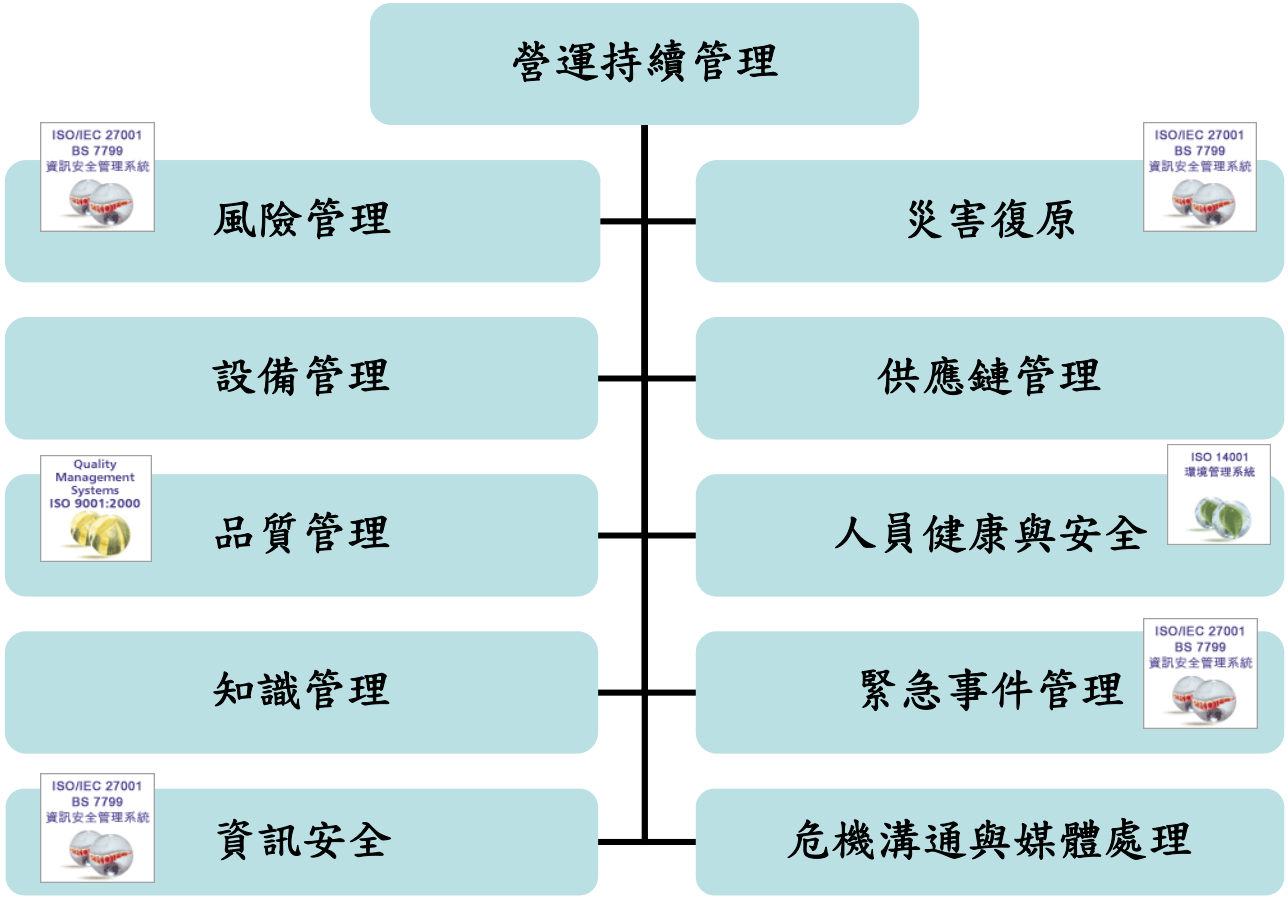
Source: BS 25999-1

業務永續營運管理(BCM)生命週期



BCM是一個整合性管理流程

- 營運持續管理為一管理流程，包含多個項目，且可與現有管理制度充分整合



他山之石- 新加坡金融局BCM演練

- BCM計畫與演練涵蓋服務供應鏈流程

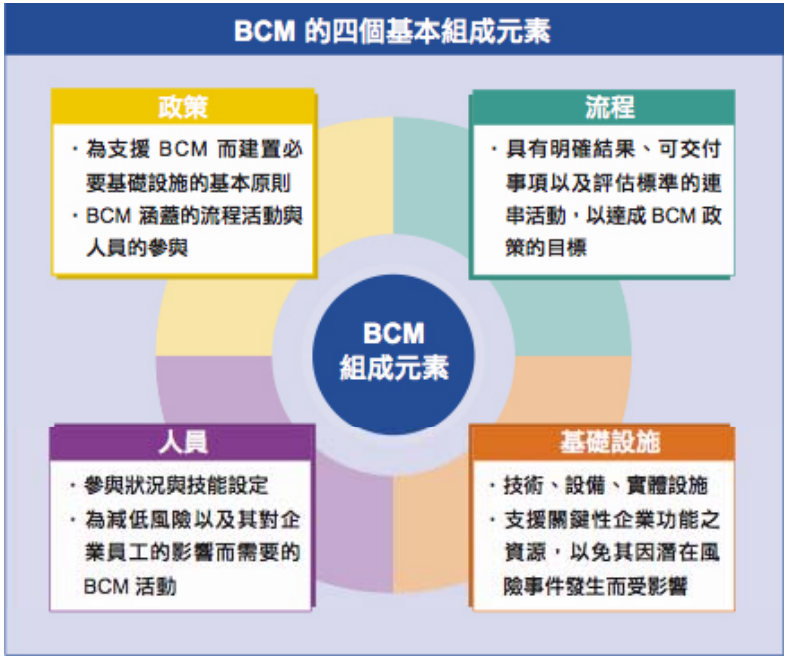
執行演練之前，新加坡金融管理局花了約4～5個月做準備，包括公布計畫、鼓勵企業參與，在確定參與的企業和人員之後，彙整所需的資源，包括提供場地作為緊急應變中心等。另一方面，也展開演練設計，藉由找尋相關資料並與產、官、學界合作，找出災難發生時可能發生哪些事件。等到一切備妥後，再召開演練前說明會。

演練當天，透過網站等方式，宣布災難發生後的各種情境，為了讓模擬情境更加逼真，還邀請電臺記者透過網站進行報導。舉例來說，當爆炸發生時，會有電力中斷、系統中斷、客戶打電話、其他分行員工打電話、相關新聞報導、警察到現場等等狀況發生，而企業便需隨著各個情境的發生做出相對應的回應，且必須記錄演練時的細節，以作為之後檢討的依據。

他山之石- 新加坡金融局BCM演練(續)

- 新加坡政府公開BCM標準與作業守則

新加坡政府技術參考文件 TR19：2005 將 BCM 描繪成涵蓋六大領域與四個基本元素：



- 2008年5月22日，新加坡政府宣布，所有向政府提供服務的服務供應商都必須擁有BCM計畫，否則，他們可能不能向政府提供服務

BCM的觀念與迷思-1

- 擔任組織的BCM主要管理人員(BCM權責主管與相關業務承辦人)，必須管理所有營運持續的相關活動!

- 正確觀念：

擔任BCM主要管理人員(BCM權責主管與相關業務承辦人)，必須負責協調所有營運持續的相關活動! 其他各單位應依據業務權責，分別擬定並管理各自的BCM計畫與活動。

BCM的觀念與迷思-2

- 應將BCM執行重點放在BCM策略規劃與執行上。人員健康與安全，是人事部門的職責，與BCM無關!

- 正確觀念：

BCM的首要任務，即是維繫人員的安全與健康。

BCM的觀念與迷思-3

- 沒有好的BCM政策，就不會有有效的BCM做法!

- 正確觀念：

好的政策，可以引導BCM活動可以符合業務目標並有效率的進行，但透過BCM各項實際活動，亦可反饋並修正組織政策!

BCM基本概念

業務永續營運管理(BCM)的演進

- 1979—Disaster Recovery(災害復原)
- 1986—Contingency Management(意外事故管理)
- 1989—Continuity Planning(持續規劃)
- 1996—BCM(業務永續管理)
- 200X—Holistic Approach(全面管理過程)

Risk Management

風險管理

BCM發展趨勢

- 成為組織管理活動重要的一環
- 已有國際組織推出業務永續營運管理相關規劃、建置、維運之指引文件，例如BCI(國際持續協會)的GPG
- 已發展出國際新標準（BS 25999）
- 整合組織所有營運功能，不再只限於IT領域
- BCM演練從個別組織單獨執行逐漸演變為整個體系／產業參與者共同執行，藉以確保供應鏈／服務鏈的營運持續能力，不會因為某個組織失去運作能力，而降低整個體系／產業的生產／服務效能

業務永續營運管理(BCM)相關標準

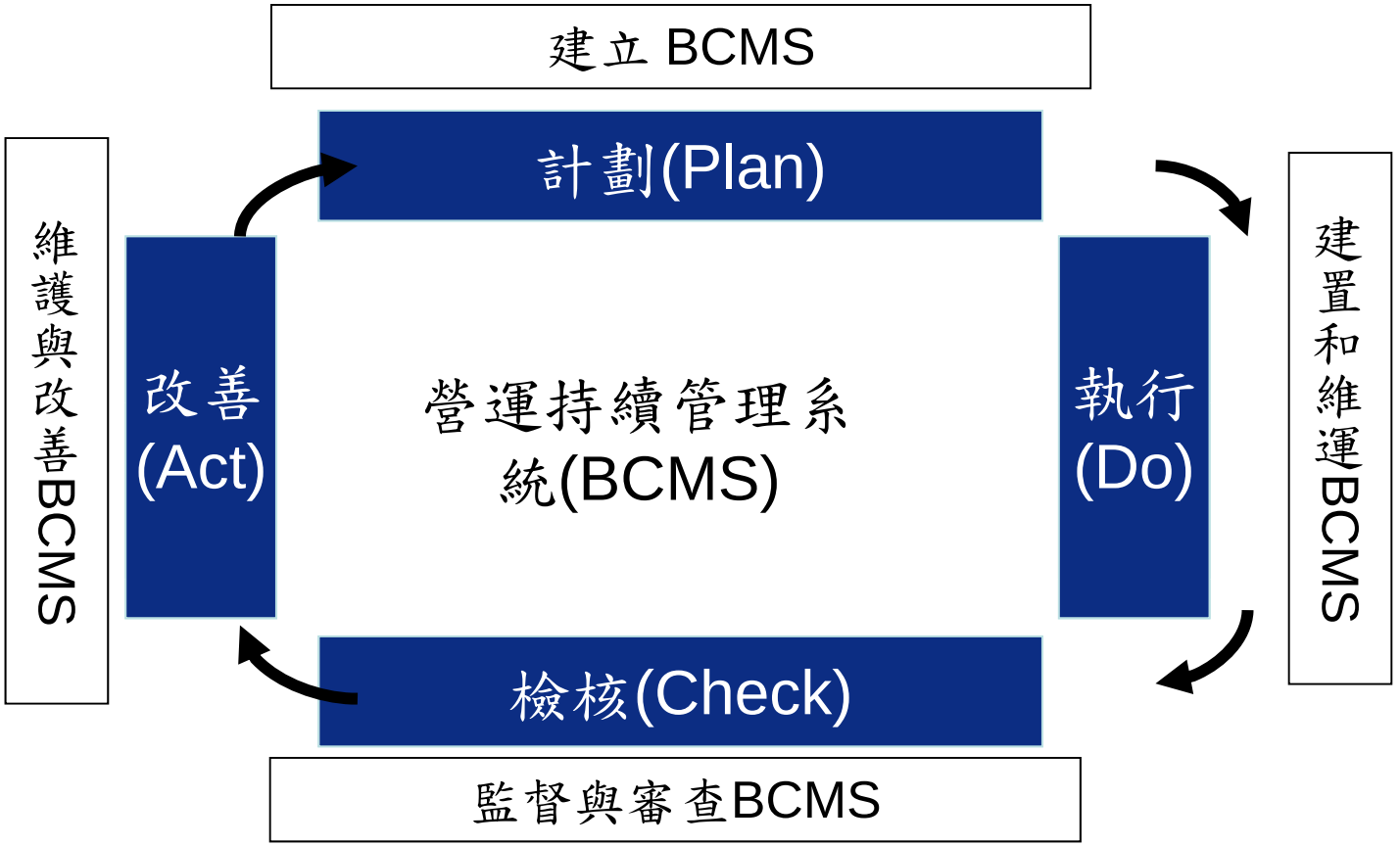
- PAS 56
- ISO 27001:2005 (A.14)
- ISO 20000 (6.3)
- ITIL (IT Continuity)
- BS 25999-1
- BS 25999-2
- BCI GPG (Good Practice Guidelines)
- PAS 77 (IT Service Continuity，未來將會成為BS 25777)

BS 25999說明

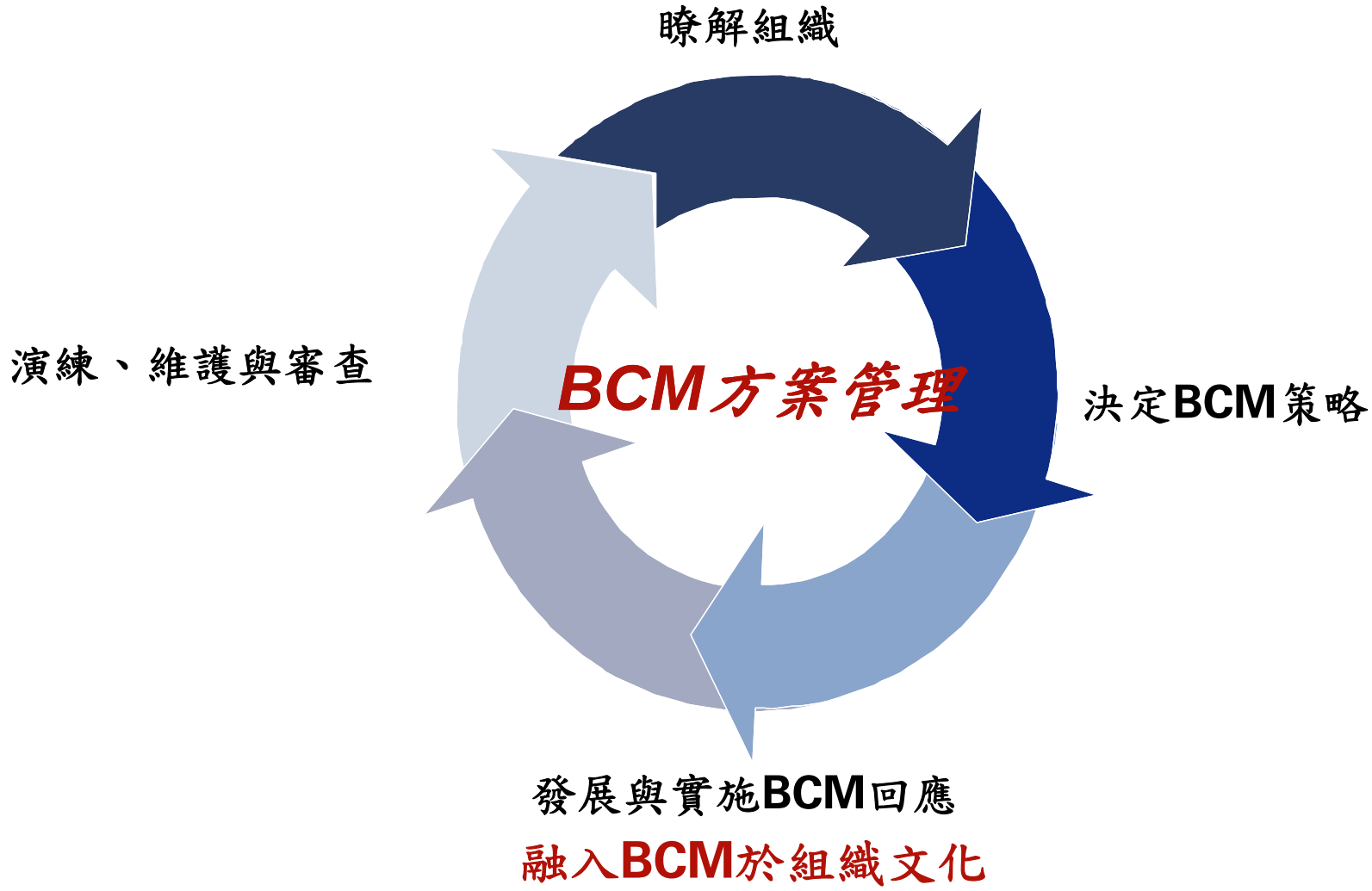
- 分成Part 1與Part 2兩個標準
- BS 25999-1:2006
  - 營運持續管理作業要點
  - 2006/11發布
  - 作為參考文件，提供營運持續的最佳作業方法指南
- BS 25999-2:2007
  - 營運持續管理系統要求
  - 2007/11發布
  - 提供營運持續管理系統之建立實施與書面化的具體要求
  - 包含建置營運持續管理系統所需要的PDCA管理架構與相關營運持續措施
  - 作為驗證標準

業務永續營運管理系統(BCMS)之PDCA架構

- BS 25999-2:2007



BCM建置與維運（生命週期）



BCM政策

- 政策與目標
- BCM管理方案範圍
- BCM組織架構（角色與責任）
- BCM政策內容

BCM管理方案範圍

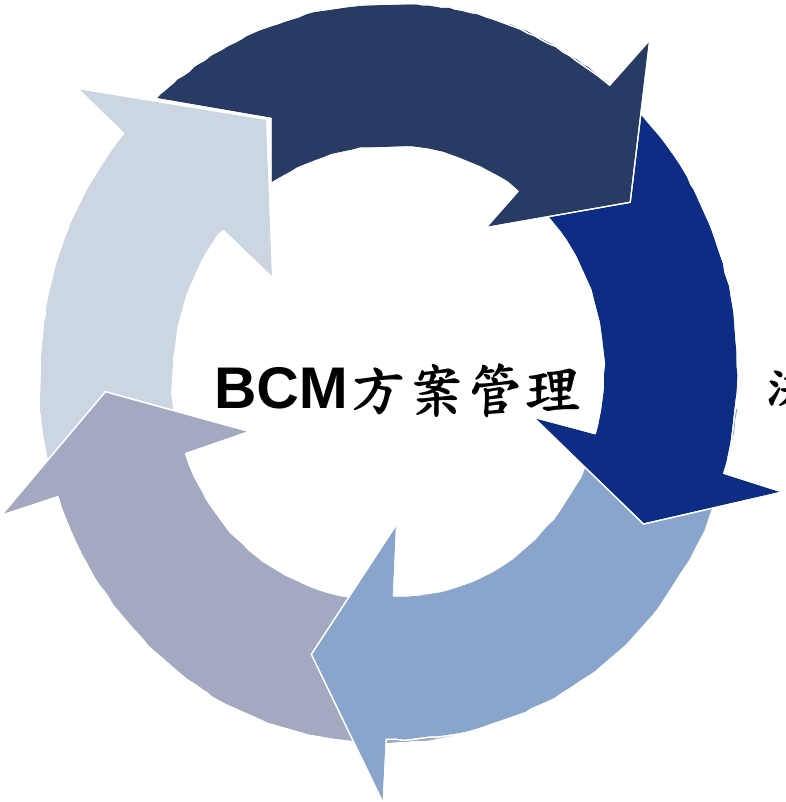
- 可同時（或部分）使用下列面向，定義與描述BCM管理方案範圍
  - 組織
  - 流程（委外與協同作業）
  - 系統／服務／產品
  - 各種邊界（例如網路邊界與實體邊界）

BCM組織架構（專案管理角色與責任）

- 管理階層應該
  - 指派專人/團隊管理BCM機制
  - 確認BCM範圍
  - 審查BCM所需預算
  - BCM績效監控
- BCM管理團隊應該
  - 發展BCM程序/決定BCM生命週期各階段之關鍵方法
  - 管理/執行BCM活動
  - 推廣BCM成果/管理BCM預算/維護BCM文件
  - 反應組織現況與法規需求
  - 進行差異報告/扮演BCM聯繫窗口/協助鑑別BCM需求與影響

BCM建置與維運(生命週期)

瞭解組織



決定BCM策略

發展與實施BCM回應

演練、維護與審查

融入BCM於組織文化

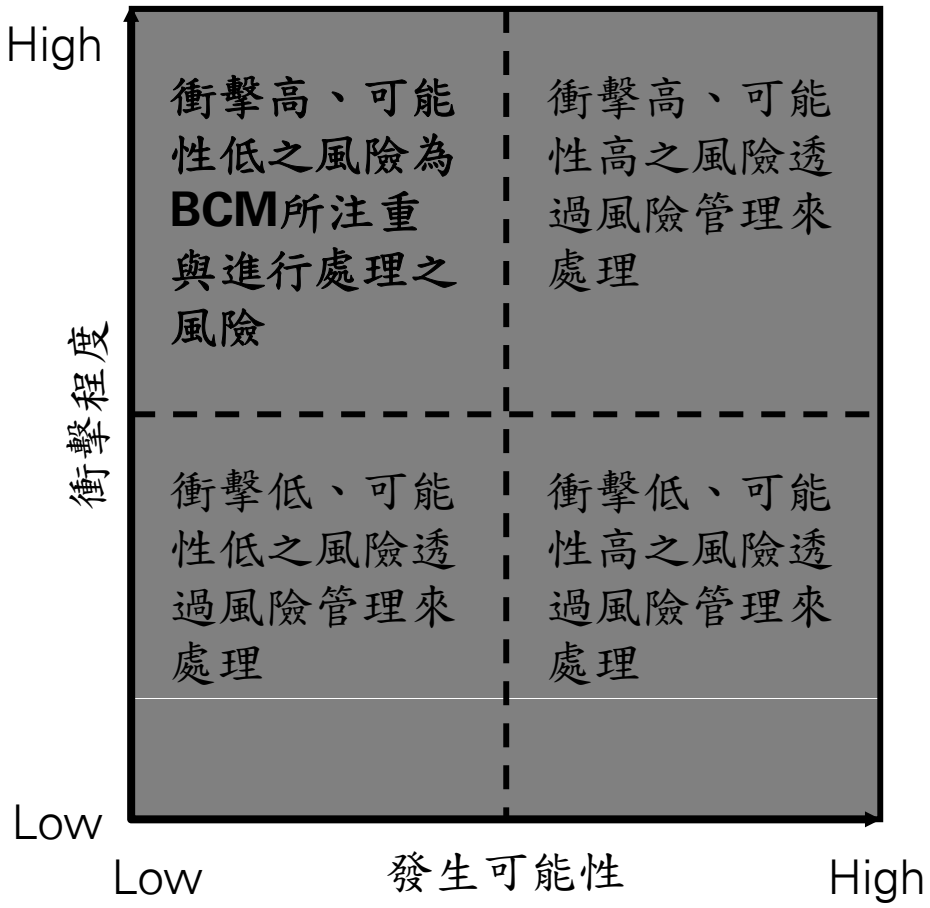
瞭解組織

- 瞭解組織之目的
  - 確認組織目標、利害關係人權利義務關係、關鍵業務、資產與資源
  - 分析重要業務中斷對於組織營運的衝擊(BIA)
  - 威脅評估與風險評鑑(Risk Assessment)
  - 風險控制與降低
  - 定義關鍵業務之最大可容忍中斷時間(MTPD) 、回復時間目標(RTO)與回復時點目標(RPO)
- 瞭解組織之方法
  - 營運衝擊分析(Business Impact Analysis；簡稱BIA)
  - 風險評鑑(Risk Assessment；簡稱RA)
  - 營運衝擊分析(BIA)執行要早於風險評鑑(RA)--BCM建議做法

營運衝擊分析(BIA)之目的

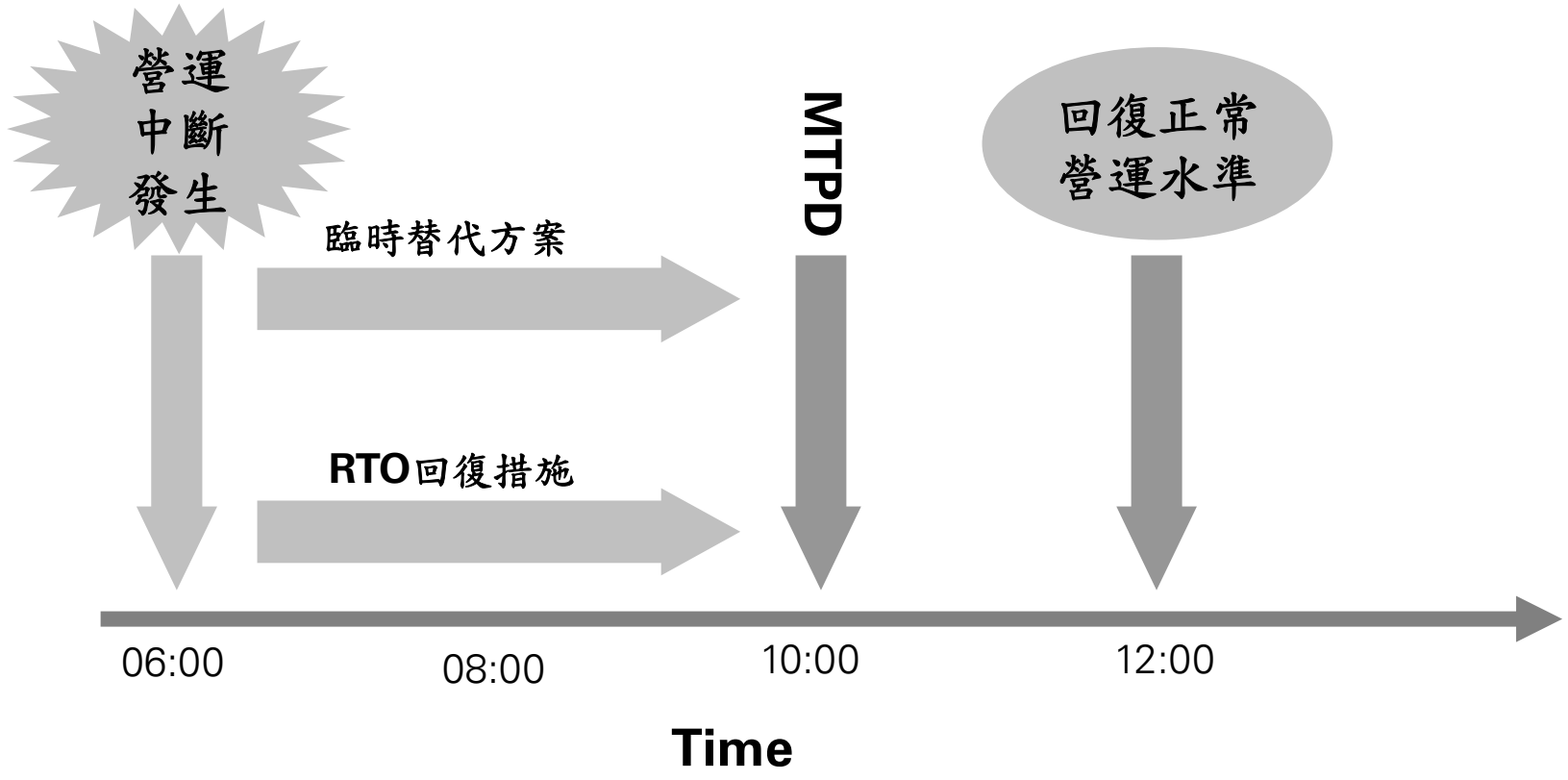
- 鑑別關鍵業務活動
- 鑑別相關衝擊
- 評鑑中斷時間對其衝擊程度
- 評估關鍵業務活動的最大可容忍中斷時間(MTPD)
- 鑑別支持關鍵業務活動的依存活動(包括供應商與委外廠商)
- 估計繼續每一關鍵業務活動的所需資源，並將利害關係者納入考量
- 評估復原目標時間(RTO)與復原時點目標(RPO)
- 定期或於組織活動有重大變化要進行營運衝擊分析
- 營運衝擊分析所評估之對象為高衝擊與低可能性之風險所導致後果

營運持續管理與風險管理之關係



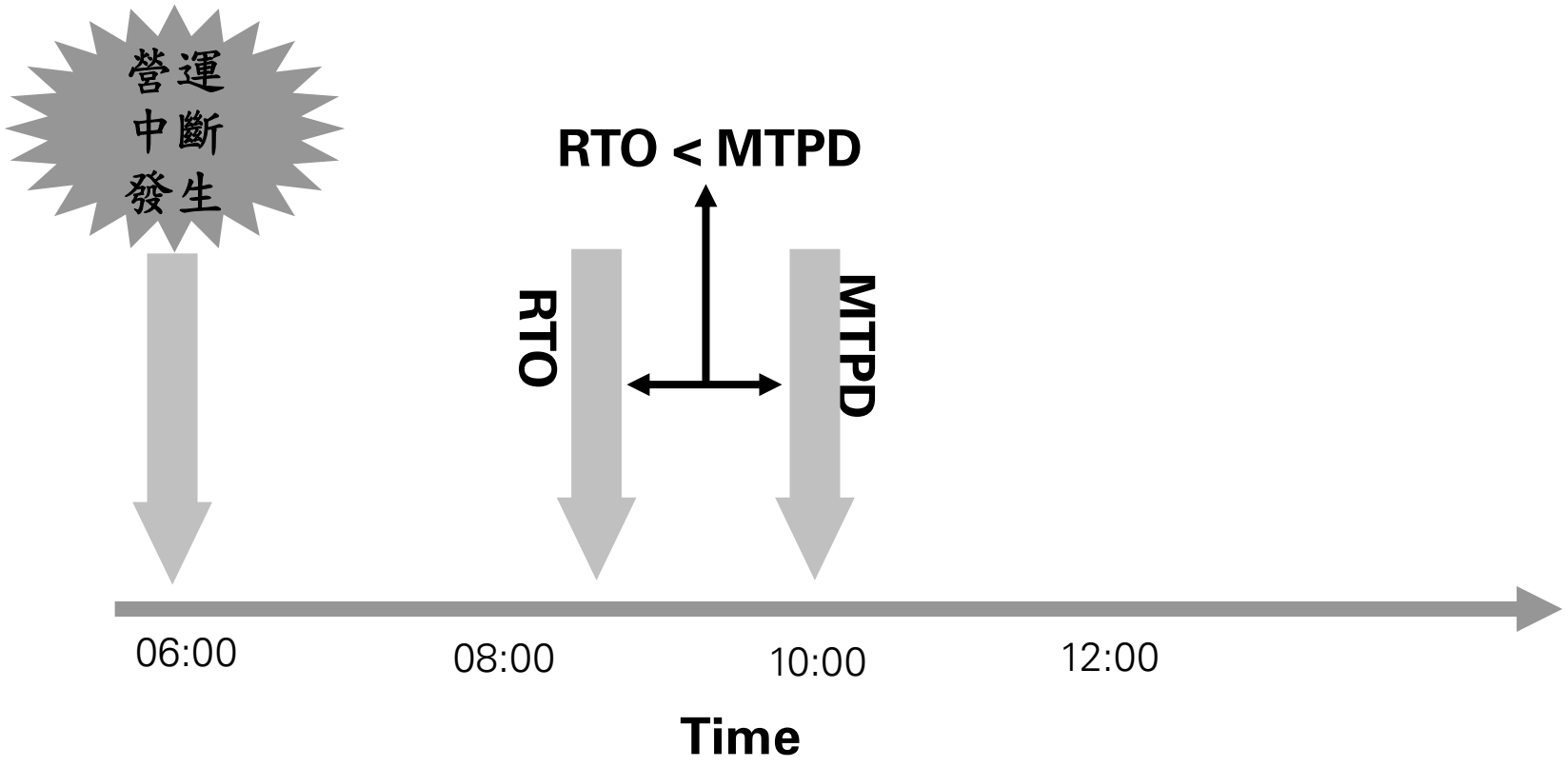
MTPD與RTO關聯示意圖

- 思考營運持續管理措施要從”worst case”出發，如此才會充分考量到中斷事故所帶來之最大損害



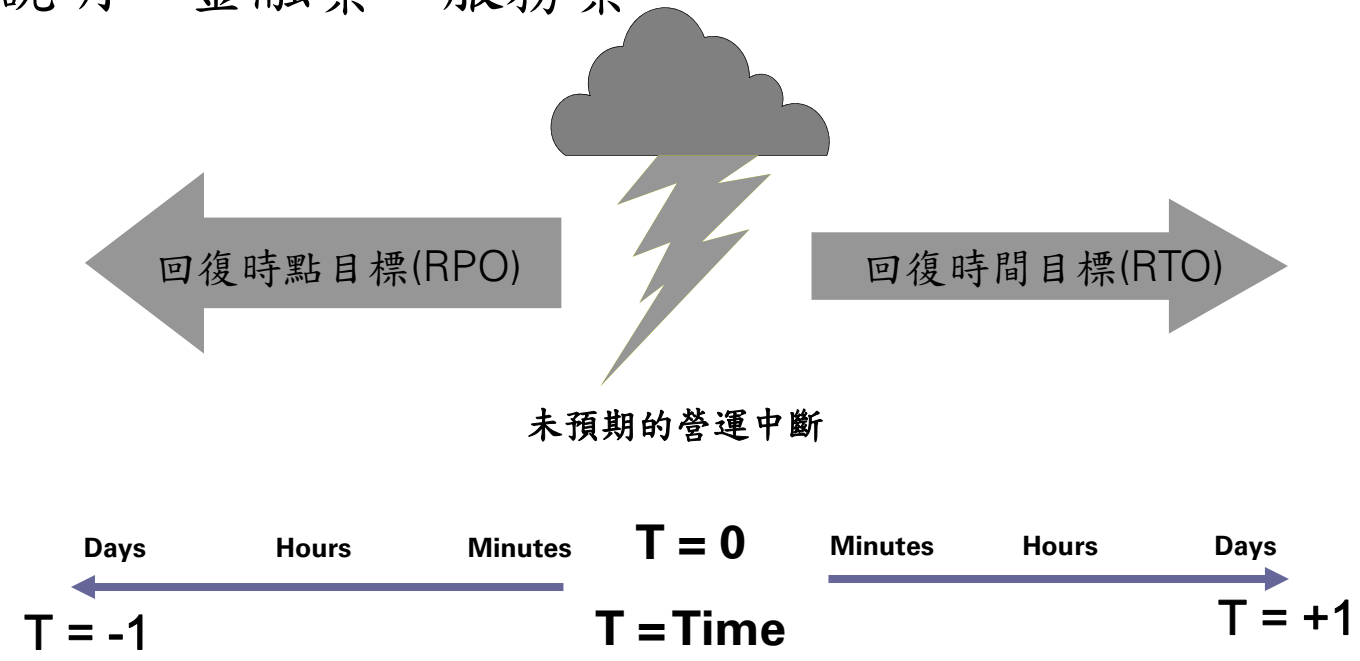
MTPD與RTO關聯示意圖(續)

- 回復時間目標(RTO)=執行營運持續計畫所需要的時間

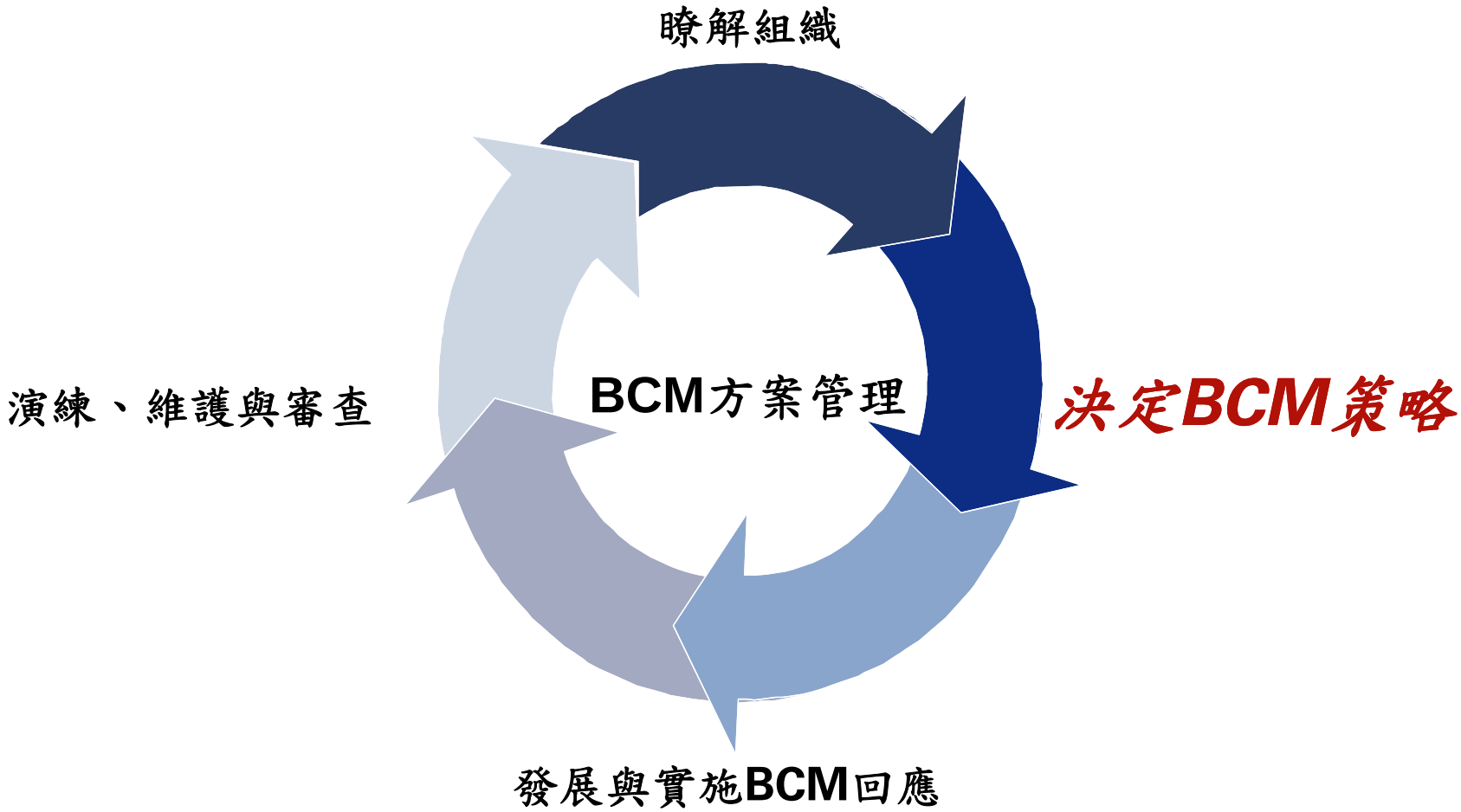


BCM的3個重要時間指標

- MTPD (Maximum Tolerable Period of Disruption) 最大可容忍中斷時間
- RTO (Recovery Time Objective) 回復時間目標
- RPO (Recovery Point Objective) 回復時點目標
- 案例說明：金融業、服務業



BCM建置與維運(生命週期)



決定 BCM 策略

- 組織決策可讓關鍵業務活動具有持續運作能力
- 實施可降低中斷事故發生可能性之措施
- 規劃包括復原時間目標(RTO)的復原活動
- 與主要利害關係人、外部機構的關係管理
- BCM策略要以具有成本效益比之方式來支持組織之策略、目標與義務

BCM策略選項

- 緩和損失
  - 不讓業務中斷時間超過MTPD
  - 讓業務中斷導致之衝擊不要超過事先設定之最大值
- 程序轉移
  - 採用委外策略，將業務流程外包出去，由專業服務/生產業者提供服務或產品代工製造
  - 委外廠商需具備一定之業務永續營運管理(BCM)能力

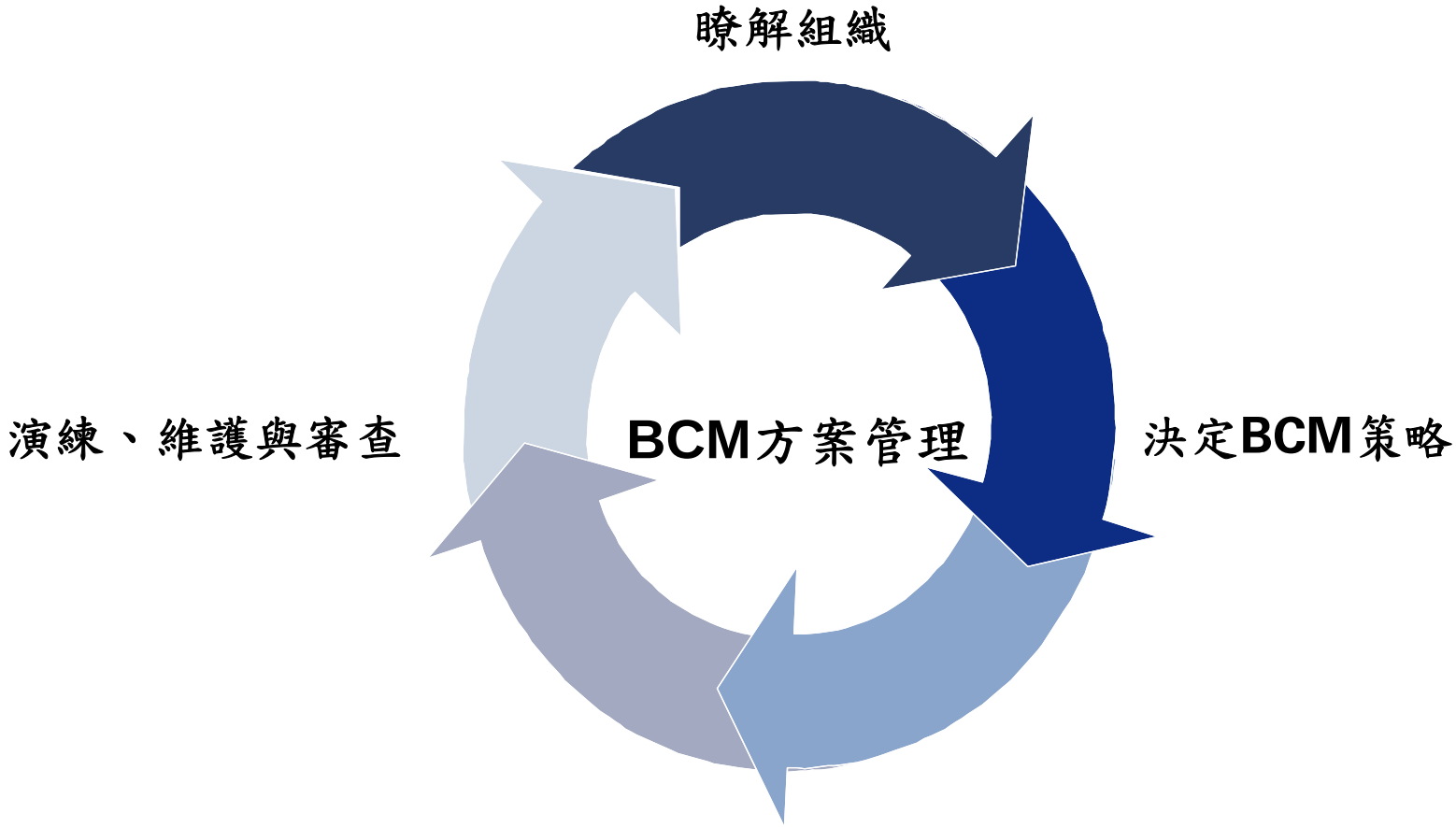
BCM策略選項(續)

- 終止或改變
  - 經瞭解組織過程後，發現某些業務流程沒有存在價值或者是為維持該業務流程需支付龐大成本，可思考終止該業務流程
  - 改變該業務流程運作方式，一方面或可提升運作效能，另一方面可降低該業務流程發生中斷事故之可能性
- 保險
  - 將組織因營運中斷所導致之財務損失風險轉嫁出去
  - 保險不可為組織唯一運用之BCM策略，應該需要搭配其他策略共同使用
- 不做任何事

決定策略選項應考量之要素

- 最大可容忍中斷期間(MTPD)
- 成本
  - 成本=事故前準備成本+事故處理成本
- MTPD越短之業務流程，為維持其營運持續能力(與RTO相關)需投入之成本可能會越多

BCM建置與維運(生命週期)



發展與實施 BCM 回應

- 事故回應架構
- 事故與復原的管理計畫
- 溝通
- 公共及媒體關係

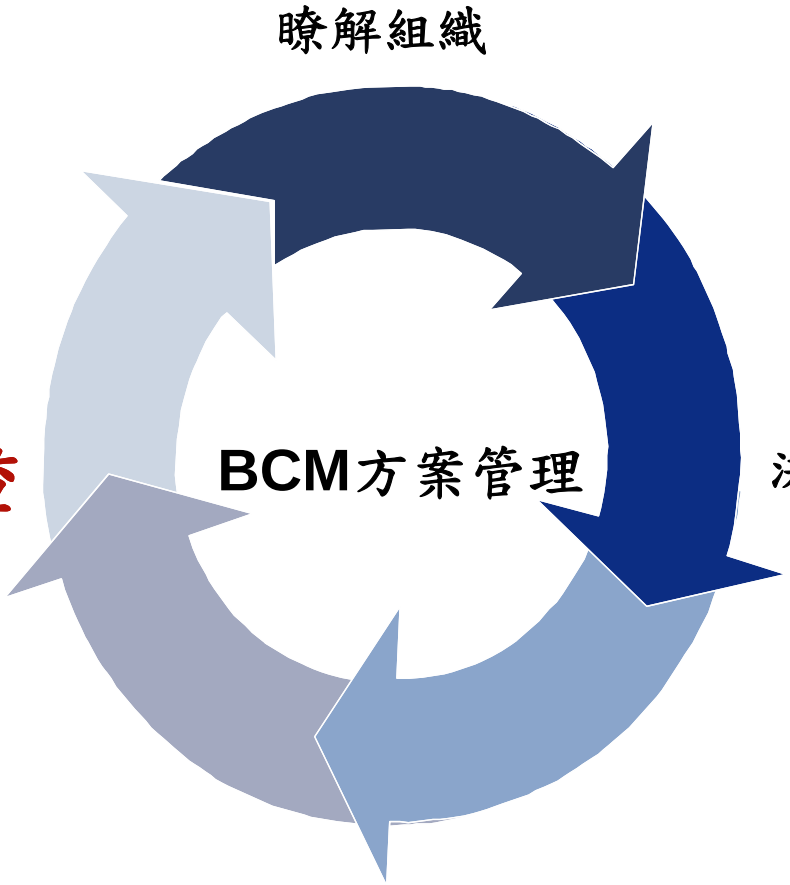
事故回應架構

- 針對中斷事故建立有效的回應與回復
- 針對中斷事故有一個清楚之升級與控管程序
  - 通報升級條件要明確定義
  - 上班時間/非上班時間之通報方式
  - 通報升級方式應簡單且不應輕易受外在任何因素干擾
- 與利害關係者有良好溝通機制
- 有確保人員安全的良善計畫
- 針對遭中斷之業務有重啟計畫

回復計畫應有項目

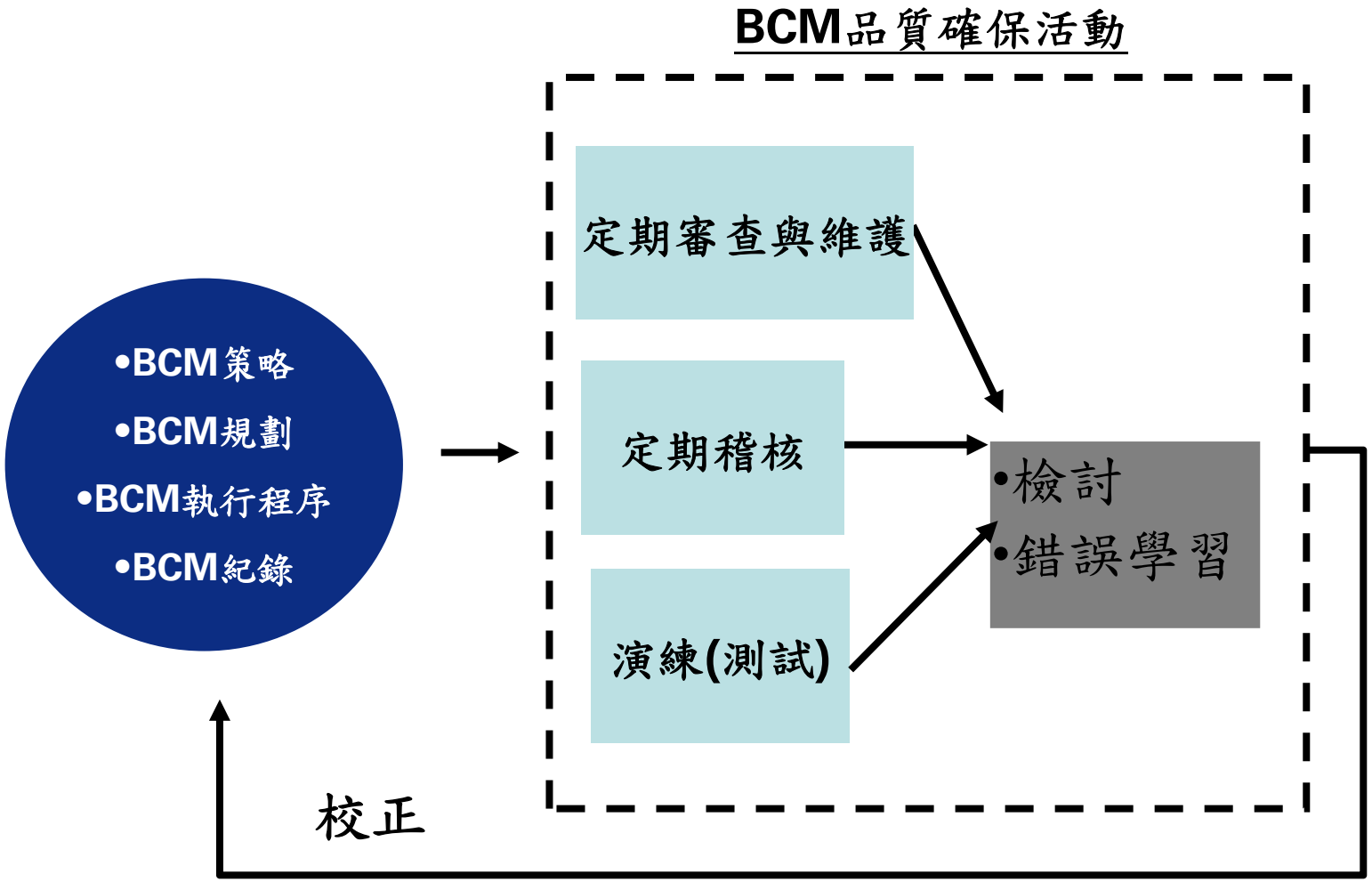
- 目的與範圍
- 角色與權責
- 計畫要文件化
- 文件要更新維護
- 聯絡清單

BCM建置與維運(生命週期)



融入BCM於組織文化

BCM的品質確保活動


BCM品質確保活動
定期審查與維護
定期稽核
演練(測試)
•檢討
•錯誤學習
•BCM策略
•BCM規劃
•BCM執行程序
•BCM紀錄
校正

演練、維護和審核

- 本階段的目的是透過持續性改善行動，確保BCM專案的有效性、正確性和實用性
- 「演練」指的是根據 BCP 中記錄的流程，對團隊成員進行持續性培訓和排練。如此可確保營運持續性的計畫能獲得定期驗證，並持續採取改善措施
- 「維護」指的是定期修正並更新流程，以確保所計畫的流程方案不會因時間而失效
- 組織應對整套 BCM 專案進行稽核，以確定計畫是否適當、充足及有效，進而滿足持續性的需求

維護BCM

- 因為某些因素改變，計畫也許必須更新，包括：
  - 法令
  - 營運策略
  - 風險(作業面及財務面風險)
  - 場所、設施和資源
  - 承包商、供應商和主要客戶
  - 採購新設備/作業系統升級
  - 新增或刪除作業
  - 人員、住址或電話號碼

組織常見的BCM相關稽核發現

- 異地備援場所空間不足
- 回復策略評估不正確
- 缺乏業務單位的參與，或未得到業務單位的同意
- 忽略部門或應用系統相依的關係
- 忽略部分重要資源（Internet、E-mail、供應補給等...），造成業務運作的瓶頸
- 支援資源不足
- 回復計畫不夠詳細，仍需依賴熟悉業務/系統的人員執行
- 缺乏適當的維護更新機制
- 通常只測試資訊相關系統與設備，缺乏完整流程測試

5種演練類型

演練類型	程序	建議參與人員	常用工具或技巧	複雜度(成本)	頻率
書面審查	計畫內容檢討並提出改善意見(沙盤推演)	BCM工作小組主管、承辦人員與觀察員	•Plan & Guideline	低	高
局部計畫演練	以角色挑戰BCP之各項程序	業務承辦人員、委外廠商與觀察員	•Check List •RACI •SOP •Workshop		需定期舉行
模擬	運用情境驗證BCP可行性	業務承辦人員、委外廠商、相關流程協同單位與觀察員	•Simulator •Testing Env.		
關鍵活動演練	針對部份關鍵流程，啟動可控制之情境，不危及營運作業	業務承辦人員、委外廠商、相關流程協同作業單位與觀察員	•Partial Production Env.	高	低
完整BCM演練	針對業務流程實際環境，大範圍演練	組織內業務流程所有人員	•Real Production Env.		

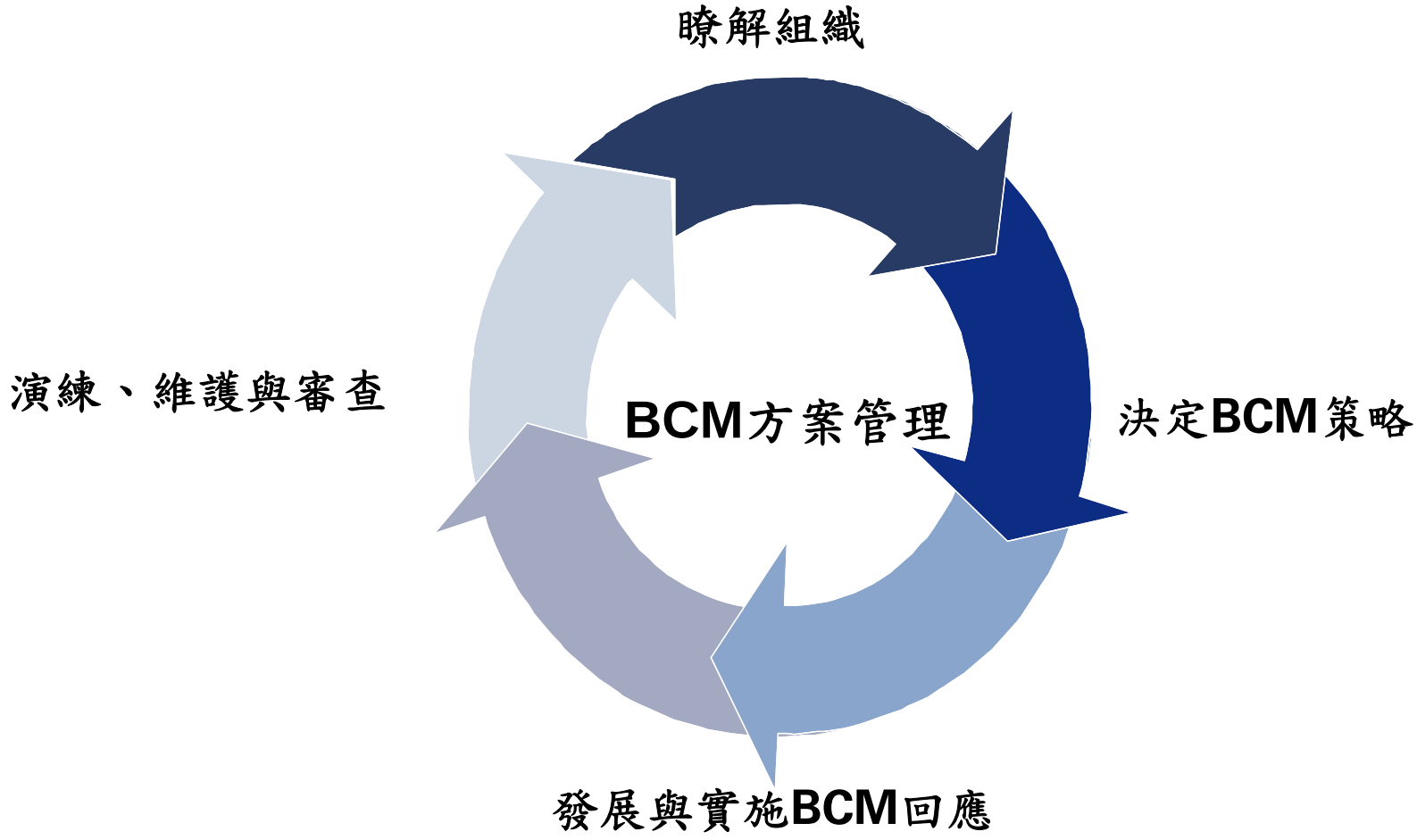
前置作業規劃

- 損害預防
- 通知
- 演練所需資源或情境準備
  - 人員
  - 場地
  - 資訊設備
  - 通訊設備
  - 其他物料
  - 資料
  - 委外供應商
  - 協同作業單位

如何進行演練檢討

- 人-各流程負責人員是否熟練?溝通是否順暢?指揮與發言是否恰當?相關單位是否已納入?
- 事-回復方案是否可行?有無發生其他突發狀況?各項作業次序安排是否合理?
- 時-演練結果是否符合時間目標(RTO/RPO) ?有無工作瓶頸?
- 地-各項規劃空間(緊急處理場所、重置或備援場所)是否充足?是否充分考慮環境因素?
- 物-各項回復所需資源是否充足?

BCM建置與維運(生命週期)



融入BCM於組織文化

BCM內化為組織文化之關鍵成功要素

- 管理層的了解與支持
- 考慮組織策略層次
- 全面落實並與日常工作結合
- 循序漸進的強化BCM所需資源
- 納入所有利害關係人
- 完整訓練與專業的知識
- 合理的獎賞與表揚制度
- 有效的代理人制度
- 適度引進新技術與新科技
- 從事件/事故中檢討
- 適度進行同質組織的參訪與學習

BCM訓練與宣導

- 一般基礎概念與意識訓練
- 特定組織或功能專業訓練
- 跨單位整合訓練
- 多元的宣導活動

區網中心如何推動BCM

業務永續營運管理(BCM)推動建議

- 建議以簡化方式來推動BCM生命週期(六大步驟)
  - 找出關鍵業務活動(透過營運衝擊分析與風險評鑑)，並嘗試訂出MTPD、RTO與RPO(如果有需要)
  - 針對關鍵業務活動練習訂定BCP或BRP(DRP)與相關作業程序(可成為BCP或BRP之附件)
    - 建議資料來源：應用單位內現有相關營運復原、緊急應變與通報處理等相關程序書，或參考其他部門之相關作法與應用文件
  - 針對所訂定之BCP、BRP(DRP)與相關作業程序來進行演練與審查，以確認該計畫或相關作業程序之可行性與合理性

問題與討論

簡報完畢，敬請指教。