如何洞燭機先，善用預防制度規劃無法預料的事，已經是組織管理必備之管理技能。

營運持續管理（BCM）概觀

◎紀佳妮

在資訊發展迅速的現代，風險的發生已經超越了以往的經驗！2010年全球災難不斷，地震、熱浪、洪水、火山爆發、超級颱風、暴風雪、山崩，以及旱災頻發，造成的災害可能使得仰賴資訊設備提供服務的組織業務中斷，許多異常事件若無妥善管理，將迅速擴大為危機與災難。因此如何洞燭機先，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。

一、何謂營運持續管理

營運持續管理（Business Continuity Management, BCM）主要目標為確保組織在遭逢天災或人禍等意外時，保護重要營運過程不受重大資訊系統失效或災害的影響，仍然可以繼續運作。然而要達到此目標，應以風險管理為基礎，建立切合組織業務與目標的營運持續計畫，並且依照適當的管理程序，定期測試與維護，使得營運持續管理不是紙上談兵而已，而是一套具體可行的方案。

營運持續管理透過預防與復原控制措施的組合，將組織的衝擊最小化，把風險造成的影響降低到可以接受的等級。而在規劃過程中，必須了解組織面臨風險發生的可能性與衝擊，能夠鑑別出影響組織成敗的重要業務，以及維運這些重要業務時所需要的資產，包括：人員、軟硬體、行政資源、通訊資源等等。根據風險評鑑的結果發展營運持續策略，以決定營運持續的整體作法。

二、營運持續管理生命週期

在資訊安全管理標準CNS27001中載明對營運持續管理的要求，也就是說在一個完整的資訊安全管理系統中，必然要包括營運持續管理。其產生的結果，如營運持續計畫和災難復原計畫也都要符合資訊安全管理原則，而內容可能包括人員安全的管理、存取控制的管理及實體環境安全的管理等。營運持續管理生命週期，各階段的說明如下：

(一)了解組織的關鍵營運活動

了解組織的關鍵營運活動的方法有：

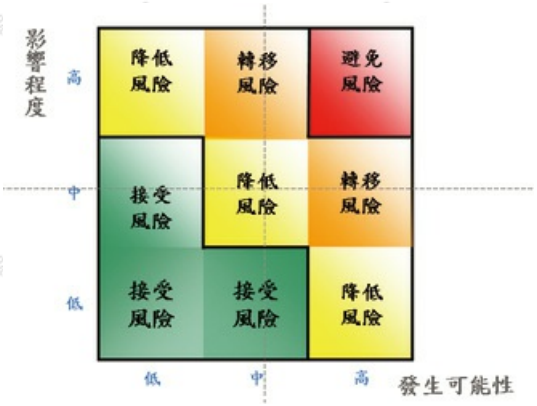
1.風險評鑑Risk Assessment（RA）：目的在鑑別、定義及評估所面對的威脅、弱點及風險，並對所有資產鑑別出的風險進行評鑑。

2.營運衝擊分析Business Impact Analysis（BIA）：目的在於鑑別營運無法持續時的營運衝擊（亦即損失或中斷），與復原運作到最低的作業水準；藉此可以清楚了解組織裡關鍵營運與流程，以及支持這些流程所需的要求，以協助評估復原所需要的時間與相關資源。 RA與BIA可協助了解組織所面臨風險之可能性與衝擊，鑑別關鍵營運活動與其優先順序。

(二)決定營運持續管理策略

組織在處理風險的策略大致分為以下４種，而面對風險的態度可依影響的程度與發生的可能性等因素加以考量。有關風險處理的原則參考圖示。

1. 避免風險：決定不涉入或退出風險處境。
2. 降低風險：選擇使用適當技巧及管理原則，以減低風險影響或其發生機率。
3. 轉移風險：透過立法、合約、保險或其他方式，將損失之責任及其成本轉移至其他團體。
4. 接受風險：特意或非特意承擔風險所造成之損失，或為組織之財物損失負責。



(三)發展與實行營運持續管理計畫

根據營運衝擊分析的結果與組織現況建立營運持續計畫（BCP），應考量權責分工、作業程序、文件化、公告及教育訓練等相關措施。規劃過程應著重在所需的營運目標，例如在可接受的時間內恢復提供客戶的特定通信服務，也應該要識別所需的服務和資源。包括員工、非資訊處理資源及資訊處理

設施的備援安排，此備援安排可包括與第三方的協議，其可為互惠協議形式或商業預訂服務形式。 擬定營運持續計畫，內容應該包含：

1. 計畫啟動條件：應該清楚說明各項計畫須遵守的啟動條件，像是地震危害組織到達何種程度時就該啟動計畫的鑑別辦法，與應參與計畫的人員等。
2. 職責說明：應該要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。
3. 緊急程序：在危急事故發生後，應採取那些行動，應包括公共關係管理的安排，以及與相關機關（如警察、消防單位和當地政府）保持有效的聯繫；若地震發生造成硬體故障，必須通報相關設備的管理員（如主機管理員）或硬體廠商進行處理。
4. 備援程序：必須在要求時間內完成最低營運水準之復原工作，需特別注意與外部的營運依存要件及合約的適當性；如果地震造成部分主要機器的損壞，應該通知緊急應變處理小組負責人，指揮進行緊急採購，並將相關硬體運送至備援場地。
5. 復原程序：應採取那些行動來復原正常營運作業？應該包含聯絡廠商採購新系統做硬體功能回復，並將作業系統與應用系統重新建立、備份資料拿回做系統功能回復等相關工作。
6. 程序文件化：以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，例如疏散計畫或任何現有的備援作業。
7. 維護時間表：應指定如何、何時測試BCP計畫，說明並維護該計畫的程序。
8. 認知與教育訓練：讓參與者了解營運持續過程，確保該過程持續有效，並針對議定的緊急程序及過程，進行適當的員工訓練，其中包括危機管理訓練等。

(四)營運持續計畫測試與維護

營運持續計畫應定期測試與更新，以確保維持在最新且有效可用的狀態。測試的方法可參考表1。

表1　營運持續管理（BCM）測試方法

測試方法	描述	贊同率 (%)
結構化排練測試	主要是為了確認計畫可以被落實執行，由相關權責單位共同對處理方式進行逐項討論，並對計畫中所有細節確認可行性。	57.6
檢查表測試	建立計畫中的查核點與檢查方法，據以制訂檢查表，以便相關權責單位能夠利用此檢查表對營運持續計畫進行測試。	55.8
模擬測試	模擬災害發生時的特殊情境，讓相關人員在此環境中進行營運持續計畫演練。	51.9
平行測試	在組織資源許可的情況下，可能擁有備援平台，此備援平台有實際資料或作業在運行，因此在備援平台上進行測試更接近真實作業環境，也無害組織的正常運作。	50.4

營運持續計畫應該定期維護，因為外在或內在環境都會因時間而變化，維護時機與重點可參考以下幾項建議：

1. 定期檢討可用性
   包含檢視實體環境是否變動、營運持續計畫是否依照變動的架構調整、外部支援的資源狀況是否持續等。此外，應注意安全性和技術性考量，對原有的計畫是否因新技術的出現而有更好的解決方案，或是在軟硬體設備、替代方案及備援系統方面有更安全的措施，應檢討相關設備及方案是否仍然能夠支援營運持續計畫等。
2. 定期檢討遵循性
   包含相關法規的遵循，應檢視法令法規是否修改，營運持續計畫是否應調整以符合法規要求。在營運策略方面，應檢討組織營運策略是否有修正，營運持續計畫是否應調整以符合組織目標。
3. 不定期檢視
   常發生在組織營運策略變動時，例如採購新的設備、更新作業系統時、使用新的問題偵測與控制技術（例如火災偵測）、使用新的環境控制技術、人員與組織的調整變動、契約當事者或是供應商的調整變動、業務流程的變動、新建或是撤銷作業流程、實務作業的變更及法規變更時等，皆需不定期檢視營運持續計畫。

三、結語

天有不測風雲，組織如何能夠在多變的災難中持續經營，未雨綢繆之風險管理是有必要的；組織須建立BCM文化，使危機處理深入員工的工作認知與技能。目前組織的業務有漸漸改採委外作業的趨勢，因此如何在狀況發生時，能迅速結合內外部各項資源，在可接受的時間內恢復運作，並使營運持續管理提供很好的防護管理框架，則完善規劃與執行將是組織不敗的第一法門。

四、參考文獻

[1]英國標準協會 BS 25999:2006 。
[2]中華民國國家標準 CNS 27001:2006 。
[3]行政院研考會資安數位課程「營運持續管理(BCM)概觀」，2008年。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心工程師）

▲Top

化資安機制，落實人員訓練，建構防護網路，確保資通安全。

以中科院為例談專案管理資安防護機制

◎王百祿

在科技昌明的21世紀，國際社會的權力關係已逐漸由早期藉由武力、財力的硬性較量，發展成為以知識力柔性競爭的型態；無論是商業用途或是軍事用途的尖端科技資訊，各國正無時無刻進行著攻防激烈的隱形戰爭。有專家學者指出，資訊安全防護的重要性已可與機密資訊的產出相提並論。

最近爆發軍中通信電子資訊高階人員涉嫌將極機密資料洩漏交付中共當局案，顯示國軍現行保密防諜的作法仍存許多精進的空間，亟待全面補強。隨著ECFA的簽訂，兩岸在經貿、文化、觀光等領域的交流日益頻繁；儘管兩岸關係逐漸改善，但在軍事、外交方面仍是敏感禁忌，對岸的善意不可恃，雙方的情報工作是不會有休止的一天。行政院吳敦義院長表示，中共仍不斷對我方軍事情報進行偵搜並謀滲透我方資訊通信，因此政府及國民必須保持高度警惕；同時指示國防部，今後應強化官兵的忠貞信念，將武德教育及相關保密防諜作為列為優先要務，積極落實辦理。

以軍事科技研發機構為例，國防部軍備局中山科學研究院（簡稱中科院）為我國國防科技研發的重鎮，四十餘年來研發成果輝煌，前後完成了天弓飛彈（圖一）、天劍飛彈（圖二）、雄風飛彈（圖三）、探空火箭（圖四）等武器系統與專案計畫的研發自製，並陸續投入戰備。長期以來，中科院儼然成為維護國家安全的要角，也無可避免地變成敵人或其他有心人士積極情蒐與刺探的目標。中科院除致力於國防科技研發外，亦因應政府發展產業之需要，以「轉化國防科技，創造產業價值」為定位，大力推動經濟部科專計畫及軍民通用科技發展；中科院與產、官、學、研各界的資訊交流，諸如參觀訪問、成果發表、文章發表、媒體採訪、電子郵件、傳真文件…等等，業務項量可謂相當繁重。再者，由於研發任務的屬性特殊，中科院員工的日常工作，經常性接觸之國家機密亦屬軍事機密或國防秘密的資訊，可能會因習以為常，或因業務繁忙，一時鬆懈保密警覺，而肇生洩密事件。因此，有必要研訂資訊安全防護機制，確保每位員工都能深切體認敵人對我陰謀滲透已達無孔不入的事實，嚴肅面對中共「網軍」密集進襲的挑戰；唯有人人做好資訊安全防護措施，人人自我養成時時保密的習性，才能杜絕洩密，避免造成個人及國家的重大傷害。

圖一　天弓飛彈連續發射

圖二　天劍飛彈發射

圖三　雄風飛彈發射

圖四　探空五號火箭

本文所稱「機密資訊」係包含〈國家機密保護法〉所稱「國家機密」、〈陸海空軍刑法〉所稱「軍事機密」、〈刑法〉」第109條至第112條所稱「國防秘密」及第132條所稱「國防以外秘密」等所應秘密之一切文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，及其他得以讀、看、聽，或以技術、輔助方法理解之任何紀錄內之訊息。

茲就中科院專案管理保密措施的作業規範要項說明如下，以作為國內科技研發機構強化資安防護機制之參考與借鏡。

一、在計畫建案階段

有關建案之底價（開標前）、需求文件（含機敏圖書、設計圖）、系統分析報告、投資綱要計畫、總工作計畫、分年工作計畫等各項資訊及其草稿，應賦予機密屬性、機密等級及保密期限，並經權責長官完成核定；另依需要訂定「代名」，以隱匿文件內容。訪商時不得顯現建案目的，亦不得在一般行政會議上論及本案相關內容。各項審查作業宜採取集中作業及紙本審查方式，於獨立之處所進行審查，並由建案單位專人專責管制會議文件，文件不得攜出；若無法集中審查者，審查資料應依機密文件傳遞方式，針對每份文件簽署個別保密切結書及簽名受領，接密人員名單列冊管制，並適時檢討修訂。涉及友軍、外國政府、外籍顧問、技師或民營廠商時，應簽訂明確而具體之保密契約（條款），參與人員應建冊列管，並簽訂保密切結。

專案任務建案後，應依實況成立專案辦公室（存放區、檔案櫃），並策訂作業規範（守則），嚴格管制。電子資訊僅可存放於專用隔離之電腦中，嚴禁上網傳輸。

二、在計畫執行階段

所有接密人員於奉命接觸該機密資訊時，應登錄接密人員管制簿，以明責任；調閱相關機密資訊（含電子檔）時，均須奉權責長官核准，受領單位非經原製作單位同意，不得私自複製留存，並依規定完成管制。對於技術合作、委商產製等專業服務，應依據國防部〈國防部結合民間發展國防科技工業保密作業規定〉，防範關鍵性技術或軍品外洩；執行期間，應視狀況指派專人實施履約督訪或全程監督（應訂於合約內）。各項簡報資料以投影片配合口頭說明為主，減少資料外洩管道。尚未解密之資訊、軍品、管制區域，未經核准，不得對外公開。

三、在計畫結案階段

主計畫應要求分計畫將研發報告及成果資料統一集中管理，並適時辦理資料銷毀作業，以降低存管負荷。交付合作單位之機密資訊（含產製之瑕

疵品）應於合約內註明管制方式，否則於結案時清點收繳或派員監督登記銷毀。除專案需要，研發人員撰寫之報告或發表之論文，均不得涉及機密專案部分。

資訊安全工作是一項防患於未然的風險管理過程，為有效防杜敵人情蒐，根絕洩密事件肇生，各科技研發機構應制訂強化資訊安全防護體系的整體性政策，針對機敏（專案）任務屬性與作業流程，嚴採相關保密檢管措施與手段，藉以明確劃分保密責任，提升機密資訊維護的強度。有鑑於資安保密工作之重要性，中科院已擬定「強化資安機制、落實人員訓練、建構防護網路、確保資通安全」的資安政策，持恆宣導與落實推行，並建立層層資安檢審機制，持續鞏固並強化現行的資訊安全防護措施與全院員工的保密意識。

除頒布相關資安規定與作法外，管理制度的建立，以及資訊使用人的實踐履行，實為未來資安工作強化精進的核心重點。當資安保密成為每位員工的工作習慣後，國內科技研發機構的資訊安全防護機制與防護網路才能達到滴水不漏的境界。

【參考資料】

一、國防部軍備局中山科學研究院新新季刊第34卷第３期
二、國防部軍備局「強化保密安全維護機制」實施規定

▲Top