

102 年度

我國電腦機房異地備援機制委託研究計畫案

電腦機房異地備援機制參考指引

(V1.0)

委託機關：行政院

執行單位：財團法人國家實驗研究院  
國家高速網路與計算中心

中華民國 103 年 03 月

## 報告摘要

報告名稱	電腦機房異地備援機制參考指引
機密等級	<input type="checkbox"/> 機密 <input type="checkbox"/> 密 <input type="checkbox"/> 內部使用 <input checked="" type="checkbox"/> 普通
相關撰稿人	鍾沛原、曾賢寶、楊嘉麗、李柏毅、蔡一郎
閱讀對象	<input checked="" type="checkbox"/> 管理階層 <input checked="" type="checkbox"/> 資安人員 <input checked="" type="checkbox"/> 資訊人員 <input checked="" type="checkbox"/> 一般人員
內容摘要：	<p>「電腦機房異地備援機制參考指引」旨在協助組織於營運持續管理的程序中，進行重要（關鍵）資訊系統所在之機房或環境評估，並考量各項可能風險，藉以規劃或改善異地備援機房，使其於有限資源內可達成對應之作為，達到緊急應變與營運持續的目標。</p> <p>本指引由營運持續管理的角度切入，參考國際規範 ISO 22301:2012、ISO/IEC 24762:2008 等內容，並比較國際組織與各先進國家異地備援機制之相關規範和技術文件（例如：NIST SP 800-34、TIA-942），分析與比較其特色，進而提供符合我國國情之電腦機房異地備援機制評估準則。</p> <p>使用單位可使用本指引之參考項目進行異地備援機制規劃，並就組織之需求與資源進行調整，以符合實際狀況。</p>
關鍵詞	營運持續管理、災害（難）復原、營運復原時間、資訊資料回復點

# 目 次

一、前言 .....	1
(一) 目的 .....	1
(二) 適用對象 .....	1
(三) 章節架構 .....	4
(四) 使用建議 .....	6
(五) 專有名詞解釋對照表 .....	8
二、電腦機房異地備援相關規範 .....	10
(一) 國際電腦機房異地備援發展趨勢 .....	10
(二) 國際組織電腦異地備援相關標準 .....	12
(三) 先進國家異地備援相關規範 .....	16
(四) 我國電腦機房異地備援相關規範 .....	19
三、電腦機房異地備援機制 .....	26
(一) 電腦機房異地備援機制管理 .....	27
(二) 瞭解電腦機房異地備援的需求 .....	32
(三) 發展電腦機房異地備援機制的策略 .....	34
(四) 制定和實施電腦機房異地備援機制 .....	40
(五) 演練、測試與持續改善 .....	43
四、電腦機房異地備援機制評估準則 .....	48
(一) 一般原則 .....	49
(二) 營運持續 .....	55
(三) 系統架構 .....	61
(四) 網路配置 .....	72
(五) 建置環境 .....	73
(六) 地理位置 .....	78
(七) 支援作業 .....	85
五、結論 .....	93
六、參考文獻 .....	95
七、附件 .....	99

## 圖 目 錄

圖 1	電腦機房異地備援機制流程圖.....	6
圖 2	電腦機房異地備援機制與 ICT 持續管理之關係.....	26
圖 3	電腦機房異地備援機制管理流程圖.....	27
圖 4	電腦機房異地備援機制管理組織架構.....	28
圖 5	瞭解電腦機房異地備援需求.....	32
圖 6	發展電腦機房異地備援機制策略.....	34
圖 7	制定和實施電腦機房異地備援機制.....	40
圖 8	演練、測試與持續改善.....	44
圖 9	電腦機房異地備援機制評估準則架構圖.....	48
圖 10	RPO, RTO, RLO 流程示意圖.....	56
圖 11	關鍵 ICT 持續管理時間軸.....	57
圖 12	異地備援系統架構示意圖.....	62
圖 13	臺灣活動斷層分佈圖.....	80

## 表 目 錄

表格 1	電腦機房異地備援機制參考指引適用人員對應表.....	3
表格 2	資訊系統安全等級設定原則評估表.....	7
表格 3	專有名詞解釋對照表.....	8
表格 4	國際組織電腦異地備援相關標準.....	13
表格 5	各國異地備援相關規範.....	17
表格 6	異地備援系統架構比較表.....	25
表格 7	政府機關（構）資訊安全責任等級分級作業施行對照表.....	49
表格 8	災害復原 RLO 值評估表.....	60
表格 9	3 種資料備份類型比較表.....	64
表格 10	備份方式比較表.....	67
表格 11	異地備援架構等級條件評估表.....	71

# 一、前言

## (一) 目的

「電腦機房異地備援機制參考指引」(以下簡稱本指引)旨在協助組織於營運持續管理(Business Continuity Management, BCM)的程序中,進行重要(關鍵)資訊系統所在之機房或環境評估,並考量各項可能風險,藉以規劃或改善異地備援機房(Disaster Recovery Site, DR Site),使其於有限資源內可達成對應之作為,達到緊急應變與營運持續的目標。

本指引由 BCM 角度切入,參考國際規範 ISO 22301:2012、ISO/IEC 24762:2008 等內容,並比較國際組織與各先進國家 DR Site 相關之規範和技術文件(例如:NIST SP 800-34、TIA-942),分析與比較其要求和特色,進而提供一套 DR Site 評估準則,可供使用者檢視組織的機房風險,並著手可行的改善措施。

本指引著重營運持續之觀念,以考量 DR Site 趨勢,如跨國性異地備援、雲端災害復原服務等,並未考量主機房建置趨勢,例如綠能機房(Green Data Center)等。此外,關鍵基礎設施(Critical Infrastructure)、國安或高度營運持續需求等相關組織,建議除參閱本指引之內容外,另宜再就所在區域、業務特性、服務對象等,援引、遵循必要的法令和國際標準,以符合實際的需求與狀況。

## (二) 適用對象

本指引可供政府機關、企業組織、學術機關與其他單位參考,並適合分屬以下不同機房階段的組織,在進行營運持續管理時的重要參酌。

- 無機房階段：此階段組織多因資訊系統的可容許中斷時間較長，且缺乏足夠的資源建置、維運機房，常見於國民中小學等單位。在業務營運持續的考量下，這類組織應建立必要的異地備份機制，並評估可能的機房運作模式，例如：「聯合維運」、「專業委外」（可參閱本指引 3.3.5 營運方式選擇），避免因負荷過重的機房維護成本，造成業務運作的困難。
- 擁有主機房階段：此階段組織資訊系統的可容許中斷時間較短，擁有基本的資源支應機房維運，方式多採用「自行維運」、「聯合維運」、或「專業委外」（可參閱本指引 3.3.5 營運方式選擇），此類組織常見於一般政府機構或大專校院。由於需要相當程度的業務營運持續能力，在有限的資源下，宜先行評估、改善既有機房的威脅弱點，在可能限制條件下需強化重要項目，建立可行之異地備援機房模式。
- 擁有主機房與異地備援機房階段：此階段之組織除具備相當的資源外，亟需進行業務營運持續，以及資訊系統較短暫的可容許中斷時間，多半是中央或重要政府機構較為常見。在具備相當程度的異地備援及營運持續管理情況下，組織仍須識別各機房間的威脅弱點與互補狀態，考量可運用的資源及成本，強化現有的機制，包括第二異地備援機房的可能性，朝更完善的營運持續架構努力。

為便於上述各階段人員閱讀及應用本指引，建議參閱的層級分為「管理階層」（例如：組織負責人、資訊主管、資安主管）、「資安人員」、「資訊人員」（例如：機房人員、系統人員）與「一般人員」，對應之章節重點詳見表格 1。

表格 1 電腦機房異地備援機制參考指引適用人員對應表

章 節		管理 階層	資安 人員	資訊 人員	一般 人員
二、電腦機房異地備援相關規範					
2.1	國際電腦機房異地 備援發展趨勢	○	○	○	○
2.2	國際組織電腦機房 異地備援相關規範	○	○	○	○
2.3	先進國家電腦機房 異地備援相關規範	○	○	○	○
2.4	我國電腦機房異地 備援相關規範	◎	◎	◎	○
三、電腦機房異地備援機制					
3.1	電腦機房異地備援 機制管理	◎	◎	◎	○
3.2	瞭解電腦機房異地 備援需求	◎	◎	◎	○
3.3	發展電腦機房異地 備援機制策略	◎	◎	◎	○
3.4	制定和實施電腦機 房異地備援機制	◎	◎	◎	○
3.5	演練、測試與持續改 善	◎	◎	◎	○
四、電腦機房異地備援機制評估準則					
4.1	一般原則	◎	◎	◎	○

4.2	營運持續	◎	◎	◎	○
4.3	系統架構	◎	◎	◎	○
4.4	網路配置	◎	◎	◎	○
4.5	建置環境	◎	◎	◎	○
4.6	地理位置	◎	◎	◎	○
4.7	支援作業	◎	◎	◎	○
五、結論		◎	◎	◎	○
六、參考資料		○	○	○	○
七、附件		◎	◎	◎	○

◎：建議詳閱      ○：建議參考

### (三) 章節架構

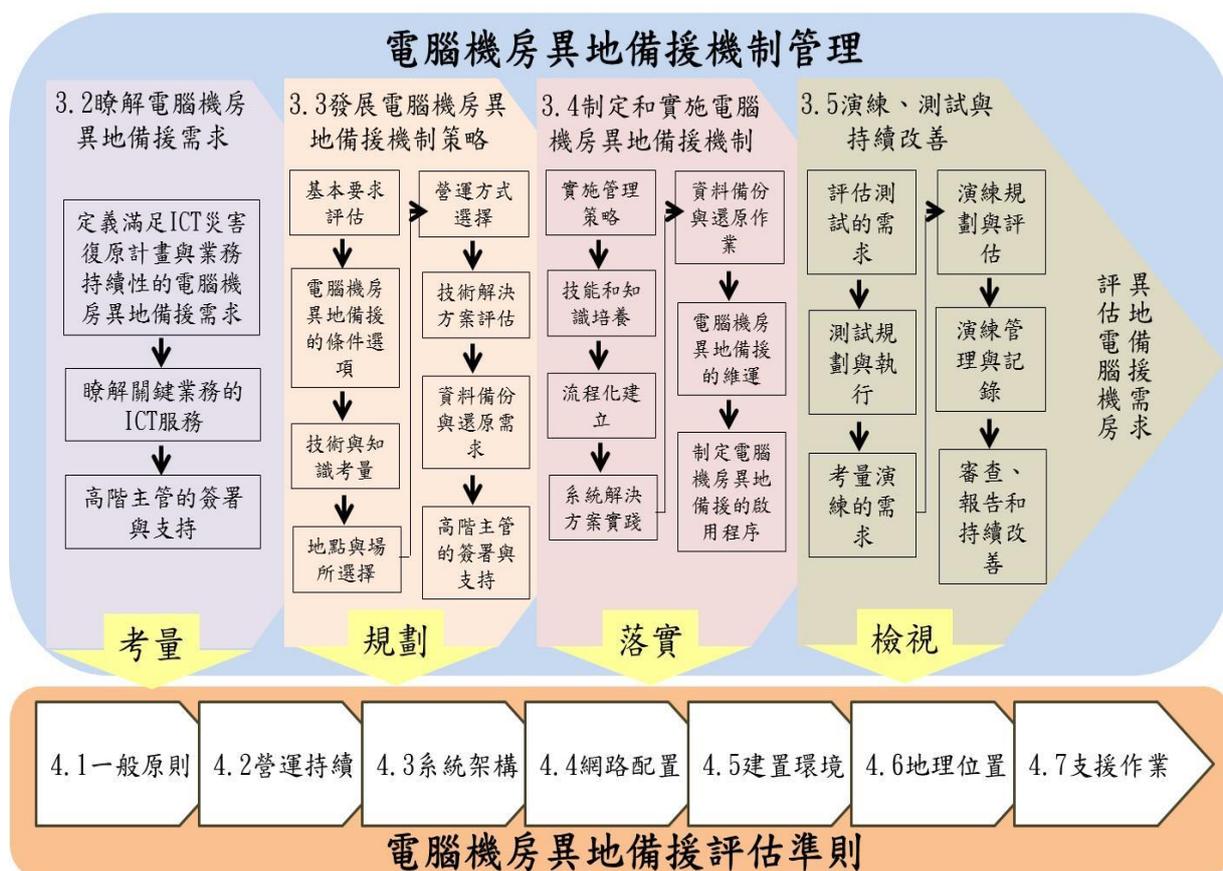
本指引主要彙整國內外營運持續管理、機房管理及 DR Site 建置等相關規範與標準，並提供可評估機房或 DR Site 現況之參考準則，共分成以下 7 個章節：

- 第一章「前言」：說明編撰本指引之目的、適用對象、章節架構和使用建議。
- 第二章「電腦機房異地備援相關規範」：說明國內外相關管理、建置之規範與標準要求，包括：
  - 國際電腦機房異地備援發展趨勢。
  - 國際組織電腦機房異地備援相關規範。
  - 先進國家電腦機房異地備援相關規範：包括美國、日本、韓國等。

- 我國電腦機房異地備援相關規範。
- 第三章「電腦機房異地備援機制」：說明電腦機房異地備援機制整個管理流程，包括：
  - 電腦機房異地備援機制管理。
  - 瞭解電腦機房異地備援需求。
  - 發展電腦機房異地備援機制策略。
  - 制定和實施電腦機房異地備援機制。
  - 演練、測試與持續改善。
- 第四章「電腦機房異地備援機制評估準則」：參考國內外規範與標準內容，條列各項 DR Site 建置的評估準則。
  - 一般原則。
  - 營運持續。
  - 系統架構。
  - 網路配置。
  - 建置環境。
  - 地理位置。
  - 支援作業。
- 第五章「結論」：說明本指引之總結。
- 第六章「參考資料」：說明本指引相關之國內外參考文獻和資料。
- 第七章「附件」：說明本指引提列之附件。

## (四) 使用建議

本指引可供各類型組織在營運持續管理的程序中，建立與改善電腦機房異地備援機制。第3章「電腦機房異地備援機制」透過Plan（規劃）、Do（執行）、Check（檢查）、Action（行動）之PDCA管理流程，說明各階段的工作項目，並同時參酌第4章「電腦機房異地備援機制評估準則」所建議之相關內容，以確保電腦機房異地備援機制的完善。第3~4章的關連和運作，可參閱圖1之內容。



資料來源：本研究整理

圖 1 電腦機房異地備援機制流程圖

在評估與建立電腦機房異地備援機制過程中，組織需先進行「風險評鑑」作業，針對在同一機房或環境下之各項資訊系統，參照行政院「資訊系統風險評鑑參考指引」與「資訊系統分類分級與鑑別機制參考手冊」，將

資訊系統鑑別出「普」、「中」、「高」安全等級，各組織可根據業務特性設定安全等級原則，亦可參考表格 2 之內容自行調整。

表格 2 資訊系統安全等級設定原則評估表

安全等級 影響構面	普 (等級 1)	中 (等級 2)	高 (等級 3)
1. 資料受到保護損害	<ul style="list-style-type: none"> <li>一般性資料</li> <li>資料外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損</li> </ul>	<ul style="list-style-type: none"> <li>敏感性資料</li> <li>資料若外洩或遭竄改，將導致個人權益嚴重受損</li> </ul>	<ul style="list-style-type: none"> <li>機密性資料</li> <li>資料若外洩或遭竄改，將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損</li> </ul>
2. 影響業務運作	<ul style="list-style-type: none"> <li>系統容許中斷時間較長</li> <li>系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響</li> <li>系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低</li> </ul>	<ul style="list-style-type: none"> <li>系統容許中斷時間短</li> <li>系統故障對社會秩序、民生體系運作將造成嚴重影響</li> <li>系統故障將造成機關核心業務執行效能嚴重降低</li> </ul>	<ul style="list-style-type: none"> <li>系統容許中斷時間非常短</li> <li>系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全</li> <li>系統故障將造成機關核心業務執行效能非常嚴重降低，甚至業務</li> </ul>
3. 影響法律規章遵循	<ul style="list-style-type: none"> <li>導致機關違反法律規章並伴隨輕微不良後果</li> </ul>	<ul style="list-style-type: none"> <li>將導致機關違反法律規章並伴隨嚴重不良後果</li> </ul>	<ul style="list-style-type: none"> <li>導致機關從根本上違反法律規章</li> </ul>
4. 人員傷亡	<ul style="list-style-type: none"> <li>無</li> </ul>	<ul style="list-style-type: none"> <li>無法完全排除造成人員傷亡的可能性</li> </ul>	<ul style="list-style-type: none"> <li>可能造成人員死亡，或非常可能造成人員肢體傷害危險</li> </ul>
5. 損害組織信譽	<ul style="list-style-type: none"> <li>若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害</li> </ul>	<ul style="list-style-type: none"> <li>若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害</li> </ul>	<ul style="list-style-type: none"> <li>系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害</li> </ul>
6. 其他	<ul style="list-style-type: none"> <li>由機關視本身業務特性考量可能遭遇衝擊之其他影響構面（如：財物損失），並依需求和本質自行設定分級基準</li> </ul>		

資料來源：行政院「資訊系統分類分級與鑑別機制參考手冊」，民國 99 年 7 月

此外，組織已通過資訊安全管理系統（Information Security Management System, ISMS）驗證（例如：ISO/IEC 27001、CNS 27001），或主管機關認可之驗證（例如：教育體系資通安全管理規範），或經管理階層認可之管理機制，最後再轉換為「普」、「中」、「高」安全等級。

組織在識別各資訊系統之安全等級後，安全等級最高者即為「重要（關鍵）系統」，可依據「電腦機房異地備援機制」之流程，進行考量和分析「電腦機房異地備援機制評估準則」各項目。

### （五）專有名詞解釋對照表

表格 3 專有名詞解釋對照表

中文名詞	英文名詞	專有名詞解釋
營運持續管理	Business Continuity Management, BCM	一個系統化的管理流程，用以鑑別可能對組織產生的潛在威脅，並了解業務流程受該威脅影響時可能造成的影響。此外，亦提供一框架供組織培養有效回應之能力，以建立應變彈性，保護利害關係人之利益。
營運持續管理系統	Business Continuity Management Systems, BCMS	組織用以建立、實施、操作、監試、審查、維護與改善業務營運的持續，屬整體管理系統的一部份。
營運持續計畫	Business Continuity Plans, BCP	為一書面化的完整流程，主要內容在說明業務中斷事件發生後的應變處理、危機溝通、業務持續與回復正常等作業內容。
營運衝擊分析	Business Impact Analysis, BIA	確認組織關鍵業務流程、該流程所需之資源，並且評估流程中斷對公司造成影響程度之分析方法。

災難；災害	Disaster	資訊系統因人為或自然因素，導致運作出現嚴重的故障或停擺，致使其提供的服務水準達到不可接受的情況，進而需啟動資訊系統備援機制。
災難（害）恢復； 災害（難）復原	Disaster Recovery	一套將資訊系統從受災難影響導致故障或停擺的狀態中，恢復至可正常運作活動與流程。
災害（難）復原 計畫	Disaster Recovery Plan, DRP	一套引導相關人員於資訊系統災害復原過程中，依循規劃、作業、資訊和文件，於預定時程內恢復資訊系統之運作。
演練	Exercise	組織用來訓練、評鑑、實作及改善運作成效的流程。
N+1	N+1	即備援機制的規劃模式；在系統日常運作所需的設備數量（N）之外，再安排多 1 套的設備，以支援臨時故障的部分，降低系統中斷的風險。
營運復原水準	Recovery Level Objective, RLO	指資訊系統於中斷恢復後第一時間可提供之服務水準。
營運復原時間	Recovery Time Objective, RTO	指資訊系統由中斷後至重新恢復服務之目標時間長度。
資訊資料回復點	Recovery Point Objective, RPO	指可容忍資料損失之期間。

資料來源：本研究整理

## 二、電腦機房異地備援相關規範

### (一) 國際電腦機房異地備援發展趨勢

#### 1. 跨國性異地備援趨勢

2011年3月11日發生的日本東北大地震，改變了人們以往對於天災的想像。這個地震除了規模達到9.0以外，還伴隨著將近40公尺的海嘯以及後來所導致的東京電力核電廠事故，過去針對單一災害所進行的防災準備完全不足以應付此一類型的複合式災難。

據PCWorld調查指出，由於日本經常發生地震且已經累積相當防災觀念，其資料中心建置時便已針對地震與淹水進行良好規劃，因此儘管規模9.0的大地震與後續的海嘯，日本大部分的資料中心均毫髮無傷。

然而複合型災難的第三個階段，也就是核電廠事故所導致的電力短缺，使得資料中心的持續營運面對極大的壓力。雖然靠著不斷電系統與柴油發電機，資料中心的災難復原計畫普遍可以順利進行，然而隨著油料的消耗，成本也大幅增加。此外，由於電力短缺，日本政府規定各資料中心必須降低用電量，降幅最高達到15%，否則便會面臨高額的罰金。面對這種狀況，即使在日本國內已經規劃相當距離的異地備援機制，仍會面臨電力不足的窘境，也因此形成跨國性異地備援的需求與趨勢。

在規劃跨國性的異地備援架構時，大型的跨國企業有其優勢存在。以日本NTT電信公司為例，他們在世界各地共建置了140多個資料中心，並建立企業雲端服務對外營運。透過跨國性的異地備援，當發生單一國家的災難時，便可以將營運系統轉移到其他國家的資料中心去運作。

然而規模較小的公司與政府單位，便無法直接規劃這樣的跨國性異地備援架構，因此便形成一種趨勢，透過不同國家的公司或單位以互助互惠的方式來進行相互備援。以國內的宏碁 eDC 為例，早在 2004 年時，宏碁便與日商 Tyco Healthcare 簽約合作，相互進行異地備援。

小型公司或政府單位之間的此類合作模式，近年來也愈來愈被提倡。然而由於各國的法律與規定不同，在進行相關合作時，也必須確保進行異地備援的資料合乎相關法規，例如資料保護法。以國內目前狀況為例，若與大陸地區的公司進行異地備援合作，則必須考量資料是否會被大陸官方利用公權力進行資料的讀取與複製的風險。

## 2. 雲端災後復原服務 (Disaster Recovery as a Service, DRaaS)

在進行異地備援架構的設計時所面臨最大的問題，通常是成本的考量。為了保持良好的營運持續性，常常需要付出高昂的成本，或者是以降低資料完整或回復時間的標準來降低成本。為了要達到降低成本，卻又能達到足夠的營運持續性，因此近來在使用傳統的異地備援方式之外，亦有利用雲端服務（例如：Amazon AWS 與 EC2）來提供異地備援的趨勢。

雲端服務的特色之一為「使用時才付費 (pay per use)」，這種服務模式非常適合用於降低建置異地備援服務時所需的成本。異地備援工作通常可分為兩個階段，第一階段是系統正常運作時期，此時備援主機大部分資源的消耗是沒必要的，因此只需要進行資料複製，所需要的系統資源相當少。第二階段為故障轉移時期，此時主機房因災害停擺，需要最完整的資源來取代主機房所有的服務。

若以正常運行時間達 99% 為目標，則只有 1% 的時間需要使用最大量的

雲端服務，整體來看便可以大幅降低異地備援的成本。另外，雲端服務的虛擬化（Virtualization）特性也可以大量縮短備援主機的啟動時間，因此更容易達到更低的 RTO 標準。

研究指出，依照目前的雲端服務計費標準，雲端災害復原服務最適合提供的異地備援模式為 Warm Backup Site。這是因為 Warm Backup Site 的資料不需要進行同步寫入，因此第一階段的資料複製需要的資源相當少，因此可以節省大量的成本。而 Cold Backup Site 則由於原本的建置成本就相當低，採用雲端服務反而可能花費更多金錢。至於 Hot Backup Site，雖然以成本來看，採用雲端服務的花費與自行建置異地備援機房相差不多，但是透過雲端服務的虛擬化來降低 RTO 時間也是一個值得考量的優點。

雖然雲端災害復原服務有上述的優點，但也有一些潛在的課題需要解決。一般來說，雲端服務供應商會依照統計來假設它的客戶不會全部同時發生災害事件，因此不會替全部的客戶準備尖峰流量需求的設備，以將低營運成本。然而災害發生時，同一個地理位置的客戶確實有可能會同時產生大量的備援需求，因而超過雲端服務商原本的規劃準備。

若要解決上述問題，就有賴雲端服務供應商設計自己的異地備援機制，將此大量的需求分散至不同地理的資料中心來提供服務。另外，近來由於美國國家安全局的網路監控事件發生，採用雲端災害復原服務有可能會導致重要資料外洩，也成為在選擇此一雲端服務時的考量要點之一。

## （二）國際組織電腦異地備援相關標準

本指引之訂立，參考 ISO、IEC 及 ITU 等三個國際組織所發佈之與電腦機房異地備援相關 8 份標準。包括 ISO 22301：2012、ISO 22313：2012、ISO/IEC 27001：2013、ISO/IEC 27002：2013、ISO/IEC 27031：2011、ISO/IEC

24762：2008、ITU-T L. 92（10/2012）SERIES L、ITU-T L. 1300（11/2011）SERIES L。各標準重點彙整如表格 4，各標準之簡介、適用範圍、重點，請參閱本指引附件 3。

表格 4 國際組織電腦異地備援相關標準

	名稱	標準簡介	適用範圍
ISO	ISO 22301:2012	<ul style="list-style-type: none"> <li>• 2012 年 5 月 15 日發布，為營運持續管理的國際驗證標準。</li> <li>• 主要提供企業、組織正式的營運持續管理架構，協助發展營運持續計畫，以便發生重大業務衝擊事件期間與之後之業務持續營運。</li> </ul>	<ul style="list-style-type: none"> <li>• 為通用之營運持續管理標準，可用於任何組織或部門，不論其類型、規模和組織的性質。</li> </ul>
	ISO 22313:2012	<ul style="list-style-type: none"> <li>• 2012 年 12 月 12 日發布 ISO 22313 營運持續管理系統指南。</li> <li>• 提供規劃、建立、實施、運行、監控、審查、和不斷改進文件化的管理系統的指南，使企業在出現破壞性事件時，能夠做好準備、應對和復原。</li> </ul>	<ul style="list-style-type: none"> <li>• 通用的營運持續管理系統指南，適用於各種規模和類型的企業，包括工業、商業、政府、和非營利組織的經營。</li> <li>• 提供規劃、建立、實施、運行、監控、審查、不斷改進文件化的管理系統指南。</li> </ul>
IEC(與 ISO 合作)	ISO/IEC 27001:2013	<ul style="list-style-type: none"> <li>• 2005 年 10 月 25 日宣布為資訊安全管理系統（ISMS）的國際標準，2013 年改版。</li> <li>• 提供企業、組織建置資訊安</li> </ul>	<ul style="list-style-type: none"> <li>• 在組織整體營運風險內，建立/實作/運作/監視/審查/維持及改進已文件化之 ISMS。</li> </ul>

	<p>全管理系統導入的國際標準規範。</p> <ul style="list-style-type: none"> <li>• 要求建立、實施、維護和組織的框架內不斷完善資訊安全管理系統。</li> <li>• 根據組織的需要，進行資訊安全風險評估和矯正。</li> </ul>	<ul style="list-style-type: none"> <li>• 依據個別組織或部分單位之需求，量身打造安全控制措施。</li> </ul>
<p>ISO/IEC 27002:2013</p>	<ul style="list-style-type: none"> <li>• 由 1995 年代中期英國標準 BS7799 延續發展，ISO/IEC 於 2000 年採用成為 ISO/IEC 17799:2000。</li> <li>• 2005 年第一次更新，2007 年時重新編號以與其他 ISO/IEC 27000 系列一致。</li> <li>• 2013 年 9 月 25 日 ISO / IEC 27002 於第二次改版，提供最佳實務，包括考慮組織的資訊安全風險環境控制的選擇、實施、和管理的指導方針。</li> </ul>	<ul style="list-style-type: none"> <li>• 用於擬訂組織實施 ISO/IEC 27001 資訊安全管理系統程序控制之選擇、訊安全控制、及開發自己的資訊安全管理指導方針。</li> </ul>
<p>ISO/IEC 27031:2011</p>	<ul style="list-style-type: none"> <li>• 2011 年發布 ISO/IEC 27031 營運持續的資通訊技術 (ICT) 準備指南。主要基於 2008 年的英國 BS25777 的實務準則，由 BS25777 規範延伸整合而成。</li> <li>• 描述營運持續的資通訊技術</li> </ul>	<ul style="list-style-type: none"> <li>• 適用所有類型的組織，從 ICT 角度為營運持續提供準備指南。</li> <li>• 範圍包括可能對 ICT 基礎設施和系統影響的所有事件和事故（包括安全相關）。包括資訊安全事故</li> </ul>

		<p>準備概念和原理，提供方法和過程的框架，並提高企業的資訊和通信技術的準備，以確保業務的持續性。</p>	<p>處理和管理、資通訊技術準備計畫和服務等實務。</p>
	<p>ISO/IEC 24762:2008</p>	<ul style="list-style-type: none"> <li>• 規範第三方機構應提供資通訊災難復原服務的標準。提供營運持續管理，適用於「內部」和「委外外包」資通信技術災難恢復服務。</li> <li>• 對設施供應商提供資通訊技術的災難恢復（DR ICT）服務的指南，包括建築施工、安全措施、提供基礎設施服務，如電力、水、電信、和環境控制。</li> </ul>	<ul style="list-style-type: none"> <li>• 規定了DR服務和設施的資通訊技術的實施、運行、監控、和維護。</li> <li>• 外包資通訊技術DR服務供應商，應具實踐提供基本的安全操作環境，並協助組織DR的能力；選擇恢復地點的指南；且不斷提高資通訊技術的DR服務。</li> </ul>
<p>ITU</p>	<p>ITU-T L. 92 (10/2012) SERIES L</p>	<ul style="list-style-type: none"> <li>• 說明外部設施保護（例如：電纜、電桿、和人孔…等等），免受天然災害影響技術因素。</li> <li>• 描述外部設施於面對地震、強風和洪水等天然災害的參考對策。</li> </ul>	<ul style="list-style-type: none"> <li>• 說明典型天然災害如地震、海嘯、洪水、強風，以及面對災害時，外部設備設施（如電纜管道、地下通道、人孔、電線桿、電塔、櫥櫃等）的技術管理與處理建議，以保護工廠以外的設施免受天然災害影響。</li> <li>• 電信建築包括室內設施超出 ITU-T L. 92 範圍，電纜和設備防範雷擊的保護則由 ITU-T K. 47 建議處理）。</li> </ul>

<p>ITU-T L. 1300 (11/2011) SERIES L</p>	<ul style="list-style-type: none"> <li>• 鑑於 Data Center (DC) 可能對環境、氣候產生負面影響，因此提出如何降低影響之作法。</li> <li>• 其最佳實務應用，可幫助組織和管理人員打造未來、或改進現有的 DC，以盡環境保護之責。</li> </ul>	<ul style="list-style-type: none"> <li>• 對綠能 DC 的建設和運營提供一套規則，包括先進的策略和技術，用以改造現有 DC，或設計未來新建的 DC。</li> </ul>
---	---	---

資料來源：本研究整理

### (三) 先進國家異地備援相關規範

本指引之訂立，同時參考美國、日本、韓國等國外之機房異地備援規範。美國部分含括美國國家標準技術研究所 (National Institute of Standards and Technology, NIST) 之聯邦政府資訊系統營運持續計畫指引 (Special Publication 800-34 Rev.1 - Contingency Planning Guide for Federal Information Systems)，以及美國國家標準學會 (ANSI) 之資料中心電信基礎設施標準 (Telecommunications Infrastructure Standard for Data Centers, TIA-942)；日本則參考日本資料中心協會 (Japan Data Center Council, JDCC) 之「資料中心設施標準」(Data Center Facility Standard)；韓國為韓國電信技術協會 (Telecommunication and Technology Association, TTA) 之資訊系統災害管理指引 (TTAS.KO-10.0259 on Guidelines for Disaster Management of Information Systems)，各規範之詳細簡介、適用範圍、重點，請參閱附件 3，摘要如表格 5。

表格 5 各國異地備援相關規範

	組織名稱	標準名稱	標準簡介	適用範圍	重點摘要
美國	NIST	SP800-34 Rev. 1 -Contingency Planning Guide for Federal Information Systems	<ul style="list-style-type: none"> <li>• 美國聯邦政府資訊科技系統緊急應變規劃指引。</li> <li>• 內容涵蓋資訊系統營運持續計畫的說明、建議、注意事項與考量因素。</li> </ul>	<ul style="list-style-type: none"> <li>• 提供美國政府部門或民間企業資訊科技系統緊急應變規劃指引。</li> <li>• 使用者可以參考進行資訊系統的營運持續計畫與災難復原計畫制定。</li> </ul>	<ul style="list-style-type: none"> <li>• 應變規劃應涵蓋：營運衝擊分析、備援與復原策略、備援中心、復原計畫制定、應變計畫的技術考量。</li> </ul>
	ANSI	TIA-942	<ul style="list-style-type: none"> <li>• 美國國家標準學會（ANSI）於2005年批准頒布的「資料中心電信基礎設施」標準。</li> <li>• 資料中心建設定位、功能指標、設計技術、施工方式、驗收標準等的具體技術要求與實現。</li> </ul>	<ul style="list-style-type: none"> <li>• 國際上第一部較全面以資料中心為物件的技術規範標準，為現代的機房工程建設提出新設計理念、系統架構與技術指標，以及術與系統的工程建議與指導。</li> </ul>	<ul style="list-style-type: none"> <li>• 根據資料中心基礎設施的可用性（Availability）、穩定性（Stability）和安全性（Security）分為四個等級： Tier 1：基本資料中心。 Tier 2：基礎設施部分備援。 Tier 3：基礎設施同時可維修。 Tier 4：基礎設施故障容錯。</li> </ul>

日本	JDCC	JDCC- 資料中心設施標準 (Data Center Facility Standard)	<ul style="list-style-type: none"> <li>• 仿效 Uptime Institute 的 4 階層模式，並參考 TIA-942、FISC STD、ITR-1001B、ASHRAE、IEEE 等多份日本國內外之文獻和標準，加上因地制宜的相關衡量指標，作為日本境內 DC 營運參考依據。</li> </ul>	<ul style="list-style-type: none"> <li>• 提供日本 DC 營運管理參考。</li> </ul>	<ul style="list-style-type: none"> <li>• 除引用相關規範、標準衡量指標外，另外因應日本的特殊狀況及考量 DC 營運的需要，提出了幾項建議指標：含地震、設施、營運管控風險評估。</li> </ul>
韓國	TTA	TTAS. KO-10.0 259 on Guidelines for Disaster Management of Information Systems	<ul style="list-style-type: none"> <li>• 2007 年 12 月 26 日公告</li> <li>• 提供政府機構或企業組織完整的操作說明，協助單位進行資訊設備的災難復原計畫與作業流程設計，以因應未知的外部風險或是內部人為失誤，並降低威脅造成的潛在損失。</li> </ul>	<ul style="list-style-type: none"> <li>• 提供韓國政府部門或民間企業組織，作為資訊系統災害管理之參考。</li> </ul>	<ul style="list-style-type: none"> <li>• 包含三個主要的工作階段與災難復原系統 (1) 建立復原計畫 (2) 設計、執行災難復原計畫 (3) 維運災難復原計畫。</li> <li>• 將異地備援的類型分為 6 種不同的型態：自建、共建、互為備援、自營、聯營與委外。</li> </ul>

資料來源：本研究整理

## （四）我國電腦機房異地備援相關規範

目前國內單位主要採用之機房異地規範，包括中華民國國家標準 CNS27001、行政院及所屬機關資訊安全管理規範、教育體系資通安全管理規範、資訊作業調整移轉應變作業參考指引等 4 份，規範說明如下。

### 1. 中華民國國家標準 CNS 27001

#### （1）中華民國國家標準

中華民國國家標準（National Standard of the R.O.C）以 CNS 作為正式代號，在國際間進行資料交換。我國國家標準的權責機構為經濟部標準檢驗局，依據中華民國國家標準訂定辦法所規定的標準程序，邀請產業界、政府機構、學術研究單位的各方專家代表，共同參與標準討論與審查，並彙整各方意見，以符合國際標準組織 International Organization of Standard 對標準的定義。

#### （2）CNS 27001 資訊技術-安全技術-資訊安全管理系統-要求事項

國家標準 CNS 27001 為一資訊安全的國家標準，主要為提供一個建立、實施、操作、監督、審查、維持及改進資訊安全管理系統之模式，採用資訊安全管理系統為組織的策略性決策。經濟部標準檢驗局參考國際標準於 95 年 6 月 16 日依據國際標準 ISO 27001：2005 內容完成制訂並公告。

### (3) CNS 27001 與異地備援機制

依據 CNS 27001 對備份的定義 (A.10.5)，為維持資訊及資訊處理設施的完整性與可用性，規範中的資訊備份 (A.10.5.1)，應依據所定義的備份政策，定期進行資訊與軟體的備份與測試。

## 2. 行政院及所屬機關資訊安全管理規範

### (1) 行政院及所屬機關資訊安全管理規範簡介

行政院及所屬機關資訊安全管理規範為 88 年 09 月 15 日發布，是行政院推動各機關強化資訊安全管理所特訂的規範，目的為建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全、保障民眾權益。

### (2) 行政院及所屬機關資訊安全管理規範與異地備援機制

在此規範中的第六大項「日常作業之安全管理」，清楚定義資料備份，另外也明確的說明備援作業使用的設備及備援媒體，應存放在安全距離以外的地點，以免資料中心或電腦機房受到損害時一併受到毀損。主要內容包括：

- 應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份及備援作業，以便發生災害或儲存媒體失效時，可迅速回復正常作業。
- 系統資料備份及備援作業，應符合機關業務永續運作之需求。

- 資料備份作業原則如下：
  - 正確及完整的備份資料，除存放在主要的作業場所外，應另外存放在離機關有一段距離的場所，以防止主要作業場所發生災害時可能帶來的傷害。
  - 重要資料的備份，以維持三代為原則。
  - 備份資料應有適當的實體及環境保護，其安全標準應儘可能與主要作業場所的安全標準相同；主要作業場所對電腦媒體的安全控管措施，應儘可能適用到備援作業場所。
  - 應定期測試備份資料，以確保備份資料之可用性。
  - 資料的保存時間，以及檔案永久保存的需求，應由資料擁有者研提。

### 3. 教育體系資通安全管理規範

#### (1) 教育體系資通安全規範簡介

教育體系資通安全管理規範的制定，為提供教育體系及相關單位一套有效建置與管理資訊安全系統（ISMS）；評估各單位資訊安全管理上的需求、目標、結果，並考量加入教育體系特有之作業程序、規模、架構等因素，制訂做出有別於業界所採用之 ISMS 規範。此規範強調實行度與執行效率，期能將此資訊安全規範及相關之實施經驗推行到各單位，進而強化 TANet 中各連線學校單位的資通安全。

## (2) 教育體系資通安全規範與異地備援機制

在規範中的 (A.10) 通訊與作業安全管理中的 (A.10.5) 備份作業之管控，提供備份的規範。

- 備份作業之管控 (A.10.5)：資料備份 (A.10.5.1) 重要資訊與軟體應進行定期的備份。資料備份應：
  - 準備適當及足夠的備援設施，定期執行必要的資料及軟體備份及備援作業，以便在發生災害或是儲存媒體失效時，可迅速回復正常作業。
  - 系統資料備份及備援作業，應符合單位業務永續運作之需求。
- 資料備份作業的原則為：
  - 正確及完整的備份資料，除存放在主要的作業場所外，應另存放於安全距離的場所，防止災害發生時可能帶來的傷害。
  - 重要資料的備份，建議以維持三代以上為原則。
  - 備份資料應有適當的實體及環境保護。
  - 應定期測試備份資料，確保其可用性。
  - 資料的保存時間以及永久保存的需求，應由資料擁有者研提。
  - 應定期檢查測試回復程序，確保回復程序能在指定時間內完成復原作業程序。
  - 重要機密的資料備份，應使用加密方式來保護。

#### 4. 資訊作業調整移轉應變作業參考指引

##### (1) 資訊作業調整移轉應變作業參考指引簡介

資訊作業調整移轉應變作業參考指引，依據「行政院及所屬各機關組織調整作業手冊」所律訂，提供有關資訊作業移轉應變之相關建議與規劃做為參考，確保設施移轉時不影響既有的運作，縮小影響範圍並減少相關可能發生的風險。行政院研究發展考核委員會於民國100年04月26日發布文件初版。

##### (2) 資訊作業調整移轉應變作業參考指引與異地備援機制

參考指引提到備份與備援原則，提供完整的服務以協助部會移轉規劃相關必要程序、技術與步驟，避免移轉事件造成重大損失。

- 備份與備援規劃考量

在規劃時應全面性考量移轉業務與系統重要性，主要項目如下：

- 備份/備援系統與作業切換成本
- 備份/備援系統規劃之完整性，包含系統備份/備援與資料備份/備援之整合
- 降低平常備份/備援作業對重要系統之效能影響
- 多重獨立備份/備援路徑，應用程式作業與資料複製分立於規劃時採用之設計建議規則如下：

- ◆多層次之備份/備援規劃，以因應個別狀況，啟動本地 (Local)、遠端 (Remote) 或重建之備份/備援機制，避免不必要之備份/備援切換。
- ◆提供遠端異地備援機制之人為介入判斷半自動 (Semi-Automatic) 切換機制，以防止不必要之作業切換。
- ◆應用程式備份/備援控制與資料備份/備援複製採用個別獨立。
- ◆備份/備援計畫程序與備份/備援人員組織之建立，以因應個別資訊系統中斷狀況，啟動個別程序作業，確保建置之備份/備援技術適時有效作用。
- 整體備份/備援方案建議
  - 系統資料備份/備援架構
    - ◆資料庫主機備份/備援方法。
    - ◆應用程式主機備份/備援方法。
    - ◆資料複寫網路設計。
  - 備援網路設計
  - 專案管理與建置服務
  - 備份/備援標準作業程序
    - ◆資料庫主機。
    - ◆應用程式主機。
    - ◆備援網路。

- 備份/備援系統實機演練
- 異動管理標準作業程序
- 異地備援架構規劃建議（詳如表格 6）
  - 部會共構機房與備援中心之主機、儲存設備、網路設備採取一對一比例。
  - 部會共構機房與備援中心間之網路以 GSN VPN 相連接。
  - 部會共構機房與備援中心之磁碟陣列系統應用資料複製技術，搭配光纖網路交換器與複寫網路，即時將大量資料自部會共構機房複製至遠端異地備援中心之備援系統。
  - 考量部會共構機房之作業，分別於部會共構機房與備援中心之磁碟陣列系統應用資料映射技術，將磁碟陣列系統之資料複製一份於本地端。

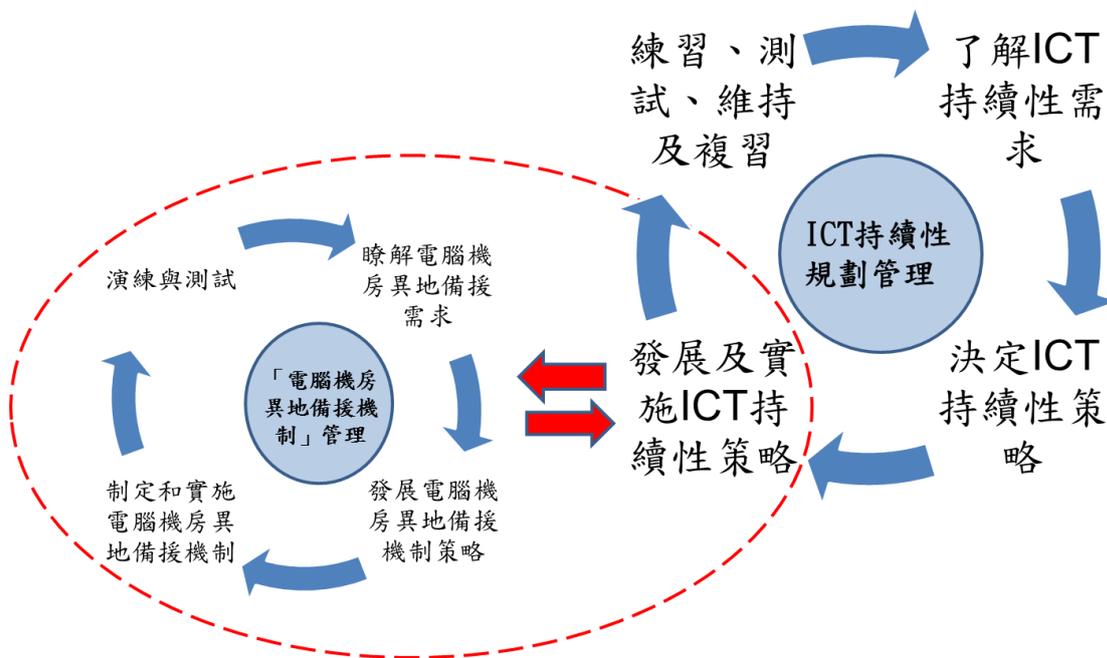
表格 6 異地備援系統架構比較表

備援機房種類	建置成本	硬體需求	通訊需求	建置所需時間	建置地點
冷備援站	低	無	無	長	固定
暖備援站	中	部分	部分/全部	中	固定
熱備援站	中/高	全部	全部	短	固定
行動備援站	高	專屬	專屬	專屬	不固定
鏡像站	高	全部	全部	無	固定

資料來源：行政院研究發展考核委員會資訊作業調整移轉應變作業參考指引

### 三、電腦機房異地備援機制

組織的資通訊技術（Information and Communications Technology, ICT）災害復原能力是影響業務持續營運成敗的關鍵因素之一，而 ICT 災害復原是組織整體業務持續性管理（BCM）的一個過程。組織在進行 BCM 的過程中，透過業務衝擊分析（Business Impact Analysis, BIA），定義出關鍵業務及其相關的資訊服務，並將這些關鍵業務的資訊服務納入 ICT 災害復原計畫管理。

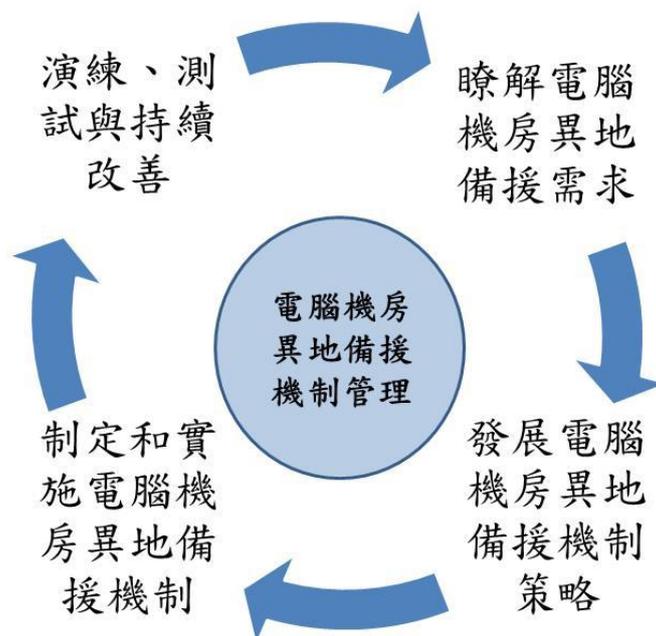


資料來源：本研究整理

圖 2 電腦機房異地備援機制與 ICT 持續管理之關係

電腦機房異地備援機制屬 ICT 災害復原計畫中的一個方案，ICT 災害復原計畫包含資源重置、異地備援、緊急應變處理及營運復原等規劃。當組織因為發生天災、人為疏失或惡意破壞等突發事故，導致組織本地端的主機房或是資訊系統服務中斷時，即可透過電腦機房異地備援機制，迅速回應 ICT 災害復原計畫與業務持續性管理（BCM）的需求，使組織業務回復正常或可接受的服務水準。關於電腦機房異地備援機制，本章節使用 PDCA 循

環說明電腦機房異地備援機制的管理，讀者可再依據流程各階段之要求，針對第 4 章「電腦機房異地備援機制評估準則」建議相關項目進行分析和考量。



資料來源：本研究整理

圖 3 電腦機房異地備援機制管理流程圖

## (一) 電腦機房異地備援機制管理

### 1. 建立電腦機房異地備援機制管理

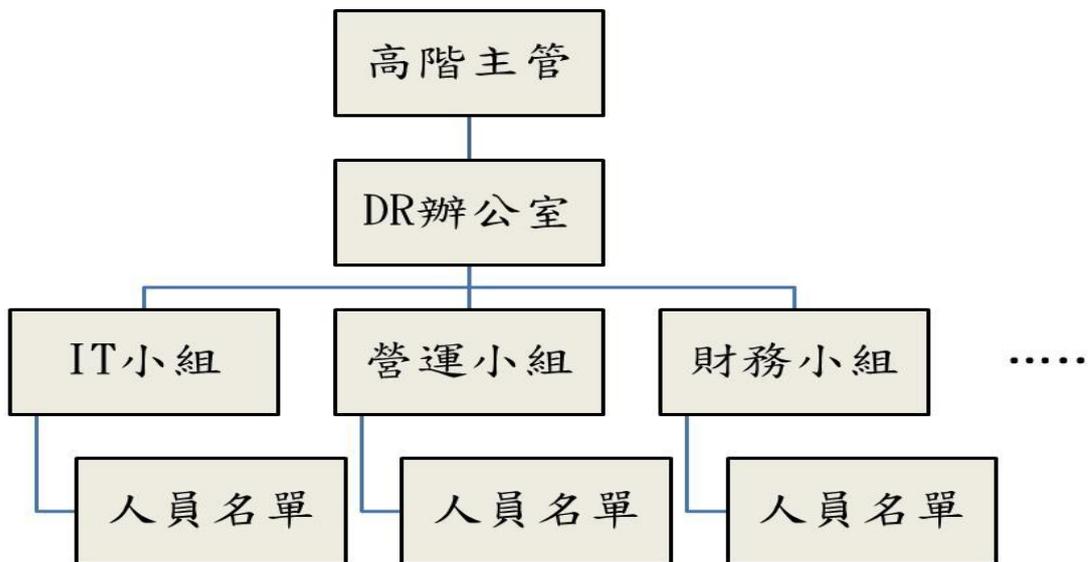
組織可採用過程導向（作法），以建立、實施、運作、維持和持續改善的管理方式，支持電腦機房異地備援機制的管理。

電腦機房異地備援機制的管理（可參閱本指引 4.1 一般原則）應確保：

- 電腦機房異地備援機制管理的目標應該清楚的定義。
- 最高管理階層對電腦機房異地備援機制作為 ICT 災害復原計畫的

一部份的承諾。

- 取得發展電腦機房異地備援機制的資源。
- 確認電腦機房異地備援機制管理的職責與角色。例如：設施復原、網路復原、平台復原、應用系統復原、損害評估與搶救、實體安全、通訊、硬體安裝、IT 運作、IT 技術、管理等小組，並建立 DR 推動與執行組織圖，範例如圖 4 所示。



資料來源：本研究整理

圖 4 電腦機房異地備援機制管理組織架構

## 2. 定義電腦機房異地備援機制的管理範圍

依照組織整體業務持續性管理（BCM）的 BIA 定義的關鍵業務、其相關的資訊服務及所擬訂的 ICT 災害復原計畫範圍，定義電腦機房異地備援所需的 ICT 持續管理與設立 ICT 技術目標的範圍（可參閱本指引 4.1 一般原則、4.2 營運持續），並適當的考慮到：

- 業務持續性管理（BCM）的政策與需求。
- ICT 災害復原計畫範圍、目標和義務（包括法律、法規與合同）。

- ICT 持續性的需求。
- 異地備援電腦機房可接受的風險與風險水平。
- 相關組織團體的利益。

### 3. 電腦機房異地備援機制管理融入組織文化

確保電腦機房異地備援機制納入日常的 ICT 業務和管理流程，並透過適當的教育訓練或宣導，以提高員工對機房異地備援機制的熟悉。(可參閱本指引 4.7.1 教育訓練)

- 意識培養
  - 透過相關的教育訓練提昇電腦機房異地備援機制的意識。
  - 確保員工了解在電腦機房異地備援機制的角色與職責。
  - 電腦機房異地備援機制的目標。
- ICT 人員的能力

確認電腦機房異地備援機制中，所有人員的能力可以執行電腦機房異地備援的任務：

- 確認電腦機房異地備援的任務所需的技術與能力。
- 依照所需的技術與能力進行人員培訓。
- 確保人員的技術與能力已滿足執行電腦機房異地備援的任務。
- 保存人員訓練、技能、經驗與資質的記錄。

#### 4. 電腦機房異地備援機制管理的文件與記錄

為滿足電腦機房異地備援作業應具備的文件與記錄，並留存一份於異地備援機房，包括（但不限於）以下幾項：

- 業務持續性管理政策。（可參閱本指引 4.1 一般原則）
- ICT 災害復原計畫。（可參閱本指引 4.1 一般原則）
- 關鍵業務及其相關的資訊服務，及其對應的 RTO 與 RPO 清單。（可參閱本指引 4.2 營運持續）
- BIA 的結果。（可參閱本指引 4.2 營運持續）
- 風險評鑑的結果。（可參閱本指引 4.1 一般原則～4.2 營運持續）
- ICT 技術文件，例如：異地備援機房配置圖、電力架構、網路架構圖、ICT 操作手冊…等等。（可參閱本指引 4.3 系統架構～4.5 建置環境）
- 交通路線圖。（可參閱本指引 4.3 系統架構～4.5 建置環境）
- 員工與支援廠商聯絡資訊。（可參閱本指引 4.1.2 災害復原計畫、4.7 支援作業）
- 相關支援團體的資訊。（可參閱本指引 4.1.2 災害復原計畫、4.7 支援作業）
- 演練與測試的程序、結果、矯正措施。（可參閱本指引 4.1 一般原則）
- 審查資料。（可參閱本指引 4.1 一般原則）

## 5. 監視及審查電腦機房異地備援機制的管理

電腦機房異地備援機制範圍內的程序、ICT 持續性技術、人員應該被監察與檢討管理，以確保異地備援機制的效率與有效性。（可參閱本指引 4.1.3 管理階層支持）

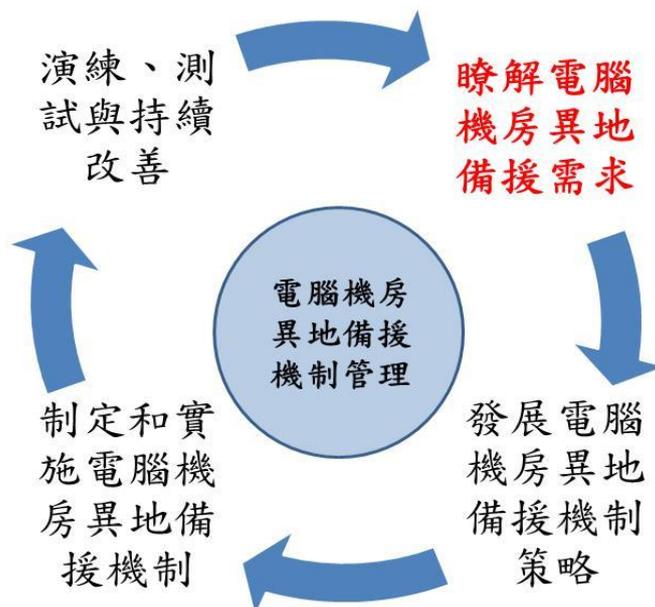
## 6. 矯正措施

組織應透過 BIA、風險評鑑、演練與測試的結果、監視與審查，確定電腦機房異地備援機制的風險與問題，並對於這些問題的影響進行預防與矯正措施。（可參閱本指引 4.1 一般原則）

## 7. 持續改善

組織應透過定期/不定期檢討業務持續性管理（BCM）的政策、ICT 災害復原計畫、稽核審查結果、矯正措施和管理審查，持續改善電腦機房異地備援機制。（可參閱本指引 4.1 一般原則）

## (二) 瞭解電腦機房異地備援的需求



資料來源：本研究整理

圖 5 瞭解電腦機房異地備援需求

### 1. 定義電腦機房異地備援需求

定義滿足 ICT 災害復原計畫與業務持續性要求的電腦機房異地備援需求（可參閱本指引 4.1 一般原則、4.2 營運持續），包括（但不限於）以下幾項：

- ICT 災害復原計畫與整體業務持續性管理（BCM）的要求與管理程序。
- 組織的 BIA，與 ICT 風險評鑑所定義的 RTO 與 RPO，將做為電腦機房異地備援機制的管理與運行的目標。
- 關鍵業務的資訊設備與服務清單，及其所涵蓋的人員/組織、ICT 技術或服務。

- 關鍵業務資訊設備與服務的日常維運作業與程序。

## 2. 瞭解關鍵業務的 ICT 服務

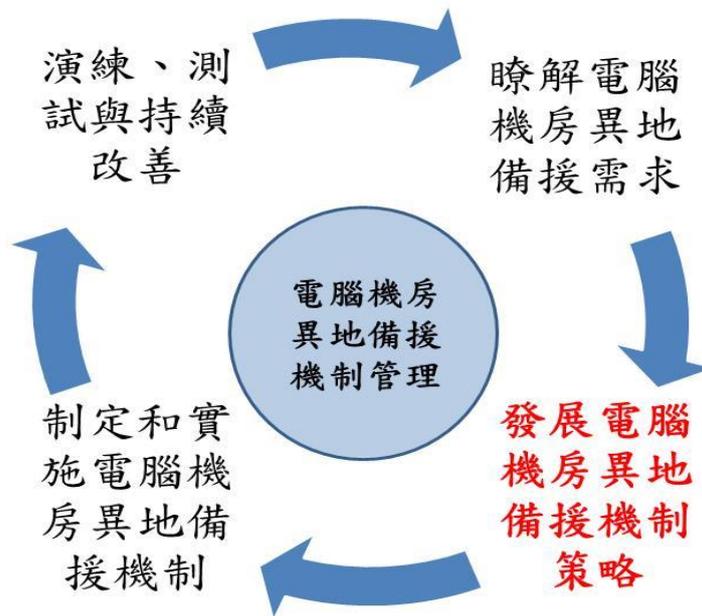
應評估重要業務的 ICT 服務需求，包括（但不限於）以下幾項：

- ICT 的人員技能與知識要求。（可參閱本指引 4.1 一般原則、4.7 支援作業）
- ICT 資源與預算。（可參閱本指引 4.1 一般原則）
- ICT 系統架構，包括軟體、硬體、作業系統、應用系統、儲存系統等的 ICT 設備。（可參閱本指引 4.3 系統架構～4.4 網路配置）
- 網路架構。（可參閱本指引 4.3 系統架構～4.4 網路配置）
- ICT 系統之間的關係與鏈接方式。（可參閱本指引 4.3 系統架構～4.4 網路配置）
- 資料儲存與備份方式。（可參閱本指引 4.3 系統架構～4.4 網路配置）
- ICT 系統運行的環境要求，包括場所、電力、空調等基礎設施的要求。（可參閱本指引 4.5 建置環境～4.6 地理位置）
- ICT 系統運行的環境，與其支持技術。（可參閱本指引 4.5 建置環境～4.6 地理位置）
- 外部服務或供應商。（可參閱本指引 4.1 一般原則、4.7 支援作業）
- ICT 服務風險評鑑的結果。（可參閱本指引 4.1 一般原則～4.2 營運持續）

### 3. 高階主管的簽署與支持

組織 BIA 與 ICT 風險評鑑的結果及其所定義的 RTO 與 RPO，應作成文件列表提供高階主管簽署核可，以取得後續發展電腦機房異地備援的機制的支持。(可參閱本指引 4.1.3 管理階層支持)

### (三) 發展電腦機房異地備援機制的策略



資料來源：本研究整理

圖 6 發展電腦機房異地備援機制策略

#### 1. 基本要求評估

在制定電腦機房異地備援機制的建置策略時，應該要考慮到建置和持續運作的資源需求。外部供應商可採簽訂契約方式，提供專業的服務與技術，發揮支持發展策略的重要作用。此外在發展策略的選擇上應該要考慮到組織內部的因素與限制（可參閱本指引 4.1 一般原則、4.2 營運持續），例如：

- 預算。
- 資源的可用性。
- 潛在的成本與效益。
- 技術的限制。
- 組織風險的可接受程度。
- 組織現有的 ICT 技術策略。

## 2. 電腦機房異地備援的條件選項

組織應該考慮一系列用於電腦機房異地備援機制的選項，這些選項主要是為了確保異地備援電腦機房用於 ICT 災難復原的能力，以及提供 ICT 災難的復原（可參閱本指引 4.3 系統架構～4.6 地理位置）。這些選項包括（但不限於）以下幾項：

- 技能與知識。
- 地點與場所的選擇。
- 營運方式。
- 技術解決方案。
- 資料備份與還原。
- 供應商。

### 3. 技能與知識考量

組織應該適當維持電腦機房異地備援機制的 ICT 技能與知識。這部份可能超出組織員工既有的 ICT 技能與知識，而需延伸到擁有 ICT 專業技能與知識的供應商或是第三方利益團體（可參閱本指引 4.7.1 教育訓練）。這些 ICT 專業技能與知識的內容包括（但不限於）以下幾項：

- 關鍵 ICT 服務執行方式的文件。
- ICT 工作人員與承包商的技能培訓。
- 避免核心技術集中的風險（確保核心技術掌握在不同的兩個以上的人）。
- 知識的保存和管理。

### 4. 地點與場所選擇

異地備援電腦機房地點與場所的選擇，應該以不與主機房受同一災難/失效影響的地理位置為原則（可參閱本指引 4.6 地理位置）。

### 5. 營運方式選擇

異地備援電腦機房營運方式應考量組織的電腦機房異地備援機制的執行預算、員工的技能與知識、潛在的成本與效益、組織風險的可接受程度與組織現有的 ICT 技術策略，予以規劃選擇。一般而言，營運方式有下列三種選項：

- 自行維運

在考量組織商業機密風險，以及在執行成本充足的考量下，可考慮採取自建自營異地備援電腦機房。

- 聯合維運

不同組織之間在未有利益競爭的條件下，可考慮聯合維運異地備援電腦機房（例如：政府部門的共構機房）。或在地理位置條件適當的情形下，採取互為異地備援機房的模式營運（例如：不同的學校組織之間）。一般而言，此種營運模式的成本最為低廉。

- 專業委外

考量組織本身 ICT 的技能與知識以及潛在的成本，在預算允許的情形下可採取專業委外的方式營運。例如專業 IDC 廠商所提供之異地備援方案。

## 6. 技術解決方案評估

異地備援電腦機房的技術解決方案，主要是以滿足 ICT 持續營運為目標。在重大 ICT 營運中斷發生時，達到 ICT 災難復原 RTO 及 RPO 的時間要求，以復原 ICT 服務水準。

組織應建立電腦機房異地備援機制的營運策略，以確保組織 BIA 過程所定義之關鍵業務資訊系統在重大中斷災難中，可以在 RTO 時間要求內完成 ICT 服務復原，進而復甦中段的關鍵業務。

除了資訊系統的 RTO 要求外，關鍵業務的持續營運也必須依賴最新或是最接近的資料。資料持續性解決方案的設計應以滿足組織定義

的 RPO 為標準。

支持 ICT 服務的技術通常需要複雜的規劃與安排，以確保持續性。因此在規劃電腦機房異地備援機制的策略時，應該考慮（但不限於）以下因素：

- 異地備援的地理位置，及與主機房的相對距離。（可參閱本指引 4.6 地理位置）
- 主機房的資訊系統數量，包含軟硬體、作業系統等。（可參閱本指引 4.3 系統架構）
- 系統架構需求。（可參閱本指引 4.2 營運持續～4.4 網路配置）
- 外部存取系統的需求。（可參閱本指引 4.3 系統架構～4.4 網路配置）
- 散熱要求。（可參閱本指引 4.5 建置環境）
- 電力要求。（可參閱本指引 4.5 建置環境）
- 網路通信需求。（可參閱本指引 4.4 網路配置）
- 異地備援電腦機房啟用方式：採自動或人工啟用。
- 自動化的要求程度。（可參閱本指引 4.2 營運持續～4.5 建置環境）
- 外部供應商和其它第三方組織網路連結方式。（可參閱本指引 4.1 一般原則、4.2 營運持續、4.7 支援作業）

## 7. 資料備份與還原需求

資料異地備份/還原仍應確保其過程的機密性、完整性與可用

性。資料異地備份和持續性策略應滿足組織業務持續性的要求（可參閱本指引 4.2 營運持續～4.4 網路配置），並考慮（但不限於）以下因素：

- RPO 的要求。
- 如何將資料安全儲存（例如：磁碟、磁帶、光碟）。
- 確保資料儲存在環境的安全。
- 在資料儲存、運輸或傳遞、距離、位置、網路連接（現場、非現場或第三方場所），規劃資料檢查的時間表。
- 資料還原的速度。

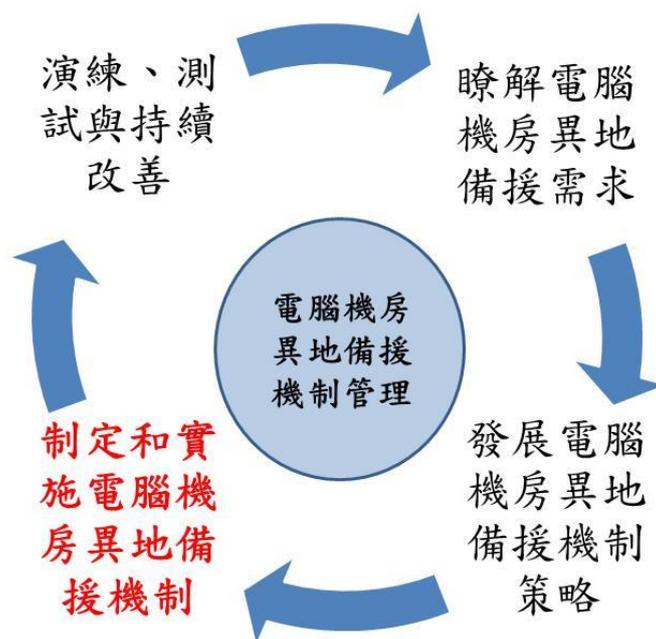
## 8. 高階主管的簽署與支持

電腦機房異地備援機制策略發展的結果，應作成書面化文件，提供高階主管簽署核可，以取得後續制定和實施電腦機房異地備援的機制的支持。（可參閱本指引 4.1 一般原則～4.2 營運持續）

電腦機房異地備援機制策略發展的結果書面化文件的內容應包括（但不限於）以下幾項：

- 滿足組織可能的業務中斷風險與影響。
- 與組織的 ICT 災害復原計畫與業務持續性策略整合。
- 符合組織可接受風險的整體目標。

#### (四) 制定和實施電腦機房異地備援機制



資料來源：本研究整理

圖 7 制定和實施電腦機房異地備援機制

##### 1. 實施管理策略

只應執行由組織最高管理階層批准的電腦機房異地備援機制管理策略。應該以專案或周期管理方式實施，納入組織的管理運作中，並透過計畫管理、程序管理、變更管理等程序，以確保每一個電腦機房異地備援機制的策略實施都能被報告與監督。(可參閱本指引 4.1 一般原則)

##### 2. 技能和知識培養

成功的實施(可參閱本指引 4.7.1 教育訓練)包括(但不限於)以下幾項：

- 過程和程序文件。
- ICT 相關的知識文件。
- 交叉訓練，以確保技能/知識的差距最小化。
- 人員銜接計畫。
- 避免熟稔的員工集中在同一位置。

### 3. 流程化建立

ICT 業務持續性、災難復原和異地備援機房啟用程序應該予以文件化，並應該明確完整詳細，以確保人員能夠執行這些程序。(可參閱本指引 4.1.2 災害復原計畫)

這些文件化的程序和 ICT 相關的操作文件除了存放於主機房外，應該至少備份一份於異地備援機房。

### 4. 系統解決方案實踐

電腦機房異地備援機制的 ICT 策略(可參閱本指引 4.3 系統架構)可能包括：

- 鏡像 (Mirror)，主機房與備援機房間的 ICT 系統作鏡像備援/備份，RPO 要求  $\approx 0$  hr，RTO 要求  $< 1$  hr。
- 熱備援 (Hot Standby)，主機房與備援機房間的 ICT 系統作熱備援/備份，RPO 要求  $\approx 0$  hr，RTO 要求  $\leq 8$ hr。
- 暖備援 (Warm Standby)，主機房與備援機房間的 ICT 系統作暖備

援/備份，RPO 要求  $\approx 24$  hr，RTO 要求  $\leq 24$  hr。

- 冷備援 (Cold Standby)，主機房與備援機房間的 ICT 系統作冷備援/備份，RPO 允許  $\approx 24$ hr，RTO 允許  $> 24$  hr。
- 委外合約，例如委外給專業 IDC 供應商或策略聯盟的組織，RPO 與 RTO 依合約要求。
- 前述不同的組合。

電腦機房異地備援機制的 ICT 策略參照本指引 4.3 系統架構。

## 5. 資料備份與還原作業

異地備份資料的可用性，應該組織 ICT 災難復原計畫的要求一致 (可參閱本指引 4.3 系統架構)，並可能包括：

- 備份週期期間，異地備份資料的可用性。
- 異地存放備份資料的機密性，尤其是委外儲存。

## 6. 電腦機房異地備援的維運

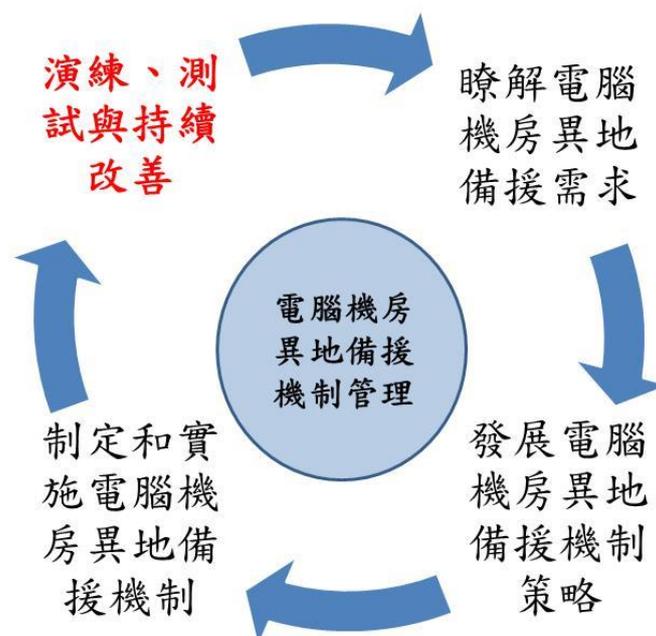
異地備援電腦機房的維運，應比照主機房的維運模式予以監控維護，並納入組織日常維運作業項目中 (可參閱本指引 4.5.3 環境監控與告警)。專業委外或聯合維運的異地備援機房，應將維運監控項目納入合約中加以規範。

## 7. 制定電腦機房異地備援的啟用程序

組織應訂定符合 ICT 業務持續性、災難復原要求的異地備援電腦機房的啟用程序（可參閱本指引 4.1.2 災害復原計畫、4.2 營運持續）。這個程序內容應該包括：

- 目的與範圍。
- ICT 復原目標。
- 角色與職責。
- ICT 復原程序（含系統與資料）。
- 附錄（內容包括 ICT 操作技術文件、聯絡資訊、供應商聯絡資訊、第三方支援團體聯絡資訊）

### （五）演練、測試與持續改善



資料來源：本研究整理

## 圖 8 演練、測試與持續改善

### 1. 評估測試的需求

異地備援電腦機房的 ICT 系統與備份資料應予以訂定週期性測試時間表。並依時間表進行 ICT 系統復原與資料還原測試，以確保異地備援電腦機房的 ICT 系統與備份資料處於備援與可用狀態。(可參閱本指引 4.3 系統架構)

### 2. 測試規劃與執行

相關測試規劃與執行之建議 (可參閱本指引 4.1.2 災害復原計畫)，可考量以下項目：

- 週期性測試時間表建議應至少每年安排一次 ICT 系統復原與資料還原測試。
- 規劃測試應避免影響主機房系統與資料的運作。
- 應規劃在測試期間遭遇緊急啟用異地備援電腦機房情形的應變措施。
- 測試後應對未能測試通過之 ICT 系統進行矯正措施。
- 所有測試應保留測試記錄。

### 3. 考量演練的需求

異地備援電腦機房的 ICT 系統復原演練，應予以訂定週期性演練時間表 (至少每年進行一次)。並依時間表進行 ICT 系統復原與資料

還原演練，以確保異地備援電腦機房的 ICT 復原能力符合 ICT 災害復原計畫與 ICT 業務持續營運的目標與要求。並藉由演練提升員工緊急應變之能力與熟悉 ICT 災害復原作業。(可參閱本指引 4.1.2 災害復原計畫)

#### 4. 演練規劃與評估

異地備援電腦機房的 ICT 系統復原演練應作成書面化之演練計畫，此計畫在實施演練前應經高階主管（例如：資訊、資安主管）簽署核可後，方可實施（可參閱本指引 4.1 一般原則）。演練計畫內容包括：

- 目的與範圍。
- 演練時程。
- 參與人員與職責。
- 執行方式。
- 執行作業流程。
- 風險情境假設。
- 成功的標準。
- 演練資料記錄/收集方式。
- 在演練期間遭遇緊急啟用異地備援電腦機房情形的應變措施。

## 5. 演練管理與記錄

演練過程中應作適當的管理（可參閱本指引 4.1.2 災害復原計畫），這可能包括：

- 足夠的觀察記錄人員。
- 啟動演練。
- 演練過程的記錄與資料收集。
- 演練時間的掌握。
- 緊急應變措施。
- 結束演練。

## 6. 審查、報告和持續改善

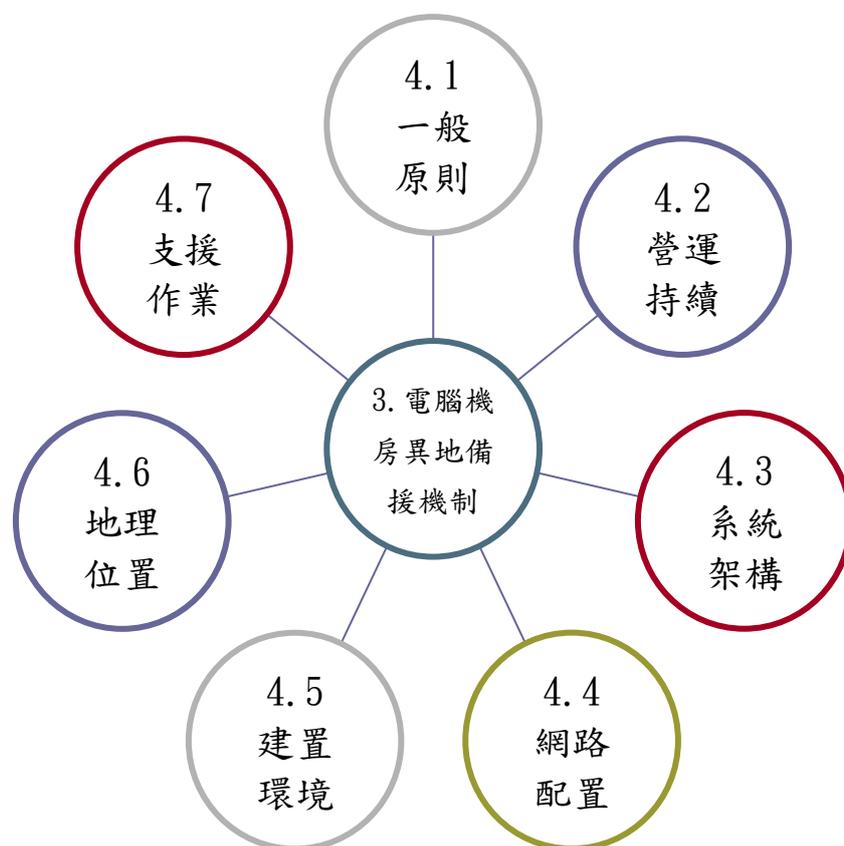
演練結束時，應及時檢討演練過程與結果（可參閱本指引 4.1 一般原則～4.2 營運持續）。包括：

- 演練過程是否符合 ICT 災難復原程序。
- RTO 與 RPO 是否達到要求。
- 分析演練過程的缺失。
- 分析未達 RTO 與 RPO 要求的原因。
- 分析演練過程與復原程序的差異與差距。
- 矯正措施與持續改善方案。

演練檢討結果應作成書面化報告，並提供最高階主管簽署核可，以取得高階主管對後續矯正措施與持續改善方案的支持。

## 四、電腦機房異地備援機制評估準則

本章節參閱營運持續相關標準文件（例如：ISO 22301：2012、NIST SP 800-34…等），也研析災害復原作業的指引資料（例如：ISO/IEC 24762:2008、Disaster Recovery:EC-Council|Press…等），並將各項評估項目分為（但不限於）七大類（如圖 9），形成「電腦機房異地備援機制評估準則」，作為各政府機關、學術單位和產業組織建立與考量相關評估準則的參考。組織可再根據需依循之法令、標準，以及業務特性、需求等項目，調整與擴增本評估準則之架構、範圍。



資料來源：本研究整理

圖 9 電腦機房異地備援機制評估準則架構圖

## (一) 一般原則

### 1. 資安稽核/自我檢視

資訊安全的議題一直以來都受到高度的重視，依據政府機關(構)資訊安全責任等級分級作業施行計畫的內容，「國家資通安全會報」將各政府機關(構)分成A~D四等級，並要求每年需進行內稽或自我檢視，B級單位以上更必須通過第三方驗證(參閱表格7)，資訊安全的重要程度可見一斑。

表格 7 政府機關(構)資訊安全責任等級分級作業施行對照表

等級作業 名稱	A 級	B 級	C 級	D 級
防護縱深	NSOC 直接防護/SOC 自建或委外、IDS、防火牆、防毒、郵件過濾裝置	SOC (選項)、IDS、防火牆、防毒、郵件過濾裝置	防火牆、防毒、郵件過濾裝置	防火牆、防毒、郵件過濾裝置
ISMS 推動作業	通過第三者驗證	通過第三者驗證	自行成立推動小組規劃作業	推動 ISMS 觀念宣導
稽核方式	每年至少 2 次內稽	每年至少 1 次內稽	自我檢視	自我檢視
資安教育訓練 (一般主管、資訊人員、資安人員、一般使用者)	1. 每年至少(3、6、18、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定	1. 每年至少(3、6、16、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定	每年至少(2、6、12、3小時)	每年至少(1、4、8、2小時)
專業證照	維持至少 2 張資安專業證照	維持至少 1 張資安專業證照	資安專業訓練	資安專業訓練
檢測機關網站安全弱點	每年 2 次	每年 1 次	每年 1 次	每年 1 次

資料來源：行政院「政府機關(構)資訊安全責任等級分級作業施行計畫」，民國 98 年

有鑑於此，組織在建立異地備援機制的過程中，宜評估、確保資安相關之管控，並能夠符合法令、主管機關或利益關係伙伴的要求。建議包含（但不限於）以下幾項考量：

- 資訊安全管理系統（Information Security Management System, ISMS）：國內對 ISMS 導入的觀念已相當成熟，該管理系統對於人員、實體、網路、存取、系統開發、營運與通報等皆有相對應的要求項目。政府機關、企業可透過第三方稽核取得 ISO 27001:2013 的認證，而教育機構可申請經教育部認可之「教育體系資通安全管理規範」認證。若組織自行評估為無接受外部認證需求，亦宜建立必要之資安管控措施，並定期執行自我檢視，以提升資訊安全防護。
- 個人資料保護（Personal Information Protection）：由於我國已於民國 101 年 10 月正式施行個人資料保護法，因此無論是哪種組織，皆應遵循法令以及主管機關的規範，建立與落實個人資料保護相關措施，以避免損害當事人的權益，造成不必要的洩漏及損失。組織除了遵守法令外，亦可考量透過第三方稽核的方式，以取得認證方式來證明組織對於個資保護的支持及保障，目前國內較為普遍的方式是通過 BS10012 驗證。

## 2. 災害復原計畫（Disaster Recovery Plan, DRP）

營運持續管理的環節中，災害復原計畫的訂定在於確保組織面對災後的各項恢復措施，能夠準確、即時的完成資訊系統上線。根據 Disaster Recovery:EC-Council|Press 的定義，DRP 可分為以下三個階段：

- 預防（災前）：組織應於事前保護系統的弱點與重要資料，並訓練災害復原團隊，確保 DRP 在災害發生時能夠容易且快速的展開。
- 持續（災中）：災害發生期間，需確保組織能夠正確的持續運作。因此，包含關鍵系統與資源的維持，例如能順利移轉至異地機房，種種都是本階段應留意的重點。
- 復原（災後）：此階段主要是將關鍵系統、資源恢復到日常運作的狀態，使組織在異地機房仍可正常營運。

因此，組織在建立一個 DRP 時，宜評估該計畫能包含（但不限於）以下各項需求：

- 計畫範圍界定：DRP 的架構以及含括的系統及設備、使用資源、執行階段等皆須明確的定義，並將其流程、操作建立一套標準作業程序（Standard of Procedure, SOP），以供相關單位、人員遵循。
- 人員規劃與訓練：需將 DRP 相關內外部單位、支援廠商的角色及人力清楚定義，提供必要的教育訓練（可參閱本指引 4.7.1 教育訓練），並適度要求參與演練作業，以提升其執行 DRP 的效率。
- 演練作業：DRP 需定期進行演練測試（可參閱本指引 3.5 演練、測試與持續改善），並要求相關單位人員的參與，進而評估演練成效，追蹤、解決過程中發現的問題，確保計畫的可執行，以及結果符合預期需求。
- 建立緊急應變小組：該小組的成立在於發起 DRP 的啟動，並即時的運作、處理、監控 DRP 的執行，以掌握實際的情況，促進 DRP 的運轉與成效。
- 資料異地備份：資料備份類型與異地資料備份方式之作法，選擇

符合組織需求的備份方式，以便於在 DRP 啟動時，能順利復原資訊系統的資料。

- 備援設備確保：備援資訊系統運作所需的環境、電力、設備、網路等要件（可參閱本指引 4.5 建置環境～4.6 系統架構），皆須確保能符合 DRP 的需求，在災害復原時能夠負荷系統的運作，達到組織預定的目標水準。
- 聯絡清單建立：建立一份 DRP 相關人員的聯絡清單，清楚表列其分組、工作執掌及緊急聯絡資訊，確保在啟動 DRP 時，能夠即刻聯繫。
- DR Site 安排：DR Site 的配置不單只是異地備援機房的評估，另外還包括執行 DRP 所需的作業空間（可參閱本指引 4.7 支援作業），以便計畫的展開與運作。

上述各項需求會因為業務的需求、特性，以及能支配的資源和經費而有規模上的差異，組織宜評估實際狀況，建立一套可執行且符合營運持續考量的災害復原計畫。

### 3. 管理階層支持

組織應設置專責主管，例如資訊或資安主管負責 DRP 的規劃與推動，相關內容可參閱 ISO 22301：2012。為了達到組織營運持續的目的，管理階層需展現其領導與承諾，以下包含（但不限於）幾項需專責主管主導之工作：

- 專責主管應建立營運持續的政策與目標，並符合組織業務的需求和方向，例如評估 DRP 之規劃能符合組織營運持續的預期水準。

- 專責主管應將組織營運持續的要求整合到營運流程當中，即視 DRP 為營運過程中的必要環節。
- 專責主管應確保營運持續所需的資源皆可被使用。例如：提撥適當經費採購資訊系統災害復原所需之設備、支援人力的配置等。
- 專責主管應傳達組織營運持續的有效且符合相關要求的重要性，此部分可透過在例行管理會議或 DRP 演練檢核會議中宣告。
- 專責主管應確保營運持續作業能達到預期結果，即 DRP 演練之成效評估符合組織預設的目標水準。
- 專責主管應提倡持續改善，在例行管理會議上檢討、審查 DRP 相關之演練、實際執行之結果。
- 專責主管應適時支持各管理階層，使其領導與承諾得以推展、落實。

DRP 的目的在於防範未然，設想的災變可能從不會發生，因此更需要管理階層的支持與認同。專責主管除指派相關負責的人員外，也需提供執行 DRP 所需的必要資源，才能達到業務持續運作的最終目的。

#### 4. 資源評估

在規劃 DRP 的過程中，除了考量組織業務的需求外，亦需評估可執行程度（例如：RTO、RPO），而這將受到組織所掌握資源的限制。

資源評估主要包含以下項目：

- 既有的資源：包含組織、利益關係夥伴、委外廠商等支應 DRP 運作可供的資源。例如：機房設施、軟硬體設備、網路傳輸、支援

人力等各類資源，組織皆應評估是否足以提供或可提供的程度。

- 成本與經費：在既有資源外之經費的持續支持以提供長時間的維運，並使 DRP 的運作能符合本指引的各項建議要求。另外亦進行營運成本的分析，評估經費支用的成效。

畢竟 DRP 只是組織營運的一環，投入太多的資源，反而可能影響組織的發展並侷限資源的運用。因此如何在防範未然與業務運作間取得平衡，對管理階層而且亦是一大挑戰。

## 5. 變更管理

變更管理的目的，在於評估各種因素的改變可能造成 DRP 營運的風險，組織宜對此提早因應，並調整災害復原程序。變更管理包含（但不限於）以下幾項考量：

- 環境變更：此部分主要針對機房建築、地理環境（可參閱本指引 4.5 建置環境～4.6 地理位置）的改變，例如風災造成機房所在位置淹水。這類的改變將可能造成 DRP 運作風險的提升，組織宜據此重新評估。
- 軟硬體變更：資訊系統相關軟硬體環境、設備、版本、設定、資料的改變都屬於此（可參閱本指引 4.3 系統架構、4.4 網路配置）。面對主系統的異動，異地備援系統宜對此進行評估、測試，確保在系統轉換上的運作無虞，避免造成 DRP 的失效。另外，重要資料的刪除/銷毀亦屬變更的一部分，須在遵循我國個資法及組織的要求下，建立相關的管控程序。

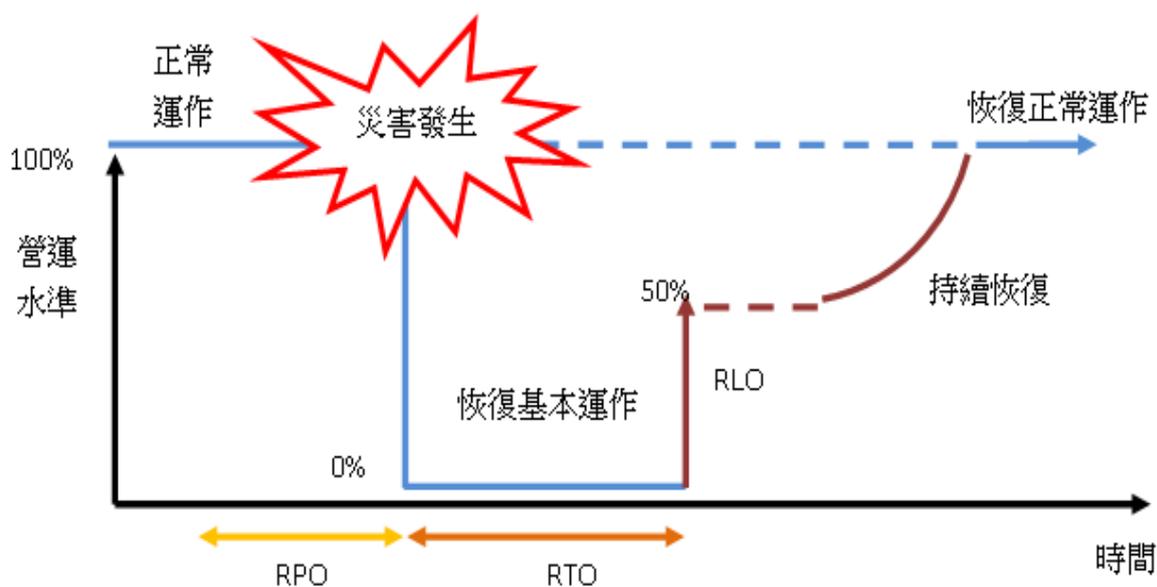
- 人員/廠商變更：DRP 相關人員的異動與合作廠商的更換，也是變更管理中須納入評估的一部份。例如：新進人員對任務的熟悉度、新廠商的服務品質等，都可能造成 DRP 運作的不順暢，影響組織的持續營運。

原則上各種的變動，組織都宜予以記錄，並監控、測試該變更對 DRP 的影響，降低因此產生的不穩定性，避免可能的風險。

## (二) 營運持續

建立 DRP 之目的在於確保組織業務的營運持續。當災害發生時，相關人員必須依據既定的程序，啟動、執行各項恢復作業，使資訊系統能在規定的時程內再次上線。通常在評估整個 DRP 成功與否的關鍵，最為常見的便是資料回復點 (RPO) 及營運復原時間 (RTO)。此為組織評估業務特性和需求，加上相關人力、資源與設備的緊急復原能力，配合測試及演練的確認，最後訂定出來營運持續的重要指標。

此外，考量成本與資源上的限制，DR Site 可能受設備、網路、廠商等因素，亦可能是災害所造成的災損影響，導致災害復原後第一時間能提供的服務水準低於日常規模。例如：地震造成電力、通訊多日中斷，或受限網路頻寬僅能提供平日一半的流量服務等。而這些都是組織必須納入考量，進而訂出資訊系統緊急復原上線後的營運復原水準 (Recovery Level Objective, RLO)。上述三項指標可參閱圖 10，以瞭解其間的相互關係。



資料來源：本研究整理

圖 10 RPO，RTO，RLO 流程示意圖

## 1. 資訊資料回復點 (Recovery Point Objective, RPO)

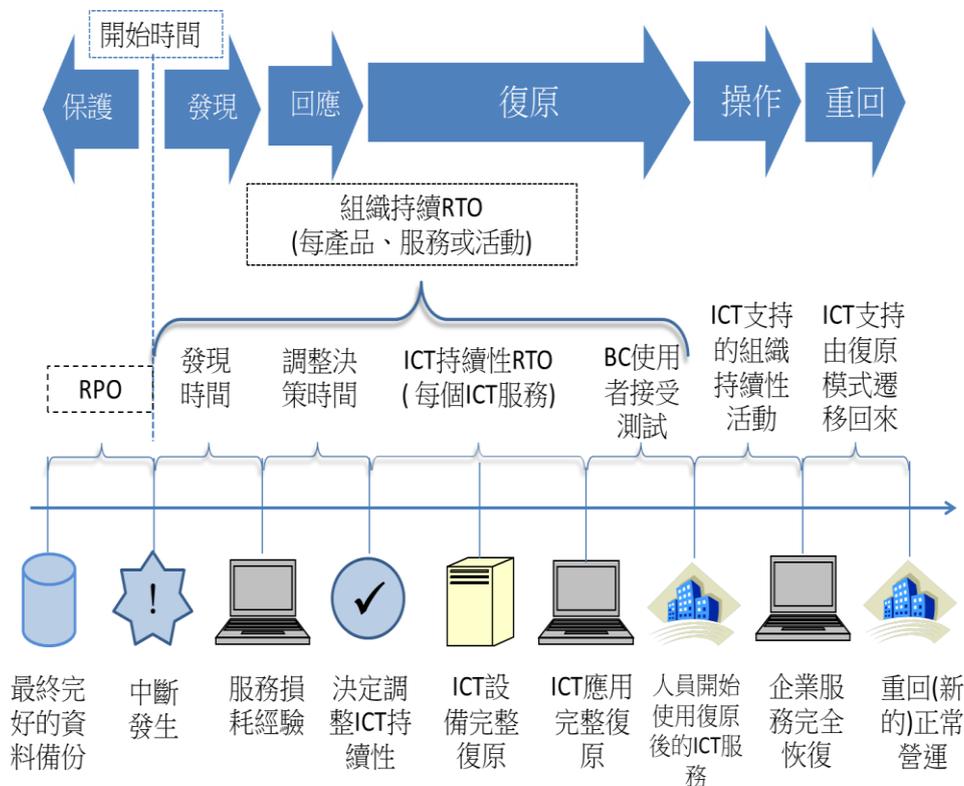
RPO 意指資訊系統運作所需的資訊資料必須被還原至災害發生之前的時間點。RPO 的制訂必須考量日常備份的作法，包括備份的類型（可參閱本指引 4.3.1 資料備份類型）及方式（可參閱本指引 4.3.2 異地資料備份方式）。以確保在災害復原的過程中，系統能取得最近一代的資料，使業務得以持續營運。組織設定 RPO 的時間越短，則所需花費的資源、成本則越高。針對 RPO 的考量，有以下幾項：

- 系統環境：針對網路、系統設備（包含程式）環境與設定的回復，除了備份的檔案外，可相容之設備亦是考量之一。須確保提供可運轉、服務的環境。
- 系統資料庫：系統存放在資料庫內的各項紀錄，將影響備份機制的設計。尤其對即時服務需求越高的系統，宜考量鏡像站（Mirror Site）的備援方案（可參閱本指引 4.3.3 系統備援方式），減少資

料庫復原的時程，降低因災害所造成的損失。

## 2. 營運復原時間 (Recovery Time Objective, RTO)

RTO 意指當災害發生後，資訊系統恢復基本或必要服務的所需時間。根據 BS 25777:2008，關鍵 ICT 持續管理時間軸可區分為保護 (Protect)、發現 (Detect)、回應 (React)、復原 (Recover)、操作 (Operate)、重回 (Return) 等六階段，其過程可參閱圖 11。



資料來源：BS 25777:2008

圖 11 關鍵 ICT 持續管理時間軸

其中在 RTO 的定義上，除了包括 ICT 相關軟硬體設備、應用程式的恢復及緊急上線測試外，還需將發現災害發生與決定啟動 DRP 過程的時間納入。例如組織評估系統復原上線的時間需要 1 小時，而當災害發生開始，到偵知、通報、評估系統受損狀況、決定啟動 DRP 等過

程需要半小時，則 RTO 應為 1.5 小時。其中，服務損耗經驗是影響 RTO 長短與 DRP 執行的重要環節之一，左右著災害復原的成敗。除了仰賴決策者的過去經驗外，更需要定期的測試與演練。

無論是服務提供者或使用者，災害發生後服務恢復時間越短越好。但這牽涉到 DR Site 所採用的系統備援模組（可參閱本指引 4.3.3 系統備援方式），也關係到 DR Site 建置和運轉的成本，同時更反映了服務提供者與使用者間對持續營運認知的落差。RTO 的制訂主要有以下幾項考量項目：

- 系統設備狀態：DR Site 所籌備的系統、設備等級高低，左右著 RTO 的長短；當然，負責人員對於緊急上線程序的熟練度，亦是考量因素之一。
- 復原成本（可參閱本指引 4.1.4 資源評估）：無論是何種程度的復原速度，這都意味著 DR Site 包括人力、設備、資源等各種成本的支出。隨著單位對 RTO 與可承受成本的認定，服務恢復的時間快慢也會有所影響。
- 服務水準協議（Service Level Agreement, SLA）：復原時程的壓力主要來自與利害關係團體（使用者、合作廠商及第三方單位）簽訂的協議。因此在制訂 RTO 時，亦需將相關合約的要求、限制一併納入考量，避免因違約而造成更大的損害。

### 3. 營運復原水準（Recovery Level Objective, RLO）

RLO 意指災害發生後，資訊系統於 RTO 要求內復原第一時間可提供之服務水準。雖然組織根據業務的需要及可能的風險，規劃 DRP 與

建立 DR Site，但受限於成本與資源，或者災害的影響程度超過預期，將導致資訊系統恢復上線的第一時間，其服務水準低於日常營運的狀態。縱然 DRP 運作符合 RPO 與 RTO 的要求，卻仍影響組織的正常營運和使用者可取得的服務。例如美國 911 事件或日本 311 地震，因受害層面太廣，系統固然能恢復運作，但可能需要數日或更久的時間，才得以恢復到平時的狀態。

其實在 BS 25777:2008 對關鍵 ICT 持續管理時間軸的說明中，就已針對 RTO 之後再定義回復正常營運的時間軸。因此 RLO 的制訂可幫助組織檢視現有 DRP 或 DR Site 在提供營運持續上的能量，包括網路、軟硬體設備、合作廠商、系統服務等服務水準的評估。組織藉此能建立不同重大災害發生時，資訊系統恢復上線時的服務規模。RLO 的評估包含（但不限於）以下幾項考量：

- 設備復原水準：泛指支援資訊系統運作之基礎運作設備。例如：網路、電力、機房等相關或延伸之營運要件。
- 系統復原水準：資訊系統本身可提供的服務，可能會受到資料庫、備份資料、程式或其他關連系統的回復狀況，而影響服務的水準。
- 服務復原水準：此部分可以包含內部人員、外部單位、支援廠商等在災害發生後能提供的服務狀況。

組織可綜合評估各項災害復原的要素，訂出合理的 RLO 值。亦或條列影響服務水準之項目，考量其災害復原後可服務之能量，並給予權重比例，推算出可接受的 RLO。可參考表格 8 之範例。

表格 8 災害復原 RLO 值評估表

評估項目	災害復原後之水準 (與日常狀態相比)	權重 (總和 100)	RLO 小計
網路頻寬	70%	20	14%
備援電力	60%	20	12%
系統功能	60%	40	24%
技術人員	100%	20	20%
RLO 總計			70%

資料來源：本研究整理

#### 4. BCP 演練

組織應定期進行 DR 緊急應變演練，藉以檢視 RPO、RTO 及 RLO 的有效性，並維持員工的警覺性，降低意外事件一旦發生造成的混亂。

DR 緊急應變演練應包括以下範圍：

- 通知、告警和溝通程序。
- 通用緊急應變設施的位置與使用。
- 對高危險作業的保護活動。
- 撤離、避難和責任歸屬程序。
- DR 緊急應變演練結束程序。

DR 緊急應變演練的應包括事前的計畫、執行、文件化記錄、和事後的檢討評估，DR 緊急應變演練應符合以下要求：

- 應該每年至少進行一次演練。
- 當異地備援電腦機房的容量和能力發生影響組織服務的重大變化時，應該進行緊急應變演練。這些變化例如：實體設施、設備、通訊和電源的變化。
- 所有演練，不論是否宣告，皆應進行適切的規劃與設計，以免導致組織服務的任何中斷。
- 演練應該採取步驟化，以確保演練狀況處於控制之下。
- 演練應該取得高階管理階層的批准與授權。
- 所有演練、演練計畫、和演練結果應該予以文件化以備後續的檢討與評估。
- 演練中發現的缺失應該盡早補救與改善。
- 應建立演練項目周期時間表，每次針對不同可能形式的意外進行演練。例如每 5 年為一周期，預先規劃 5 年的不同意外演練項目時間表，每年依該時間表執行一次演練，5 年後所規劃之意外項目都演練完後，再從頭依新規劃的演練項目時間表進行演練。

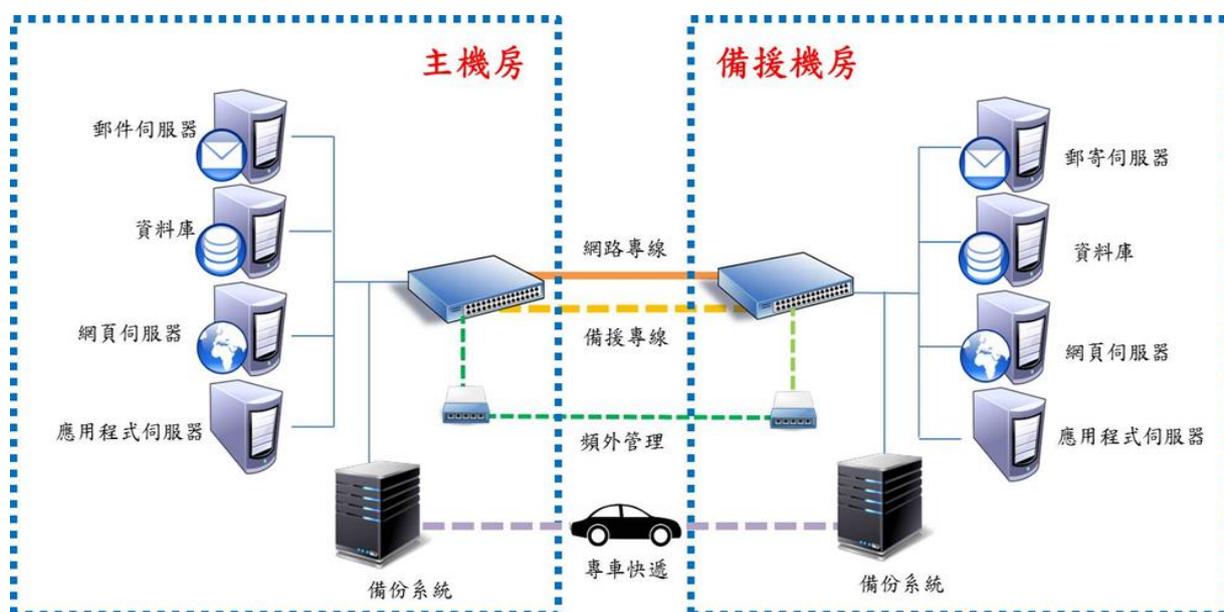
### (三) 系統架構

資訊應用系統的災難復原是建構在資料災難復原的基礎上，應在異地備援機房建立一套完整的與主機房的資訊應用系統相當的備份應用系統（可以是互為備援）。建立備援資訊系統是相當複雜的，不僅需要包括可用的資料複製，還包括網路、主機（硬體）、應用系統（軟體）、甚至 IP 等等的資源，以及各資源之間良好相容與協調。建構備援資訊系統主要的技術包括負載均衡、叢集技術。而資料災難復原是資訊應用的技術，資訊應用

系統的災難復原則是資料災難復原的目標。

在規劃資訊應用系統的災難復原的架構時，還必須要考慮多層次的廣域網路故障備援機制。主機房在多個伺服器運行一個或多種應用服務的情況下，應確保任何伺服器出現任何故障時，其運行的應用服務不能中斷，或系統應用程式應能迅速轉換到其它伺服器上運行。也就是說，在主機房本身即應有系統叢集和熱備份的功能。

在備援機房的備援資訊應用系統中，要實現完整的資訊應用系統備援，應包含主機房既有的系統安全機制、異地備份的資料複製機制，還應具有遠距的廣域網路故障備援能力和事故診斷能力。也就是說，一旦障礙發生，備援機制要有強大的障礙診斷和備援策略制訂機制，確保迅速的反應和業務接管。



資料來源：本研究整理

圖 12 異地備援系統架構示意圖

異地備援的系統架構的需求取決於組織的 BIA 與 DR 計畫。本節將針對異地備援的系統架構分成資料備份類型、異地資料備份方式、異地備援應用系統、以及系統備援方式等四個構面探討。

## 1. 資料備份類型

資料備份的目的是為了在災難發生或設備故障時，保護資料避免遭受到破壞或將破壞的程度減到最小。資料備份就是將資料從系統中複製搬移到另一備份媒體上的方法。對組織來說，資料備份最重要的是在備份與復原的時間都能降至最低，減少在資料備份/復原的作業過程中，對組織資訊系統運作帶來的衝擊。資料備份一般可分為「完整備份 (Full Backup)」、「遞增備份 (Incremental Backup)」與「差異性備份 (Differential Backups)」等 3 種基本類型。

- 完整備份 (Full Backup)

是將所有檔案資料完整備份的一種方式，通常是在備份周期中，每次皆完整複製周期時間點上的所有資料。這種備份的優點是當發生資料遺失的災難時，可以迅速恢復遺失的資料。缺點則是每個周期都對整個系統進行完整的備份，造成備份時間較長外，還會產生大量重覆備份的資料。資料完整備份的方式，不利於業務繁忙或備份時間有限的組織。

- 遞增備份 (Incremental Backup)

初次備份時，須進行一次完整備份。之後的備份僅對前一次備份的遞增差異資料進行備份，也就是將上次備份到此次備份期間，所有更改過的資料備份而已。遞增備份的優點是可以有效的節省重覆備份相同資料所花費的時間與備份儲存媒體的空間；缺點則是當災難發生時，資料的復原比較複雜，資料備份的可靠性也較差。

- 差異性備份 (Differential Backup)

初次備份時，須進行一次完整備份，之後的備份再將當時所有與原備份不同的資料（新的或修改過的）備份到儲存媒體上。差異性備份避免了前述兩種備份的缺點的同時，又具有了其所有優點。首先，它無須每次都對系統做完整備份，因此備份作業所需的時間較短，並節省了儲存媒體的空間。其次，它的災難復原也較方便，一旦發生問題，只需使用完整備份和發生問題前一次的備份即可將資料復原。

組織應選用的資料備份的類型，決定於組織 BIA 所設定之 RTO 與 RPO。另外，一般而言對於業務繁忙、資料更新速度快之組織，不適合選用資料完整備份類型。遞增備份因為復原時間所需最長，亦不利於要求 RTO 時間短的組織。差異性備份類型則最常見於網路同步/非同步備份方式。在表格 9 中，就此 3 種基本資料備份類型，作一概要之比較。

表格 9 3 種資料備份類型比較表

備份類型	備份頻率	備份所需時間	復原所需時間	每次備份資料量	資料損失時間 (RPO)	資料可靠性
完整備份	最少	最長	最短	最多	最多	最佳
遞增備份	最多	最短	最長	最少	最少	最差
差異性備份	少	短	短	少	少	佳

資料來源：本研究整理

## 2. 異地資料備份方式

主機房和異地備援機房之間的資料備份時，一般使用網路傳輸或是離線傳遞。網路傳輸又可分為「同步寫入（複製）」及「非同步寫入（複製）」。不論哪一種異地資料備份方式都可以保護資料，差別在於資料備份時所需的網路頻寬（成本），復原資料所需要花的時間（RTO），以及資料可以回復到哪一個時間點（RPO）。一般而言，異地資料備份方式分為三種基本方式：

- 網路同步寫入

網路同步寫入（同步複製技術）是指以遠距離資料備份軟體，將主機房儲存設施內的資料以完全同步的方式透過網路傳輸複製到異地備援機房的儲存設施中。其每一筆主機房內資訊系統的資料 Input/Output 作業，均必須等待遠距的備援機房的儲存設施複製完成確認訊息，方予以釋放。網路同步寫入因為網路傳輸資料頻繁、資料量大，對於資料備份的網路距離與所需要的網路頻寬皆有所限制，成本相對較高。優點則在於災難復原時間（RTO）最短，以及資料回復時間點（RPO）最短。一般而言，網路同步寫入方式應用於 Active-Active 的雙相互備援的機房，或者是資料時間差異（RPO）要求在最小的 Active-Standby 的異地備援機房架構中。

- 網路非同步寫入

網路非同步寫入（非同步複製技術）是指以遠距離資料備份軟體，將主機房儲存設施內的資料以非同步的方式透過網路傳輸複製到異地備援機房的儲存設施中。遠距離的資料複製是主機房

內的儲存設施以背景同步的方式進行的，這使主機房系統的性能遭受到的影響較小，傳輸距離較長（可達 1,000 公里以上），對於網路寬頻要求較小，成本相對較低。但相對於網路同步寫入而言，其缺點在於災難復原時間（RTO）需要較長時間，以及資料回復時間點（RPO）也需要較長時間。一般而言，網路非同步寫入方式應用於 Active-Standby 的異地備援機房架構中。

- 離線備份

離線備份通常是主機已經關機，或者服務在未執行的狀態下，進行主機房的資訊系統或儲存設施中資料的備份作業。之後再將備份的資料以網路或是交通方式，將備份資料傳遞至異地備援機房儲存設施或是資料異地儲存地點。通常離線備份會採用資料完整備份方式進行，其優點在於備份資料可靠性最佳，資料備份成本最低。缺點在於資料回復時間差異（RPO）最長，災難復原時間（RTO）也最長。一般而言，離線備份方式應用於 Active-Standby 的異地備援機房架構，或是單純的資料異地儲存地點（無資訊備援系統）。

不同的資料備份方式，其對於災難復原時間（RTO）、資料復原時間點（RPO）、及網路頻寬需求的關係皆有所不同。若要求越短的復原時間（RTO）與越密集的資料復原點（RPO），其建置/維護的成本就越高，而且是呈等比級數成長。表格 10 就以此三種常見之資料備份方式，對於復原時間（RTO）、資料復原點（RPO）與網路頻寬需求的關係整理參考：

表格 10 備份方式比較表

備份方式	網路同步寫入	網路非同步寫入	離線備份
復原時間 (RTO)	最小	中	最大
資料損失時間 (RPO)	最小	中	最大
主/備機房距離限制	Yes	No	No
適用資訊系統備援方式	Active-Active 或 Active-Standby	Active-Standby	Active-Standby 或 無資訊備援系統
網路頻寬需求	最高	低	最低
備註		資料差異時間越小，頻寬需求越大	

資料來源：本研究整理

### 3. 系統備援方式

異地備援系統是指在相隔較遠的異地，建立兩套或多套功能相同的資訊系統，當主機房因意外（如火災、地震等）停止運作時，其整個資訊應用系統可以切換到備援機房，使得原資訊系統的功能可以復原繼續運作。異地備援技術是系統高可用性技術的一個組成部分，強調處理外界環境對系統的影響，特別是災難性事件對整個資訊技術節點的影響，提供節點級別的系統恢復功能。參照國際標準 SHARE 78 定義的七個系統災難復原層次，本研究根據異地備援資料的多寡、異地備援災難復原時間 (RTO)、異地備份資料復原時的差異程度 (RPO)，以及災難復原環境的完備程度，將異地災難備援機房從高到低劃分為以下四個等級：

- 鏡像站 (Mirror Site)

鏡像站在所有方面的營運條件都與主機房完全相同，資訊和資料也與主機房同步。鏡像站也是熱備援站的進階備援等級，對資料提供最高級別的保護，並增加了自動化的功能。熱備援站對應於 1992 年國際標準 SHARE 78 災難備份技術的復原層次，是屬第 7 層次的定義。以備援機房的 4 個等級來說，鏡像站的成本是最高的，但一旦災難發生時，組織決定將資訊服務切換到備援機房，備援機房的資訊備援系統會自動接管業務，並將業務在最短的時間內復原。

- A. 適用條件：

- RPO  $\approx$  0 hr，沒有或基本沒有資料時間差異。
    - RTO  $<$  1 hr，災難復原時間在 1 個小時以內。

- B. 技術方案：

- 自建異地備援機房，租賃第三方機房，或與第三方合建機房。
    - 最高級別的 ITDR。
    - 自動監測資訊應用系統運作狀態。
    - 自動完成資訊應用系統和服務的切換。

- 熱備援站 (Hot Site)

熱備援站是所有災難復原所需的設施皆已完備，包括人員工作空間、資料儲存設備、及相關資訊系統皆一應俱全，備份資料也是最新的。熱備援站內的資訊設備與系統軟體，必須保證在還

原時與主機房的備份過來之資料完全相容，且熱備援站內的設備皆處於必要的工作狀態下。熱備援站對應於 1992 年國際標準 SHARE 78 災難備份技術的復原層次，是屬第 5 和第 6 層次的定義。熱備援站的成本較暖備援站及冷備援站為昂貴，但一旦災難發生時，BCP 團隊只需直接進駐即可開始作業，而不會有額外的時間拖延。

A. 適用條件：

- RPO  $\approx$  0 hr ，沒有或基本沒有資料時間差異。
- RTO  $\leq$  8 hr ，災難復原時間在 8 個小時以內。

B. 技術方案：

- 自建異地備援機房，租賃第三方機房，或與第三方合建機房。
  - 資料最高級別的保護，沒有或基本沒有資料遺失。
  - 採網路同步傳輸（近距離）或網路非同步傳輸（遠距離）鏡像技術備份資料。
  - 災難復原時根據預先定義的復原程序，進行手動復原作業。
- 暖備援站（Warm Site）

暖備援站除了機房既有之基礎設施外，只配備部份的資訊設備，但並不一定是對應主機房的資訊系統。暖備援站通常是配備基本的資訊設備，通常是備用設備，或是租賃的主機空間。當災難發生需要進行異地復原時，才開始進行資訊系統重新建置

(Restore) 與資料復原。暖備援站實際就是熱備援站的部份配備，只是配備的設備是備用設備或租賃的主機空間。暖備援站對應於 1992 年國際標準 SHARE 78 災難備份技術的復原層次，是屬第 3 和第 4 層次的定義。暖備援站的成本較鏡像站及熱備援站為便宜，但其缺點在於復原資訊系統的時間無法完全掌握。

A. 適用條件：

- RPO  $\leq$  24hr，允許資料差異時間在 1 天以內。
- RTO  $\leq$  24hr，災難復原時間在 1 天以內。

B. 技術方案：

- 自建異地備援機房，租賃第三方機房，或與第三方合建機房。
  - 一天內進行多次資料備份，備份資料透過網路非同步傳輸到備援機房。
  - 制定備份策略，利用資料備份軟體和工具進行備份作業。
  - 災難復原時根據預先定義的復原程序，進行手動復原作業。
- 冷備援站 (Cold Site)

冷備援站僅需配備資訊系統必要的基礎設施，例如：電力、不斷電系統、水、空調、線路管道…等。資料備份係以離線備份方式進行，但未配置資訊系統設備或其它服務。對應至 1992 年國際標準 SHARE 78 災難備份技術的第 1 和第 2 層次定義，是屬最基本的資料備份解決方案。相較其它等級之成本，冷備援站的成本

最低，但一旦需啟動這個站點做為災難復原的功能，其需要的時間也為最長。

A. 適用條件：

- RPO > 24hr ，允許資料差異時間超過 1 天。
- RTO > 24hr ，災難復原時間在超過 1 天。

B. 技術方案：

- 不需要自己建立異地備援機房（採租賃或第三方合作機房）。
- 把資料的備份媒體運輸到保存地點。

表格 11 異地備援架構等級條件評估表

	第四級	第三級	第二級	第一級
異地備援架構	鏡像站 (Mirror Site)	熱備援站 (Hot Site)	暖備援站 (Warm Site)	冷備援站 (Cold Site)
營運復原時間 (RTO)	極短	短	長	最長
資訊資料回復點 (RPO)	極短	短	長	最長
資料備份類型	差異性備份	差異性備份	差異性備份	完整備份
資料備份方式	網路同步寫入	網路非同步寫入	網路非同步寫入	離線備份
聯外網路線路	N+1	N+1	1	1
網路服務供應商 (ISP)	N+1	N+1	1	1
網路設備	N+1	N+1	1	1

資料來源：本研究整理

- 發生災難時，採用資料中心外包或使用第三方機房復原資料和資訊系統。

四種備援機房依 RPO、RTO、資料備份類型、資料備份方式、聯外網路、網路服務供應商、網路設備等條件，整理比較如表格 11 所示。

## （四）網路配置

網路通訊無論在日常運作、資料異地備份以及緊急災害復原流程中，皆扮演最為重要的角色。因此組織在建立機房或 DR Site 網路設備時，宜進行周全的考量，以確保重要時刻網路連線的暢通。參考 NIST SP 800-34 內容，主要包含（但不限於）以下幾項考量。

### 1. 網路流量

在成本與資源的考量下，組織應評估資訊系統日常運作的網路流量，以及與備援線路和 DR Site 可提供的頻寬落差。

- 頻寬需求：組織宜估算資訊系統日常運作的網路流量與所需頻寬，進而規劃備援線路或 DR Site 需準備的頻寬上限。這部分可能受到成本與資源的限制，但也會影響到災後第一時間復原的營運水準（請參閱本指引 4.2.3 營運復原水準）。
- 建物可用頻寬：機房所在建物若屬於組織專有，則在網路頻寬的規劃上將較有彈性。但若非專有或需與其他位於同建物內的單位分享，宜需進一步評估組織可使用的頻寬上限，以估算災害復原時，因建物可用頻寬而影響的系統服務。

## 2. 備援線路

無論是主機房或 DR Site，宜考量建立網路的備援線路，及採用同類型（例如：T-1）或足夠支應所需頻寬之線路，此部分除了建物內之線路外，也包含建物外連接之線路，以維持穩定的連線服務。

## 3. 備援設備

為確保災害發生時的網路連線，組織宜考量相關網路設備（例如：防火牆、路由器、交換器…等）之備援機制，並朝相同或相容的方向思考，以確保緊急切換時的順暢無虞。

## 4. 備援 ISP

為提高網路連線的穩定，組織在建立網路線路與設備的備援時，宜同時考量選擇不同 ISP 業者的服務。以確保在災害發生時，有兩組以上線路及電信機房可供連線，使 DRP 執行得以順利。

除上述幾點的考量外，組織宜在成本的估量下評估建立專線的可能性，以及與其他管線的區隔。使得在災害發生時，能夠讓資訊系統即時恢復網路連線，提供一定程度的服務水準。

## （五）建置環境

建置環境主要評估的就是機房所在的建物設施配置。由於機房的建置是資訊系統營運的重要基礎，無論是主機房或 DR Site 的所在建物，除了必須遵循政府建築、消防相關法規法令外，仍須考量支援設施包含電力、

空調、環境監控等配置，以確保資訊系統的正常運作。至於在機房能源使用效率的管控上，組織仍宜就目前機房能源使用的監控及管理機制進行評估，考量可行的方式達到降低與管控能源耗用。本節參閱 ISO/IEC 24762:2008，建置環境包含（但不限於）以下幾項考量。

## 1. 電力供給

資訊系統的運作仰賴持續且穩定的電力供應，電源的中斷或損害可能造成重要資料的遺失或影響 DRP 的運作。電力的供應主要來自市電以及發電機系統、不斷電系統（UPS）等兩類備用電源，其應考量：

- 市電：在市電來源的考量上，除了評估所在地區電源供應的充足、可靠、安全及品質外，亦可考量連結 2 個以上的變電所，以求市電來源的穩定。
- 不斷電系統（UPS）：UPS 系統的配置宜考量提供足夠負載容量，讓組織在市電失效時，在無切換時間下支持關鍵網路、系統的操作，並支撐至發電機啟動供電或人員到場關機。宜評估 UPS 系統失效造成的風險，考量備援機組的必要性。此外，UPS 系統應定期進行維護、測試或更換。
- 發電機系統：為避免市電中斷時間超過 UPS 電池系統的負載容量，組織宜考量配置發電機系統的需求，以滿足系統運作的容量要求，以及安全、可靠與品質的電力來源。發電機系統安置宜考量不會對機房（或 DR Site）運作造成干擾、危險、違反安全或有風險（例如：噪音、火災、爆炸或破壞）的位置。若安置於地下室，宜考量淹水與通風的因素。如配置於高樓層，則需評估地板承重和遮蔽的問題。至於室外置放，則需評估遭受破壞等相關可能風

險。此外，燃料的存放、庫存量及輸送管路的規劃亦需納入考量。為確保發電機系統的正常運轉，需定期進行啟動和運轉測試，運轉測試宜維持一定的時間，並考量執行關閉市電的實際演練。

另外，組織應建立程序和安裝必要的設施（例如：接地），保護資訊設備不受電壓不穩、雷擊或其他意外情形造成的損害。而在市電失效時，可藉由安全、不影響運作的切換至備用電源之方式，並提供相關人員提醒、監控的機制，以及緊急斷電開關裝置。至於電源線路的佈建，宜與網路線路適度隔離，避免可能的干擾或損壞，並定期查檢，降低可能的意外風險。

## 2. 空調配置

為確保資訊設備能穩定持續的運作，空調設備是相當重要的考量之一，其設計、配置、監控與配置宜有完整的規劃，以符合日常運作與 DRP 執行的各項所需。參考各國的作法，包含（但不限於）以下幾項考量：

- 備援機組：通常機房為 7x24 小時的運作，在保持穩定溫、濕度環境的需求下，除了配置足夠的空調數量外，另宜考量備援機組的規劃，作為定期輪替切換及緊急支援的需要，使資訊設備運作不至受到影響。
- 冷卻方式備援：除配置備援機組的考量外，為避免遭受相同風險的限制，宜再評估冷卻方式之備援，例如：水冷、氣冷機制的交替、自然進氣的緊急應用…等，使機房溫度可維持在可接受的範圍內。

- 電力供應：組織宜評估備用電源的最大容量，考量將空調設備電源連接至 UPS 與發電機，使能在市電失效時，維持一定時間的空調設備運轉。
- 管線規劃：空調設備的管線宜有完善的規劃，避免與其他線路交雜，並評估與漏液偵測設備的關係位置。另外，例如水冷式空調宜考量水路管線的配置（水塔、水源及備用水源），氣冷式空調則宜評估冷媒、水管路的規劃，以避免影響空調設備的運轉。
- 運轉監控：組織宜將空調設備的運轉納入到機房監測系統的監控中（可參閱本指引 4.5.3 環境監測與告警），讓相關人員得以第一時間掌握異常狀態並及時因應。
- 定期保養：組織宜建立空調設備定期保養的機制，並包含相關設備（例如：水塔）、管線的維護，使其能持續運轉。
- 疫病傳染防止：組織宜考量疫病傳染的可能性與影響範圍，評估加裝必要之過濾設備，並定期清洗、消毒與更換，避免造成疫情危害擴大。

空調設備是支援機房穩定運作的重要一環，組織需審慎的評估與建置，並宜考量提升、維持空調機組運轉效能的可能措施，如近年常見的冷熱通道佈建趨勢。配合日常監控與定期保養，以確保機房日常營運與 DRP 執行。

### 3. 環境監測與告警

應該建立實體偵測和警報系統以偵測溫濕度、闖入、攻擊、水災和火災等，並提供早期告警。告警的類型至少可分為溫度、濕度、煙、

火、滲水及闖入等的威脅警報。除了通報相關人員外，最理想的狀態可考量將煙、火的警報連接到當地消防隊，闖入的警報可連接到保全或當地警察局。

偵測和警報系統應該配置合適的偵測和告警報設備，並採用以下方法之一實施：

- 集中式：所有偵測告警都連接到一個集中且 24 小時都有人員監控的設施上。
- 分散式：所有偵測設備都在就地運作與管理。
- 混合式：組合集中式和分散式的方法。例如管制區的環境監視採用集中式的設施，其他告警採用就地管理方式。

偵測和告警報設備裝設的範圍至少應涵蓋(但不限於)下列區域：

- Server 機房。
- 其他電腦室。
- 資料媒體歸檔區。
- 基礎設施機房（電力、空調、通信、網路、UPS 室、電池室、配線間…等等）。

#### 4. 建物安全

建築物本身的風險亦需納入 DR Site 的安全管控範圍，避免意外發生而影響服務的持續營運，因此包括機房所在樓層、建物結構、使用建材、鄰近建物、座落位置等皆須予以評估。

- 防災機制：建物本身需符合建築、消防等相關法規的要求，並評估可能災害（可參閱 4.6.1 天然災害）造成的威脅，以便及早規劃或補強必要的防護措施。另外，機房內之消防設備，除偵測機制外，宜另配置符合國家消防法規滅火藥劑之氣體滅火系統，以即時控制災情並避免設備損害擴大。
- 環境風險：組織宜評估建物所在環境、位置的可能風險，例如鄰近建築物的結構強度或危險設施（可參閱 4.6.2 工、商業災害）的災害影響，避免建物遭受損壞，甚而影響機房的運作。
- 共用單位：若機房所在建物非屬專用，甚至有其他組織進駐，則在評估建物安全時，宜將這類單位納入評估的範圍內，考量非自身因素造成機房運作受到影響的各種可能性。

## （六）地理位置

異地備援電腦機房所處的地理位置及其環境穩定性是很重要的。異地備援電腦機房所在的建築物及所需的公用設施，例如電力供應和通訊，都可能受地理位置先天的災害風險（例如：天然災害）或環境不穩定性因素（例如：工商業災害、社會安全事件、公用設施…等等）的影響，也可能危及人員的安全。另外交通系統的中斷，亦可能影響人員及設備到達/離開異地備援電腦機房的時效性。

異地備援電腦機房所處的地理位置及其環境穩定性，可能具有某些難以接受的脆弱點，這可能意謂即使經過設計或規劃的異地備援電腦機房將仍具有不可降低的殘餘風險。因此，在選擇異地備援電腦機房的地點時，應優先考慮以下潛在的威脅。

## 1. 天然災害

本國臺灣島位於西太平洋上，東岸為太平洋，西岸隔臺灣海峽與中國大陸相望。南濱巴士海峽，北接東中國海。全島面積為 36,188 平方公里，南北長約 394 公里，南北狹長，東西窄。地勢東高西低，地形主要以山地、丘陵、盆地、台地、平原為主體。山地、丘陵約佔全島總面積的三分之二。地殼被擠壓抬升而形成的山脈，南北縱貫全臺，其中以中央山脈為主體，地勢高峻陡峭。另臺灣位處環太平洋地震帶上，地震發生頻繁，一旦發生地震，全島常常處於有感範圍內。在天氣特性方面，臺灣地理位置位在熱帶氣旋活躍的地區，每年幾乎都有颱風侵襲，氣象局平均一年發布 4~5 個颱風警報，因此颱風也是臺灣每年災害損失最嚴重的天然災害之一。

異地備援電腦機房不應該位於有天然災害風險的區域，或至少應該對風險進行評估、降低或接受。臺灣本島的天然災害包括（但不限於）以下幾項：

- 火山和地震

臺灣現有的火山，除龜山島為唯一活火山，以及近幾年學者觀察研究已可能由休火山變成活火山的大屯火山群外，其餘火山皆為休火山或死火山。另臺灣位處環太平洋地震帶上，地震發生頻繁，一旦發生地震，全島常常處於有感範圍內。

臺灣地震斷層帶影響範圍遍及全島，因此在選擇異地備援機房地點時，應進行風險評估，並納入臺灣地質及地震帶等資料。地點應選擇遠離地震斷層帶之位置，並以達到主機房及異地備援機房（含周邊公用設施）不致同時毀損為目標。



資料來源：經濟部中央地質調查所

圖 13 臺灣活動斷層分佈圖

- 颱風、龍捲風

臺灣地理位置位在熱帶氣旋活躍的地區，每年幾乎都有颱風侵襲，氣象局平均一年發布 4~5 個颱風警報，因此颱風也是臺灣每年災害損失最嚴重的天然災害之一。

另根據氣象資料統計顯示，臺灣的陸龍捲平均每年出現 1 至 2 次，水龍捲則較為少見。臺灣出現的龍捲風強度雖不及美國強烈，但其造成之災害，亦甚可觀。龍捲風發生地點北從桃園，南至屏東平原，東部的花蓮、臺東以及澎湖等地區均有所見，但主

要集中在臺南市、高雄市及屏東縣市的平坦地帶（資料來源：氣象局網站）。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入臺灣天氣及颱風歷史等資料，地點應選擇高於海平面之位置，並以達到主機房及異地備援機房（含周邊公用設施）不致同時毀損為目標。

- 海嘯

海嘯依來源可分為遠洋與近海，臺灣的遠洋海嘯來自太平洋，但因臺灣東部海岸地形陡峭，海底深達數千公尺，從太平洋傳來的波浪受到阻擋易折射出海，不易沿海岸上溯，對臺灣影響較小。但是在陸地邊緣的近海區域產生的海嘯，則須提高警覺，尤其若地震引發海底山崩，將對沿海區域造成更大災害（資料來源：科學人雜誌 2005）。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入臺灣周邊海域水文及地震等資料，地點應選擇高於海平面之位置，並以遠離海岸線之處所為佳。

- 洪水、土石流

臺灣為多山島嶼，約四分之三地區屬於山坡地，地勢陡峻、地質破碎、河短流急。不良的地質條件，加上颱風豪雨頻仍以及不時發生的地震，十分容易引發沖蝕與山崩，致生土石災害。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入臺灣地質及天候等資料，地點應選擇遠離山坡地與土石流好發區域之位置。

- 雷電

雷雨是空氣在極端不穩定狀況下，所產生的劇烈天氣現象，它常挾帶強風、暴雨、閃電、雷擊，甚至伴隨有冰雹或龍捲風出現，因此往往可造成災害。根據科學家的估計，在一場大雷雨中，所放出的能量，遠比一顆原子彈所產生的能量還高，此即為雷雨時，時有雷擊事故發生的原因（資料來源：氣象局網站）。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入臺灣天候等資料，於異地備援電腦機房建築物裝設避雷設施。

## 2. 工、商業災害

環境穩定性對異地備援電腦機房是很重要的，異地備援電腦機房所需的公用設施，如電力供應和通信，皆可能受環境不穩定的影響，人員的安全和福利也可能因不安全的外部環境而受到限制。因此，在選擇異地備援電腦機房的地點時，應先考慮的工、商業災害潛在的威脅包含（但不限於）以下幾項：

- 核電廠的安全

參考 1986 年車諾比核電廠核災與 2011 年日本福島第一核電廠的核災經驗，核電廠核災事件一旦發生，影響非常嚴重。核災發生所疏散或封鎖的區域達半徑 20~30 公里(美國標準 80 公里)。臺灣本島南北長 394 公里，北端有核一、核二電廠，南端有核三電廠，若以美國核災疏散/封鎖的 80 公里標準而言，臺灣約有一半的陸地在核電廠的核災警戒範圍內。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入臺灣核電廠位置等資料。地點應選擇遠離核電廠核災警戒範圍區域之位置，至少應達到主機房及異地備援機房（含周邊公用設施）不在同一核電廠核災警戒範圍為目標。

- 靠近處理化學製品或易爆材料的設施

處理化學製品或易爆材料的廠區（例如：煉油廠、化學製品工廠、軍方彈藥庫、彈藥製造工廠…等），屬於工安高風險區域。一旦發生工安災變，除容易波及異地備援電腦機房建築物外，異地備援電腦機房所需之公用設施及交通皆可能受到影響。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入區域內工商業廠區等資料。地點應選擇遠離處理化學製品或易爆材料的設施之位置，並確認供應異地備援電腦機房之公用設施及交通，不受區域內之處理化學製品或易爆材料的廠區發生工安災變之影響。

- 機場飛航航道的直接下方

根據飛航專家指出，飛機起降次數與失事率成正比。也就是說，飛機起降時是發生空難最大的風險，所以起降次數越多，發生空難的機率越大（資料來源：立法院公報第 91 卷第 39 期院會紀錄）。如果異地備援電腦機房處於機場飛航航道的直接下方，異地備援電腦機房建築物受空難事件影響之風險相對也較高，連帶異地備援電腦機房所需之公用設施及交通亦可能受到影響。

因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入區域內機場飛航航道等資料。地點應選擇遠離機場飛航路

線的直接下方之位置，並確認供應異地備援電腦機房之公用設施及交通，亦不在機場飛航航道的直接下方。

- 靠近繁忙的醫院

靠近繁忙的醫院，特別是應對某些特定的災害（例如：法定傳染病處理醫院），可能導致區域管制或交通壅塞。因此，在選擇異地備援電腦機房地點時，應進行風險評估，並納入區域內醫療機構等資料，地點應選擇遠離繁忙的醫院之位置。

- 社會安全之考量

異地備援電腦機房地點應遠離造成社會安全因素（罷工、示威、遊行、暴動、暴力犯罪、恐怖攻擊等等）的區域。尤其可能成為公眾示威或其他威脅目標的建築物或地點。

### 3. 交通便利因素

異地備援電腦機房地點位於交通便利的區域（可到達性），可以讓組織的人員和設備順利的遷入異地備援電腦機房，而不會有所延誤（滿足異地備援電腦機房實施 DR 計畫恢復時間要求的條件下）。交通便利（可到達性）可透過以下因素進行評估：

- 良好空中交通（如從國際到國內之機場）。
- 高鐵、鐵路交通。
- 完善的公路系統。
- 不同交通系統間的連接性。
- 主機房到異地備援電腦機房兩種以上不同的交通方式（如鐵路、

公路、航空、航海)及路線的規劃。

- 主機房到異地備援電腦機房的交通替代路線。
- 人員住宿地點到異地備援電腦機房的交通便利性。

#### 4. 公用設施的影響

異地備援電腦機房的地點不應該位於公用或其他設施的附近，因為可能受到公用設施運行的影響產生震動、干擾或破壞。這些公用設施包括（但不限於）以下幾項：

- 發/變電廠。
- 無線通信發射塔（例如：行動電話基地台）。
- 地下或地面鐵路。

#### 5. 與主機房地理距離

在可滿足組織員工在到達異地備援電腦機房實施 DR 計畫恢復時間的要求，以及異地備援電腦機房不與主機房受同一災難/失效影響的地理位置的條件下，異地備援電腦機房的地理位置與主機房的地理位置之間應該盡可能遠離，可參考 2003 年行政院國家資通安全會報之建議，主機房與異地備援機房之距離應距離 30 公里以上。

### (七) 支援作業

支援作業意指除了本指引 4.1~4.6 以外，其他 DRP 有關而有助於災害復原運作的項目，組織宜評估各種可加強營運持續作業，減少災害損失的

支援項目。其包含（但不限於）以下幾項考量。

## 1. 教育訓練

無論是對日常運作或災害復原，教育訓練對組織業務持續營運的重要性不可言喻。在上述章節中多少都有提及人員技能的培訓，而教育訓練的考量主要有以下幾項：

- 訓練課程：組織負責人應支持教育訓練的推動，由專責主管指派負責人員規劃相關人員應接受的專業課程項目。包括資訊系統運作相關技能（例如：作業系統、資料庫、防火牆…等）、專業證照（例如：ISO 27001 LA、BS 10012 LA…等）、營運持續與演練、設備維護（例如：空調、水電…等）或政府及主管機關要求（例如：消防設備師）…等。
- 訓練對象：組織負責人、高階及專責主管、DRP 相關人員、單位、廠商及一般人員皆宜配合接受課程訓練或提出符合的受訓證明，以確保人員具備必要的知識和技能。
- 訓練週期與時數：組織宜規劃各類教育訓練的週期和時數，並參考政府及主管機關的要求。

## 2. DR 專用區

異地備援電腦機房處所應該規劃 DR 專用區，並制訂在 DR 期間存放設備和使用所需的專用區域/房間的規定。在平常運作時間，DR 專用區不應該分配給其他用途。DR 專用區應包括以下用途之區域：

- 集合作業區

合適的集合作業區與公共廣播系統，使得組織能夠集合復原工作員工並進行概要簡報。集合作業區可能是開放的區域、大廳或是會議室，並能夠：

- A. 容納預先規劃的，來自不同復原小組的大量復原人員。
- B. 能在各種天氣氣候下運行和讓人感到舒適的。
- C. 滿足組織的保密性，使該區域的簡報和交談不會被相鄰的區域所聽到。

- 設備裝卸區

異地備援電腦機房處所應該設置 DR 期間所專用的電腦以及相關 DR 設備裝卸和檢查的區域。

設備裝卸區應該建立管理設備裝卸與移動的方針或是程序，包括在使用設備裝卸區時，專責人員到場監控、處理違規和意外的程序。

- 設備測試過渡區

異地備援電腦機房處所應該設置設備測試過渡區，並配置合適的電源以用於測試電腦和相關設備。設備測試過渡區的電源應該與復原設施的其他部份相隔開，以防止在設備測試中的意外“失誤”影響到復原設施其他部份的電力供應。如果在設備測試過渡區進行網路測試，亦應考慮網路的區隔。

設備裝卸區應該建立管理設備測試與移動的方針或是程序。包括在必要時，應指定專責人員到場監控、處理違規和意外的程序。

- 設備存放區

應該制訂使組織能夠將電腦及相關設備放到安全環境的規定，以防止未經授權的實體存取、改變或移除。

### 3. 緊急應變中心 (Emergency Operation Center, EOC)

異地備援電腦機房處所應該設置緊急應變中心 (EOC)，並配備合適的設備。以使組織進行 DR 作業時，能夠管理和維持與其業務部門及外部各方的溝通。

- 設備和供應

EOC 中應該於平時即備妥基本辦公設備與文具，使得組織能夠在 DR 啟動時，可立即在 EOC 中運作。這些設備與供應：

- A. 通信設備，如電話專線、電話機和傳真機…等。
- B. 辦公設備，如 PC、印表機、影印機…等。
- C. 辦公必需文具，如筆、筆記本、訂書針/機、膠水、膠帶、手電筒、影印紙…等。

- 專用的實體設備/設施

EOC 應該確保具備專用的實體設備/設施。包括：

- A. 語音通訊室：設置專用的通訊室以方便電話交談，並應該配備適當數量的專用電話、配備接收外界即時新聞訊息的設備（例如：電視機、收音機…等），以及不受其他噪音干擾。
- B. 會議室：設置專用的會議室，以供 DR 期間的會議使用。這

些會議室應該有足夠的空間可容納最多可能的組織員工（如復原小組主管），並配備白或黑板、投影機、DR 進度看板、以及接收外界即時新聞訊息的設備（例如電視機、收音機…等）。

C. 媒體聯絡區/室：設置專用的媒體聯絡區/室以方便與媒體溝通。媒體聯絡區/室應位於遠離 EOC 及電腦機房的隔離區域（如異地備援電腦機房建築物外的區域），以防止媒體未經授權進入 DR 場所、接觸訪問員工或存取機密資訊。媒體聯絡區/室仍應進行門禁管制，只有被邀請的媒體或訪客可以進入。媒體聯絡區/室應考量足夠空間供媒體人員作業，並亦應設置合適的設備（例如麥克風擴音設備、桌椅…等）。

D. 復原小組的工作室：規劃提供各不同業務復原工作小組的工作室或區域，並配備辦公所需的設備/設施，如辦公傢俱、電話、傳真機、列/影印機、文具等。另在不同業務復原工作小組的工作室或區域，亦備妥紙本的業務手冊、DR 計畫、各項設施設備操作手冊，以及資訊系統/設施相關備份軟體（例如系統安裝軟體、操作控制軟體…等等），並應予以隨時更新。

#### 4. 人員管理

- 人員安全分類

應將與異地備援電腦機房相關之人員，依安全需求建立人員的分類，例如：

- A. 提供異地備援電腦機房服務方的人員。
- B. 組織的員工。
- C. 廠商。
- D. 訪客。

- 管制區域

應該將異地備援電腦機房所處的建築物建立實體隔離的安全區域。基於人員安全的分類，建立每一管制區域人員進出的正式管制系統，並且進行 7\*24 的管控。管制區域分類例如：

- A. 管制區域：關鍵設備和維運的區域/房間，例如 Server 或其他電腦設備、通信交換機、電力、UPS、發電機、空調、其它相關設備、佈線、資料儲存媒介…等。
- B. 一般區域：所有人員皆可使用的區域/房間，且沒有任何內部安全管制，例如接待區、餐廳、茶水間、洗手間…等。

- 門禁控制

應建立異地備援電腦機房所處的建築物，及管制區域的正式門禁管理的策略與程序，以確保只能在專用通道進出，並在出入口處識別與驗證所有人員與設備。

- 員工以外的人員

建立員工以外的人員進入異地備援電腦機房所處的建築物活動的正式策略與程序，以確保：

- A. 進入異地備援電腦機房所處的建築物和存取設施的請求得

到預先的確定與安排。例如：透過電子郵件、會議或是事前的申請文件。

B. 配合安全人員的確認與檢查。

C. 發放外部人員識別證。

D. 專責人員接待與管制區域員工全程陪同。

E. 對於進入管制區域進行維護的廠商進行全程監視，並防止其進入允許進入區域以外的區域，或碰觸其他未經授權的設備/設施。

F. 門禁管制登記（內容包括外部人員姓名/身份/組織、進入的目的、接待人員、進入/離開時間、相關人員的簽署…等）。

- 在管制區的人員行為

應建立人員在管制區域內行為的正式規定或指南，包括：

A. 禁止吸煙。

B. 禁止飲食。

C. 在敏感設備的區域/房間禁止使用無線射頻設備條款，例如：行動電話。

D. 使用行動儲存（如智慧型手機、USB 隨身硬碟）或照相設備的條件。

- 安全的職能與角色

異地備援電腦機房應該建立維護安全的職能與角色，包括：

A. 專責的實體安全的職能與角色。

B. 職務代理人的機制。

C. 適當的職前培訓與在職教育訓練。

D. 建立對安全的職能與角色的員工進行測試的程序，以確保維持其警覺性與對突發事件的反應能力。

- 授權

異地備援電腦機房處所和管制區的實體存取的授權，應該：

A. 基於執行業務所需要的最低資源存取權限為原則，進行授權。

B. 定期進行審查和更新。

## 5. 保險

組織制訂 DRP、建立 DR Site 的目的，在於將各種災害產生的風險降至最低。但無論在多麼完善的規劃，都沒辦法徹底避免災害的發生，亦即無論風險值控制到多低，仍有殘餘風險（Residual Risk）的存在。因此，組織宜針對災害發生後造成的損失，評估可接受的程度。

考量自身或要求相關人員、廠商投保各類保險的需求性，這些事後的補償可能給予組織得以更快的恢復到營運的狀態。投保的標的可包括實體資產（例如：建築、設備…等）、人員、服務或其他（例如：資訊安全…等）。投保的額度則可依據估算後的可能損失、合約規範或政府及主管機關要求，予以投保適當的水準，以取得更多一層的保障。

## 五、結論

營運持續管理在組織面對各項可能影響業務運作的風險上，一直是相當重要的決策規劃，而 DRP 的制訂與 DR Site 的建立，將可保障組織避免營運中斷，尤其是面對重大災害所導致的難以預期損害。事實上，研讀國外的研究與文獻，不難看出各國對於這類議題的重視。

國內對於 BCM 之觀念已相當成熟，多投入相當程度的資源以確保業務的營運持續。但無論是在規劃「異地備援機房」或「異地備援機制」時，常認為所謂的「異地」，只要是兩處不同之空間便足夠，而忽略了其中連動影響的可能風險。「異地」並非單就距離一項進行討論，在評估的過程中，應朝「不遭受同一風險或事件影響」的方向思考，才能達到電腦機房異地備援機制的真正目的。

本指引旨在建立可供國內各組織參閱的電腦機房異地備援機制評估準則，從第 1 章開始援引行政院已公告之參考指引、手冊，進而說明整個評估機制的操作流程，接著於第 2 章概述、分析國內外相關的標準和規範，作為建立評估準則的參考基礎。第 3 章則針對建立或維運異地備援機房應納入的各類評估準則，共分成八大項次予以清楚解說，組織可藉此檢視 DRP 與 DR Site 的完善程度，若是現在不具備異地備援機制的單位，仍可透過評估準則檢討備援作業的不足，並考量增強甚至建立 DR Site 的計畫。

為便於各組織進行各項準則的評估，可參閱「電腦機房異地備援機制操作手冊」，內容條列各評估準則的考量項目，並提供自評表，讓相關人員依據重要（關鍵）資訊系統安全等級，分析、比較建議要求和組織現況間的落差，進而識別現階段宜優先著手調整、改善之方向。

組織營運持續的能力在一般時期也許難以顯現，但當災難來臨之時，日常所積聚的能量，將能有效降低損失，確保業務的運作，甚至獲得更多的機會，領先其他的競爭對手。因此，如何建立一套可靠的 DRP，並在成本與資源的考量下，規劃滿足組織需求的 DR Site，將會左右組織營運持續的成效，進而影響後續的發展。透過本指引所建議的評估準則，可有助於組織自我檢視，在災害發生前防範未然，以提供更為穩定、持續的服務。

## 六、参考文献

- [1] ANSI/BICSI, ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices, 2011.
- [2] Amazon, Disaster Recovery as a Service, <http://aws.amazon.com/>
- [3] BSI, BS 25777 : 2008 Information and communications technology continuity management — Code of practice, 2008.
- [4] Communication and Information Technology Commission, Kingdom of Saudi Arabia, Guidelines on Disaster Recovery Planning for ICT Industry.
- [5] Dilley, Maxx. Natural disaster hotspots : A global risk analysis. Vol. 5. World Bank Publications, 2005.
- [6] Diefenbach, Thomas. "Are case studies more than sophisticated storytelling? : Methodological problems of qualitative empirical research mainly based on semi-structured interviews." *Quality & Quantity* 43.6 (2009): 875-894, 2009.
- [7] Data Center Council, Data Center Facility Standards, Japan.
- [8] ISO, ISO 22301 : 2012 Societal security -- Business continuity management systems --- Requirements, 2012.
- [9] ISO, ISO 22313 : 2012 Societal security -- Business continuity management systems - Guidance, 2012.
- [10] ISO/IEC, ISO/IEC 27001 : 2013 Information technology -- Security techniques -- Information security management systems - Requirements, 2013.
- [11] ISO/IEC, ISO/IEC 27002 : 2013 Information technology -- Security techniques -- Code of practice for information security controls, 2013.
- [12] ISO/IEC, ISO/IEC 27031 : 2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity, 2013.
- [13] ISO/IEC, ISO/IEC 24762 : 2008 Information technology -- Security techniques -- Guidelines for information and communications

- technology disaster recovery services, 2013.
- [14] InformationWeek, Cloud Computing's Tipping Point, Michael Biddick, 2011
  - [15] International Telecommunication Union, ITU-T L.1300 (11/2011) SERIES L: CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT – Best Practices for Green Data Centers, 2011.
  - [16] IBM, IBM System Storage Business Continuity: Part 1 Planning Guide.
  - [17] Maine State Government, Current Information Technology (I.T.) Environment, <http://www.maine.gov/>, 2013
  - [18] NIST, NIST Special Publication 800-34 Rev.1, Contingency Planning Guide for Federal Information Systems.
  - [19] OIG Audit Report No.13-09, Audit of NARA's Data Backup Operations, 2013.
  - [20] Telecommunication Technology Association, Korea, TTAS.KO-10.0259\_Guideline for Disaster Management of Information System.
  - [21] The Telecommunication Industry Association, TIA-942 Telecommunications Infrastructure Standard for Data Centers.
  - [22] Timothy Wood, Emmanuel Cecchet, K.K. Ramakrishnan, Prashant Sheony, Jacobus Van Der Merwe and Arun Venkataramanu, Disaster Recovery as a Cloud Service: Economic Benefit & Deployment Challenges, 2010.
  - [23] U. S. Department of Health & Human Services, HIPAA Security 101, <http://www.hhs.gov/>
  - [24] Shon Harris, CISSP All-in-One Exam Guide, 6th Edition, 2012.
  - [25] 2010 資通訊安全政策白皮書，行政院科技顧問組，2010 年。
  - [26] 行政院主計總處，電腦應用概況報告-民國 100 年，中華民國 101 年 10 月編印。
  - [27] 行政院研究發展考核委員會，100 年電子化政府報告書，2011 年。

- [28] 行政院研究發展考核委員會，資訊作業調整移轉應變作業參考指引，2011年。
- [29] 行政院研究發展考核委員會，行政院及所屬機關資訊安全管理規範，1999年。
- [30] 行政院國家資通安全會報，國家資通訊安全發展方案（102年至105年），中華民國102年12月25日核定。
- [31] 行政院國家資通安全會報，資訊系統分類分級與鑑別機制，2010年。
- [32] 行政院國家資通安全會報，建立我國通資訊基礎建設安全機制計畫，2004年核定通過，2007年核定修正。
- [33] 行政院及所屬委員會共構機房經營維運服務資訊網，<http://sdc.nat.gov.tw/>。
- [34] 立法院，立法院資訊系統異地備援中心簡介，曹志強，2006年。
- [35] 經濟部標準檢驗局，CNS 27001，資訊技術-安全技術-資訊安全-管理技術-要求事項。
- [36] 教育部，教育體系資通安全管理規範，2007年。
- [37] 臺中市政府，資料備份與回復管理程序 TC-ISMS-2-19，2013年。
- [38] 臺中市政府，災害復原作業程序 TC-ISMS-2-07，2012年。
- [39] 臺中市政府資訊中心第15期電子報，臺中市政府備份備援機制簡介，2013年。
- [40] 政府機關資訊通報第288期，中央研究院「集中化虛擬儲存設備建置暨異地備援」介紹，2011年。
- [41] 中央研究院，異地備援規劃報告，葉大業，2012年。
- [42] 資訊安全管理系統政策探微：根基-政府機關之異地備援個案，樊國禎、黃健誠、林樹國，2011年。
- [43] 非營利單位資訊災難備援機制建置之研究，謝昆霖、呂易儒，2006年。
- [44] 金融機構異地備援中心建置模式之研究，金真芳，2005年。
- [45] 企業建置異地備援之決策以金控集團旗下票券公司為例，蘇玉龍、畢純芝、詹文俊、許婕渝、張家豪，2010年。

- [46] 調查研究第 3 期，焦點團體法在調查研究上的應用，頁 51-74，周雅容，1997 年。
- [47] 資策會 FIND，2012 臺灣企業產業鏈資訊化情形及需求報告，蔡郁薇，2012 年。
- [48] 仁愛醫療財團法人資訊室，從資料異地備援看風險管理。
- [49] Tier 功能驗證，綠智網，2011 年。
- [50] 財金資訊季刊第 73 期，金融資訊系統邁向服務不中斷之路，葉清維、蔡佩珍，2013 年。

## 七、附件

附件 1 電腦機房異地備援機制操作手冊

附件 2 電腦機房異地備援機制中英文名詞對照表

附件 3 電腦機房異地備援相關規範

## 七、 附 件

## 【附件 1】

### 電腦機房異地備援機制操作手冊

102 年度

我國電腦機房異地備援機制委託研究計畫案

電腦機房異地備援機制操作手冊

(V1.0)

委託機關：行政院

執行單位：財團法人國家實驗研究院  
國家高速網路與計算中心

中華民國 103 年 03 月



## 目 次

一、前言.....	1
二、章節架構.....	1
三、使用說明.....	1
四、評估準則與資訊系統安全等級對照.....	2
(一) 一般原則.....	3
(二) 營運持續.....	6
(三) 系統架構.....	9
(四) 網路配置.....	11
(五) 建置環境.....	14
(六) 地理位置.....	17
(七) 支援作業.....	20
五、電腦機房異地備援機制評估準則自評表.....	29
六、自評表使用案例.....	50
(一) 組織背景與電腦機房異地備援機制概述.....	50
(二) 自評過程.....	50
(三) 改善建議.....	58

## 表 目 錄

表格 1 電腦機房異地備援機制評估準則與資訊系統安全等級對照表 ..	24
表格 2 電腦機房異地備援機制評估準則自評表 .....	32
表格 3 電腦機房異地備援機制評估準則自評表 (使用案例) .....	50



## 一、前言

「電腦機房異地備援機制操作手冊」(以下簡稱本手冊)旨在協助已參閱「電腦機房異地備援機制參考指引」(以下簡稱參考指引)之讀者，進一步針對組織現有異地備援機房 (DR Site) 之狀態，及災害復原計畫 (DRP) 準備程度，評估重要 (關鍵) 資訊系統所需之營運持續作法，並分析現況之差異。

## 二、章節架構

本手冊旨為引導讀者進行「電腦機房異地備援機制評估準則」之操作，透過評分工具的使用，判別出組織現行電腦機房異地備援機制的狀態，以作為後續強化改善的參考。共分為以下幾個章節：

- 第一章「前言」：說明編撰本手冊之目的。
- 第二章「章節架構」：說明本手冊之章節架構。
- 第三章「使用說明」：說明使用本手冊自評表格的方式與相關規則。
- 第四章「評估準則與資訊系統安全等級對照」：說明「電腦機房異地備援機制評估準則」及其對應之各資訊系統安全等級之建議要求。
- 第五章「電腦機房異地備援機制評估準則自評表」：說明自評表之使用規則和相關內容。
- 第六章「自評表使用案例」：介紹自評表使用案例，透過範例的方式說明自評表之使用過程。

## 三、使用說明

在使用本手冊提供之自評工具前，建議讀者應先閱讀參考指引，並依

循行政院「資訊系統分類分級與鑑別機制參考手冊」，或藉由已通過之 ISMS（資訊安全管理系統）驗證，或主管機關認可之驗證，或管理階層認可之管理機制（可參閱參考指引 1.4 使用建議），鑑別出重要（關鍵）資訊系統所屬之安全等級。

另外，因應部分組織營運持續之作為多限於資料備份作業，本手冊針對資訊系統安全等級「普」級部分，針對資料備份作業再區隔出「普」（等級 0）一類〔此類之影響構面考量與原「普」（等級 1）相同〕，最後形成出「普」（等級 0）、「普」（等級 1）、「中」（等級 2）、「高」（等級 3）等共四階層之資訊系統安全等級。

組織在識別各資訊系統之安全等級後，安全等級最高者即為「重要（關鍵）系統」，可參閱本手冊第 4~5 章內容，進行該系統或其他安全等級系統的評估與分析。

針對本手冊所條列之各項電腦機房異地備援機制評估準則及不同資訊系統安全等級的要求敘述，皆是研究團隊根據國際標準或各國規範文件彙整出的建議項目，組織可自行依據業務的特性與需求，增編評估準則與調整安全等級要求，以貼近實際的狀況，分析出完整的比較結果。另外，若是組織目前礙於現況尚未具備異地備援/備份，亦可藉參考指引與本手冊評估業務營運持續上的限制及資訊系統需求，再行後續的考量和規劃。

#### 四、評估準則與資訊系統安全等級對照

本章節主要針對「電腦機房異地備援機制評估準則」及各項對應之資訊系統安全等級進行說明，其中部分評估準則之不同安全等級實施建議敘述相同〔例如 3.1.1 資安稽核/自我檢視中（等級 2）與普（等級 1）〕，主要考量該等級宜落實程度的完整性，至於這類評估準則的自評操作方式，在第 4 章將再進行說明。

## (一) 一般原則

### 1. 資安稽核/自我檢視

在資安稽核/自我檢視部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜通過資訊安全與個資保護驗證或符合主管機關之要求。

例如資訊安全方面通過 ISO 27001:2013 或教育體系資通安全管理規範驗證，個資保護方面通過 BS 10012 驗證。

- 中（等級 2）：宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行 1 次個資保護自我檢視。

例如資訊安全方面通過 ISO 27001:2013 或教育體系資通安全管理規範驗證，個資保護方面則遵循個人資料保護法或主管機關規定，並定期自我檢視執行成效。

- 普（等級 1）：宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行 1 次個資保護自我檢視。

此部分與前一安全等級要求相同。

- 普（等級 0）：宜定期每年至少進行 1 次資訊安全和個資保護自我檢視。

例如資安方面遵循行政院或主管機關之規定，個資保護方面則遵循個人資料保護法或主管機關規定，並定期自我檢視執行成效。

## 2. 災害復原計畫 (DRP)

在災害復原計畫 (DRP) 部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高 (等級 3)：宜針對各項可能風險建立 DRP。

例如針對已識別出的各類可能風險，評估需因應之對策，彙整入 DRP 中。

- 中 (等級 2)：宜針對主要風險建立 DRP。

例如針對影響範圍較大或發生機率較高之可能風險，建立完整的 DRP。

- 普 (等級 1)：宜建立基本之 DRP。

例如參考指引手冊之說明，建立必要且可行的災害復原機制。

- 普 (等級 0)：宜評估 DRP 之建立。

例如針對異地備份機制評估可行的復原程序。

## 3. 管理階層支持

在管理階層支持部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高 (等級 3)：管理階層宜定期主持會議並給予重要支持。

例如資訊或資安主管固定主持資安管審會議，並對各項重要議題給予指示與支持，或同意相關經費的規劃。

- 中（等級 2）：管理階層宜定期主持會議並給予重要支持。

此部分與前一安全等級要求相同。

- 普（等級 1）：管理階層宜不定期主持會議並給予必要支持。

例如資訊或資安主管主持年度資安管審會議，並針對議題中的急迫項目，給予指示與支持。

- 普（等級 0）：管理階層宜給予適時的支持。

例如資訊或資安主管指派人員負責 DRP 的規劃與運作。

#### 4. 資源評估

在資源評估部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜評估資源與經費上的需求，並每年擬定預算及估算支出成本。

例如每年進行異地備援機制的經費規劃與提撥，並估算其支出成本，確保獲得可供持續營運的資源。

- 中（等級 2）：宜評估資源與經費上的需求，並規劃預算及估算支出成本。

例如評估異地備援機制的設備需求和營運成本，固定編列經費以支應其運作。

- 普（等級 1）：宜評估資源與經費上的需求，並規劃預算。

例如評估異地備援機制的設備需求，規劃往後年度的經費編列額

度。

- 普（等級 0）：宜評估資源與經費上的需求。

例如考量異地備份設備的使用年限，評估汰換規劃或經費需求。

## 5. 變更管理

在變更管理部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜評估與測試變更造成的影響，並持續監控。

例如評估及測試系統更換的影響，並規劃日常查檢機制進行確認。

- 中（等級 2）：宜評估與測試變更造成的影響，並定期監控。

例如評估及測試系統更換的影響，後續再透過演練再次檢視。

- 普（等級 1）：宜評估與測試變更造成的影響。

例如評估系統更換的影響，並規劃測試程序進行確認。

- 普（等級 0）：宜評估變更造成的影響。

例如評估系統更換對異地備份機制的可能影響。

## （二）營運持續

### 1. 資訊資料回復點

在資訊資料回復點部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：最近一代資訊資料容許在 0~1 小時。  
例如可恢復災害發生前半小時的資訊資料。
- 中（等級 2）：最近一代資訊資料容許在 0~1 小時。  
此部分與前一安全等級要求相同。
- 普（等級 1）：最近一代資訊資料容許在 1~24 小時。  
例如可恢復災害發生前 12 小時的資訊資料。
- 普（等級 0）：最近一代資訊資料容許>24 小時。  
例如可恢復災害發生前 30 小時的資訊資料。

## 2. 營運復原時間

在營運復原時間部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：營運復原容許時間在 0~1 小時。  
例如可在災害發生後半小時內恢復基本系統服務。
- 中（等級 2）：營運復原容許時間在 1~8 小時。  
例如可在災害發生後 4 小時內恢復基本系統服務。
- 普（等級 1）：營運復原容許時間在 8~24 小時。  
例如可在災害發生後 12 小時內恢復基本系統服務。
- 普（等級 0）：營運復原容許時間>24 小時。  
例如可在災害發生後 30 小時內恢復基本系統服務。

### 3. 營運復原水準

在營運復原水準部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：災後第一時間復原之營運水準容許在 80%~100%。

例如考量頻寬與系統上線狀態的限制，災後復原第一時間可提供日常營運 90%之水準狀態。

- 中（等級 2）：災後第一時間復原之營運水準容許在 60%~80%。

例如考量頻寬與系統上線狀態的限制，災後復原第一時間可提供日常營運 75%之水準狀態。

- 普（等級 1）：災後第一時間復原之營運水準容許<60%。

例如考量頻寬與系統上線狀態的限制，災後復原第一時間可提供日常營運 50%之水準狀態。

- 普（等級 0）：無要求。

### 4. BCP 演練

在 BCP 演練部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜定期執行完整異地備援機制的演練與測試。

例如每半年進行 1 次完整演練與異地備援系統上線測試，並檢討過程中可再改善之處。

- 中（等級 2）：宜定期執行完整異地備援機制的演練與測試。  
此部分與前一安全等級要求相同。
- 普（等級 1）：宜定期執行重要異地備援機制的演練與測試。  
例如每半年進行 1 次模擬演練與異地備援系統上線測試。
- 普（等級 0）：宜定期執行基本異地備份機制的演練與測試。  
例如每半年進行 1 次紙本演練，每年進行 1 次備份資料倒回測試。

### （三）系統架構

#### 1. 資料備份類型

在資料備份類型部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜使用完整備份與差異性備份。  
例如每週進行 1 次完整備份，每日夜間進行差異備份。
- 中（等級 2）：宜使用完整備份與差異性備份。  
此部分與前一安全等級要求相同。
- 普（等級 1）：宜使用完整備份與遞增備份。  
例如每週進行 1 次完整備份，每日夜間進行遞增備份。
- 普（等級 0）：宜至少使用完整備份。  
例如每週進行 1 次完整備份。

## 2. 異地資料備份方式

在異地資料備份方式部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜使用網路同步寫入。

例如異地備援機制之資料採取網路同步寫入方式。

- 中（等級 2）：宜使用網路同步寫入。

此部分與前一安全等級要求相同。

- 普（等級 1）：宜使用網路非同步寫入。

例如異地備援機制之資料採取每日 2 次網路非同步寫入方式。

- 普（等級 0）：宜至少使用離線備份。

例如異地備份機制之資料採取每週假日進行離線備份。

## 3. 系統備援方式

在系統備援方式部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜使用鏡像站。

例如異地備援機制之設備與主系統相同，且資料即時同步，當 DRP 啟動時，系統將自動切換。

- 中（等級 2）：宜使用熱備援站。

例如異地備援機制之設備與主系統相仿，備份資料為最新紀錄，當 DRP 啟動時，只要負責人員到場作業即可開始營運。

- 普（等級 1）：宜使用暖備援站。

例如異地備援機制之設備可支應主系統運作，備份資料為前一日紀錄，當 DRP 啟動時，預計可在 2 小時內上線服務。

- 普（等級 0）：宜使用冷備援站。

例如異地備份機制之設備僅可支應主系統基本運作，當 DRP 啟動時，預計隔天可上線服務。

#### （四）網路配置

##### 1. 網路流量

在網路流量部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜評估與建立完整異地備援網路頻寬。

例如建立至少一條以上與主機房相同之網路頻寬線路，供異地備援機制運作。

- 中（等級 2）：宜評估與建立足夠異地備援網路頻寬。

例如建立一條可供異地備援機制正常運作之網路頻寬線路。

- 普（等級 1）：宜評估與建立必要異地備援網路頻寬。

例如建立一條可供異地備援機制基本運作之網路頻寬線路。

- 普（等級 0）：宜評估與建立必要異地備份網路頻寬。

例如建立一條可供異地備份機制基本運作之網路頻寬線路。

## 2. 備援線路

在備援線路部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜建立完整異地備援線路（N+1），及考量專線的需求。

例如建立 2 路獨立網路線路供異地備援機制運作，另外兩地機房之連線包含 1 條專用線路。

- 中（等級 2）：宜建立必要異地備援線路（N+1）。

例如建立 2 路獨立網路線路供異地備援機制運作。

- 普（等級 1）：宜評估必要異地備援線路。

例如建立 1 路異地備援網路線路，並評估另一備援線路的需求。

- 普（等級 0）：無要求。

## 3. 備援設備

在備援設備部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜建立完整異地備援設備（N+1），及考量自動切換的需求。

例如建立 2 套可自動切換之異地備援網路設備。

- 中（等級 2）：宜建立完整異地備援設備（N+1）。

例如建立 2 套可透過手動方式切換之異地備援網路設備。

- 普（等級 1）：宜評估必要異地備援設備。

例如建立 1 套異地備援網路設備，並評估準備另一備援設備的可能性。

- 普（等級 0）：無要求。

#### 4. 備援 ISP

在備援 ISP 部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜取得備援 ISP 的服務（N+1）。

例如除專線外，再向 2 家以上不同線路之 ISP 業者承租網路服務。

- 中（等級 2）：宜取得備援 ISP 的服務（N+1）。

此部分與前一安全等級要求相同。

- 普（等級 1）：宜評估備援 ISP 的服務。

例如評估向 2 家以上不同線路之 ISP 業者承租網路服務的需求。

- 普（等級 0）：無要求。

## (五) 建置環境

### 1. 電力供給

在電力供給部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：除基本備用電源的配置外，宜考量市電、備用電源的備援機制（N+1）。

例如配置有備援 UPS 系統與發電機系統，每月定期維護保養，並半年進行演練測試。

- 中（等級 2）：宜具備 UPS 系統與發電機系統的配置。

例如配置有 1 組 UPS 系統與發電機系統，每季定期維護保養，並考量 UPS 系統備援的規劃。

- 普（等級 1）：宜具備 UPS 系統並考量發電機系統的配置。

例如配置有 1 組 UPS 系統，每季定期維護保養，並針對市電中斷的可能問題，已規劃發電機系統的評估與採購。

- 普（等級 0）：宜具備 UPS 系統的配置。

例如配置有 1 組 UPS 系統，每半年定期維護保養。

### 2. 空調配置

在空調配置部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜配置空調系統及備援機制（N+1），並考量空調效能的評估。

例如空調系統具備備援機制，提供 7x24 自動切換機制，並在機房溫度過高時，自動啟動備援機組支應，另透過冷熱通道配置提高空調系統效能。

- 中（等級 2）：宜配置空調系統及備援機制（N+1）。

例如空調系統具備備援機制，提供 7x24 自動切換機制。

- 普（等級 1）：宜配置空調系統，並考量備援機制的需求。

例如備援系統所在機房有配置空調系統，並已規劃其備援機組的預算。

- 普（等級 0）：宜考量空調系統的配置。

例如備份系統所在機房配有基本的空調系統。

### 3. 環境監測與告警

在環境監測與告警部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜建立完善的監測與告警系統，並建立處理程序。

例如環控系統 24 小時監測、紀錄機房溫濕度、空調、電力使用等狀態，異常時以簡訊通知相關人員，單位也已建立緊急反應處理的程序與權責。

- 中（等級 2）：宜建立完善的監測與告警系統，並建立處理程序。

此部分與前一安全等級要求相同。

- 普（等級 1）：宜建立必要之監測與告警系統。

例如人員每日透過環控系統監測機房溫濕度，門窗皆設有警報器，24 小時與保全連線。

- 普（等級 0）：宜考量必要之監測與告警機制的建立。

例如人員每日進機房紀錄溫濕感應器數據。

#### 4. 建物安全

在建物安全部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜符合政府法規要求，並考量機房相關防災機制，另降低建物風險。

例如除法規遵循與機房防護外，並已要求其他單位移出化學藥品。

- 中（等級 2）：宜符合政府法規要求，並考量機房相關防災機制，另評估建物風險。

例如除法規遵循與機房防護外，也針對建物內其他單位的業務特性或可能危害建物安全之風險進行評估。

- 普（等級 1）：宜符合政府法規要求，並考量機房相關防災機制。

例如機房配置有偵測設備與氣體滅火裝置。

- 普（等級 0）：宜符合政府法規要求。

例如機房所在建物定期檢修消防安全設備，符合政府消防法規要

求。

## (六) 地理位置

### 1. 天然災害

在天然災害部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高(等級3): 宜避免或降低與主機房遭受同類天然災害的可能性。

例如備援機制所在機房附近無斷層帶，且建物、機房設施的防震措施皆已加強。

- 中(等級2): 宜評估可能遭受的天然災害，並加強防護措施。

例如為避免颱風期間可能的水災影響，備援機制所在機房已加裝防水牆設施。

- 普(等級1): 宜評估可能遭受的天然災害。

例如瞭解機房附近地理環境，分析可能遭受的天災種類與程度。

- 普(等級0): 無要求。

### 2. 工、商業災害

在工、商業災害部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高(等級3): 宜避免或降低與主機房遭受同類工、商業災害的可能性。

例如備援機制所在機房離最近核電廠位置超過 100 公里。

- 中（等級 2）：宜評估可能遭受的工、商業災害，並加強防護措施。

例如機房所在附近道路常是遊行活動必經途徑，已評估加強警衛等進出入管控機制。

- 普（等級 1）：宜評估可能遭受的工、商業災害。

例如瞭解機房附近地理環境，分析可能遭受的工、商業災害種類與程度。

- 普（等級 0）：無要求。

### 3. 交通便利因素

在交通便利因素部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜考量交通便利狀況，規劃兩種以上交通方式。

例如當 DRP 啟動時，已規劃必要人員採取搭乘火車或自行開車方式於 1 小時內抵達異地備援機房。

- 中（等級 2）：宜考量交通便利狀況，規劃交通方式。

例如當 DRP 啟動時，已規劃必要人員採取自行開車方式於 1 小時內抵達異地備援機房。

- 普（等級 1）：宜評估交通便利狀況。

例如瞭解機房所在的交通運輸方式與狀況。

- 普（等級 0）：無要求。

#### 4. 公用設施的影響

在公用設施的影響部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜避免或降低與主機房遭受同類公用設施影響的可能性。

例如備援機制所在機房距離鐵路幹線達 10 公里，避免因火車經過產生的震動而有所影響。

- 中（等級 2）：宜評估可能遭受的公用設施影響，並加強防護措施。

例如備援機制所在機房附近設有多座高頻基地台，已定期請臺電檢測電磁波等影響。

- 普（等級 1）：宜評估可能遭受的公用設施影響。

例如解機房附近地理環境，分析可能遭受公用設施影響的種類與程度。

- 普（等級 0）：無要求。

#### 5. 與主機房地理距離

在與主機房地理距離部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜避免或降低與主機房之地理距離內，遭受同一災害的可能性。

例如備援機制所在機房離主機房位置超過 30 公里，過去這兩個區域並無遭受同一災害的紀錄。

- 中（等級 2）：宜評估與主機房之地理距離內，可能遭受的同一災害，並加強防護措施。

例如備援機制所在機房與主機房過去曾遭受同一淹水災害，因此在規劃機房樓層時有予以評估，並加強建物的防水設施。

- 普（等級 1）：宜評估與主機房的地理距離。

例如分析異地備份機制所在機房與主機房的地理距離。

- 普（等級 0）：無要求。

## （七）支援作業

### 1. 教育訓練

在教育訓練部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照。

例如每年要求一般主管、資訊人員、資安人員、一般使用者分別需接受 3、6、16、3 小時以上之資安和 DRP 相關教育訓練，負責人員需另外取得 ISO 27001 LA 證書。

- 中（等級 2）：相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照。

此部分與前一安全等級要求相同。

- 普（等級 1）：相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數。

例如每年要求一般主管、資訊人員、資安人員、一般使用者分別需接受 2、6、12、3 小時之資安和 DRP 相關教育訓練。

- 普（等級 0）：人員宜取得足夠或符合主管機關要求之必要教育訓練時數。

例如每年要求一般主管、資訊人員、資安人員、一般使用者分別需接受 1、4、8、2 小時之資安和 DRP 相關教育訓練。

## 2. DR 專用區

在 DR 專用區部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜具備完整 DR 專用區的配置。

例如設置可供 DR 專用的空間與設備。

- 中（等級 2）：宜具備必要 DR 專用區的配置。

例如設置可供 DR 使用的必要空間與設備。

- 普（等級 1）：宜評估 DR 專用區的配置。

例如評估 DRP 所需之專用空間與設備。

- 普（等級 0）：無要求。

### 3. 緊急應變中心

在緊急應變中心部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級3）：宜具備緊急應變中心的配置。  
例如置可供緊急應變中心專用的空間與設備。
- 中（等級2）：宜具備緊急應變中心的配置。  
此部分與前一安全等級要求相同。
- 普（等級1）：宜評估緊急應變中心的配置。  
例如評估緊急應變中心所需之空間與設備。
- 普（等級0）：無要求。

### 4. 人員管理

在保險部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級3）：宜建立完整全區域的人員管控措施。  
例如除全區域配置監控與門禁設備外，人員皆配掛識別證，設定各區域進出之權限，外部人員需提前申請並全程由專責人員陪同。
- 中（等級2）：宜建立基本全區域的人員管控措施。  
例如全區域配置監控與門禁設備，外部人員需登記並由人員陪同。

- 普（等級 1）：宜建立機房進出管控措施。

例如機房配有門禁系統，外部人員進出需登記並由人員陪同。

- 普（等級 0）：宜對外部人員進行基本機房進出管控。

例如要求外部人員進機房前需先登記。

## 5. 保險

在保險部分，對照不同資訊系統安全等級之實施建議，由高至低分別為：

- 高（等級 3）：宜投保必要的保險機制。

例如已投保地震險等相關產物保險，另評估投保資安保險的需求性。

- 中（等級 2）：宜投保必要的保險機制。

此部分與前一安全等級要求相同。

- 普（等級 1）：宜評估必要的保險機制。

例如評估投保必要產物保險的需求性。

- 普（等級 0）：無要求。

上述各項評估準則及各級資訊系統安全等級實施建議彙整如表格 1 所示。

表格 1 電腦機房異地備援機制評估準則與資訊系統安全等級對照表

資訊系統 安全等級  評估 準則	普 (等級 0)  (資料備 份)	普 (等級 1)	中 (等級 2)	高 (等級 3)
<b>4.1 一般原則</b>				
4.1.1 資安稽核/ 自我檢視	宜定期每年至少進行1次資訊安全 and 個資保護自我檢視	宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行1次個資保護自我檢視	宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行1次個資保護自我檢視	宜通過資訊安全與個資保護驗證或符合主管機關之要求
4.1.2 災害復原計畫	宜評估 DRP 之建立	宜建立基本之 DRP	宜針對主要風險建立 DRP	宜針對各項可能風險建立 DRP
4.1.3 管理階層支持	管理階層宜給予適時的支持	管理階層宜不定期主持會議並給予必要支持	管理階層宜定期主持會議並給予重要支持	管理階層宜定期主持會議並給予重要支持
4.1.4 資源評估	宜評估資源與經費上的需求	宜評估資源與經費上的需求，並規劃預算	宜評估資源與經費上的需求，並規劃預算及估算支出成本	宜評估資源與經費上的需求，並每年擬定預算及估算支出成本

4.1.5 變更管理	宜評估變更造成的影響	宜評估與測試變更造成的影響	宜評估與測試變更造成的影響，並定期監控	宜評估與測試變更造成的影響，並持續監控
<b>4.2 營運持續</b>				
4.2.1 資訊資料回復點 (RPO)	最近一代資訊資料容許 >24 小時	最近一代資訊資料容許在 1~24 小時	最近一代資訊資料容許在 0~1 小時	最近一代資訊資料容許在 0~1 小時
4.2.2 營運復原時間 (RTO)	營運復原容許時間 >24 小時	營運復原容許時間在 8~24 小時	營運復原容許時間在 1~8 小時	營運復原容許時間在 0~1 小時
4.2.3 營運復原水準 (RLO)	無要求	災後第一時間復原之營運水準容許 <60%	災後第一時間復原之營運水準容許在 60%~80%	災後第一時間復原之營運水準容許在 80%~100%
4.2.4 BCP 演練	宜定期執行基本異地備份機制的演練與測試	宜定期執行重要異地備援機制的演練與測試	宜定期執行完整異地備援機制的演練與測試	宜定期執行完整異地備援機制的演練與測試
<b>4.3 系統架構</b>				
4.3.1 資料備份類型	宜至少使用完整備份	宜使用完整備份與遞增備份	宜使用完整備份與差異性備份	宜使用完整備份與差異性備份
4.3.2 異地資料備份方式	宜至少使用離線備份	宜使用網路非同步寫入	宜使用網路同步寫入	宜使用網路同步寫入
4.3.3 系統備援方式	宜使用冷備援站	宜使用暖備援站	宜使用熱備援站	宜使用鏡像站

4.4 網路配置				
4.4.1 網路流量	宜評估與建立必要異地備份網路頻寬	宜評估與建立必要異地備援網路頻寬	宜評估與建立足夠異地備援網路頻寬	宜評估與建立完整異地備援網路頻寬
4.4.2 備援線路	無要求	宜評估必要異地備援線路	宜建立完整異地備援線路 (N+1)	宜建立完整異地備援線路 (N+1)，及考量專線的需求
4.4.3 備援設備	無要求	宜評估必要異地備援設備	宜建立完整異地備援設備 (N+1)	宜建立完整異地備援設備 (N+1)，及考量自動切換的需求
4.4.4 備援 ISP	無要求	宜評估備援 ISP 的服務	宜取得備援 ISP 的服務 (N+1)	宜取得備援 ISP 的服務 (N+1)
4.5 建置環境				
4.5.1 電力供給	宜具備 UPS 系統的配置	宜具備 UPS 系統並考量發電機系統的配置	宜具備 UPS 系統與發電機系統的配置	除基本備用電源的配置外，宜考量市電、備用電源的備援機制 (N+1)
4.5.2 空調配置	宜考量空調系統的配置	宜配置空調系統，並考量的備援機制的需求	宜配置空調系統及備援機制 (N+1)	宜配置空調系統及備援機制 (N+1)，並考量空調效能的評估

4.5.3 環境監測與告警	宜考量必要之監測與告警機制的建立	宜建立必要之監測與告警系統	宜建立完善之監測與告警系統，並建立處理程序	宜建立完善之監測與告警系統，並建立處理程序
4.5.4 建物安全	宜符合政府法規要求	宜符合政府法規要求，並考量機房相關防災機制	宜符合政府法規要求，並考量機房相關防災機制，另評估建物風險	宜符合政府法規要求，並考量機房相關防災機制，另降低建物風險
<b>4.6 地理位置</b>				
4.6.1 天然災害	無要求	宜評估可能遭受的天然災害	宜評估可能遭受的天然災害，並加強防護措施	宜避免或降低與主機房遭受同類天然災害的可能性
4.6.2 工、商業災害	無要求	宜評估可能遭受的工、商業災害	宜評估可能遭受的工、商業災害，並加強防護措施	宜避免或降低與主機房遭受同類工、商業災害的可能性
4.6.3 交通便利因素	無要求	宜評估交通便利狀況	宜考量交通便利狀況，規劃交通方式	宜考量交通便利狀況，規劃兩種以上交通方式
4.6.4 公用設施的影響	無要求	宜評估可能遭受的公用設施影響	宜評估可能遭受的公用設施影響，並加強防護措施	宜避免或降低與主機房遭受同類公用設施影響的可能性

4.6.5 與主機房地理距離	無要求	宜評估與主機房的地理距離	宜評估與主機房之地理距離內，可能遭受的同一災害，並加強防護措施	宜避免或降低與主機房之地理距離內，遭受同一災害的可能性
<b>4.7 支援作業</b>				
4.7.1 教育訓練	人員宜取得足夠或符合主管機關要求之必要教育訓練時數	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照
4.7.2 DR 專用區	無要求	宜評估 DR 專用區的配置	宜具備必要 DR 專用區的配置	宜具備完整 DR 專用區的配置
4.7.3 緊急應變中心	無要求	宜評估緊急應變中心的配置	宜具備緊急應變中心的配置	宜具備緊急應變中心的配置
4.7.4 人員管理	宜對外部人員進行基本機房進出管控。	宜建立機房進出管控措施。	宜建立基本全區域的人員管控措施。	宜建立完整全區域的人員管控措施。
4.7.5 保險	無要求	宜評估必要的保險機制	宜投保必要的保險機制	宜投保必要的保險機制

資料來源：本研究整理

## 五、電腦機房異地備援機制評估準則自評表

為協助組織進行現有電腦機房異地備援機制的評估，研究團隊提供一可操作的自評表格，讀者可藉此分析各項評估準則的「資訊系統安全等級」和「實際符合等級」間的差距。(無異地備援機房者亦可就現有主機房、異地備援機制或異地備份機制作評估)

自評表各欄位及使用說明如下：

- 資訊系統名稱：組織挑選欲進行各項評估準則分析之對象，若有 2 個以上重要（關鍵）資訊系統（即資訊系統安全水準鑑別最高等級者），且座落於相同機房，配置相同的異地備援機制，建議一併填寫以作評估。另亦可對其他安全等級之資訊系統進行異地備援機制之評估。
- 系統服務說明：概述資訊系統的服務、功能等相關基本背景。
- 自評日期：填寫自評表之起迄時間。
- 資訊系統安全等級（A）：指組織針對該資訊系統評估後之安全等級；依循參考指引建議之「重要（關鍵）系統識別」作法，識別出資訊系統所屬的「普」（等級 0）、「普」（等級 1）、「中」（等級 2）、「高」（等級 3）其中一等級。若該資訊系統安全水準為「高」（等級 3），則其分數為 4 分，即  $A=4$ 。
- 構面與評估項目：為電腦機房異地備援機制評估準則各項評估項目，自評表依據操作手冊列舉出七大構面共 30 項建議自評項目，詳細說明可參閱操作手冊第 3 章。
- 等級說明：即針對各評估準則之各「普」（等級 0）、「普」（等級 1）、「

「中」(等級 2)、「高」(等級 3) 的實施建議說明，讀者可藉以評估現有作為與等級說明間的異同，再行勾選符合的「實際符合等級」。部分評估準則之不同安全等級實施建議敘述相同，例如本手冊 4.1.1「普」(等級 1) 與「中」(等級 2)、4.1.3「中」(等級 2) 與「高」(等級 3) …等，讀者在填寫時宜再留意。

- 實際符合等級 (B)：為組織目前的實施現況，讀者可依據等級說明或本手冊第 4 章的範例，評估符合現有運作狀態的分數，若評估的結果符合「中」(等級 2)，則其分數為 4 分，即  $B=4$ 。另外，針對部分評估準則之不同安全水準實施建議敘述相同的狀況，例如本手冊 4.1.3「中」(等級 2) 與「高」(等級 3)，若一開始的「資訊系統安全等級」鑑別為「中」(等級 2)，即  $A=3$ ，而「實際符合等級」鑑別結果同時符合「中」(等級 2) 與「高」(等級 3) 敘述 (因為等級說明相同)，則應選擇與資訊系統安全水準相同的「中」(等級 2)，即  $B=3$ ，不宜勾選「高」(等級 3)。

註：針對此類等級說明相同，使用者在填寫「實際符合等級」時，需選擇與「資訊系統安全等級」一致分數的項目，將會加註「\*」。

- 差異分數  $C=A-B$ ：計算「資訊系統安全等級」與「實際符合等級」間的差異，同一構面差異分數相加得「差異分數小計」，最後在完成所有評估準則差異評比後，再加總各構面的「差異分數小計」得到「差異分數總計」。
- 現況/差異說明：若「資訊系統安全等級」與「實際符合等級」相同，則組織可說明目前運作或配置的狀態，如有分數上的落差，可就差異的部分再行說明，並提出已規劃後未來預期的作法方向。
- 差異分數總計：以下就各差異分數總計的級距進行說明。

- 差異分數總計  $\leq 5$ ：表示「資訊系統安全等級」與「實際符合等級」差距不大，宜考量資訊系統的需求，提高相關評估準則的作為，使持續運作規劃更有保障。
- $5 < \text{差異分數總計} \leq 10$ ：表示「資訊系統安全等級」與「實際符合等級」有段差距，宜針對資訊系統較急迫之需求，提高相關評估準則的作為，確保持續運作的可靠性。
- $10 < \text{差異分數總計}$ ：表示「資訊系統安全等級」與「實際符合等級」差距極大，宜積極改善、加強資訊系統相關評估準則的作為，確保持續運作得以維持一定的水平。
- 某項評估準則  $C \geq 2$ ：組織宜針對該項目進行檢討，評估可行的改善、加強作為，提高持續運作的可靠性。
- 自評人員與主管簽章：針對各項電腦機房評估準則的「資訊系統安全等級」與「實際符合等級」評分結果，以及相關現況/差異說明，填寫人員需簽名以示負責，而資訊或資安主管同時也應簽名以示審閱和認可，進而後續指示、支持各項改善工作的進行。

「電腦機房異地備援機制評估準則自評表」請參閱表 2；此外，為幫助填寫人員使用自評表，本手冊第 6 章另提供一自評案例，讀者可再行參閱。

表格 2 電腦機房異地備援機制評估準則自評表

資訊系統名稱：		自評日期： / / ~ / /			
系統服務說明：		資訊系統安全等級 (A)			
		<input type="checkbox"/> 高 (等級 3) 4 分	<input type="checkbox"/> 中 (等級 2) 3 分		
		<input type="checkbox"/> 普 (等級 1) 2 分	<input type="checkbox"/> 普 (等級 0) 1 分		
4.1 一般原則					
評估項目	等級說明		實際符合等級 (B)	差異分數 C=A-B	現況/差異說明
4.1.1 資安稽核/自我檢視	高 (等級 3)	宜通過資訊安全與個資保護驗證或符合主管機關之要求	<input type="checkbox"/> 高 (等級 3) 4 分		
	*中 (等級 2)	宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行 1 次個資保	* <input type="checkbox"/> 中 (等級 2) 3 分		

		護自我檢視			
	*普(等級1)	宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行1次個資保護自我檢視	* <input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜定期每年至少進行1次資訊安全和個資保護自我檢視	<input type="checkbox"/> 普(等級0) 1分		
4.1.2 災害復原計畫	高(等級3)	宜針對各項可能風險建立DRP	<input type="checkbox"/> 高(等級3) 4分		
	中(等級2)	宜針對主要風險建立DRP	<input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜建立基本之DRP	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜評估DRP之建立	<input type="checkbox"/> 普(等級0) 1分		
4.1.3 管理階層支持	*高(等級3)	管理階層宜定期主持會議並給予重要支持	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	管理階層宜定	* <input type="checkbox"/> 中(等級		

		期主持會議並給予重要支持	2) 3分		
	普(等級1)	管理階層宜不定期主持會議並給予必要支持	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	管理階層宜給予適時的支持	<input type="checkbox"/> 普(等級0) 1分		
4.1.4 資源評估	高(等級3)	宜評估資源與經費上的需求，並每年擬定預算及估算支出成本	<input type="checkbox"/> 高(等級3) 4分		
	中(等級2)	宜評估資源與經費上的需求，並規劃預算及估算支出成本	<input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜評估資源與經費上的需求，並規劃預算	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜評估資源與經費上的需求	<input type="checkbox"/> 普(等級0) 1分		
4.1.5	高(等級3)	宜評估與測試	<input type="checkbox"/> 高(等級3)		

變更管理		變更造成的影響，並持續監控	4分		
	中(等級2)	宜評估與測試變更造成的影響，並定期監控	<input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜評估與測試變更造成的影響	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜評估變更造成的影響	<input type="checkbox"/> 普(等級0) 1分		
差異分數小計 C1					

#### 4.2 營運持續

評估項目	等級說明		實際符合等級 (B)	差異分數 C=A-B	現況/差異說明
4.2.1 資訊資料回復點 (RPO)	*高(等級3)	最近一代資訊資料容許在 0~1 小時	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	最近一代資訊資料容許在 0~1 小時	* <input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	最近一代資訊	<input type="checkbox"/> 普(等級1)		

		資料容許在 1~24 小時	2 分		
	普 (等級 0)	最近一代資訊 資料容許>24 小 時	<input type="checkbox"/> 普 (等級 0) 1 分		
4.2.2 營運復 原時間 (RTO)	高 (等級 3)	營運復原容許 時間在 0~1 小時	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	營運復原容許 時間在 1~8 小時	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	營運復原容許 時間在 8~24 小 時	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	營運復原容許 時間>24 小時	<input type="checkbox"/> 普 (等級 0) 1 分		
4.2.3 營運復 原水準 (RLO)	高 (等級 3)	災後第一時間 復原之營運水 準 容 許 在 80%~100%	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	災後第一時間 復原之營運水 準 容 許 在 60%~80%	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	災後第一時間	<input type="checkbox"/> 普 (等級 1)		

		復原之營運水準容許<60%	2分		
	普(等級0)	無要求	<input type="checkbox"/> 普(等級0) 1分		
4.2.4 BCP 演 練	*高(等級3)	宜定期執行完整異地備援機制的演練與測試	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	宜定期執行完整異地備援機制的演練與測試	* <input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜定期執行重要異地備援機制的演練與測試	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜定期執行基本異地備份機制的演練與測試	<input type="checkbox"/> 普(等級0) 1分		
差異分數小計 C2					
<b>4.3 系統架構</b>					
評估項	等級說明		實際符合等	差異	現況/差異說明

目			級 (B)	分數 C=A-B	
4.3.1 系統備 援類型	*高(等級3)	宜使用完整備份與差異性備份	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	宜使用完整備份與差異性備份	* <input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜使用完整備份與遞增備份	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜至少使用完整備份	<input type="checkbox"/> 普(等級0) 1分		
4.3.2 異地資 料備份 方式	*高(等級3)	宜使用網路同步寫入	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	宜至少使用網路同步寫入	* <input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜使用網路非同步寫入	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜至少使用離線備份	<input type="checkbox"/> 普(等級0) 1分		
4.3.3 系統備	高(等級3)	宜使用鏡像站	<input type="checkbox"/> 高(等級3) 4分		

援方式	中 (等級 2)	宜使用熱備援站	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜使用暖備援站	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	宜使用冷備援站	<input type="checkbox"/> 普 (等級 0) 1 分		

差異分數小計 C3

#### 4.4 網路配置

評估項目	等級說明		實際符合等級 (B)	差異分數 C=A-B	現況/差異說明
4.4.1 網路流量	高 (等級 3)	宜評估與建立完整異地備援網路頻寬	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜評估與建立足夠異地備援網路頻寬	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估與建立必要異地備援網路頻寬	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	宜評估與建立必要異地備份	<input type="checkbox"/> 普 (等級 0)		

		網路頻寬	1 分		
4.4.2 備援線 路	高 (等級 3)	宜建立完整異地備援線路 (N+1), 及考量專線的需求	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜建立完整異地備援線路 (N+1)	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估必要異地備援線路	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	無要求	<input type="checkbox"/> 普 (等級 0) 1 分		
4.4.3 備援設 備	高 (等級 3)	宜建立完整異地備援設備 (N+1), 及考量自動切換的需求	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜建立完整異地備援設備 (N+1)	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估必要異地備援設備	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	無要求	<input type="checkbox"/> 普 (等級 0)		

			1 分		
4.4.4 備援 ISP	*高(等級3)	宜取得備援 ISP 的服務 (N+1)	* <input type="checkbox"/> 高 (等級 3) 4 分		
	*中(等級2)	宜取得備援 ISP 的服務 (N+1)	* <input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估備援 ISP 的服務	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	無要求	<input type="checkbox"/> 普 (等級 0) 1 分		

差異分數小計 C4

#### 4.5 建置環境

評估項目	等級說明		實際符合等級 (B)	差異分數 C=A-B	現況/差異說明
4.5.1 電力供給	高 (等級 3)	除基本備用電源的配置外，宜考量市電、備用電源的備援機制 (N+1)	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜具備 UPS 與發電機的配置	<input type="checkbox"/> 中 (等級 2) 3 分		

	普 (等級 1)	宜具備 UPS 並考量發電機的配置	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	宜具備 UPS 的配置	<input type="checkbox"/> 普 (等級 0) 1 分		
4.5.2 空調配置	高 (等級 3)	宜配置空調系統及備援機制 (N+1), 並考量空調效能的評估	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜配置空調系統及備援機制 (N+1)	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜配置空調系統, 並考量備援機制的需求	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	宜考量空調系統的配置	<input type="checkbox"/> 普 (等級 0) 1 分		
4.5.3 環境監測與告警	*高 (等級 3)	宜建立完善的監測與告警系統, 並建立處理程序	* <input type="checkbox"/> 高 (等級 3) 4 分		
	*中 (等級 2)	宜建立完善的監測與告警系	* <input type="checkbox"/> 中 (等級		

		統，並建立處理程序	2) 3分		
	普 (等級 1)	宜建立必要之監測與告警系統	<input type="checkbox"/> 普 (等級 1) 2分		
	普 (等級 0)	宜考量必要之監測與告警機制的建立	<input type="checkbox"/> 普 (等級 0) 1分		
4.5.4 建物安全	高 (等級 3)	宜符合政府法規要求，並考量機房相關防災機制，另降低建物風險	<input type="checkbox"/> 高 (等級 3) 4分		
	中 (等級 2)	宜符合政府法規要求，並考量機房相關防災機制，另評估建物風險	<input type="checkbox"/> 中 (等級 2) 3分		
	普 (等級 1)	宜符合政府法規要求，並考量機房相關防災機制	<input type="checkbox"/> 普 (等級 1) 2分		
	普 (等級 0)	宜符合政府法規要求	<input type="checkbox"/> 普 (等級 0) 1分		

差異分數小計 C5

4.6 地理位置

評估項目	等級說明		實際符合等級 (B)	差異分數 C=A-B	現況/差異說明
4.6.1 天然災害	高 (等級 3)	宜避免或降低與主機房遭受同類天然災害的可能性	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜評估可能遭受的天然災害，並加強防護措施	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估可能遭受的天然災害	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	無要求	<input type="checkbox"/> 普 (等級 0) 1 分		
4.6.2 工、商業災害	高 (等級 3)	宜避免或降低與主機房遭受同類工、商業災害的可能性	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜評估可能遭受的工、商業災	<input type="checkbox"/> 中 (等級 2)		

		害，並加強防護措施	3分		
	普（等級1）	宜評估可能遭受的工、商業災害	<input type="checkbox"/> 普（等級1） 2分		
	普（等級0）	無要求	<input type="checkbox"/> 普（等級0） 1分		
4.6.3 交通便利因素	高（等級3）	宜考量交通便利狀況，規劃兩種以上交通方式	<input type="checkbox"/> 高（等級3） 4分		
	中（等級2）	宜考量交通便利狀況，規劃交通方式	<input type="checkbox"/> 中（等級2） 3分		
	普（等級1）	宜評估交通便利狀況	<input type="checkbox"/> 普（等級1） 2分		
	普（等級0）	無要求	<input type="checkbox"/> 普（等級0） 1分		
4.6.4 公用設施的影響	高（等級3）	宜避免或降低與主機房遭受同類公用設施影響的可能性	<input type="checkbox"/> 高（等級3） 4分		
	中（等級2）	宜評估可能遭	<input type="checkbox"/> 中（等級2）		

		受的公用設施 影響，並加強防 護措施	3分		
	普（等級1）	宜評估可能遭 受的公用設施 影響	<input type="checkbox"/> 普（等級1） 2分		
	普（等級0）	無要求	<input type="checkbox"/> 普（等級0） 1分		
4.6.5 與主機 房地理 距離	高（等級3）	宜避免或降低 與主機房之地 理距離內，遭受 同一災害的可 能性	<input type="checkbox"/> 高（等級3） 4分		
	中（等級2）	宜評估與主機 房之地理距離 內，可能遭受的 同一災害，並加 強防護措施	<input type="checkbox"/> 中（等級2） 3分		
	普（等級1）	宜評估與主機 房的地理距離	<input type="checkbox"/> 普（等級1） 2分		
	普（等級0）	無要求	<input type="checkbox"/> 普（等級0） 1分		
差異分數小計 C6					

### 4.7 支援作業

評估項目	等級說明		實際符合等級 (B)	差異分數 C=A-B	現況/差異說明
4.7.1 教育訓練	*高(等級3)	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照	* <input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	人員宜取得足夠或符合主管機關要求之必要教育訓練時	<input type="checkbox"/> 普(等級0) 1分		

		數			
4.7.2 DR 專用 區	高 (等級 3)	宜具備完整 DR 專用區的配置	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜具備必要 DR 專用區的配置	<input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估 DR 專用區的配置	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	無要求	<input type="checkbox"/> 普 (等級 0) 1 分		
4.7.3 緊急應 變中心	*高 (等級 3)	宜具備緊急應變中心的配置	* <input type="checkbox"/> 高 (等級 3) 4 分		
	*中 (等級 2)	宜具備緊急應變中心的配置	* <input type="checkbox"/> 中 (等級 2) 3 分		
	普 (等級 1)	宜評估緊急應變中心的配置	<input type="checkbox"/> 普 (等級 1) 2 分		
	普 (等級 0)	無要求	<input type="checkbox"/> 普 (等級 0) 1 分		
4.7.4 人員管 理	高 (等級 3)	宜建立完整全區域的人員管控措施。	<input type="checkbox"/> 高 (等級 3) 4 分		
	中 (等級 2)	宜建立基本全區域的人員管	<input type="checkbox"/> 中 (等級 2)		

		控措施。	3分		
	普(等級1)	宜建立機房進出管控措施。	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	宜對外部人員進行基本機房進出管控。	<input type="checkbox"/> 普(等級0) 1分		
4.7.5 保險	*高(等級3)	宜投保必要的保險機制	* <input type="checkbox"/> 高(等級3) 4分		
	*中(等級2)	宜投保必要的保險機制	* <input type="checkbox"/> 中(等級2) 3分		
	普(等級1)	宜評估必要的保險機制	<input type="checkbox"/> 普(等級1) 2分		
	普(等級0)	無要求	<input type="checkbox"/> 普(等級0) 1分		
差異分數小計 C7					
C1+C2+C3+C4+C5+C6+C7 差異分數總計				自評人員：	主管：

## 六、自評表使用案例

### (一) 組織背景與電腦機房異地備援機制概述

該組織屬財團法人，員工約 3000 人。已通過 ISO 27001、ISO 20000 認證，於 102 年完成機房電力、空調整改。承租之主機房位於內湖，該機房為 7x24 三班輪值人員，並通過 Uptime Tier II facility 認證。異地資料備份 storage 承租台中 IDC 機房。系統架構為主機 x2(Active-Active)、儲存設備 (x1)、鏡像儲存設備 (x1)、異地資料備份儲存設備 (x1)、異地備援機房主機 (x1)，即時與主機房鏡像儲存設備資料同步。異地資料備份儲存設備每日與鏡像儲存設備排程備份。

### (二) 自評過程

以下自評表僅摘錄自評出的實際符合等級項目。

表格 3 電腦機房異地備援機制評估準則自評表 (使用案例)

資訊系統名稱：電子郵件服務系統	自評日期：103/02/25～ 103/02/25	
系統服務說明： 提供全公司同仁使用，於個人業務聯繫、專案及部門對外服務窗口，並依據服務水準協議，提供帳號及郵件收	資訊系統安全等級 (A)	
	<input checked="" type="checkbox"/> 高 (等級 3) 4 分	<input type="checkbox"/> 中 (等級 2) 3 分

發服務。	<input type="checkbox"/> 普 (等級 1) 2 分	<input type="checkbox"/> 普 (等級 0) 1 分
------	--	--

#### 4.1 一般原則

評估項目	等級說明		實際符合水準 (B)	差異分數 C=A-B	現況/差異說明
4.1.1 資安稽核/自我檢視	*中(等級 2)	宜通過資訊安全驗證或符合主管機關之要求，並每年至少進行 1 次個資保護自我檢視	*■中(等級 2) 3 分	1	電子郵件服務已通過資訊安全驗證，並每季進行資訊安全內部稽核及個資保護檢視。
4.1.2 災害復原計畫	中(等級 2)	宜針對主要風險建立 DRP	■中(等級 2) 3 分	1	郵件服務平台，並與其他服務互相串連，部分風險產生於其他服務，郵件服務僅針對主要風險進行 DRP 及 BCP 演練
4.1.3 管理階層支持	*高(等級 3)	管理階層宜定期主持會議並給予重要支持	*■高(等級 3) 4 分	0	每月定期產出服務水準報告，包含服務時間、事件、事故及容量管理，並於主管會議中進行檢討。
4.1.4 資源評估	高(等級 3)	宜評估資源與經費上的需求，並每年擬定預算及估算支	■高(等級 3) 4 分	0	每年編列設備維護、人員教育訓練等預算，以符合服務水準協議要求。

		出成本			
4.1.5 變更管理	高(等級3)	宜評估與測試變更造成的影響，並持續監控	■高(等級3) 4分	0	已有完整的評估及測試機制，變更造成的影響，均可由評估及測試程序，發現並修正。
差異分數小計 C1				2	
<b>4.2 營運持續</b>					
評估項目	等級說明		實際符合水準 (B)	差異分數 C=A-B	現況/差異說明
4.2.1 資訊資料回復點 (RPO)	*高(等級3)	最近一代資訊資料容許在 0~1 小時	*■高(等級3) 4分	0	已建立鏡像機制，同步資料至備份儲存設備，再同步至異地備援伺服器。
4.2.2 營運復原時間 (RTO)	高(等級3)	營運復原容許時間在 0~1 小時	■高(等級3) 4分	0	已建置雙主機機制，以及異地備援主機。
4.2.3 營運復原水準 (RLO)	高(等級3)	災後第一時間復原之營運水準容許在 80%~100%	■高(等級3) 4分	0	可於 1 小時內，恢復 95% 的營運水準

4.2.4 BCP 演 練	高(等級3)	宜定期執行完 整異地備援機 制的演練與測 試	■高(等級3) 4分	0	每半年即擬訂演練計畫 並經管理階層核准執 行，並直接參與演練。
差異分數小計 C2				0	
<b>4.3 系統架構</b>					
評估項 目	等級說明		實際符合水 準 (B)	差異 分數 C=A-B	現況/差異說明
4.3.1 系統備 援類型	*高(等級3)	宜使用完整備 份與差異性備 份	*■高(等級 3) 4分	0	每周完整備份，每日差 異備份。
4.3.2 異地資 料備份 方式	*高(等級3)	宜使用網路同 步寫入	*■高(等級 3) 4分	0	儲存設備每日同步寫入
4.3.3 系統備 援方式	高(等級3)	宜使用鏡像站	■高(等級3) 4分	0	於備援機房建立備援主 機，每日同步資料
差異分數小計 C3				0	
<b>4.4 網路配置</b>					
評估項 目	等級說明		實際符合水 準 (B)	差異 分數	現況/差異說明

				C=A-B	
4.4.1 網路流量	高(等級3)	宜評估與建立完整異地備援網路頻寬	■高(等級3) 4分	0	已依據服務惟運資料及容量管理，規劃並建置網路頻寬。
4.4.2 備援線路	高(等級3)	宜建立完整異地備援線路(N+1)，及考量專線的需求	■高(等級3) 4分	0	向三家不同線路的ISP承租網路，並建立site-to-site VPN。
4.4.3 備援設備	高(等級3)	宜建立完整異地備援設備(N+1)，及考量自動切換的需求	■高(等級3) 4分	0	已建立N+1備援線路
4.4.4 備援ISP	*高(等級3)	宜取得備援ISP的服務(N+1)	*■高(等級3) 4分	0	已向3家不同線路ISP業者承租線路
差異分數小計 C4				0	
<b>4.5 建置環境</b>					
評估項目	等級說明		實際符合水準(B)	差異分數 C=A-B	現況/差異說明
4.5.1 電力供給	高(等級3)	除基本備用電源的配置外，宜考量市電、備用電源的備援機	■高(等級3) 4分	0	機房採UPS(N+1)及雙迴路設計，市電及備用發電機，分別連接至大樓配電盤，提供UPS備

		制 (N+1)			援電力。
4.5.2 空調配 置	高 (等級 3)	宜配置空調系 統及備援機制 (N+1), 並考量 空調效能的評 估	■高(等級 3) 4 分	0	空調系統採備援機制, 並分時啟動, 每日定時 間交互運轉。機房 PUE 約為 1.49 - 1.57, 符合 Green Grid 銀級目標。
4.5.3 環境監 測與告 警	高 (等級 3)	宜建立完善的 監測與告警系 統, 並建立處理 程序	■高(等級 3) 4 分	0	已建立環控系統, 即時 監測溫、濕度, 並設定 告警臨界值範圍。超過 告警範圍, 即啟動告警 機制, 以簡訊通知管理 人員。
4.5.4 建物安 全	中 (等級 2)	宜符合政府法 規要求, 並考量 機房相關防災 機制, 另評估建 物風險	■中(等級 2) 3 分	1	建物、機房均符合法規 要求, 惟建物啟用已超 過 20 年, 需重新評估管 線、梁柱等結構風險。 已向大樓管理處提案, 並規劃備援機房及主機 房搬遷計畫。
差異分數小計 C2				1	
<b>4.6 地理位置</b>					
評估項 目	等級說明		實際符合水 準 (B)	差異 分數 C=A-B	現況/差異說明
4.6.1 天然災	中 (等級 2)	宜評估可能遭 受的天然災	■中(等級 2) 3 分	1	建物未設置在落雷密集 區域, 且附近有其他高

害		害，並加強防護措施			樓設置完善避雷設備。惟公司位於10樓，地震等天災發生較難疏散。
4.6.2 工、商業 災害	高(等級3)	宜避免或降低與主機房遭受同類工、商業災害的可能性	■高(等級3) 4分	0	主機房與備援機房無存在同類工、商業災害的狀況
4.6.3 交通便利因素	高(等級3)	宜考量交通便利狀況，規劃兩種以上交通方式	■高(等級3) 4分	0	公司距離捷運、公車站牌近，且有多線公車停靠。路旁巷弄可提供車輛雙向通行，並有多處停車場。
4.6.4 公用設施的影響	中(等級2)	宜評估可能遭受的公用設施影響，並加強防護措施	■中(等級2) 3分	1	公司附近設有多座高頻基地台，定期請臺電檢測電磁波等影響。
4.6.5 與主機房地理距離	高(等級3)	宜避免或降低與主機房之地理距離內，遭受同一災害的可能性	■高(等級3) 4分	0	備援機房位於桃園，與主機房距離超過20公里。
差異分數小計 C3				2	
<b>4.7 支援作業</b>					
評估項目	等級說明		實際符合水準(B)	差異分數 C=A-B	現況/差異說明

4.7.1 教育訓練	高(等級3)	相關人員宜取得足夠或符合主管機關要求之相關專業教育訓練時數與證照	■高(等級3) 4分	0	相關人員每半年接受2小時教育訓練
4.7.2 DR專用區	高(等級3)	宜具備完整DR專用區的配置	■高(等級3) 4分	0	已建置DR專用區域
4.7.3 緊急應變中心	高(等級3)	宜具備緊急應變中心的配置	■高(等級3) 4分	0	於備援機房樓上，即為緊急應變中心
4.7.4 人員管理	高(等級3)	宜建立完整全區域的人員管控措施。	■高(等級3) 4分	0	進出入皆須經過申請，未經授權區域無法進入，且都配置門禁與監視設備
4.7.5 保險	高(等級3)	宜投保必要的保險機制	■高(等級3) 4分	0	已投保相關產物保險
差異分數小計 C8				0	
C1+C2+C3+C4+C5+C6+C7 差異分數總計				5	自評人員： 主管：

### (三) 改善建議

依據自評的結果，屬於差異分數總計 $\leq 5$ 階段，表示預期與現實狀況差距不大，但組織宜再就各項次之差異分數進行分析，並參考電腦機房異地備援機制參考指引，進行相關內容之改善：

- DRP 的規劃與建立上，宜再考量與郵件服務相關之業務的可能風險，並將已識別的風險因素納入 DRP 的考量中，以建議更為完善的營運持續機制。
- 機房所在建物已啟用超過 20 年，相關管線、樓板、牆壁、梁柱等風險的評估宜再積極要求大樓管理處進行，或委託專業之單位協助實施，以盡早取得各項風險評估及改善方向，亦或可早日提出和執行機房搬遷計畫。

上述改善建議將可降低該組織的可能風險，加強 DRP 的完整，後續可再藉由參考指引與本手冊提供之自評表，針對其他重要（關鍵）資訊系統進行評估，以掌握各系統的營運持續規劃狀態，確保業務之永續。

## 【附件 2】

### 電腦機房異地備援機制中英文名詞對照表

## 中英文名詞對照表

英文	中文
- A -	
acceptance	驗收；接受
access control	存取控制
accountability	可歸責性
application system	應用系統
approach	導向；作法
aspect	層面
assessment	評鑑
asset	資產
audit	稽核
authentication	鑑別
authorized	授權
availability	可用性
awareness	認知
- B -	
business continuity management	營運持續管理
- C -	
classification	分類
communication	通信
compliance	遵守；遵循；遵循性
confidentiality	機密性
confidentiality agreement	保密協議
conformance	符合性
cryptographic	密碼
- D -	
development	開發；發展
diagnostic	診斷
disaster	災難
disciplinary	懲處
disposal	汰除；作廢
- E -	
equipment	設備
evaluation	評估
event	事件

evidence	證據
- F -	
facility	設施
forum	論壇
framework	框架
fraudulent	詐欺
- H-	
handling	處置
hazard	危險
- I-	
identify	識別
impact	衝擊
implement	實作
incident	事故
information	資訊
information security	資訊安全
integrity	完整性
intellectual property right (IPR)	智慧財產權
information security management system (ISMS)	資訊安全管理系統
- K-	
key management	金鑰管理
- L-	
label	標籤；標示
log	日誌；存錄
- M -	
maintain	維持；維護
malicious code	惡意碼
media	媒體
misuse	誤用
mobile computing	行動計算
monitor	監視
- N-	
non-repudiation	不可否認性
- O-	
objective	目標
operation	作業；操作；運作

outsource	委外
- P -	
password	通行碼
policy	政策
privilege	特權
procedure	程序
- R-	
registration	註冊
requirement	要求
responsibility	責任
review	審查
residual risk	剩餘風險
risk	風險
risk acceptance	風險接受
risk analysis	風險分析
risk assessment	風險評鑑
risk assessment approach	風險評鑑作法
risk evaluation	風險評估
risk management	風險管理
risk treatment	風險處理
routing	選路
- S -	
scope	範圍
screening	篩選
segregation	區隔
statement of applicability	適用性聲明
storage area network; SAN	儲存區域網路
storage pool	儲存池
synchronization	同步
- T -	
teleworking	遠距工作
third party	第三方
threat	威脅
- U-	
unattended	無人看管
- V-	
validation	確認

vulnerability	脆弱性
- W -	
weakness	弱点

## 【附件 3】

### 電腦機房異地備援相關規範

## 一、國際電腦機房異地備援相關標準與規範

### (一) 國際標準化組織 (International Organization for Standardization, ISO)

ISO 為現今國際標準化領域中最重要的國際組織。1946 年由 25 個國家的代表在倫敦召開會議，決定發起成立一個國際組織，其目的是促進國際間合作和各領域標準的統一。是以 ISO 於 1947 年 2 月 23 日正式成立，其總部則設在瑞士的日內瓦。ISO 為非政府組織，目前成員包括 164 個會員國，包括各會員國的國家標準機構和主要公司。ISO 自成立以來已出版了超過 19,500 份國際標準，內容幾乎涉及所有食品安全、資訊、農業與醫療保健等方面的技術和業務。

#### 1. ISO 22301 : 2012 Societal Security - Business Continuity

#### Management Systems - Requirements (社會安全-營運持續管理系統-要求要項)

- 標準簡介

ISO 22301 為營運持續管理的國際驗證標準，ISO 於 2012 年 5 月 15 日發布這項標準，主要提供企業、組織正式營運持續管理架構，協助企業、組織發展營運持續計畫，以確保發生重大業務衝擊事件期間與之後的業務持續營運。

ISO 22301 內容大部份與英國的 BS 25999-2 相似，ISO 22301 融合了來自多個國家標準，其中包括來自美國、日本、新加坡、加拿大和澳大利亞的要求，但 ISO 22301 內容要求大部份仍與英國的 BS 25999-2 相似。

ISO 22301 規範的要求是通用的，適用於不論其類型，規模或性質的所有組織或其部分。應用這些規範要求的程度取決於組織的經營環境和複雜性。ISO 22301 要求規劃、建立、實施、監控、以及審查，以保持並持續改進文件化的管理系統，以確保於重大業務衝擊事件出現時能夠防止或降低業務中斷發生的可能性。

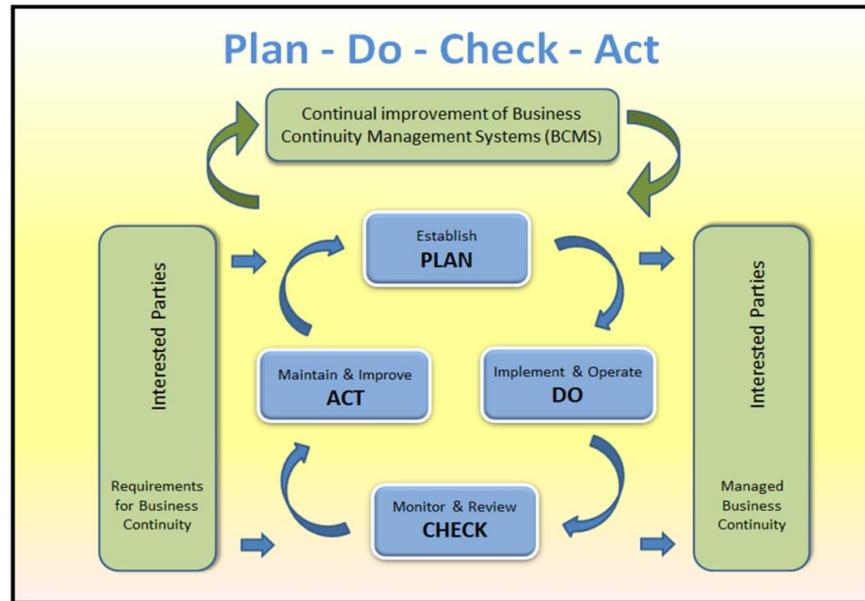
- **適用範圍**

ISO 22301 是一個通用的營運持續管理標準，它可以用於不論其類型、規模和性質的任何組織或任何組織的部分。

- **重點摘要**

ISO 22301 是業務營運持續管理制度的驗證標準，而 ISO 22313 則是業務營運持續管理制度的施行準則。ISO 22301 國際標準仍沿用 PDCA (Plan-Do-Check-Act) 架構，以 ISO Guide 83 為制定管理系統高階架構為準則，制訂出 0-10 條

之條文標準。



資料來源：ISO 22301

圖 1 ISO22301 PDCA 模組

ISO 於 2012 年新頒行的 ISO 22301，加強計畫階段的工作，強調需瞭解高階管理階層承諾、組織內涵與利害關係人的需求，使其更能以系統結構的方式展開業務營運持續管理制度。其 0-10 條的重點摘要如下：

- 簡介 (Introduction): 以規劃，實施、運作與改進 (PDCA) 概略敘述業務營運持續管理系統的基本要素，例如：組織的政策、人員、架構、績效評鑑、管理審查等。也就是管理系統的基本架構：PDCA 循環。
- 範圍 (Scope): 說明本標準是一個通用的營運持續管理標

準，它可以用於不論其類型、規模和性質的任何組織或任何組織的部分。

- 引用標準 (Normative references)：無引用標準。
- 用語與定義 (Terms and definitions)：以本標準為目的的用語與定義。
- 組織的情況 (Context of the organization)：要求先研究瞭解組織目前所處的狀況(例如：產業特性、營運方針、地理位置、資源狀況…等等)，以及與利害關係者的期望與要求，以訂定組織業務持續的範圍與目標。
- 領導 (Leadership)：最高管理階層的支持、承諾與決心是管理系統執行成敗的關鍵因素之一。本標準要求管理階層應該展現所有有關業務持續性管理系統 (BCMS) 活動的決心、支持、領導力與承諾。
- 規劃 (Planning)：本章節要求從瞭解組織目前所處的狀況、以及與利害關係者的期望與要求，定義出BCM的範圍，以營運衝擊分析 (BIA) 展開找出業務持續營運的關鍵，再分析這些關鍵業務的風險以決定後續相對應的策略，並訂定業務持續運作的目標以及達成之計畫，此外，對於業

務持續運作的目標應該予以文件化保存。

➤ 支援 (Support): 本章節要求包括提供資源、BCM 相關員工之職能培訓、組織內員工對 BCM 認知、以及組織與 BCMS 相關的內外部溝通的需求。為了 BCMS 有效性，組織應決定將需要的文件化資訊予以保存。

➤ 運作 (Operation): 本章節主要為 PDCA 循環中的 “Do” 的階段，分別以運作的規劃與管制、營運衝擊分析與風險評鑑、營運持續策略、建立與實施營運持續程序、以及演練與測試等五個部份，敘述在 “Do” 階段的施作要求。

績效評估 Performance evaluation: 本章節主要敘述 ISO 22301 標準對於 BCMS 績效評估的要求，也就是 PDCA 中的 “Check” 的階段。要求組織應評估 BCMS 的績效與有效性。

➤ 改善 (Improvement): 本章節主要為 PDCA 中的 “Action” 的階段。包括矯正措施與持續改善，以持續改善 BCMS 的適合、正確或有效性。

## 2. ISO 22313 : 2012 Societal security - Business Continuity

### Management Systems - Guidance (社會安全-營運持續管理系統-指南)

- 標準簡介

繼 ISO 於 2012 年 5 月 15 日發布 ISO 22301 國際驗證標準後，同年 12 月 12 日接著發布 ISO 22313 營運持續管理系統指南，ISO 22313 在國際慣例基礎上，提供規劃、建立、實施、運行、監控、審查和不斷改進文件化的管理系統的指南，使企業在出現破壞性事件時，能夠做好準備、應對和復原。

ISO 22313 目的並非建立普遍一致的 BCMS 結構，但針對組織設計 BCMS 時，要求需要符合其利益相關需求。這些需求來自於法律、法規、組織、產業、產品及服務所採用的程序、經營環境、組織的規模和結構、及其利益團體之要求。

ISO 22313 是通用的，適用於各種規模和類型的企業，包括工業、商業、政府和非營利組織的經營，以建立、實施、保持和改進 BCMS，確保組織營運持續政策的一致性，或做一個符合本標準的自我評估和聲明。ISO 22313 與 ISO 22301

的差異在於 ISO 22301 是 BCMS 的驗證標準，而 ISO 22313 則是 BCMS 的建構指南。

- **適用範圍**

ISO 22313 屬通用性質，適用於各種規模和類型的企業，包括工業、商業、政府和非營利組織的經營，提供規劃、建立、實施、運行、監控、審查和不斷改進文件化的管理系統的指南。

- **重點摘要**

ISO 22301 是驗證標準，而 ISO 22313 則為 ISO 22301 驗證標準的實施指引，提供建立和管理 ISO 22301 一個有效的業務持續管理系統（BCMS）的指導。ISO 22313 的章節條款可直接對應到 ISO 22301 的章節條款，並在每個章節條款加以提供細部的實施準則參考或說明。ISO 22313 標準的各章節重點請參考本文前節 ISO 22301：2012 之重點摘要。

## **（二）國際電工委員會（International Electrotechnical Commission, IEC）**

IEC 於 1906 年在英國倫敦正式成立，已經有超過百年歷史，是世界上最早的國際性電工標準化機構。初期總部位於倫敦，於 1948

年時，才將總部遷至目前的日內瓦。1947 年 ISO 成立後，IEC 便與 ISO 合作，根據 1976 年 ISO 與 IEC 的協議，將電工、電子領域之國際標準化工作，規劃由 IEC 負責，其他領域的國際標準化工作，則由 ISO 負責，二者皆保持行政與財務上的獨立性。IEC 目前在電子、電機相關領域之國際標準發展，居領導地位的國際性標準發展組織，其領域範圍包含電子工程、電磁、電聲、多媒體、電訊、能源製造與傳送、及相關的一般性原則。IEC 的最高權力單位是委員會，由成員國的國家委員會組成，每個國家僅能有一個機構代表其參與會員，目前有 83 個國家委員會代表（60 個正式會員，23 個準會員）。委員會會議一年召開一次，稱為 IEC 年會，輪流在各個成員國召開。

## **1. ISO/IEC 27001 : 2013 Information Technology - Security**

### **Techniques - Information Security Management Systems -**

### **Requirements (資訊技術-安全技術-資訊安全管理系統-要求事項)**

- **標準簡介**

ISO/IEC 於 2005 年 10 月 25 日宣布 ISO/IEC 27001 是資訊安全管理系統 (ISMS) 的國際標準，提供企業、組織建置資訊安全管理系統導入的國際標準規範。ISO/IEC 27001

主要起源於 1995 年廣泛應用於資訊安全管理的英國 BS7799 標準，由 BS7799-2 規範延伸整合而成。ISO/IEC 27001 於 2013 年 9 月 25 日作了第一次改版。

ISO/IEC 27001 的要求屬通用的，旨在適用於不論其類型，規模或性質的所有組織。ISO/IEC 27001 提供技術及供應商中立的管理系統架構，使組織能確保其本身的資訊安全措施是有效的。包括組織本身和其利益相關者資訊的持續可用性、保密性和完整性以及法律法規符合性。ISO/IEC 27001 規定在建立、實施、維護和組織的框架內，不斷改善資訊安全管理系統的要求。包括用於根據組織的需要進行資訊安全風險評估和矯正。

ISO/IEC 27001 結構與其他管理系統的標準相容，如 ISO 9001 和 ISO 14001。雖有一些條款編號不盡相同，其共同要素包括文件化、審查和稽核要求，使組織能夠開發形成一整合的管理系統。

- **適用範圍**

ISO/IEC 27001 涵蓋各類型的組織（例如：商業企業、政府機構及非營利組織），規定在組織整體營運風險內建立、

實作、運作、監視、審查、維持及改進已文件化之 ISMS 要求。其規定依據個別組織或部分單位之需求，量身打造安全控制措施的實作要求。

- **重點摘要**

國際標準組織 ISO 自 2005 年發佈 ISO/IEC 27001 以來，為因應企業組織不同的需求及挑戰，陸續制定資訊安全的相關的指引提供參考。因此資訊安全在 ISO 的標準中也形成了 ISO/IEC 27000 一系列的標準或指引。例如已經公佈的 ISO/IEC 27002 : 2013 (Information technology -- Security techniques -- Code of practice for information security controls)、ISO/IEC 27010 : 2012 (Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications)、ISO/IEC 27011 : 2008 (Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002)、ISO/IEC 27031 : 2011 (Information technology -- Security techniques -- Guidelines for information

and communication technology readiness for business continuity) …等，其中 ISO/IEC 27001 是 ISO/IEC 27000 系列中最重要之驗證標準。ISO/IEC 27001 是一份驗證要求之標準，規範了 ISMS (Information Security Management System) 之建立實施與文件化之具體要求，以及依據個別組織的需求規定要實施之安全控制措施的要求。

ISO/IEC 27001 在 2013 年作了第一次之改版，新版本與原 2005 年版一樣分成「本文」及「附錄 A」兩個部份，「本文」的部份共分成 0~10 共 11 個條文，主要規範了組織的建立、實作、維持，及持續改善 ISMS，並適度運用資訊科技，落實執行管理規範。新版本(2013 年版)的 ISO 27001，則考量許多企業組織不同的要求，導入一個以上的管理系統(如：資訊安全管理系統、品質管理系統…等)，卻常被不同系統間整合所困擾，故制訂新的架構(依據 ISO 組織的 Annex SL 要求- High level structure)。另有關於資訊安全風險評鑑與處理流程，新版標準則要求應與 ISO 31000 的原則與一般性指引相校準。

「附錄 A」的部份，主要係為 ISMS 的風險項目的控制目標與控制措施，原 2005 年版共分為 11 個資訊安全作業領

域、39 個控制目標、133 個控制措施。在 2013 年版則調整成 14 個資訊安全作業領域、35 個控制目標、與 114 個控制措施。其中與本研究範圍比較相關的部份為「A.14 營運持續管理 (2005 年版)」，在 2013 年版則調整為「A.17 營運持續管理的資訊安全層面」，此調整係因 2012 年版「ISO 22301 社會安全-營運持續管理系統-要求」的頒行，讓 ISO 27001 中對 BCM 的要求聚焦在資訊安全層面。

因此，2013 年版的「A.17 營運持續管理的資訊安全層面」下的控制目標調整成兩項：「A17.1 資訊安全持續性」與「A17.2 複式措施 (Redundancies)」。「A17.2 複式措施 (Redundancies)」主要是要求確保資訊處理設施的可用性，其控制項目「A.17.2.1 資訊安全處理設施的可用性」則要求資訊處理設施應以複式措施來實作，以充分符合可用性要求。

## **2. ISO/IEC 27002 : 2013 Information technology - Security**

### **Techniques - Code of Practice for Information Security Controls**

(資訊技術 - 安全技術-資訊安全管理之作業規範)

- 標準簡介

ISO/IEC 27002 是由發表於 1995 年代中期的英國標準 BS7799 所延續發展而來。ISO/IEC 於 2000 年採用 BS7799-1 成為 ISO/IEC 17799：2000，並在 2005 年時第一次更新。2007 年時重新編號以便與其他 ISO/IEC 27000 系列一致化。ISO / IEC 27002 於 2013 年 9 月 25 日作了第二次改版。

ISO/IEC 27002 提供了一種用來初始化的最佳實務，包括考慮組織的資訊安全風險環境控制的選擇、實施和管理的指導方針。

- **適用範圍**

ISO/IEC 27002 主要設計用來擬訂組織 ISO/IEC 27001 實施時，資訊安全管理系統程序控制的選擇、資訊安全控制、以及開發自己的資訊安全管理指導方針。

- **重點摘要**

ISO/IEC 27001 是驗證標準，而 ISO/IEC 27002 則為 ISO/IEC 27001 驗證標準的實施指引，提供建立和管理 ISO/IEC 27001 一個有效的資訊安全管理系統（ISMS）指導原則。ISO/IEC 27002 的章節條款可直接對應到 ISO/IEC 27001 附錄 A 的章節條款，並在每個章節條款提供細部的實

施準則參考或說明。ISO 27002：2013 標準的各章節重點請參考本文前節 ISO/IEC 27001：2013 之重點摘要。

### **3. ISO/IEC 27031：2011 Information Technology - Security Techniques - Guidelines for Information and Communication Technology Readiness for Business Continuity**（資訊技術-安全技术-營運持續的資通訊技術準備指南）

- **標準簡介**

ISO/IEC 於 2011 年發布 ISO/IEC 27031 營運持續的資通訊技術（ICT）準備指南。ISO/IEC 27031 主要基於 2008 年的英國 BS 25777 實務準則，由 BS 25777 規範延伸整合而成的國際標準。

ISO/IEC 27031 主要說明營運持續的資通訊技術的準備概念和原理，並提供方法和過程架構來識別，指定各流程（如效能準則、設計、實施）用以提高企業資通信技術的準備，以確保業務的持續性。其適用於任何組織發展其營運持續計畫的資通訊技術準備，要求其 ICT 服務/基礎設施做好準備，以因應可能影響關鍵業務持續營運所出現的事件、事故，以及相關業務中斷（包括安全性）。ISO/IEC 27031 同時為

ISO/IEC 27000 系列標準之一，可從營運持續方面對資訊安全管理系統（ISMS）進行深化與完善。

- **適用範圍**

ISO/IEC 27031 適用所有類型的組織，從 ICT 為營運持續支援的角度，提供了 ICT 的準備指南，ISO/IEC 27031 的範圍包括可能對 ICT 基礎設施和系統影響的所有事件和事故（包括安全相關）。其包括和延伸的資訊安全事故處理和管理、資通訊技術準備計畫和服務等實務。

- **重點摘要**

ISO/IEC 27031 係為資訊安全管理系統（ISMS）與業務持續性管理系統（BCMS）的實施和操作的一部分，主要制定和實施有關 ICT 服務的準備計畫，以確保關鍵重要業務的持續性。為使組織能夠實現 ICT 業務持續性，IRBC（ICT Readiness for Business Continuity）需要放在一個管理系統的過程中，以預防、預測和管理 ICT 破壞或具有破壞 ICT 的潛在事件。ISO/IEC 27031 仍沿用 PDCA（Plan - Do - Check - Action）循環的過程。透過 PDCA 循環過程的 IRBC 運行，以保持 ICT 服務的彈性，並確保事件不會演變成災難，

以及當災難發生時，ICT 服務可以復原到組織 BCM 要求或約定的復原期限。

表格 1 IRBC 的 PDCA 循環

<b>Plan</b>	依照組織的整體業務持續性的政策和目標，和 ICT 相關的風險管理與改善的結果，建立 IRBC 政策、目標、指標與程序。
<b>Do</b>	實施和運行 IRBC 政策、控制、流程和程序。
<b>Check</b>	評估及衡量 IRBC 政策、目標、實施過程和實施的績效，並將結果報告給管理層進行評審。
<b>Action</b>	將管理審查的結果，採取矯正和預防措施，以持續改善 IRBC。

資料來源：ISO/IEC 27031：2011

ISO/IEC 27031：2011 強調 ICT 整備的概念與原則，提供了方法與過程的架構，以鑑別與說明資訊安全的各個面向，例如組織改善 ICT 整備的績效衡量指標、設計及實施等。並要求需符合組織 BCMS 和 ISMS 的需求，因此將 IRBC 的 PDCA 循環與 BCMS 的 PDCA 模組整合（參閱圖 2）。

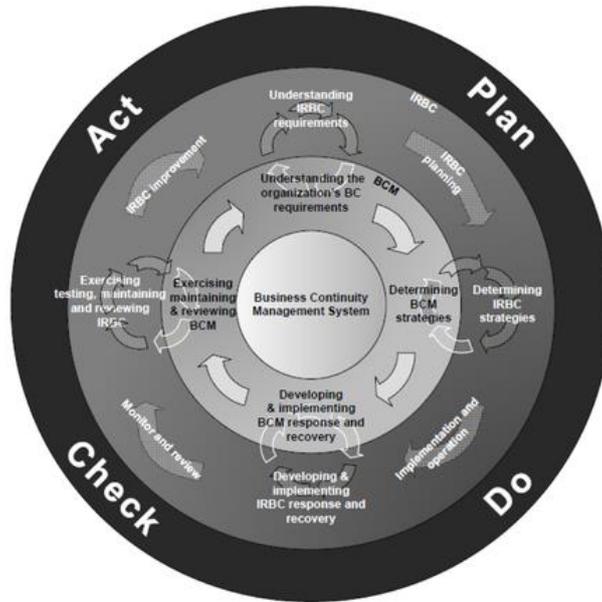
ISO/IEC 27031 與 ISO/IEC 24762 的差異在於，ISO/IEC 24762 的重點在於 DR 供應者應該解決的技術問題。而

ISO/IEC 27031 是比較高層次的框架，描述在 IT 的 DR 活動中，作為一個企業級的營運持續計畫的一部分。ICT 的準備對於業務持續性的目的很重要的，因為：

- ICT 是普及的，許多組織都高度依賴於 ICT 支持的關鍵業務流程。
- ICT 本身還支持業務持續性，災難和緊急應變，以及相關的業務管理流程。
- 一般業務持續性計畫可能未完整充分的考慮和保護 ICT 的可用性和持續性。

ICT 的準備包括：

- 對於不可預見之環境風險，和影響 ICT 與其相關業務的持續性的事件，組織應事先準備 ICT（即 IT 基礎架構，操作和應用程序）與其相關的流程和人員。
- 利用業務連續性管理活動和 ICT 安全事件因應的資源，精簡災難復原與緊急應變。



資料來源：ISO/IEC 27031：2011

圖 2 整合 IRBC 與 BCMS 的 PDCA 模組

ISO/IEC 27031:2011 內容共分成 0-9 條之主章節條文，以及四個附錄（附錄 A-D），內容架構如下：

- 引言（Introduction）
- 範圍（Scope）
- 引用標準（Normative references）
- 用語與定義（Terms and definitions）
- 名詞簡稱（Abbreviated terms）
- 概述（Overview）

◆ IRBC 在業務持續性管理的角色。

- ◆ IRBC 的原則。
- ◆ IRBC 的要素。
- ◆ IRBC 的成果和收益。
- ◆ 建立 IRBC。
- ◆ 使用 PDCA 來建立 IRBC。
- ◆ 管理職責。
- ◆ 管理層的承諾。
- ◆ IRBC 策略。

➤ IRBC 規劃 (IRBC Planning)

- ◆ 概述。
- ◆ 資源。
- ◆ 定義需求。
- ◆ 確定 IRBC 策略選項。
- ◆ 停止活動。
- ◆ 提高 IRBC 能力。

- ◆ ICT 就緒執行準則。

- 實施和運行 (Implementation and Operation)

- ◆ 概述。

- ◆ 實施 IRBC 策略的關鍵要素。

- ◆ 事件回應。

- ◆ IRBC 規劃文件。

- ◆ 意識、能力和培訓方案。

- ◆ 文件控制。

- 監控與評審 (Monitor and Review)

- ◆ 維持 IRBC。

- ◆ IRBC 內部稽核。

- ◆ 管理評審。

- ◆ ICT 就緒執行準則的測量。

- IRBC 的改善 (IRBC Improvement)

- ◆ 持續改善。

◆ 矯正措施。

◆ 預防措施。

➤ 附錄 A（資料性附錄）中斷時的 IRBC 和時間表

➤ 附錄 B（資料性附錄）高可用性嵌入式系統

➤ 附件 C（資料性附錄）評估故障情況

➤ 附錄 D（資料性附錄）開發執行準則

#### **4. ISO/IEC 24762 : 2008 Information Technology - Security**

##### **Techniques - Guidelines for Information and Communications**

##### **Technology Disaster Recovery Services（資訊技術-安全技術-資訊和通訊技術服務的災難恢復指南）**

- 標準簡介

ISO/IEC 24762 主要是規範第三方機構應提供資通訊災難復原服務的標準。有別於其他 ISO/IEC 27000 系列標準都是由英國標準延伸而成 ISO/IEC 標準，ISO/IEC 24762 主要基於 2005 年新加坡的 SS 507 國家標準，由 2007 年版的 SS 507 規範延伸整合而成的國際標準。此外，新加坡標準 SS 507 是一個國家認證的標準，目前一些組織在新加坡已經通過該

認證，ISO/IEC 24762 目前仍定義為一套國際標準的準則。

SS 507 當初係因 SARS 事件（2003~2004 年間），使得營運持續計畫中供應商的 DR (Disaster Recovery) 服務（包括品質、完整性、可用性）面臨衝擊，也造成新加坡經濟衰退。因此新加坡在 2005 年發布了 SS 507 標準，以確定服務供應商的可靠性和生存能力，經由取得認證，以確認其提供 DR 服務的保證。

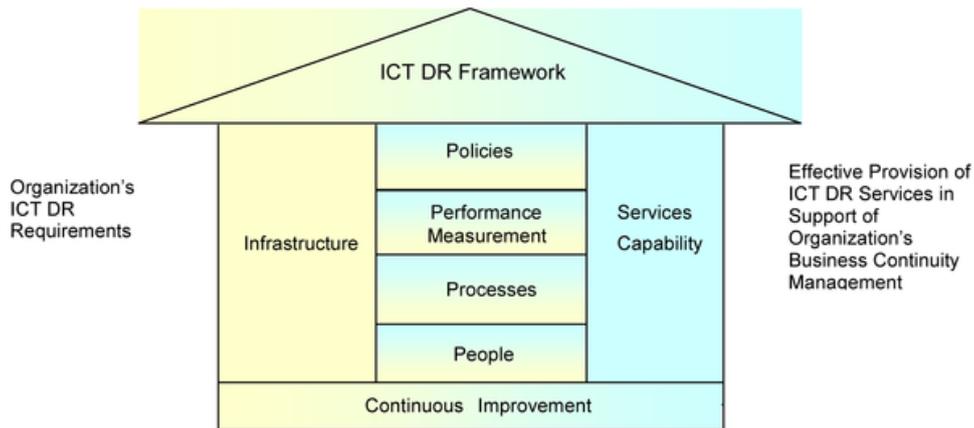
ISO/IEC 24762 提供營運持續管理，同時適用於“內部”和“外包”資通信技術災難恢復服務，另一部份也對設施供應商提供資通訊技術的災難恢復（DR ICT）服務的指南，這些指南包括建築施工、安全措施、提供基礎設施服務，如電力、水、電信和環境控制。相反的，另一種 ISO/IEC 27031 標準，重點在於組織最終的 IT (Information Technology) 災難恢復。比較以此兩個標準，ISO 24762 重點在於 DR 供應商應該解決的技術問題。而 ISO/IEC 27031 則是一個比較高層次的框架，描述在 IT 的 DR 活動中，作為一個企業級的營運持續計畫的一部分。

- **適用範圍**

ISO/IEC 24762 規定 DR 服務和設施相關資訊技術的實施、運行、監控和維護。外包資訊技術災難恢復服務供應商應該具備和實踐提供基本的安全操作環境，並促進組織的恢復工作的能力、選擇恢復地點的指南、和指導資訊技術災難恢復服務供應商，不斷提高他們的資訊技術的 DR 服務。

- **重點摘要**

ISO/IEC 24762 規範了 DR 服務和設施的資訊和通信技術的實施、運行、監控和維護的要求。主要是為業務持續運作管理中有關資訊服務的災難復原提供指南。ISO/IEC 24762：2008 考慮 ICT DR 服務提供係由不同的要素組成，故定義了 ICT DR 的架構（如圖 3）。ISO/IEC 24762 以 ICT DR 架構中結構層的綜合觀點、成本效益和考慮標準要求之間的平衡，所訂定出的資訊和通信技術服務的災難恢復指南。



資料來源：ISO/IEC 24762：2008

圖 3 ICT DR 的架構

ISO/IEC 24762：2008 共分成 0-9 條之主章節條文，各條文摘要重點如下：

➤ 介紹 (Introduction)：ISO/IEC 24762：2008 規範 ICT DR

係屬業務持續性管理，是整體性風險管理不可分割的一部份。並透過以下活動來保護組織的關鍵利益、聲譽、品牌和增值包括：

◆ 確定可能對組織的運作造成不利影響的潛在威脅以及相關的風險。

◆ 為組織提供強化業務持續運作的架構。

◆ 提供有效應對災難和失效所需的能力、設施、流程、緊急工作組名單等。

➤ 範圍 (Scope)：ISO/IEC 24762 規範了 DR 服務和設施相

關資通信技術的實施、運行、監控和維護的要求（包括內部或是外包）。

➤ 引用標準（Normative references）包括：

◆ ISO/IEC 27001：2005，Information technology — Security techniques — Information security management systems — Requirements

◆ ISO/IEC 27002：2005，Information technology — Security techniques — Code of practice for information security management

➤ 用語與定義（Terms and Definitions）：以本標準為目的的用語與定義。

➤ 名詞（Abbreviated terms）：名詞簡稱定義，例如：

◆ ICT DR 資訊和通信技術災難復原。

◆ UPS 不斷電系統。

◆ SLA 服務水準協議。

◆ DBA 資料庫管理員等等。

➤ ICT 災難復原（ICT Disaster Recovery）：本章節主要敘

述不論是內部或是外部提供的 ICT DR 服務，應參照以下條款所規範的項目，作為最佳實務方向的考量，包括：

- ◆環境穩定性：環境穩定性對 ICT 災難復原處所是很重要的，例如人員的旅途、人員的安全、公用設施等等，都可能受環境的不穩定的影響。
- ◆資產管理：ICT DR 服務提供者應該確保在其 ICT DR 處所的資產，能夠在組織需要時，可及時被識別、定位與檢索。
- ◆場所的相鄰性（距離）：不受與主場所同一災難/失效影響的地理位置為要求。
- ◆廠商管理：ICT DR 服務提供者應該建立程序以確保從其供應商獲得重要設備的支持。
- ◆外包作業：ICT DR 服務提供者應與其廠商訂定臨時或是長期的外包作業。
- ◆資訊安全：ICT DR 服務提供者應確保不損害組織的資訊安全，並且為為此可能需進行額外投資以隔離或保持組織的資訊安全。

- ◆ 災難復原計畫的啟動與解除：ICT DR 服務提供者應與組織共同建立啟動和解除 ICT DR 服務的條件與程序。
  - ◆ 培訓與教育：ICT DR 服務提供者應與組織向所有服務提供方員工、任何相關的組織員工進行培訓計畫，尤其是對新進員工的適當培訓，以確保其能夠稱職的承擔與履行工作職責。
  - ◆ ICT 系統的測試：ICT DR 服務提供者應確保災難復原的所有核心 ICT 系統都進行定期測試，以確保其持續維持 DR 計畫的能力。
  - ◆ ICT DR 服務供應者的 BC：ICT DR 服務供應者應確保能適當處理其自身的業務持續性，包括災難復原和要求。
  - ◆ 文件和定期審查：所有方針、計畫和條款應該形成文件，並確保每一文件經過審查與定期更新。
- ICT 災難復原設施( ICT Disaster Recovery Facilities )：  
本章節主要規範提供組織復原工作的實體運作環境的基本要求，包括環境控制、通訊、持續的電源和非復原工作的生活設施。考量的項目包括：
- ◆ 復原場所地點：復原場所地點可能具有某些難以接受的

脆弱點，意味經過設計和裝配的復原場所具有不可降低的殘餘風險。

- ◆實體門禁控制措施：保護復原場所的關鍵要素是實體門禁控制，重要的是在建築物的所有出入口設置和維護實體控制措施。
- ◆實體設施的安全：應根據風險評鑑的結果，設置實體安全控制措施和程序，以保護電子資訊系統、建築物和設備避免受未經授權的實體改變或是損壞。
- ◆專用區：應制訂在組織復原期間存放設備和使用所需的專用區域/房間的規定。
- ◆環境控制：ICT DR 服務供應者應該確保設置有保護電子資訊系統、設備和實施免受天然災害和/或環境災害影響的方針和程序。
- ◆通訊：通訊為復原場所與外部之間提供關鍵的聯結。應該確保送出/送達復原場所的所有訊息（包括語音、資料、視訊…），可及時、有效、不受中斷和維持品質的傳送，並且應防止竊聽。
- ◆電源：所有資訊設備的正常的運作，需依賴持續而穩定

的電力供應。

- ◆佈線管理：ICT DR 服務供應者應採取保護所有輸送電力以及電子訊息的線路，免受外界損壞和干擾的措施。
- ◆消防：ICT DR 服務供應者應設置合適的消防系統，以保護復原場所的資訊設備和人員。
- ◆緊急運作中心（EOC）：ICT DR 服務供應者在復原場所提供 EOC，並配備合適的設備，以使組織在災難或失效發生時，能夠管理與維持與其業務部門與外界各方的溝通。
- ◆禁區：ICT DR 服務供應者應該確保設施得到相對應級別的保護，只允許預定目的並經授權的訪問進入。
- ◆非復原用的生活設施：ICT DR 服務供應者應該確保在復原場所所需的設施與設備之外，對在復原期間進駐其處所的員工提供生活和福利所需的設施。
- ◆實體設施和支援設備的生命周期：ICT DR 服務供應者應透過設施和設備的生命周期的管理，確保所有實體設施和支援設備持續適合於預定目的。

◆測試：ICT DR 服務供應者應該確保測試構成設施和設備具備所要求的高品質條件。

➤外包服務供應商的能力（ Outsourced Service Provider’ s Capability）：組織應對其外包 ICT DR 服務供應者，進行組織所要求的基本能力，包括：

◆審查組織業務復原狀態。

◆設施要求。

◆專業技能。

◆邏輯訪問控制。

◆ICT 設備和運行的準備。

◆支援同時進行復原的能力。

◆服務級別。

◆服務類型。

◆服務的相鄰性。

◆共享服務的訂購比例。

◆啟動所訂購的服務。

- ◆組織的測試。
- ◆能力的變化。
- ◆緊急應變計畫。
- ◆自我評估。

➤ 復原場所的選擇 (Selection of Recovery Sites): ICT DR 服務供應者應在外部環境的穩定基礎、地理位置內良好的基礎設施、和具當地熟練的人工的可用性，建立和運行其復原場所的有利設施。考量的項目包括：

- ◆基礎設施。
- ◆熟練的人力與支援。
- ◆大量集中的廠商與供應商。
- ◆本地 ICT DR 服務供應者的紀錄。

➤ 持續改善 (Continuous Improvement): ICT DR 服務供應者應該持續透過追蹤 ICT DR 發展趨勢、績效量測、可擴展性的規劃與持續的風險消滅，持續改善其服務。

### (三) 國際通信聯盟 (International Telecommunication Union, ITU)

國際通信聯盟(International Telecommunication Union, ITU)的成立和發展，和電信科技的發展如影隨形。ITU 主要負責確立國際無線電與電信的管理制度和標準。其前身是 1865 年 5 月 17 日在巴黎創立的國際電報聯盟，是世界上最悠久的國際組織。主要任務是制訂標準、分配無線電資源、組織各個國家之間的國際長途互連方案。ITU 也是聯合國的一個專門機構，總部設在瑞士的聯合國日內瓦辦事處。ITU 制訂的國際標準一直被稱作「建議」(RECOMMENDATIONS)，由於 ITU 具備國際組織的長期性和聯合國的特別機構的特殊地位，ITU 發布的標準，比大多數其他同一級別的技术規範制定組織擁有更高的國際認同度。作為聯合國的機構，所有聯合國的成員國都可以是 ITU 成員，他們也被叫做「成員國」。公司和其他組織可以按照「部門成員」或者「聯盟者」身份加入，這兩種成員資格都可以直接參與標準的制定(此與 ISO 組織不同)。ITU 不同的下屬部門還與其它組織保持「聯絡關係」。

#### **1. ITU-T L.1300 (11/2011) SERIES L: CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT - Best Practices for**

## **Green Data Centers (L 系列：建築，安裝和保護外部纜線及其他外部設備 - 資料中心綠能最佳實務)**

- **標準簡介**

ITU-T L. 1300 旨在描述降低 Data Center(DC)對環境、氣候負面影響的最佳建議與做法。尤其人們普遍意識到，DC 未來可能不斷增加對環境的影響時，ITU-T L. 1300 定義的最佳實務應用，可以幫助組織和管理人員透過打造未來或改進現有的 DC 方式，進行達成對環境保護的責任，ITU-T L. 1300 的最佳建議與做法有助於降低 ICT 對環境及氣候變化的影響。

- **適用範圍**

ITU-T L. 1300 為發展綠能 DC 的最佳實務。其綠能的定義為：被設計為最大能源效率和對環境影響最小。ITU-T L. 1300 對於綠能 DC 的建設和運營提供了一套規則，包括先進的策略和技術，以進行改造現有的 DC，或者計畫、設計或興建未來新的 DC。

ITU-T L. 1300 最佳實務包括建議：DC 的利用率、管理和規劃、DC 設備和服務、DC 的空調、C 的電力設備、DC 的

建設、與 DC 監控。

- **重點摘要**

ITU-T L.1300 最佳實務旨在發展綠色 DC 的最佳實務。綠色 DC 可以被定義為機械、照明、電力和計算機等系統被設計為最大的能源效率和對環境影響最小的資料儲存、管理和傳送的 DC。綠色 DC 的建設和營運包括先進的技術和策略。ITU-T L.1300 提供了一套規則，包括先進的策略和技術，以進行改造現有的 DC，或者計畫、設計或興建未來新的 DC。

建議的最佳實務包括：

- DC 的利用率，管理和規劃。
- ICT 設備和服務。
- 冷卻。
- DC 的電力設備。
- DC 的建設。
- 監控。

ITU-T L.1300 建議書有關綠色 DC 的最佳實務的建議內容，主要敘述於 Clause 6 - Clause 13，並在各條款中提

供了共 151 條的節能最佳實務參考，各條款的重點摘要如下：

- 綠色數據中心的最佳實務的介紹 (Introduction to Best Practices for Green Data Centres)：為了提高 DC 的能源效率，從設計到施工所有階段，都有有必要考慮能源效率問題，即使在 DC 的建設已經完成，仍必須繼續進行管理和維護，以確保高效的能源利用。ITU-T L.1300 建議書描述了節能的建設、營運和基本組件，包括 ICT 設備和服務、冷卻、電力設備，DC 建築物等綠色 DC 管理的最佳實務。
- DC 的規劃、利用與管理 (Planning、Utilization and Management of Data Centres)：對於維持一個 DC 的經濟效率和環境效益來說，訂定一個全面的策略與管理方法是非常重要的。其中應考慮包括：
  - ◆ 組織團體的參與。
  - ◆ 一般政策。
  - ◆ 彈性的水平和供應。
- ICT 設備與服務 (ICT equipment and services)：IDC

對電力和冷源起於 ICT 設備，規範 ICT 設備的使用，將可以增加有效的能源供應，降低電力消耗和冷卻的使用。為了確保設備能夠在有較大範圍之溫濕度環境內操作，應考慮以下的管理措施：

- ◆選擇新的 ICT 設備。
- ◆選擇新的電信設備。
- ◆新的 ICT 服務部署。
- ◆新電信服務的部署。
- ◆現有的 ICT 設備和服務管理。
- ◆數據管理。

➤ 冷卻 (Cooling)：DC 的冷卻經常是最消耗能量的，因此要提高 DC 的節能效率，降低冷卻的影響是最明顯的方向。

因此可考慮以下方案：

- ◆氣流的設計和管理。
- ◆散熱管理。
- ◆溫濕度設定 (免費和節約冷卻、高效率的冷卻裝置)。

◆ 機房空調。

◆ DC 餘熱的再利用。

➤ DC 的電力設備 (Data Centre Power Equipment) : DC 其他主要的基礎設施的功率調節和輸送系統。包括 UPS、配電盤、佈線和備用發電機等設備。因此可考慮以下因素：

◆ 電力設備選擇和部署。

◆ 電力設備的管理。

➤ 其它 DC 設備 (Other Data Centre Equipment) : 能源也可能消耗在非用於 DC 建築、在辦公室、存儲空間的地方。在非 DC 領域的能源效率應根據建築有關的標準，如歐盟相關標準，LEED，BREEAM 等進行優化。

➤ DC 的建築物 (Data Centre Building) : DC 建築物的位置和實體佈局對於實現靈活性和效率是非常重要的。例如新鮮空氣冷卻的技術需要顯著實體設備空間及通風空間，現有的建築物可能就無法滿足。DC 的建築物的節能方案應考慮：

◆ 建築物實體的佈局。

◆建築物的地理位置。

➤ 監控 (Monitoring)：以能源監測和報告管理策略的制定和實施為核心，經營一個高效能的 DC。監控的項目包括：

◆能源利用和環境測量。

◆能源利用和環境收集的記錄。

◆能源利用和環境報告。

◆ICT 報告。

➤ 網路的設計 (Design of network)：此包含了 DC 與 DC 之間的網路設計的要求、與連接設備規範。

## 二、先進國家異地備援相關規範

### (一) 美國

#### 1. 聯邦政府資訊系統營運持續計畫指引

美國國家標準技術研究所 (National Institute of Standards and Technology, NIST)，前身為國家標準局 (NBS, 1901 年~1988 年)，是一國家測量標準實驗室，屬於美國商務部的非監管機構。NIST 總部位於馬里蘭州的蓋瑟斯堡，在科羅拉多州的博爾德市亦有分部運作。主要活動為組織實驗室研究計畫和校外研究計畫。自 2010 年 10

月 1 日起，NIST 縮減所屬的 10 間實驗室為 6 間。其分別為：工程實驗室、資訊科技實驗室、材料測量實驗室、物理測量實驗室、奈米科技中心、NIST 中子研究中心。

NIST 內部約有 2,900 名科學家、工程師、科技工作者，以及後勤和管理人員，外部約有 1,800 名（來自美國公司和國外的工程師和研究員），另外還有 1,400 名專家分佈在美國約 350 個附屬研究中心。該研究所的主要任務為：促進美國的創新和產業競爭力，推展度量衡學、標準、技術以提高經濟安全並改善我們的生活質量。

- 標準簡介

NIST Special Publication 800-34 Rev.1 -  
Contingency Planning Guide for Federal Information  
Systems（聯邦政府資訊系統營運持續計畫指引）

NIST Special Publication 800-34 Rev.1 為美國聯邦政府資訊科技系統緊急應變規劃指引，內容主要涵蓋資訊系統營運持續計畫的說明、建議、注意事項與考量因素。使用者可以參考 NIST SP800-34 Rev.1 進行資訊系統的營運持續計畫與災難復原計畫制定。此外，此份指南也針對異地備援機制的資料備份和系統備援的部份，提供了適用的技術規範

與具體建議策略。

- **適用範圍**

提供給美國政府部門或民間企業，作為資訊科技系統緊急應變規劃指引。

- **重點摘要**

- **營運衝擊分析 (BIA)**

營運衝擊分析的目的是為了連結特定的系統模組和其所提供服務，透過這些資訊進一步了解產生系統中斷服務的原因，因此需將營運衝擊分析的結果對應到各單位組織的 COOP、BCP 和 BRP 的分析和策略制定的項目上。

在完成營運衝擊分析須具備以下三項條件：

- ◆ **確認復原時間和備援等級。**以其服務中斷和停電影響，來預估停機時間。停機時間表示其單位組織可以忍受最大停機時間。
- ◆ **確認資源需求。**需盡快恢復其服務功能，因此必須把設施、人員、設備、軟體、資訊文件等重要紀錄進行全面性的資源評估。

◆ 確定系統資源復原優先層級。依據先前業務結果和系統

資源對應到其備援等級，依序恢復其服務功能。

表格 2 NIST SP 800-34 營運衝擊分析表

項 目	說 明
制定應變計劃政策	<ul style="list-style-type: none"> <li>● 確認法令或監控要求。</li> <li>● 制定 IT 應變計劃的政策說明。</li> <li>● 呼應 FIPS199。</li> <li>● 發布政策。</li> </ul>
進行營運衝擊分析	<ul style="list-style-type: none"> <li>● 確認業務流程及恢復的重要性。</li> <li>● 找出停電的影響及評估停機時間。</li> <li>● 確認需求資源。</li> <li>● 確認系統恢復的優先等級。</li> </ul>
找出預防控制措施	<ul style="list-style-type: none"> <li>● 識別控制。</li> <li>● 實施控制。</li> <li>● 維持控制。</li> </ul>
建立應變策略	<ul style="list-style-type: none"> <li>● 備份與恢復。</li> <li>● 研究 FIPS199。</li> <li>● 確認角色及其職權。</li> <li>● 備援機房地址。</li> <li>● 確認設備及成本的考量。</li> <li>● 導入系統架構。</li> </ul>
制定應變計畫	<ul style="list-style-type: none"> <li>● 恢復策略文件。</li> </ul>
測試計劃、教育訓練及演練	<ul style="list-style-type: none"> <li>● 測試計劃。</li> <li>● 人員培訓。</li> <li>● 演練計劃。</li> <li>● TT&amp;E 活動。</li> </ul>
維護計畫	<ul style="list-style-type: none"> <li>● 重新檢視及更新計畫。</li> <li>● 協調內部/外部組織</li> <li>● 控制分布。</li> <li>● 更改文件。</li> </ul>

資料來源：NIST SP 800-34

## ➤ 備援與復原策略

在制定備份與復原策略中，應考量到迅速且有效地恢復其中斷時的系統。制定時應考量成本、最大停機時間、安全性、復原等級與整體積分組織等級的備援計畫，表格 3 是一個範例可用來協助確定 FIPS 其災難復原等級、備份和恢復策略。

表格 3 FIPS 199 備份範疇及策略

	災難復原等級	備份/復原策略
低	當服務中斷時尚未對單位組織造成任何影響與損害。	備份：磁帶備份 復原策略：搬遷或冷備援站
中	當服務中斷時會對單位組織的網路或系統造成中度影響與損害。	備份：光學媒體備份，同步備份 復原策略：冷備援站或暖備援站
高	當服務中斷時會對單位組織的網路或系統造成重度影響與損害。	備份：鏡像站，磁碟備份 復原策略：熱備援站

資料來源：NIST SP 800-34

## ➤ 備援中心

雖然重大傷害很少發生，但對於所有高風險的系統，在計畫中應考量復原及備援設備長時間運作相關等策略，一般來說有下面幾種類型的備援中心可以提供選擇：

- ◆冷備援站：通常有足夠的空間和基礎設備(電力、電信、環境控制)，以支援資訊系統進行恢復。
- ◆暖備援站：通常有部分設備及足夠的辦公空間，包含些系統所需的軟硬體，及部分或全部的電信及電力資源。
- ◆熱備援站：通常會配置適當的設備來支持系統的需求，並且配置必要的系統硬體及基礎設備與技術人員。
- ◆行動備援站：通常包含特制的電信設備及系統設備，並且架設於運輸交通工具。
- ◆鏡像備援站：通常有完整的設備並且自動執行資料鏡像備份，且鏡像備援站與主要機房擁有相同的技術。

表格 4 可以做為選擇備援中心評估的參考，備援中心的選擇應該由組織進行分析，包含應考慮企業影響及營運衝擊分析中定義停機時間等相關因素，選擇適當的備援中心來符合組織的要求標準。

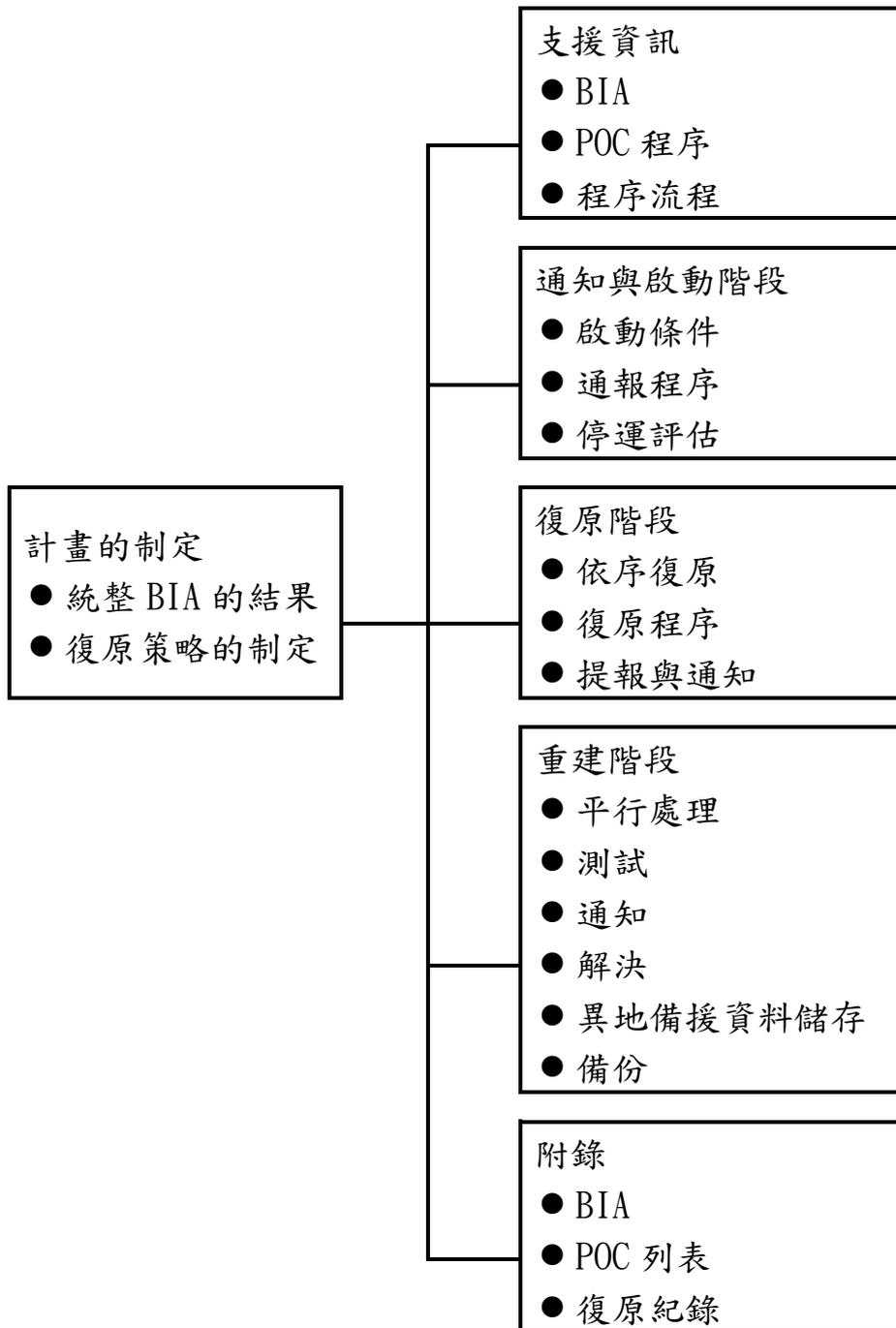
表格 4 NIST 備援中心評估的參考

	成本	硬體需求	電信	建置時間	位置
冷備援站	低	無	無	長	彈性
暖備援站	中	部分	部分/完整	中	彈性
熱備援站	高	完整	完整	短	彈性

資料來源：NIST SP 800-34

➤ 復原計畫制定

復原計畫制定中應包含詳細的職權、責任、團隊與資訊系統中斷後的復原程序。復原計畫的制定用來支援復原過程的技術準則，復原計畫需要在詳細度和靈活運用程度間取得平衡；通常計畫制定越詳細，其執行時就會越缺乏彈性和通用性。在這份文件中提供的復原計畫制定是屬於指導性，各單位組織需要制定成符合所需並滿足其特定的系統與操作需求的版本。復原計畫制定的格式必須能夠讓不熟悉的人員進行復原操作時有快速明確的指導。計畫應明確、簡潔、容易在緊急情況下執行。復原計畫的五個主要部分如圖 4 所示。



資料來源：NIST SP 800-34

圖 4 NIST 持續運作制定流程

➤ 應變計畫的技術考量

◆ 共同需要的考量

- 使用 BIA 彙整的相關資訊。
  - 資料上的安全與整合性及備份策略和程序的發展。
  - 保護相關設備及系統資源。
  - 堅持遵循 NIST SP 800-53 的規範。
  - 備援機房適當的電源管理系統與環境控制。
  - 將線上運作的系統導入高可用度的系統與備用系統資源做結合。
- ◆ 備份與維護資料的安全性、完整性：備份與維護資料的安全性及完整性是應變計畫的重要關鍵所在，資料備份應定期的對所有相關系統進行備份，系統備份可備份於個人電腦或是其他集中化的儲存設備如 NAS 或 SAN 上，執行系統備份有三種常見的方法。
- ◆ 完整備份：完整的備份應該包括磁碟上所有的檔案或是所選的資料夾上的所有文件，因為所有備份的檔案都存放在單一的備份媒體或是許多個備份媒體上，所以如果要尋找特訂的文件會比較簡單的。相對的，要執行完整備份所需的時間相對的比較久，如果文件經常不會變

動，完整備份可能會造成資料過多浪費許多不必要的空間。

◆遞增備份：增量備份會針對上次備份後，所有後來變動的資料去做備份，在做備份的時間相對的縮短，當需要從增量備份回復系統的話可能需要從不同的備份媒體進行恢復。例如，如果今天需要恢復某特定的目錄，則需要將完整備份和之前所做的所有增量備份來恢復原有目錄。

◆差異備份：差異備份根據完整備份的資料以後所新增或是修改過的文件，因此如果一個文件在之前的完整備份有修改過的話，那差異備份將會備份之後的所新增或是修改過後文件，差異備分相對的比完成備份的時間少了許多。差異備份在恢復資料上，比起增量備份所需的備份媒體相對的少，因差異備份只需要上次的完整備份及上次做的差異備份方可還原。

因此，組織可以根據系統配置和恢復的需求來選擇不同的備份方法，在思考如何規劃備份方法的同時也需要考慮到下列問題

- ◆儲存的資料要放哪裡，要用哪種儲存媒體儲存？
- ◆要備份什麼類型資料及多久要備份一次？
- ◆當發生緊急事件時候需要花多快的時間去檢索備份的資料？
- ◆誰可以檢索備份的資料？
- ◆誰可以從儲存的媒體恢復備份的資料？
- ◆備份的資料要保存多久？
- ◆有什麼儲存媒體的標籤格式？
- ◆怎樣的環境適合存放儲存媒體？
- ◆有什麼相對的備份方法適合在相對的儲存媒體？
- ◆用什麼方式傳送資料？

除了上述幾項之外，當選擇適合的備份解決方案也必須考慮下列相關問題：

- ◆儲存設備與系統的相容性是否良好：為方便恢復，備份的設備是否與應用程式及操作平台有良好的相容性，可以容易的安裝到不同型號或不同類型的系統。

- ◆磁碟的大小，為確保足夠的空間儲存資料，選擇儲存的空間時，應確定適當的備份方法。
- ◆儲存媒體的壽命，不應過度依賴特定的儲存媒體，因每種儲存媒體有其不同的使用方法與壽命。
- ◆備份軟體，當選擇適合的備份解決方案時，會有相對適合的備份軟體，在某些大型備份傳輸的情況，應該考慮軟體是否可以自動的完成備份動作。

備份媒體應存在安全的異地機房，當選擇異地機房位置，應該考慮多久可以到異地機房、如何方便存取備份媒體、儲存媒體的限制、以及多久測試備份媒體等相關問題，備援處理設施提供了一個地點提供原有單位當災害發生的時候，以便系統進行恢復，以下提供三種主要的類型：

- ◆冷備援站 (Cold Sites)：具備基本的基礎設施（如電器及空調）的位置，但是沒有軟硬體設備或通信設備，有足夠空間容納相關設備來維持系統運作。冷備援通常為較便宜的異地機房，當發生災害後需要採購相關設備且安裝測試，所以需要花費數周較長時間來進行恢復。

◆暖備援站 (Warm Sites)：暖備援站包含冷備援站的基礎設施，與冷備援站不同，它有硬體及通訊相關設備，但設備本身不會有相關的系統或是備份資料。平常這個機房可能為一個測試或開發用的機房，當發生災害後相關人員可以利用現有的設備重建系統進行恢復的動作，所需的時間取決於系統複雜度及備份資料多寡，相較冷備援站恢復的時間較短。

◆熱備援站 (Hot Sites)：熱備援站有較完整的軟硬體相關設備，設備上會有最新的系統與備份資料，在許多情況下，熱備援站的資料都與系統都與主系統及資料庫同步更新，在某些情況下，熱備援站會搭配主要機房作附載平衡，因為系統及備份資料與異地機房作同步，所需要花費建置的成本較高，但相對上述備援機房恢復的時間短少許多，可能只需要幾分鐘到幾小時，即可恢復運作。

對於資訊系統應變計畫中，相關人員規劃系統恢復策略應該從下面兩個角度進行技術上的考量。

◆完善的應變解決方案，討論突發狀況發生的因素及相關

技術。

- ◆應變解決方案的根本在於技術，並且用於實施應變策略。

表格 5 NIST 應變計畫需要考量及解決方案比較表

	桌上型電腦/伺服器	電信系統	大型主機系統
應變計畫考量			
將廠商本身資訊、系統及設定檔製作成相關文件	X	X	X
鼓勵員工進行備份	X		
討論應變計畫的解決方案與安全策略的關係	X	X	X
討論應變計畫的解決方案與系統安全控制的關係	X	X	X
考量與熱備援機房的互惠利益	X		X
與供應商進行協調		X	X
制定廠商的 SLAs (Service Level Agreements)	X	X	X

提供個人電腦資料備份的指導手冊	X		
對硬體、軟體及周邊設備作規範	X		
儲存備份媒體於 off-site	X	X	X
儲存軟體於 off-site	X	X	X
應變計畫解決方案			
對系統、應用程式及資料進行備份	X	X	X
確保元件之間操作相容性	X		
辨識單點故障		X	
製作硬碟映像檔	X		
在關鍵元件實施容錯			X
實施負載平衡	X		X
在重要的元件上實施備援	X	X	X
實施儲存的解決方案			X
整合無線相關技術及遠端存取	X	X	
複製資料	X		X
使用 UPS 不斷電系統	X		X

資料來源：NIST SP 800-34

## 2. TIA-942

TIA-942 是由美國國家標準學會(ANSI)於 2005 批准頒布的「資料中心電信基礎設施標準」(Telecommunications Infrastructure Standard for Data Centers)，是資料中心建築地點、功能指標、設計技術、施工方式、驗收標準等方面的具體技術要求與實現。TIA-942 是國際上第一部較為全面地以資料中心為標的的技術規範標準，為現代的機房工程建設提出了新的設計理念、系統架構與技術指標，並提供許多的技術與系統的工程建議與指導。

TIA-942 標準包括電信(Telecommunications:網路架構、佈線、佈纜、路由、備用電源、配線架等 12 項)、電力(Electrical:介接設施、電力引進、配管線、不斷電系統、發電機、儲油量、電力架構、抗諧波裝置、接地系統、緊急斷電設施、系統監控、電池配置、電池種類、動態不斷電系統、備用發電機系統架構、負載測試、設備維護等 68 項)、建築(Architectural:挑選環境位置、住戶、停車、結構、出入口、屋頂、門窗、大廳、管理室、警衛室、操作室、休息室、UPS 機房、進出貨區、門禁、監控、防火時效、閉路電視、耐震設計等 107 項)及機械(Mechanical:冰水系統、冷房系統、環控系統、配管、燃油系統、消防滅火系統等 35 項)四大評估架構總計 222 評估項目，確保業主依營運整體可靠度需求來設計資訊機房(共分 4 等

級 Tier1~4)，目前國際認證單位有 Uptime Institute 及 TIA 等。

在美國標準 TIA-942 資料中心電信基礎設施標準，主要是根據資料中心基礎設施的可用性 (Availability)、穩定性 (Stability) 和安全性 (Security) 分為四個等級：「Tier I」、「Tier II」、「Tier III」、「Tier IV」。其中這四個等級可用性的劃分是源於美國標準 The Uptime Institute Inc. 的 Industry Standard Tier Classifications Define Site Infrastructure Performance。在該標準中，美國 The Uptime Institute 依據工程需求與實踐，採用分類等級的方式定義場地基礎設施性能的工業標準。在 TIA-942 標準中依資料中心各等級的特性，電腦機房資料中心機房可分為四級：

- **Tier I：基本資料中心**

此等級的資料中心（機房），對於有計畫或無計畫的營運中斷反應最為敏感，相對來說，所受影響程度也最大。這類機房都配置了電腦電力分配及冷卻，需要有一台 UPS 或一台發電機，但不強制擁有高架地板。而這些系統的關鍵負荷，可達到 N 的 100%。基於預防性檢修的需求，每一年度場地內基礎設施需要被完全停止運作一次。此外，Tier I 機房僅具備由電力及冷卻分配的一條單向管路，並無多餘的組成部

分，因此僅可提供 99.671%可用度。

- **Tier II：基礎設施部分備援**

此等級的資料中心所採用的設備，具有部分備援的水準，因此比起 Tier I 機房，對於有計畫或無計畫的營運中斷反應相對較低，其內部已有高架地板，也有一台 UPS 及發電機，而動力設計為 N+1，擁有一條單一的分配線路，關鍵負荷可達到 N 的 100%，因應其關鍵線路的維修，以及場地內其他基礎設施的維修維護，需有一次處理性的關閉中斷。Tier II 係由電力與冷卻分配的一條單向通路組成，但夾帶額外的備援組成部分，故可提供 99.749%可用度。

- **Tier III：基礎設施同時可維修**

此等級的資料中心，具有能夠進行任何有計畫的場地基礎設施活動，而又不致因為電腦系統運行狀況而中斷之能力。所謂有計畫的活動，包括預防性及程式性的維修、修理，抑或汰換零組件，增添或調整組件的容量，以及執行組件與系統的測試。在於空調系統部分有兩套獨立管路，當其中一條管路進行維修或測試的同時，另一條管線也能保持運轉不中斷。在系統上的關鍵負荷不超過 N 的 90%，而當企業期望獲

得正常而合理的額外保護時，Tier III 場地將被有計畫地設計成為「可升級至等級 Tier IV」，其係由多條有效的電力和冷卻分配道路所組成，然其中只有一條通路執行運轉，另外多餘的組成部分，則在運轉的同時進行維修，足以提供 99.982% 的可用度。

- **Tier IV：基礎設施故障容錯**

這個等級的資料中心，具有能進行任何有計畫的維修活動，且不會對關鍵負荷造成中斷的能力，在此同時，也可提供基礎設施足額的電力與空調容量，因此任何無計畫性的故障，都不會影響其關鍵負載，其需要同時執行的電路分配，通常為 S+S 的雙電源系統組態，每套電力系統都有 N+1 備援的兩個獨立 UPS。在一個系統上的關鍵負載不會超過 N 的 90%，而全部硬體設備都需要有故障容錯之雙電源輸入。在嚴格的故障容錯機制下，Tier IV 擁有維持無計畫故障或運行錯誤時，不致產生電腦機房運作中斷的能力，其係由多條有效的電力與冷卻分配道路組成，有額外的備援組成，而且是故障容錯，所以能提供高達 99.995% 的可用度。

表格 6 TIA-942 規格比較表

	項目	Tier1	Tier2	Tier3	Tier4
機房認證必要項目	機電設備	無備援	N+1	N+1	N=N
	供電策略	市電為主	市電為主	自行供電為主	自行供電為主
	管線分佈	1	1	1 條主要線路+1 條備援線路	2 條皆為主要線路
	具備可同時維修性	否	否	是	是
	具備可容錯能力	否	否	否	是
參考設計條件(非必要)	建築物類型	租用	租用	獨立專用	獨立專用
	每個機櫃可提供之電力	小於 1000 瓦	1000~3000 瓦	大於 3000 瓦	大於 4000 瓦
	每平方英尺地面可承載公斤數	約 36.36 公斤	約 45.45 公斤	約 68.18 公斤	68.18 公斤以上
	機房可用率	99.67%	99.75%	99.98%	99.99%
	機房年停機時間	28 小時	22 小時	1.6 小時	2.4 分鐘

資料來源：Uptime Institute

## (二) 日本

日本資料中心協會 (Japan Data Center Council, JDCC)，JDCC 成立於 2008 年底，屬非營利組織，旨在建立日本資料中心標準，進而提升日本 DC 在國際上的成本、效能、安全性及可靠性，編撰有「資料中心設施標準」，並致力於相關的研究與推動。

- 標準簡介

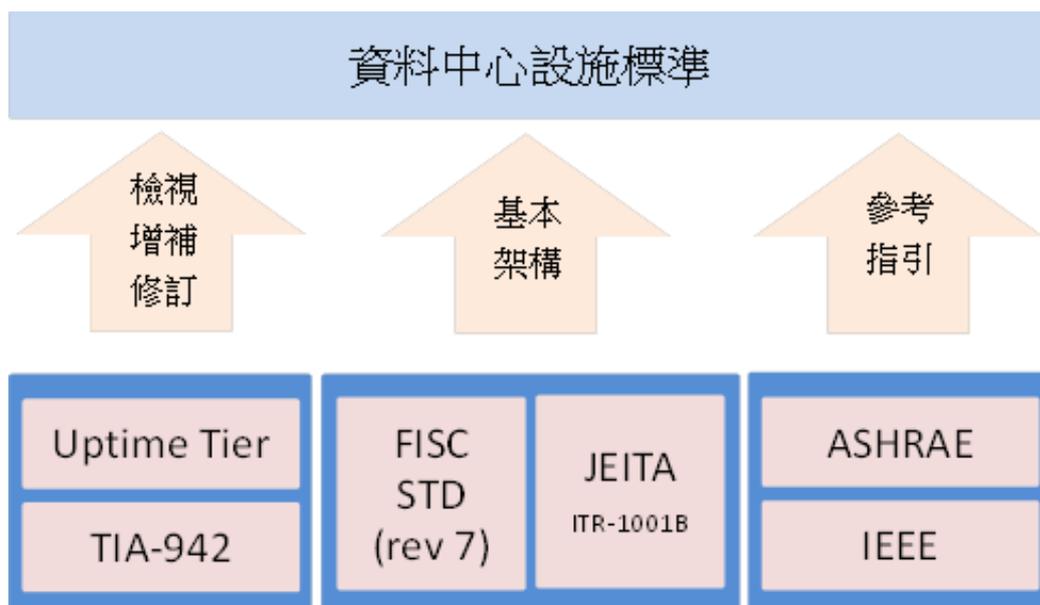
「資料中心設施標準」(Data Center Facility Standard) 仿效 Uptime Institute 的 4 階層模式，並參考 TIA-942、FISC STD、ITR-1001B、ASHRAE、IEEE 等多份日本國內外之文獻和標準，加上因地制宜的相關衡量指標，作為日本境內 DC 營運的參考依據。

- 適用範圍

此標準主要提供日本 DC 營運管理之參考。

- 重點摘要

JDCC 建立的「資料中心設施標準」，除了引用相關規範、標準之衡量指標外，另外因應日本的特殊狀況及考量 DC 營運的需要，提出了幾項建議指標：



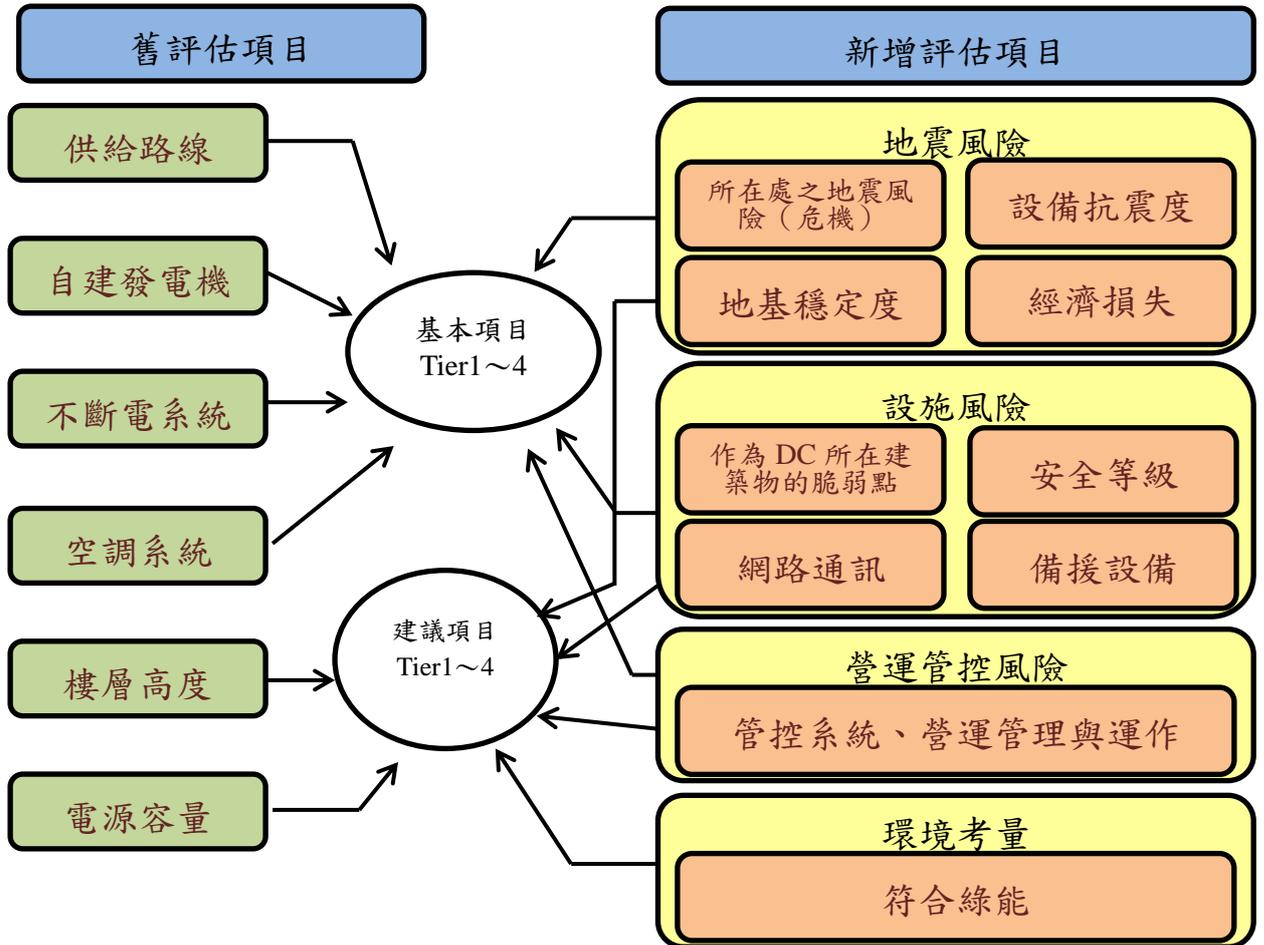
資料來源：Outline of Data Center Facility Standard，JDCC

圖 5 JDCC 標準之架構

- 地震風險評估：包括地震所造成的危害、地基穩定度、設備抗震度等風險因子的評估，藉以衡量出 PML (Probable Maximum Loss)。
- 設施風險評估：當建築物作為 DC 之用，其安全、網路通訊、設施等可能面臨到的風險，皆須予以識別。
- 營運管控風險評估：針對 DC 的管理系統及營運管理過程中可能面臨的風險，需加以評估和考量。

整份標準將 DC 安全需求區分成基本項目(Basic Items)與建議項目 (Recommended Items)，後者在 4 階層 (Tier1~4) 中僅部分項目有提列相關的要求，評估項目之架構如

圖 6 所示。



資料來源：Outline of Data Center Facility Standard，JDCC

圖 6 JDCC 標準之評估項目架構

基本項目 (Basic Items) 之評估主要包含以下 6 項：

➤ 建物

- ◆ 建物使用狀況 (是否為 DC 專用)。
- ◆ 防震安全 (PML 評估與建築法規遵循)。

➤ 安全

◆安全防護管理的程度。

➤ 電力設備

◆電力線路的備援。

◆電力供應的備援（資訊設備到 UPS）。

◆電力供應的備援（UPS 到配電裝置）。

◆內部發電機的備援。

◆UPS 設備的備援。

➤ 空調設備

◆熱源/空調設備的備援。

◆空調設備電源供應的備援。

➤ 通訊設備

◆線路與支架的備援。

◆建物內的網路備援。

➤ 設備管理

◆管理系統（人員監控）。

◆管理系統營運與操作（包含培訓操作員）。

建議項目（Recommended Items）之評估主要包含以下

8 項：

➤ 所在環境與其他風險

◆土壤穩定度。

◆設施附近環境。

➤ 建物

◆防震措施（設備防護、考量未來 50 年內發生機率 10% 以上的地震強度）。

◆地震發生後初始復原系統與準備措施。

◆建物的防火措施。

➤ 伺服器室與資料儲存室

◆防火與隔離措施。

◆伺服器室的預備室。

◆伺服器室內的高感測度感測器。

◆氣體滅火系統。

- ◆ 滲漏感測系統。

- 安全

- ◆ 進出管制措施。

- ◆ 安全監控措施。

- 電力設備

- ◆ 電力/UPS 室。

- ◆ 伺服器室的照明電力供應備援。

- ◆ UPS 運作時間確保。

- ◆ 儲備油料數量。

- ◆ 監控設備的備援。

- 空調設備

- ◆ 熱源設備維修室的區隔。

- ◆ 空調的儲備水源。

- ◆ 熱源/空調設備電力供應的備援。

- ◆ 管道設施的備援（水冷式空調設備）。

➤ 通訊設備

- ◆ MDF 室與網路室的區隔。
- ◆ MDF 室與網路室的備援。
- ◆ 建物內工訓設備的備援 (Router/Switch)。
- ◆ 通訊設備電力供應的備援。
- ◆ 通訊線路與電力線路的分隔。

➤ 設備管理

- ◆ 能源管理 (包括電力、溫度、濕度等的持續監控)。

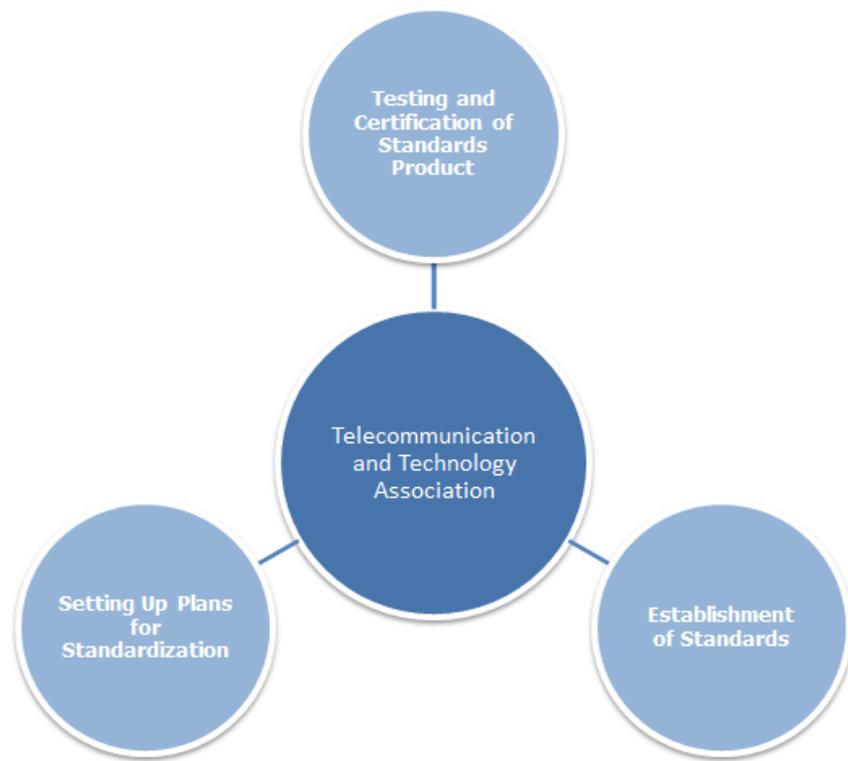
### (三) 韓國

韓國電信技術協會 (Telecommunication and Technology Association, TTA) 成立於 1988 年，是一個非營利的非政府組織，針對資通訊 (Information and Communications Technology, ICT) 技術標準提供測試與認證的服務。此外，韓國電信技術協會也就資訊通信技術產業的發展趨勢與需求，進行技術標準與規範的研析與制定，並提供資訊通信技術產品所需的測試方法以及認證制度。

韓國電信技術協會由成立至今，累計已編審了 12,024 份 TTA 標準，並提供 18,467 種測試或認證服務。由此可知，韓國電信技術協

會在韓國資訊通訊技術產業的技術發展與產業運作推動上，皆扮演著相當重要的角色。韓國電信技術協會的主要任務為：

- ▶ 制定、審閱並推廣資通訊相關之電信標準：韓國電信技術協會負責擬定、重新檢閱以及推廣資通訊相關的電信標準，類別包含網路通訊技術( IPv4, IPv6)、無線電通訊(Radio Communication)、藍芽通訊、4G 行動網路、5G 行動網路，或是其他資訊技術，例如網路加密技術、電子商務應用…等。
- ▶ 進行資通訊電信標準的前瞻研究：觀察並分析未來資通訊技術的發展趨勢，進行技術開發與前瞻研究，促進產業發展，提升學術研究能量。
- ▶ 資通訊設備的測試以及認證作業：提供資通訊產業相關的產品評估與技術服務，支援包含軟體與硬體設備的測試與認證服務，提升韓國國內資通信產業的產品研發水準，並有效提升產業競爭力。



資料來源：韓國電信技術協會官方網站

圖 7 韓國電信技術協會主要任務示意圖

- 標準簡介

TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems (資訊系統災害管理指引), 是韓國電信技術協會於 2007 年 12 月 26 日公告的參考指南。這一份參考指南提供了政府機構或是企業組織一份完整的操作說明, 讓參考單位了解該如何進行資訊設備的災難復原計畫與作業流程設計, 以因應未知的外部風險或是內部人為失誤, 並降低這些威脅所可能造成的潛在損失。

「TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems」這份指引中，包含了三個主要的工作階段與災難復原系統之解說：(1) 建立復原計畫；(2) 設計、執行災難復原計畫；(3) 維運災難復原計畫。

- **適用範圍**

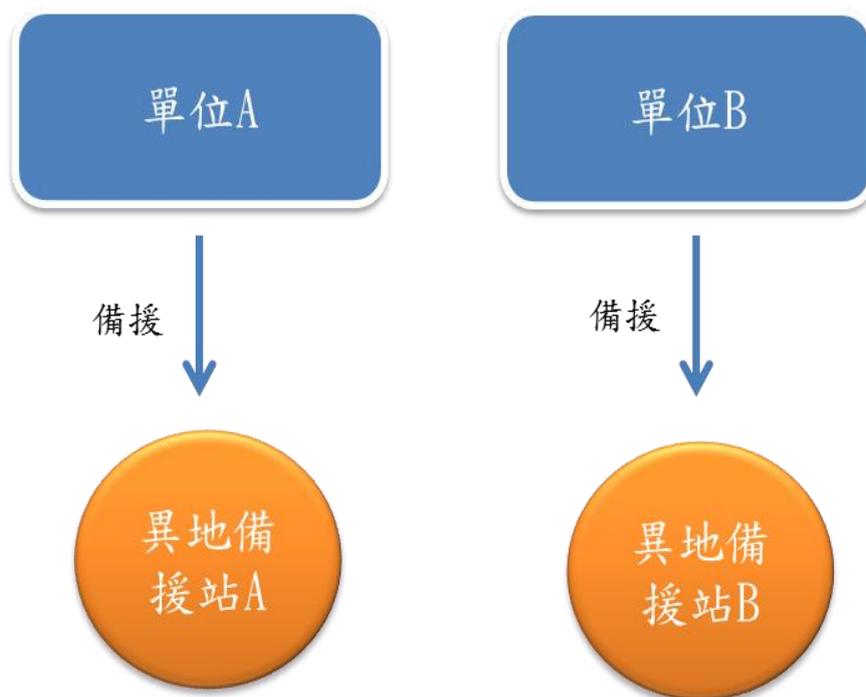
提供給韓國政府部門或民間企業組織，作為資訊系統災害管理之參考。

- **重點摘要**

「TTAK.KO - 10.0259 資訊系統災害管理指引」依據建造與營運方式的不同，將異地備援的類型分為以下 6 種不同的型態，包含：自建、共建、互為備援、自營、聯營與委外：

- ▶ 依建造方式的不同

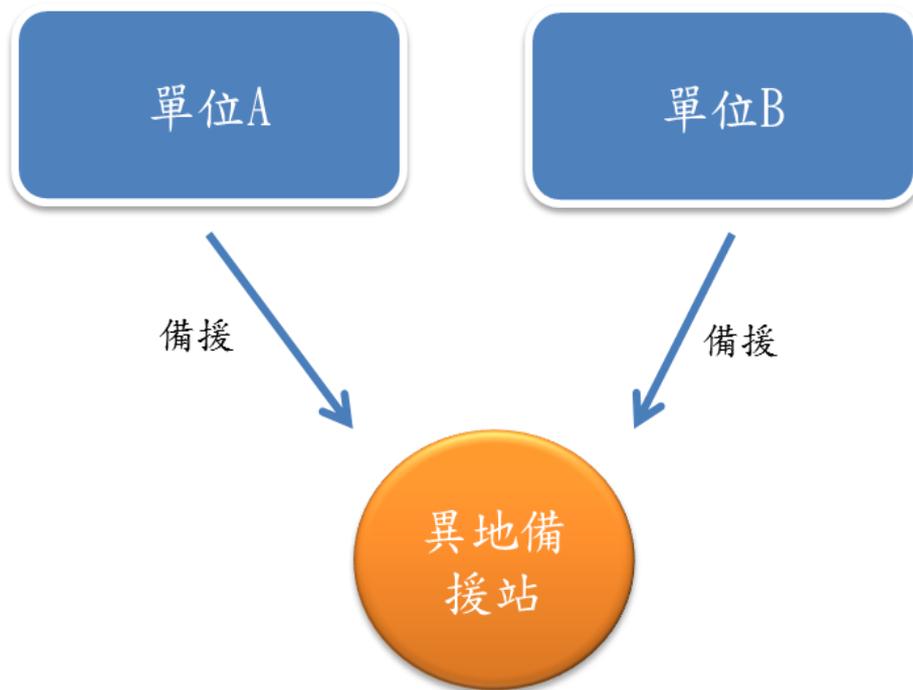
- ◆ 自建：自行建造專屬的異地備援系統，包含土地取得、機房設計與設備佈建等。此異地備援建置類型的建置成本與管理成本皆為最高，但是在安全與可靠度上可以獲得最大的保障與最佳的可靠度。



資料來源：TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems

圖 8 TTAK.KO - 10.0259 資訊系統災害管理指引自建型態

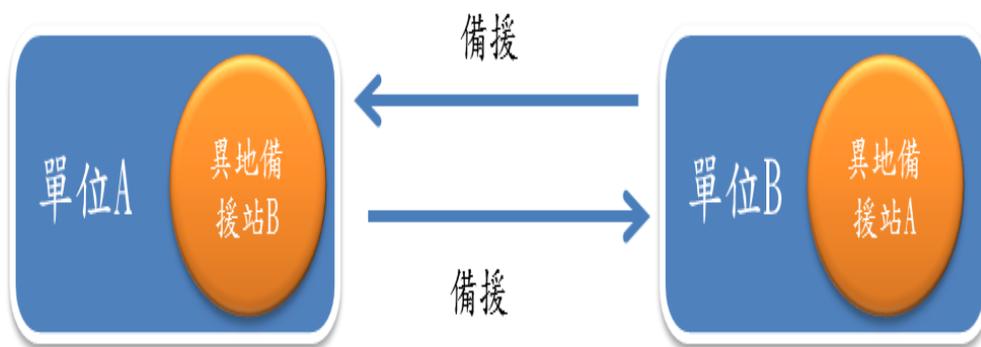
- ◆ 共建：由兩個以上的單位共同建置異地備援系統，合作方式包含簽署書面契約、備忘錄等，建置成本由所有參與單位共同承擔；另外，異地備援系統也是由參與單位共同管理。因此，共建的異地備援系統之總成本較低，但仍可維持一定的安全性與可靠度。



資料來源：TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems

圖 9 TTAK.KO - 10.0259 資訊系統災害管理指引共建型態

- ◆互為備援：由已具合作關係的兩個（含）以上之單位，互相分享機房空間與通訊服務，做為異地備援系統。此種型態為互惠模式，故建置成本與管理成本皆為最低，但是在安全性與可靠度上的要求，則必須視雙方的資訊安全系統執行成效而定。因此，整體上來說，互為備援這種異地備援方式的建置與管理成本皆為最低，但在安全性與可靠度上的要求也是最低。



資料來源：TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems

圖 10 TTA.KO - 10.0259 資訊系統災害管理指引互為備援型態

表格 7 TTA.KO - 10.0259 資訊系統災害管理指引建造方式比較表

類型	說明	建置成本	管理成本	安全性	可靠度
自建	獨立建造的異地備援系統	高	高	高	高
共建	兩個以上的單位共同建立的異地備援系統	中	中	中	中
互為備援	多個單位間互相進行異地備援機制的建立	低	低	低	低

資料來源：TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems

► 依管理方式的不同

- ◆ 自營：由單位自行進行異地備援機制的管理工作。管理成本最高，但擁有充分的自主權，故安全性與可靠度皆可獲得最高程度的保障。

- ◆ 聯營：由多個單位共同進行異地備援系統的管理，管理成本較自營方式低，但是安全性與可靠度則必須視彼此的合作方式而定。
- ◆ 委外：將異地備援系統委託專業的網路資訊中心（Internet Data Center，IDC）或第三方機構進行專業管理。整體管理成本、安全性與可靠度將視合約內容與服務水準的要求而定。

表格 8 TTAK.KO - 10.0259 資訊系統災害管理指引管理方式比較表

類型	說明	管理成本	安全性	可靠度
自營	自己管理異地備援系統	高	高	高
聯營	兩個以上的單位共同進行異地備援系統的經營管理	中	視單位間的服務方式而定	視單位間的服務方式而定
委外	委託專業第三方進行異地備援機制的維運	低	視單位間的服務方式而定	視單位間的服務方式而定

資料來源：TTAS.KO - 10.0259 on Guidelines for Disaster Management of Information Systems

除了異地備援的建造與管理模式外，「TTAK.KO - 10.0259 資訊系統災害管理指引」也提到了異地備援的 4 種主要系統架構，包含：鏡像站、熱備援站、暖備援站與冷備

援站。

◆鏡像站 (Mirror Site)：異地備援中心採用與主機房相同等級的設備與系統，並使用 Active-Active 的系統架構，建置成本與管理成本為最高，但可確保兩地的系統設定與資料內容保持同步。在主機房發生異常狀況時，異地備援中心可以立刻取代主機房提供服務，確保資訊系統的可用性 (Availability)，故不會造成資料遺失或損毀，也不會導致服務中斷。因此，資料回復點 (RPO) 與營運復原時間 (RTO) 皆為 0。

◆熱備援站 (Hot Site)：異地備援中心採用與主機房相似的設備與系統，並使用 Active-Standby 架構，讓異地備援中心平時處於待命狀態，並使用同步 (Synchronous) 或非同步 (Asynchronous) 的方式，與主機房進行高頻率的資料同步。因此，異地備援系統僅會損失極少部份的資料，且可在短時間內取代主系統。故資料回復點 (RPO) 趨近於 0，營運復原時間 (RTO) 則為 4 小時內。

◆暖備援站 (Warm Site): 備有基本設備與系統，並保持週期性的系統資料備份機制。但在異常狀況發生時，異地備援中心需要一段時間才可完成設定並正式上線。故資料回復點(RPO)約為1小時，而營運復原時間(RTO)則為1天。

◆冷備援站 (Cold Site): 該站僅有最基本的环境設備，需要進行完整的設備遷移與系統重建工作，故耗時最長，但建置與維護成本為最低。因此，資料回復點 (RPO) 約為1天，而營運復原時間 (RTO) 則為2天以上。

#### (四) 沙烏地阿拉伯

- 標準簡介

對沙烏地阿拉伯來說，通信基礎設施是一個成功的災難復原 (DR) 的關鍵因素，可以減少對生命和財產造成的不利影響。因此，有必要落實防範措施，建立資通訊產業的災難復原計畫在，以確保基本設施的連續性以及對緊急通信的幫助。因此，沙烏地阿拉伯通信與資訊科技委員會 (Communications and Information Technology Commission) 出版了資通訊產業災難復原計畫指南

(Guidelines on Disaster Recovery Planning for ICT Industry)，內容說明災難復原計畫的基礎建設應變措施及方法，包含地理位置、建築物附近環境、建築物基礎建設、電力、火災偵測、警報與消防設備、空調系統、漏水偵測和防護系統、環境監測系統、建築物內部的存取控制系統和機房。

• **適用範圍**

災難復原的主要目的，是確保企業組織業務在無法預期之天災或人為因素影響之下，可在容許時間內恢復業務服務之管理功能。詳細的範圍如下表格 9 所示：

表格 9 沙烏地阿拉伯營運管理範圍表

BC/DR 的權責	<ul style="list-style-type: none"> <li>● 定義 DR 的權責主管</li> <li>● 定義企業持續營運功能，以及組織內部的角色和適用範圍</li> </ul>
風險評估	<ul style="list-style-type: none"> <li>● 評估潛在風險</li> <li>● 根據嚴重性和可能性的發生，確定風險優先等級</li> <li>● 說明可能的特殊狀況</li> </ul>
營運衝擊分析	<ul style="list-style-type: none"> <li>● 確定災害對持續營運的潛在影響</li> <li>● 確認可容許的營運中斷時間</li> <li>● 識別關鍵業務</li> <li>● 對於重要的企業流程，建立復原目標</li> </ul>

<b>災難復原計畫 發展</b>	<ul style="list-style-type: none"> <li>● 規劃備份與備援策略並將其文件化。</li> <li>● 確認災難復原計畫所需之相關資源。</li> <li>● 執行成本效益分析，以確定最佳復原策略</li> </ul>
<b>發展 DR 計畫</b>	<ul style="list-style-type: none"> <li>● 危機管理的組織結構和程序（包括相關人員和災難復原小組的通報）</li> <li>● DR 計畫的內容須包含：介紹、通報和啟動步驟、復原步驟、重建階段、其他附錄。</li> </ul>
<b>災難復原計畫 測試和維護</b>	<ul style="list-style-type: none"> <li>● 復原目標確認</li> <li>● 功能測試</li> <li>● 計畫演練</li> <li>● 結果分析</li> <li>● 計畫維護</li> </ul>

資料來源：Guidelines on Disaster Recovery Planning for ICT Industry

• **重點摘要**

沙烏地阿拉伯的資通訊產業災難復原計畫指南

(Guidelines on Disaster Recovery Planning for ICT Industry) 的指引說明如下：

➤ **地理位置**

建物位址之選擇應避免座落在以下幾個地區：

◆ 過去有水災和土石流的歷史。

◆ 距離河道 1.5 公里內。

- ◆低於海平面。
- ◆在紅海沿岸（海嘯危險）1.5 公里內。
- ◆易發生下陷或在礦物開採的地方。
- ◆在飛行路徑，或重要民用或軍用機場旁。
- ◆靠近運輸有害物質的交通幹道。

➤ 建築物的周圍

建物周圍之相關設施應考慮：

- ◆種植 2 公尺高的成排樹木，可減少來自車輛或是恐怖行動之威脅。
- ◆內部通道應設計為 90 度，以減緩交通速度。
- ◆停車場應設在圍牆外面，或距離主建築物 100 公尺以上。
- ◆在距離主建築物 60 公尺處設置車輛安檢站。車輛安檢站須具備故障排除功能，當系統故障時，仍可以透過手動控制，允許緊急服務車輛進入。

➤ 建築物的基礎建設設施

建築物的基礎建設設施應包含以下：

- ◆ 電力。
- ◆ 火災偵測，預警和消防設備。
- ◆ 空調系統。
- ◆ 防雷擊設備。
- ◆ 漏水偵測和防護系統。
- ◆ 環境監視系統。
- ◆ 門禁系統。
- ◆ 佈線。
- ◆ 機房。

➤ 電力

◆ 主要電力

穩定的電力供給對於資通訊產業來說是很重要的，

須要考慮到：

- 重要的建築物需要雙重或多重獨立電源。

- 各獨立電源應在不同的點進入大樓。
- 獨立電源不得共享通道。
- 電力應該來自不同的電力供應商。
- 須確認電源進入建築物後，有無單點故障導致電力中斷之可能。

除此之外，還要考慮以下三點：

- 每間交換機房（Switch Room）需要有一個以上的配電盤（Power Distributed Union）。
- 每個 PDU 連接到獨立的電力來源。
- 安裝在電腦或交換機房的所有硬體連接至兩個獨立的 PDU。

#### ◆ 不斷電系統與發電機

不全然依賴主電力，UPS 通常由發電機電池備份的組合，並偶爾電源平滑設備。

- 緊急照明、電梯、消防系統與環境監測須連接至不斷電系統。

- UPS 應能夠提供足夠電力供給，直到至少一個發電機順利啟動供電。
- 發電機的滿載發電量應大於用電量的歷史峰值，確保可提供足夠電力。
- 發電機之儲油槽應允許最低 N+2 天連續滿載運行，N 是等於在該地區最大連續節日（年節假日除外）的數量。
- 應與燃料供應商簽訂契約，確保發電機燃料的取得無虞
- 發電機應至少每年進行一次定期檢修。
- 發電機應具有監控系統。
- 應定期檢查備用電池的容量
- 應定期培訓與演練相關機電人員對於發電機操作與備用電池之更換作業。

➤ 火災偵測、預警和消防設備

◆ 偵測

- 建築的每個房間應配有煙霧偵測器。

- 所有偵測器應每年進行至少兩次測試。

- 主要房間和公共區域應裝有手動警報系統。

#### ◆ 警報

- 火災報警系統應進行定期測試。

#### ◆ 消防

- 消防系統應安裝並覆蓋所有重要設施。

- 交換機機房或是電腦機房應避免使用水來進行消防作業。

- 應與供應商簽訂維護契約，確保消防系統的內物更換可在 24 小時內完成。

#### ◆ 火災偵測和監控系統

- 每棟樓至少都要有一個中央監控系統，監控管理所有煙霧偵測器、火災警報器與消防系統。

- 中央監控系統應該要能夠掌握所有煙霧偵測器、火災警報器與消防系統之系統狀態。

➤ 空調處理

- ◆ 空調系統應採高可用性 (High Availability) 設計。
- ◆ 採用「N+2」設計理念的空調系統，在部份空調系統組件維修或故障狀態下，並不會造成系統失效並影響業務運作。
- ◆ 空調系統應連接至不斷電系統。
- ◆ 空調系統應定期檢修。若空調系統之「平均修復時間」大於可容許之系統中斷時間，則必須要準備熱待機的備援機組以備切換。
- ◆ 所有的空調系統應被連接到兩個以上的獨立電源。
- ◆ 空調系統應該納入環境監控系統之管理範圍內，方便辨識設備故障以及機房內部熱點。

➤ 漏水偵測和防護系統

- ◆ 建議電腦機房或是交換機機房中不要有水或是水管線路。
- ◆ 重要機房以及其下方之房間，應安裝漏水偵測器。
- ◆ 交換機機房或電腦機房應設置排水溝渠，以利將積水導

出。

- ◆漏水偵測系統應該納入環境監控系統之管理範圍內，方便辨識系統警示訊息以及運作狀態。

➤ 環境控制系統

- ◆環控控制系統應該管理與監控所有的安全和環境偵測系統，而值班室（Operation Room）則是應該遠離重要資訊機房。

- ◆環控系統應設備用值班室，並與主值班室位於不同的建築物。

- ◆所有安全或作業區工作人員應進行培訓，以識別潛在的災難和行為。

- ◆環控系統的監控範圍應包含本地機房以及各遠端機房。

- ◆環控系統應連接到不斷電系統，並使用獨立的備援電池。

➤ 門禁系統

- ◆須設有電子式的人員進出管制系統，以及 2 個具備聲音

警報器的緊急出入口。

◆建物內部的人員進出管制系統須同時具有電子系統管制以及安全人員查核機制，並借助人力資源部門的協助進行員工身份辨識。

◆電子門禁系統應能夠在緊急情況下，切換為手動模式操作。

◆需設立 CCTV 監視系統。

➤ 機房

◆通常擺放發電機與空調設備，應具有密封門，以保護設備不受沙塵暴或其他災害影響。