中央研究院

資訊科學研究所

營運持續管理作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I307

版　　本：1.0

核准日期：115 年 4 月 24 日

文件制／修訂紀錄表

版次	修訂日期	修訂單位	修訂者	核准者	修訂內容
1.0					新擬訂文件

目錄

壹、目的

中央研究院資訊科學研究所(以下簡稱本所)為維持資通系統的正常運作，確保遭受不可抗力之天然災害或人為破壞時，能在最短時間內回復正常運作，針對於可能造成系統無法正常運作的災害，如任何人為或天然災害等，除了確保員工安全，並使各作業單位有效管理其相關電腦軟硬體設備、資通系統及資料的安全性，並提供各項資通安全事件的作業應變處理程序及通報作業流程，提供本所相關單位人員在危害系統事件發生時，採取正確的應變措施，以降低對資通系統正常運作的威脅所造成的衝擊，訂定「營運持續管理程序書」(以下簡稱本說明書）以資遵循。

貳、依據

一、 資通安全管理法及其子法

二、 中央研究院資通安全暨個人資料保護政策及規範

三、 中央研究院資通安全管理規範實施要點

四、 ISO/IEC 27001 資訊安全管理系統（Information Security Management System，ISMS）

參、範圍

凡對本所資通系統作業流程或資產造成傷害，使得營運無法持續的緊急事件，例如：長時間電力供應中斷、嚴重火災、嚴重水災、破壞性地震、電腦系統遭受駭客侵入等，均納入營運持續管理範圍內；另短期內不可復原的大型災難事件，例如：核電廠事故、國際恐怖攻擊事件、戰爭……等，因涉及範圍太廣，不在本說明書範圍內。

肆、權責

一、 資通安全長

評估資訊安全事故之影響範圍及衝擊程度，依實際狀況及事故評估結果，決定是否啟動營運持續計畫。

二、 資通安全管理委員會

(一) 審議營運衝擊分析之結果與營運持計畫之適切性。

(二) 監督營運持續計畫之演練。

三、 資安推動小組

於資通安全事件發生時，應與執法機關、主管機關和資訊服務供應商取得適當之聯絡，以保障本所權益。

四、 緊急應變小組

為任務編組，當重大資通安全事件發生時，由資通安全長負責聯絡及召集「緊急應變小組」，統籌緊急應變處理。

(一) 規劃危機處理程序，清查危機事件原因、確定影響範圍及損失評估，執行應變措施，辦理資通安全通報，並執行解決辦法等危機處理事項。

(二) 當災害發生時，配合救災單位負責搶救人員、物資與設備等，以及現場指揮工作。

(三) 進行營運衝擊分析。

(四) 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

(五) 發展、維護及更新修訂關鍵業務流程的營運持續計畫。

(六) 依據事件評估之結果，得依現況建請資通安全長決議是否啟動營運持續計畫。

(七) 擬訂營運持續演練計畫，並召集相關人員進行演練。

(八) 執行災害復原工作。

(九) 負責災後協調、指揮清理災害現場。

(十) 負責規劃原營運場所或異地備援場所之應變、處理、復原及運轉測試工作。

伍、作業說明

一、 設定營運持續管理目標

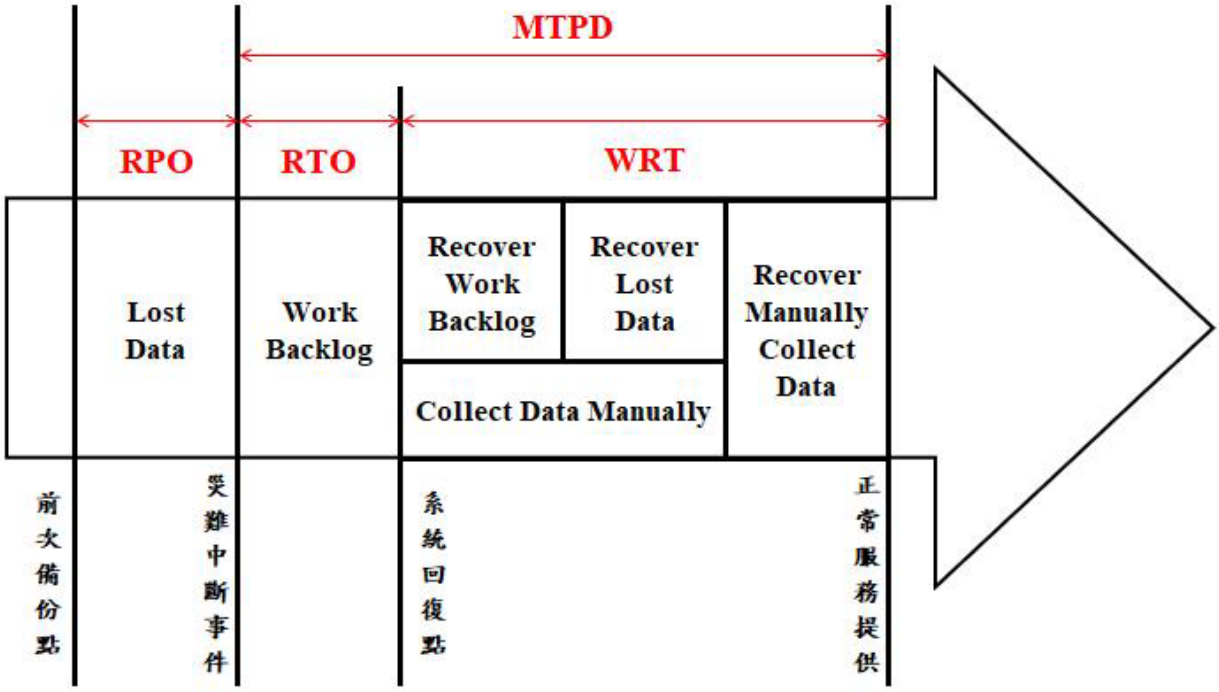
防止業務活動中斷，確保重要業務流程不受重大故障和災難的影響，並結合預防和復原措施，將風險造成的影響降低到可以接受的等級。最終針對災難、安全缺失和服務損失等後果，制訂和實施應變計畫，確保在要求的時間內恢復業務流程。

二、 營運衝擊分析

(一) 本所緊急應變小組應定期（每年辦理一次）針對重要業務進行衝擊分析

進行營運衝擊分析（Business Impact Analysis：BIA）並將分析結果彙整成營運衝擊分析表。

(二) 營運衝擊分析的目的是鑑別關鍵性業務流程，以及支援關鍵性業務流程所需之資源，並瞭解利害關係人之需求。此外，亦應識別各項關鍵性業務流程最大可容忍中斷時間、復原時間目標與關鍵性業務流程恢(圖1)。



- MTPD－Maximum Tolerable Period of Disruption（可以忍受最大服務中斷期間）
- RPO－Recovery Point Objective（資料回復點）
- RTO－Recovery Time Objective（系統回復時間）
- WRT－Work Recovery Time（資料復原時間）

圖 1：營運衝擊分析圖

(三) 完成營運衝擊分析後，需指派關鍵性業務流程負責人。

三、 規劃營運持續的資源需求

(一) 辦公環境

為維持業務的持續運作能力，辦公環境設施的整備需求為必要規劃項目，基本的需求包含：

1. 電腦作業環境

2. 事務機

3. 網路作業環境

4. 電話

5. 傳真

(二) 資通系統服務

為維持資通系統能持續提供服務，需確保下列服務正常，包含：

1. 重要業務系統伺服器

2. 網路連結設備

3. 重要業務系統與網路服務

4. 網路與安全監控服務

(三) 資料與日誌

資訊與紀錄為業務能是否持續服務之重點，應定期辦理下列事項，包含：

1. 備份處理

2. 回復測試

四、 維護緊急聯絡人員資料

(一) 緊急連絡資訊

當本所發生重大災難事件時，人員應立即回報並進行搶救與復原工作，優先集結地點及聯絡資訊為：

1. 地點：中央研究院資訊科學研究所一樓前空地

2. 地址：台北市南港區研究院路二段 128 號

3. 聯絡電話：02-27883799

如無法於本所一樓前空地集結時，應於「院本部前廣場」集結，視災害等級得由本所資通安全長授權資安推動小組人員負責，並依本院「資通安全管理規範實施要點」，聯繫資通安全事件通報總窗口(本院資訊服務處，以下簡稱本院總窗口)，以進行後續處理。

(二) 作業單位與緊急應變小組於平時即應建立並適時更新各負責單位人員

的緊急聯絡人員名冊，包括各單位主管、電腦機房管理人員、各系統管理人員、本院資安聯絡總窗口及外部聯絡資料，如軟硬體廠商人員、電力公司、自來水公司、中華電信、天然瓦斯等，聯絡資料應明確指定人員姓名或公司名稱、防災專線或緊急聯絡電話。

五、 研擬營運持續計畫

(一) 目的在防止當發生重大故障或災害造成本所相關硬體、軟體、網路通信線路或其他周邊設備故障，導致關鍵性業務服務中斷。

(二) 由緊急應變小組依據營運衝擊分析結果制定營運持續計畫，以備關鍵業務服務中斷時據以實施。

(三) 緊急應變小組應盡可能模擬各項情境，例如電腦機房受損或環境設施故障、應用系統異常或錯誤事件處理、電力受損事件、資通安全系統入侵事件等情境，並規劃該模擬情境所需之應變與復原作業程序，納入營運持續計畫。

六、 啟動營運持續計畫

(一) 由資通安全長召集「緊急應變小組」進行復原時程評估，若所需復原時程大於復原目標時間（RTO）或資料回復點目標（RPO）時，由資通安全長決定是否啟動營運持續計畫。

(二) 重大災害發生造成嚴重損失時（如：火災、爆炸、地震、颱風等），得不經損害評估，逕行啟動營運持續計畫。

(三) 計畫啟動後，緊急應變小組將事件情況與分類通報本院總窗口(資訊服務處) ，並至本院通報平台(Redmine) https://csirt.its.sinica.edu.tw/ 進行填寫。

七、 演練營運持續計畫

(一) 營運持續計畫可能會因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，因此需要定期演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。

(二) 營運持續計畫應定期（每年辦理一次）進行演練，每次至少選擇一項模擬情境，並產出一份營運持續演練計畫，交由資通安全管理委員會核准後進行演練，以減少演練完整營運持續計畫的需求及頻率。

(三) 緊急應變小組應從營運持續計畫中選擇一項模擬情境及其相關之應變與復原程序進行演練。於演練前，應備妥營運持續演練計畫，以選定之模擬情境作為演練情境，規劃演練程序並將備妥之應變與復原程序列入其中，準備參與演練之相關人員資料，以及實際演練時查檢演練程序之各項步驟的紀錄表。

(四) 營運持續計畫之演練結果應詳實記錄於「營運持續演練報告」。

八、 更新營運持續計畫

(一) 營運持續計畫應配合業務、組織及人員的調整變更而定期更新，以發揮計畫的最大投資效益，並確保計畫持續有效。

(二) 一旦營運持續計畫有所更改，就必須更新演練計畫，並確定計畫的完整性。應納入營運持續計畫更新之事項包括：

1. 採購新的設備，或是更新作業系統。
2. 使用新的問題偵測及控制技術（例如火災偵測）。
3. 使用新的環境控制技術。
4. 人員及組織上的調整變動。
5. 部門及人員地址及電話號碼的變動。
6. 契約當事者或是委外廠商的調整變動。
7. 應用系統變動、新建或是撤銷應用系統。
8. 實務作業的變更。
9. 法規上的變更。

(三) 緊急應變小組須負責計畫變更事宜，營運持續計畫每年至少應檢討評估一次，包括執行營運衝擊分析、組織權責與成員之調整、災害應變程序及回復策略之檢討，並將檢討與更新的結果提報本所資安推動小組。

陸、參考文件

無

柒、使用表單

一、 B330-I307-01 營運衝擊分析表

二、 B330-I307-02 營運持續計畫

三、 B330-I307-03 營運持續演練計畫

四、 B330-I307-04 營運持續演練報告