京城銀行
King's Town Bank

營運持續管理程序書

文件編號：IS-2-006
版　　本：V2.6
修訂日期：113.09.24
機密等級：□機敏■內部□一般

京城銀行 King's Town Bank

文件制／修訂紀錄表

版本	修訂日期	修訂內容摘要	修訂單位	修訂人	文管人員
V1.0	105.11.22	初版發行	風管部	徐炯培	徐炯培
V1.1	106.11.16	新增機密等級	風管部	徐炯培	徐炯培
V2.0	108.11.21	因應主管機關要求及「資通安全管理法」與其子法頒布，修訂本程序書之文件名稱、文件編碼及相關內容，並增訂相關表單	風管部	徐炯培	徐炯培
V2.1	109.12.14	基於核心資訊系統範圍之管理及操作效率之故，資訊室可逕行產製表單作業，並修訂該範圍之核定權責	風管部	徐炯培	徐炯培
V2.2	111.09.15	為強化本行 ISMS 及因應安永顧問建議，故納入屬驗證範圍且為非核心資訊系統為本程序書之適用範圍，並須規劃及辦理 BCP 相關作業	風管部	徐炯培	何思凝
V2.3	112.07.26	依「金融機構資通安全防護基準」之核心定義及安永顧問建議，故修訂相關內容	風管部	徐炯培	何思凝
V2.4	112.10.04	因應安永顧問建議，故修訂 MTPD 之名詞定義	風管部	徐炯培	何思凝
V2.5	113.06.12	因應 ISO 27001 改版，故增加重要網路設備為本程序書之適用範圍及其相關內容	風管部	徐炯培	何思凝

V2.6	113.09.24	因應「金融機構資訊作業韌性規範」頒布，故修訂相關內容	風管部	徐炯培	何思凝

目錄

第一條、目的

為確保京城商業銀行（以下簡稱本行）遭受嚴重災害或資通安全事件時，能迅速有效回復至最小可接受服務水準(以下簡稱 MASL)，以降低本行營運之衝擊，特訂定營運持續管理程序書（以下簡稱本程序書），以資遵循。

第二條、適用範圍

本行之核心資通系統及資訊安全管理制度驗證範圍系統(以下簡稱驗證範圍系統)，均屬於本程序書之適用範圍。

第三條、權責

一、總經理：負責本程序書核定。

二、資訊安全管理委員會（以下簡稱資安會）：

(一)、負責審查核心資通系統範圍。

(二)、負責審查適用範圍系統之 RPO、RTO、MTPD 或 MASL。

(三)、為營運持續管理審查單位，負責審查銀行公會「金融機構資訊作業韌性規範」所要求之營運持續管理事項。

三、資訊安全推動單位（風險管理部資訊安全科）：為營運持續管理推動協調單位，負責推動與協調銀行公會「金融機構資訊作業韌性規範」所要求之營運持續管理事項。

四、資訊安全執行單位（資訊室）：

(一)、負責執行除上述作業以外之本程序書控制措施要求。

(二)、負責執行銀行公會「金融機構資訊作業韌性規範」所要求之營運持續管理事項。

第四條、依據

一、IS-1-001 資訊安全政策。

二、IS-2-002 資訊安全管理委員會設置程序書。

三、IS-2-003 資訊資產管理程序書。

四、IS-2-019 電腦系統資訊安全評估計畫。

五、金融機構辦理電子銀行業務安全控管作業基準。

六、金融機構資通安全防護基準。

七、金融機構資訊作業韌性規範。

第五條、名詞定義

一、核心業務：係指由銀行依業務運作中斷對客戶影響數等風險評估結果予以決定，評估範圍如：存款業務、放款業務、匯款業務、外匯業務等(參照銀行公會「金融機構資訊作業韌性規範」第二條之規範用詞定義)。

二、核心資通系統：係指支持核心業務持續運作必要之系統或設備(參照銀行公會「金融機構資訊作業韌性規範」第二條之規範用詞定義)；針對必要之系統或設備的範圍如下：

(一)、必要系統：係指支持核心業務持續運作之直接相關主機的必要「軟體類」資訊資產。

(二)、必要設備：即重要資訊設備，並區分如下：

1、重要硬體設備：係指支持核心業務持續運作之直接相關主機的必要「硬體類」資訊資產。

2、重要網路設備：係指支持核心業務持續運作之必要「通訊類」資訊資產。

三、重要支援資訊系統：係指支持核心資通系統或驗證範圍系統持續營運所需之重要支援資訊系統(例：核心資通系統或驗證範圍系統之相依資訊系統、重要之資安防護系統等)(參照銀行公

會「金融機構資訊作業韌性規範」第二條之規範用詞定義與規範頒布時之規範逐條說明)。

四、營運持續計畫（Business Continuity Plan；BCP）：係指為確保組織發生嚴重災害或資通安全事件時，可持續營運之計畫。

五、營運衝擊分析（Business Impact Analysis；BIA）：評估業務中斷對本行所造成衝擊之分析方法(參照銀行公會「金融機構資訊作業韌性規範」第二條之規範用詞定義)，相關名詞定義如下：

(一)、復原時間目標（Recovery Time Objective；RTO）：係指中斷事故發生後，從中斷事故發生到回復至 MASL 之目標時間(參照銀行公會「金融機構資訊作業韌性規範」第二條之規範用詞定義)；時間要求愈短，則系統備援策略所須投入之成本愈高。

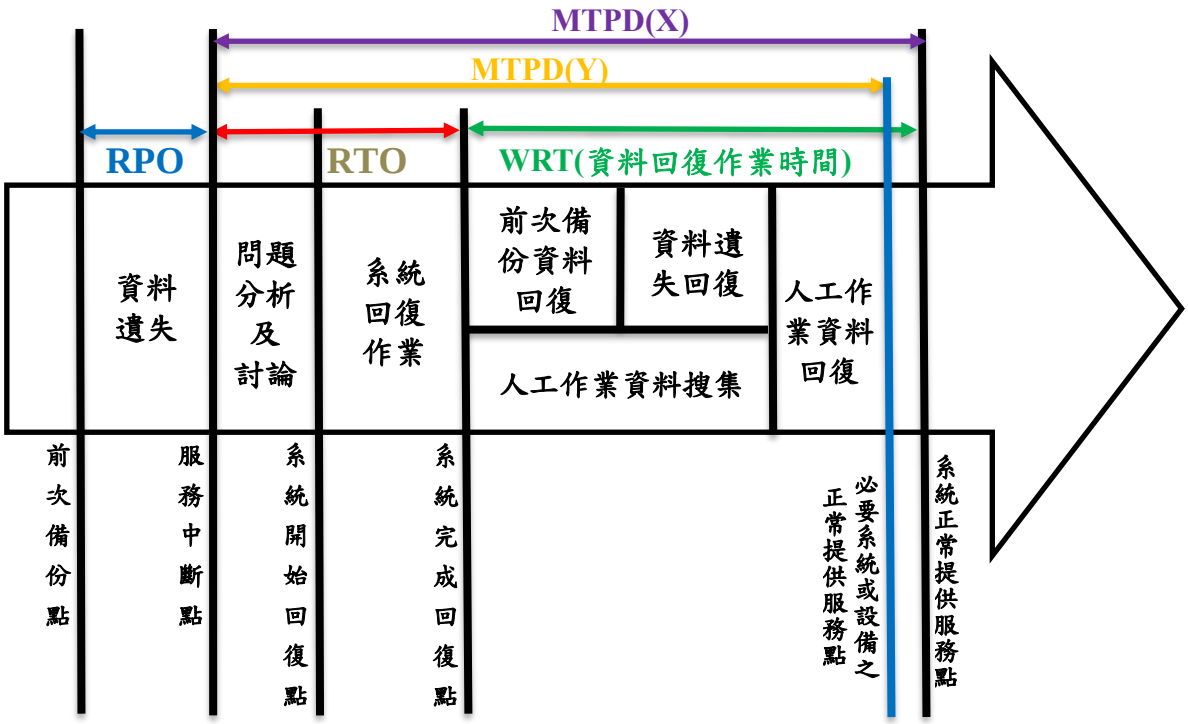
(二)、資料回復時點目標（Recovery Point Objective；RPO）：係指中斷事故發生時，業務流程資料可被回復之最近時間點(參照銀行公會「金融機構資訊作業韌性規範」第二條之規範用詞定義)；時間要求愈短，則資料備份策略所須投入之成本愈高。

(三)、最大可容忍中斷時間（Maximum Tolerable Period of Disruption；MTPD）：

1、係指業務發生中斷事故之最大可容許中斷時間(以下簡稱X)；屬核心業務者，應考量法規及利害關係人(包含但不限於主管機關、客戶、供應商、合作夥伴、內部員工及其家屬、媒體)等面向予以決定。(參照銀行公會「金融機

構資訊作業韌性規範」第二條之規範用詞定義及頒布時之規範逐條說明)。

2、除依據前項說明計算該系統之 MTPD(X)外，支持該系統持續運作所需之重要支援資訊系統，因相關情境發生而致「服務中斷至能正常提供服務時，所能容許之時間區間(以下簡稱 Y)」，亦須一併納入考量。



六、最小可接受服務水準(Minimal Acceptable Service Level；MASL)：係指依據業務之復原目標，針對其對應之業務所訂期望於 RTO 內回復之最低服務水準(參照銀行公會「金融機構資訊作業韌性規範」第二條之規範用詞定義)。

七、程序演練(Table Top Exercise；TTX)：係指一種紙上驗證作業程序的方法，用於假想情境發生並推估局勢發展，依據事先規劃的作業程序模擬執行，以驗證情境應變之完整性(參照銀行公

會「金融機構辦理電子銀行業務安全控管作業基準」第二條之基準用詞定義)。

八、核心資通系統之供應商：係指提供銀行核心資通系統之軟硬體產品開發、建置或維運服務的組織或個人，包含其受託者與跨機構合作夥伴。

第六條、作業程序

一、核心業務範圍

(一)、範圍：存款業務、放款業務、匯款業務及外匯業務。

(二)、每年至少於資安會討論一次範圍之妥適性。

二、核心資通系統範圍

(一)、資訊安全執行單位應依如下條件進行識別，若均符合時，即為核心資通系統。

1、支持核心業務持續運作必要之系統或設備：

(1)、必要系統：僅針對本行最核心之 AS/400 主機群的系統。

(2)、必要設備之重要硬體設備：僅針對本行最核心之 AS/400 主機群的硬體。

(3)、必要設備之重要網路設備：包含但不限於核心網路交換器(Core Switch)等。

2、若必要之系統或設備運作中斷時，將影響本行客戶達數萬人以上。

3、必要之系統或設備的機密性(C)、完整性(I)或可用性(A)，其風險量化值(參照「IS-2-003 資訊資產管理程序書」之「附錄 B」)之任一項為最大值。

(二)、資訊安全執行單位應每年重新識別核心資通系統及其重要支援資訊系統之範圍，並將識別結果併核心業務範圍送資安會審查識別結果及討論核心業務範圍之妥適性。

(三)、當發生影響核心業務及核心資通系統之重大變更(例：新核心資通系統上線、對其他可能對本行服務或業務產生重大影響之變更等)時，宜評估是否提前發動前項作業。

三、驗證範圍系統

(一)、資訊安全執行單位應每年識別重要支援資訊系統之範圍，並將識別結果送資安會審查。

(二)、當發生影響驗證範圍系統之重大變更(例：對其他可能對本行驗證範圍系統服務或業務產生重大影響之變更等)後，宜評估是否提前發動前項作業。

四、營運衝擊分析

資訊安全執行單位應針對本程序書適用範圍之系統，偕業務管理單位依「IS-2-006-01 營運衝擊分析表」進行營運衝擊分析，應考量之控制措施說明如下：

(一)、核心資通系統

1、應每年進行 RPO、RTO、MTPD 及 MASL 之評估，且應將評估結果送資安會審查，經審查通過後始可規劃 BCP 相關作業。

2、應依據核心業務之重要性或 RTO，列出核心業務之復原優先順序。

(二)、驗證範圍系統

1、應進行首次 RPO、RTO 及 MTPD 之評估，且應將首次評估結果送資安會審查，經審查通過後始可規劃 BCP 相關作業。

2、若資訊安全執行單位與業務管理單位達成 RPO、RTO 及 MTPD 之異動共識後，亦須將異動結果送資安會審查，經審查通過後始可規劃 BCP 相關作業。

(三)、針對 MASL，應注意如下：

1、應識別滿足 MASL 之業務管理單位及資訊安全執行單位所需資源(例：場地、電力/供水/用油/空調/消防等基礎設施、網路、電話線路、資訊系統、辦公用軟硬體、復原系統必要之供應商、廠商/委外人員/公會/其他金融機構等復原業務必要之外部單位、人員或文件等)(參照銀行公會「金融機構資訊作業韌性規範」規範頒布時之規範逐條說明)。

2、為能於 RTO 內回復至 MASL，應擬定滿足 MASL 所需資源之解決方案。

3、若資源無法於 RTO 內取得、準備完成或系統備援能力不足者，應考量下列因素擬定措施(例：如何加強資源之解決方案以補足資源落差或選擇承擔未能於 RTO 內回復至 MASL 之風險等)，經資安會審查，並視情況報請層峰核准。

(1)、組織可能承擔之風險的數量和類型。

(2)、相關之成本和利益。

(四)、核心業務、核心資通系統或重要支援資訊系統經重新識別後或資安會討論後確有異動者，亦應重新執行營運衝擊分析。

(五)、資訊安全執行單位若基於管理及操作效率之故，可參照「IS-2-006-01 營運衝擊分析表」，逕行產生表單格式進行評估填寫，惟評估時仍應納入該表之評估欄位，以求周延。

五、營運持續計畫演練

組織為確保符合資訊安全規範及控管措施，並能持續性落實於組織之營運持續管理流程中，應考量下列控制措施：

(一)、規劃資訊安全持續

應確認與資訊安全控管相關之要求事項，以規劃因應嚴重災害或資通安全事件發生而不利於本行營運之 BCP，應考量之控制措施說明如下：

1、核心資通系統：應每年至少規劃演練一次 BCP 相關情境。

2、驗證範圍系統：應依資訊安全評估作業辦理頻率（參照「IS-2-019 電腦系統資訊安全評估計畫」第六條之二），於所屬電腦系統類別之辦理期限內，至少規劃演練一次 BCP 相關情境。

3、BCP 相關作業之規劃，應注意如下：

(1)、應考量成本效益及評估可行性。

(2)、應確認相關人員之角色、權限及責任，各系統負責人視需要得要求業務管理單位、相關單位或供應商提供必要之協助與配合。

(3)、應包含但不限於如下之項目或內容：

A、 目的：說明計畫欲達成之目標。

B、 範圍：說明計畫所含括之範圍。

C、 監控：說明演練期前之監控作為。

D、 風險情境：針對已識別可能造成服務中斷之風險情境(例：天然災害、人為災害及資通訊安全事件等)設計演練情境並說明。

E、 測試及演練：說明計畫測試及演練之項目與執行方式。

F、 事件通報：說明事件分級及通報程序。

G、 應變處理：說明災害調查、評估步驟及臨時指揮中心建置等。

H、 回復作業：說明回復場所之清理、清查與準備，及設備、網路與系統回復程序等。

(4)、應參酌「IS-2-006-01 營運衝擊分析表」之 RTO、RPO 及 MTPD 進行規劃，以確保符合營運持續之要求。

(5)、應於一個或多個異地位置保存 BCP 及相關資料，以確保相關人員能夠取得。

(二)、實作資訊安全持續

應實作演練 BCP 相關作業，以確保於營運不利情況期間得以實作因應，應考量之控制措施說明如下：

1、BCP 相關作業之規劃事宜，應經單位權責主管核可後始可進行演練作業。

2、演練之測試方式及注意事項：

(1)、測試方式：

A、 程序演練(Table Top Exercise)：依據事先規劃之假想情境於紙上驗證之作業演練。

B、 模擬測試(Simulation tests)：於模擬環境進行演練。

C、 平行測試(Parallel tests)：於備援平台進行演練。

D、 完全測試(Full interruption tests)：於實際作業環境進行演練。

(2)、注意事項：

A、 演練時得依實務需求，可採上述任一測試方式進行並留存紀錄。

B、 於實際作業環境進行演練，演練前應識別可能造成之風險(例：因演練可能造成正式資料之錯誤或遺失、演練可能造成之資安防護水準下降或演練可能造成之客戶權益損害等)，並事先擬定保護措施。

(3)、屬核心資通系統者，除須遵循上述相關要求外，亦應遵循如下要求：

A、 針對已識別可能造成服務中斷之風險情境，可規劃每年針對所有情境或輪流針對部分情境進行演練。

B、 應每年依需求規劃為同地或異地系統備援演練、同地或異地資料備份回存測試；針對無備援之核心資通系統或重要支援資訊系統，可考量同地或異地系統重建演練。鼓勵異地備援演練時，納入對外實際運作驗證。

C、 演練參與人員應包含核心資通系統復原負責人員、重要支援資訊系統復原負責人員、復原核心資通系統必要之供應商及核心業務執行人員。

(三)、 查證、審查並評估資訊安全持續

應定期查證、審查並更新所建立之 BCP 相關作業，以確保其於不利情況期間實作之有效性，應考量之控制措施說明如下：

1、應配合內、外部稽核之定期查核及演練之結果，針對須改善事項擬定行動方案，積極追蹤改善。

2、應於演練 BCP 前先行審查 BCP 相關作業，並視需要更新，以因應與其有關之主管機關法規或本行組織、規範及技術的變更，審查時可參酌以下事項：

(1)、採購新設備或更新作業系統。

(2)、使用新式問題偵測及控制技術。

(3)、人員及組織之調整變動。

(4)、部門及辦公場所之變動。

(5)、契約當事者或供應商之調整變動。

(6)、應用系統之變動、開發或停用。

(7)、實務作業之變更。

(8)、法規之變更。

3、應於演練 BCP 後進行如下作業：

(1)、應召開檢討會議，檢視 RPO、RTO、MTPD 或 MASL 之合理性及可行性。

(2)、應保留由管理階層核可之相關演練紀錄及檢討會議紀錄。

(3)、若有須異動 RPO、RTO、MTPD 或 MASL，則須偕業務管理單位及相關單位先行確認，再送資安會審查。

六、多重備援

應確保資訊處理設施之可用性，應考量下列控制措施：

(一)、資訊處理設施之可用性

應對資訊處理設施實作充分之多重備援，應考量之控制措施說明如下：

1、應確保系統之資訊處理設施具多重備援，以符合營運持續要求。

2、應於演練測試 BCP 相關作業時，確保多重備援系統之可用性。

七、營運持續教育訓練

屬核心資通系統者，相關單位應每年辦理營運持續相關教育訓練，以確保人員及其代理人了解應辦理事項中之角色及權責，應考量之控制措施說明如下：

(一)、辦理單位及參與人員(含其代理人)

1、資訊安全推動單位之負責範圍：營運持續管理權責單位(營運持續管理審查單位及營運持續管理推動協調單位)。

2、資訊安全執行單位之負責範圍：核心資通系統復原負責人員、重要支援資訊系統復原負責人員及復原核心資通系統必要之供應商。

3、核心業務管理單位之負責範圍：核心業務執行人員。

(二)、應紀錄人員受訓結果，並每年檢視其訓練內容之妥適性。

八、本程序書適用範圍之系統亦應遵循銀行公會「金融機構資通安全防護基準」有關「營運持續管理」之要求。

九、本程序書若有未盡事宜，悉依主管機關之相關法規及本行之規定辦理。

十、本程序書經總經理核定後施行；修訂時亦同。惟如因組織調整僅需修改本程序書所列之單位名稱者，授權由資訊安全長核定之。

第七條、輸出文件

一、IS-2-006-01 營運衝擊分析表。