中央銀行

資通安全事件通報及應變程序

110 年 7 月修正

目　次

壹、目的

中央銀行(以下簡稱本行)為因應於發生資通安全事件時，迅速完成通報、損害控制或復原作業，降低對業務之衝擊影響，並確保相關跡證保存，依據資通安全管理法第 14 條之規定，制定本資通安全事件通報及應變程序(以下稱本程序)。

貳、名詞定義

一、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。包含但不限於發生下列情事，影響資訊業務運作：

(一)資料遭洩露。

(二)資料遭竄改。

(三)系統服務中斷。

(四)系統效能突然大幅下降。

(五)網路遭非法入侵。

(六)電腦病毒感染。

二、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經行政院定期檢視並公告之領域。

三、核心業務：指依中央銀行法足認為本行核心權責所在之業務，或本行維運、提供關鍵基礎設施所必要之業務。

四、核心資訊系統：指支持本行核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高之系統。

五、一般公務機密：指行政院文書處理手冊第五十一點所稱本行持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。

六、敏感資訊：指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。

七、國家機密：指依國家機密保護法第二條所稱為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依該法核定機密等級者。

參、作業原則

一、本行所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本行應於資通安全事件發生前，確保所管之特定非公務機關制定及落實資通安全事件通報及應變程序，並依規定指定其知悉資通安全事件之通報以及完成應變作業後之結案登錄方式。且於知悉其資通安全事件後，依規定向行政院通報。

三、本行應視必要性，與受託廠商約定，使其制定其資通安全事件通報及應變程序，並於知悉資通安全事件後向本行進行通報，於完成事件之通報及應變程序後，依本行指示提供相關之紀錄或資料。

四、本行應於知悉資通安全事件後，依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依行政院指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、事件通報窗口

一、本行之資通安全事件通報窗口為資訊處，資訊作業問題申告專線為(02)2357-1333。

二、本行應以適當方式使相關人員明確知悉本行之通報窗口及聯絡方式。

三、本行所屬人員發現資通安全事件後，應立即向資訊處通報。

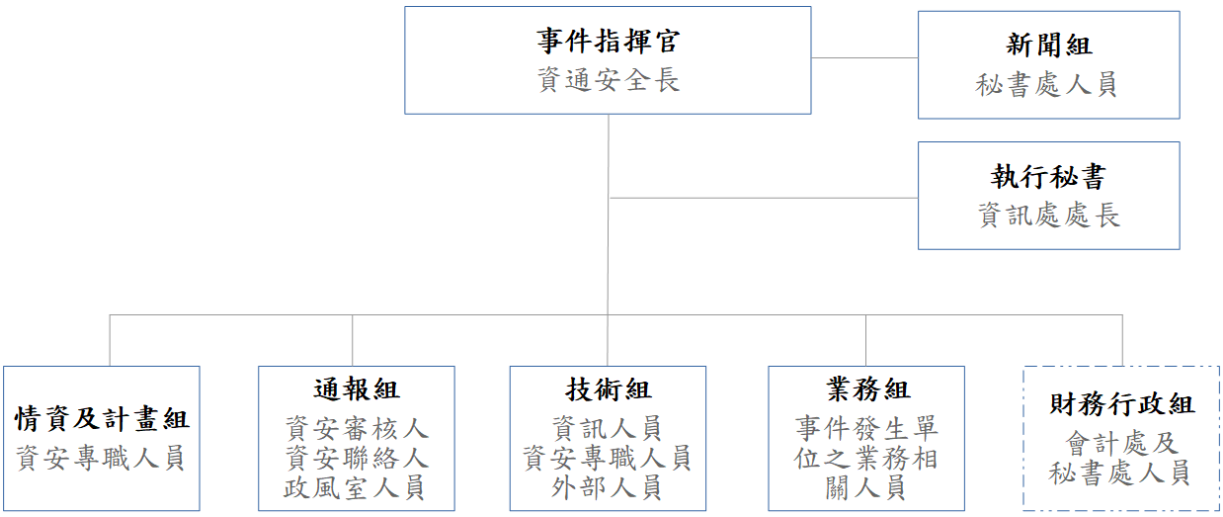
四、本行應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達 1 小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

伍、資通安全事件通報及應變小組

本行成立資通安全事件通報及應變小組(以下簡稱通報應變小組)，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。

一、通報應變小組小組組成及分工

通報應變小組組成如圖一，其任務如下：



圖一、通報應變小組組成

(一)事件指揮官

為通報應變小組總召集人，綜理全般業務；由資通安全長擔任。

(二)執行秘書

為事件指揮官幕僚，負責督辦通報應變小組各項業務；由資訊處處長擔任。

(三)情資及計畫組

1. 本分組負責辦理下列事宜：

(1)資安事件情資處理：

A. 透過資通安全監控中心(SOC)、防毒軟體及系統，釐清事件影響、並清查受影響情形。

B. 分享惡意程式、IoC 等情資給有關單位及所管機構。

(2)應變策略及計畫研擬：依據事件情況研擬損害控制、復原作業及跡證保存計畫。

2. 本分組由資通安全專職人員組成。

(四)通報組

1. 本分組負責資通安全事件各階段通報。

2.本分組成員及分工如下：

(1)本行資安聯絡人、資安審核人：負責至國家資通安全通報應變網站辦理通報及通報審核；由資訊處人員擔任。

(2)政風室人員：視事件需要通報執法機關。

(五)技術組

1.本分組負責辦理下列事宜：

(1)應變執行

A.損害控制：依據情資及計畫組研擬之應變策略及計畫，調度人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。

B.復原：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。

(2)後勤調度(事後追查及改善)

A.跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

B.事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。

C.提出改善建議：依據事件調查根因，提出短、中、長期改善建議。跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

2.本分組成員及分工如下：

(1)負責應用系統維護及作業環境維護管理之資訊人員、資安專職人員：負責應變處理、跡證保存相關作業；原則為資訊處人員。

(2)外部人員：視事件情形得邀請外部人員支援，如：委外廠商、外部專家、主管機關或相關機關人員。

(六)業務組

於該單位發生資通安全事件時，參與危機通報及緊急應變處理作業；由事件發生單位之業務相關人員組成。

(七)新聞組

負責綜整與定期更新訊息及擬定溝通計畫，為資通安全事件對外發布新聞或說明之單一窗口；由秘書處人員組成。

(八)財務行政組

負責辦理預算調撥及提供行政支援事宜；視事件需要由會計處或秘書處人員組成。

二、運作原則

若經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長召開會議研商相關事宜，並得請相關機關提供協助；接獲本行所屬機關或受託廠商所通報之資通安全事件時，亦同。

通報應變小組之各分組應密切合作以進行事件之處理，並使**通報組**適時掌握事件處理之進度及其他相關資訊。

技術組應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

陸、通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

情資及計畫組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。
4. 本行業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

	機密性 資訊遭洩漏		完整性 資訊/資通系統遭竄改		可用性 業務/資通系統運作受影響	
影響程度 業務性質 /資通系統別	洩漏程度		竄改程度		於可容忍時間內回復	
	輕微	嚴重	輕微	嚴重	可	不可
非核心業務	1 級	2 級	1 級	2 級	1 級	2 級
非核心資通系統	—	—	1 級	2 級	—	—
核心業務 (未涉及 CI 維運)	2 級	3 級	2 級	3 級	2 級	3 級
核心資通系統 (未涉及 CI 維運)	—	—	2 級	3 級	2 級	3 級
核心業務 (涉及 CI 維運)	3 級	4 級	3 級	4 級	3 級	4 級
核心資通系統 (涉及 CI 維運)	—	—	3 級	4 級	3 級	4 級
一般公務機密 、敏感資訊	3 級	4 級	3 級	4 級	—	—
國家機密	4 級	4 級	4 級	4 級	—	—

表一、資通安全事件分級表

(二)除事件之等級外，**情資及計畫組**亦應透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並對資通安全事件之影響範圍、損害程度及本行因應之能力進行評估。若屬第 3 級或第 4 級之資通安全事件，應依據事件情況研擬損害控制、復原作業及跡證保存計畫。

(三)**情資及計畫組**於完成資通安全事件等級之判斷及相關評估後，應儘速陳報**事件指揮官**，包括事件影響範圍、程度、估計損失、預計處理時間及處理方式，並通知本行相關業務單位、會計處及政風室。

(四)**通報組**應於知悉資通安全事件後 1 小時內至國家資通安全通報應變網站進行事件通報，通報內容應包括下列項目：

1. 發生機關。
2. 發生時間。
3. 狀況之措述。
4. 等級之評估。
5. 因應事件所採取之措施。
6. 外部支援需求評估。
7. 其他相關事項。

(五)若屬第3級或第4級之資通安全事件，應以電話或其他適當方式通知行政院，**事件指揮官**應召開會議研商相關事宜。

(六)若因網路或電力中斷等事由，致無法依前項規定方式為通報者，**通報組**應於知悉資通安全事件後1小時內以電話或其他適當方式，將該次資安事件應通報之內容及無法通報依規定方式通報之事由，告知行政院，並於事由解除後，依原方式補行通報。

(七)本行於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，**通報組**應於知悉資通安全事件後1小時內，將該事件依行政院所指定或認可之方式，通知該機關。

(八)本行執行通報應變作業時，得視情形向行政院或相關機關提出技術支援或其他協助之需求。

(九)**情資及計畫組**應考量有無通報執法單位、媒體或向社會大眾說明之必要，如有上述必要，應向**事件指揮官**報告，並由**新聞組**、**政風室**配合辦理。

(十)倘涉及個人資料外洩，**業務組**及**新聞組**應評估通知當事人之適當方式，依個人資料保護法第12條規定辦理。

二、接獲自身或所管特定非公務機關通報之評估作業程序

(一)**通報組**於接獲自身或所管特定非公務機關之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核：

1. 通報為第1級或第2級之資通安全事件，於接獲通報後8小時內。

2. 通報為第3級或第4級之資通安全事件，於接獲通報後2小時內。

(二)**通報組**進行前項之審核過程中，得請求通報之特定非公務機關提供級別判斷所需之資料或紀錄。

(三)本行於必要時得依據審核之結果，逕行變更資通安全事件之等級，並應於完成審核後1小時內，由**通報組**將審核結果通知行政院，並提供審核依據之相關資訊。

(四)本行於完成所管特定非公務機關資通安全事件之審核後，若審核結果為第3級或第4級資通安全事件者，**通報組**應於1小時內依行政院指定或認可之方式通知行政院；若為第1級或第2級資通安全事件者通

報後，**通報組**應依行政院指定或認可之方式，定期彙整相關資訊送交行政院。

三、對所管特定非公務機關之協助

本行所管特定非公務機關知悉資通安全事件，向本行通報時，本行資通安全長應視必要性於以下時限內，決定是否組成緊急應變小組，以協助所管特定非公務機關執行通報及應變程序，並視情形提供必要之支援或協助：

(一)通報為第1級或第2級之資通安全事件，於完成複核後2小時內。

(二)通報為第3級或第4級之資通安全事件，於接獲通報後1小時內。

柒、應變程序

一、損害控制或復原作業

(一)於完成第3級或第4級資通安全事件之初步損害控制後，應召開事件應變會議，由**事件指揮官**主持討論下列事項：

1. 資通安全事件概況。

2. 評估受影響範圍。

3. 其他必要之討論事項。

(二)由**技術組**執行損害控制或復原作業，並辦理下列事項：

1. 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。

2. 評估各系統是否於可容忍中斷時間內恢復服務、需否啟動異地備援機制及對利害關係人之影響，決定是否對外公告事件之相關內容。

3. 若需啓動異地備援機制，則協調相關人員依照各資訊系統災害復原計畫及業務持續運作計畫進行事件排除與復原。

(三)資通安全事件等級如有變更，**技術組**應告知**通報組**，使其續行通報作業。

(四)第1級、第2級資通安全事件，本行應於知悉事件後72小時內完成損害控制或復原作業；第3級、第4級資通安全事件，本行應於知悉事

件後36小時內完成損害控制或復原作業，**通報組**並定時向事件指揮官、通報應變小組成員、行政院回報控制措施成效。

(五)**通報組**應於完成損害控制或復原作業後，依行政院指定之方式完成通知作業，並應將資通安全事件之處理方式、處理時間、影響範圍、處理結果等，詳實記錄於「資通安全事件通報處理紀錄單」，並依事件等級陳報後歸檔備查。

(六)本行於知悉受託廠商發生與受託業務相關之資通安全事件時，**技術組**應於知悉委外廠商發生第1、2級資通安全事件後72小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第3、4級資通安全事件後36小時內，確認委外廠商完成損害控制或復原事項之辦理。

二、發生資通安全事件時，**技術組**應依下列原則進行跡證保存：

(一)進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。

(二)若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。

(三)若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。

(四)若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

捌、資安事件後之復原、鑑識、調查及改善機制

一、本行完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，**技術組**並應於事件發生後1個月內完成資通安全事件調查、處理及改善報告。

二、由**技術組**執行事件根因分析，辦理事項如下：

(一)保存相關跡證，如發現惡意程式，應上傳至 Virus Check 網站(https://viruscheck.tw/)進行檢測；因故無法上傳時，應送交防毒軟體或資安服務公司檢測。

(二)除設備故障外，**技術組**應依據前目保存跡證，督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如有發現惡意程式，應提出惡意程式分析。

(三)依據事件調查報告，應評估短、中、長期資安管理改善策略，其內容如下：

1. 短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。

2. 中期：依據事件根因提出 3 至 6 個月內完成之強化作為，例如盤點機關老舊設備，並訂定汰換期程。

3. 長期：依據事件受害情形，視需要提出 2 年內完成之管理改善建議，例如培養機關資安人員能力。

(四)由**執行秘書**將事件調查根因及改善策略提報**事件指揮官**裁處，並由**通報組**彙整送交行政院。

三、進行事件改善追蹤時，**事件指揮官**或**執行秘書**應召開會議，並據以辦理下列事項：

(一)評估改善作為期程。

(二)評估執行成效，並據以調整改善策略。

(三)配合行政院辦理相關改善作為。

(四)第 3 級或第 4 級資通安全事件，應由**執行秘書**將各階段改善措施執行成效定期回報**事件指揮官**至完成各項改善措施為止，並由**通報組**彙整送交行政院。

(五)應於完成損害控制或復原作業後 1 個月內，依會議決議及行政院指定之方式，送交調查、處理及改善報告；第 3 級或第 4 級資通安全事件，**通報組**應另以密件公文將該報告送交行政院。

(六)送交調查、處理及改善報告後，相關改善事項應納入定期追蹤管考。

四、資通安全事件調查、處理及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

五、本行指示所管特定非公務機關提出資通安全事件調查、處理及改善報告之期限，若其逾期未提出，本行除應使其儘速提出外，並應為其他必要之監督及指示。

六、本行完成通報及應變程序之辦理，或於接獲所管特定非公務機關之損害控制、復原與事件之調查及處理作業完成通知後，**通報組**應依行政院所指定或認可之方式進行結案登錄。

七、本行應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資通安全事件通報處理紀錄單」上留存完整之紀錄，該文件並應經承辦之權責人員簽核，並陳報資通安全長。

八、本行於完成資通安全事件之通報及應變程序後，應依據「資通安全事件通報處理紀錄單」之內容及實際處理之情形，於必要時對本程序、人力配置或其他相關事項進行修正或調整。

玖、日常作業

一、事件發生前之防護措施規劃

本行應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資通安全事件之發生。

二、紀錄留存及程序之調整

於日常維運資通系統時，應保存全部資通系統與各項資通及防護設備最近6個月之日誌紀錄(log)，並定期備份於外部設備。保存項目包含：

(一)作業系統日誌(OS event log)。

(二)網站日誌(web log)。

(三)應用程式日誌(AP log)。

(四)登入日誌(logon log)。

三、於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商應保存與受託業務相關之資通系統與各項資通及防護設備最近6個月之日誌紀錄(log)，並定期備份於外部設備；於知悉資通安全事件時，應即向本行之權責人員或窗口，以指定之方式進行通報，並應進行跡證保存。

拾、演練作業

一、本行應每年依資通安全事件通報應變辦法之規定辦理社交工程演練、資通安全事件通報及應變演練，並於完成後1個月內，將執行情形及成果報告送交行政院。

二、本行應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程演練。

(二)資通安全事件通報及應變演練。

(三)網路攻防演練。

(四)情境演練。

(五)其他資安演練。

附錄、資安事件通報及應變流程圖