事件管理程序

|  |  |
| --- | --- |
| ◎文件編號： | SO-18-001 |
| ◎文件版次： | V 3.1 |
| ◎發行日期： | 2023/12/21 |

文件修訂履歷

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 修訂版次 | 修訂日期 | 發行與變更說明 | 權責  人員 | 核准  人員 | 備註 |
| V1.0 | 2009/10/30 | 新版文件 | 施雷蜀華 | 梁維誠 |  |
| V1.1 | 2009/12/11 | 修改第六章作業內容以符合事件管理運作現況。 | 施雷蜀華 | 梁維誠 |  |
| V1.2 | 2009/12/24 | 修訂F級事件目標處理時間。  修訂六章第四節有關事件結案之作業內容。 | 施雷蜀華 | 梁維誠 |  |
| V1.3 | 2011/1/21 | 修訂事件分級原則 | 施雷蜀華 | 周宗亮 |  |
| V1.4 | 2011/10/21 | 因應公司更名，修訂文件公司名稱。 | 施雷蜀華 | 周宗亮 |  |
| V2.0 | 2011/11/18 | 因應公司文件核准層級，文件名稱配合變更。 | 施雷蜀華 | 周宗亮 |  |
| V2.1 | 2012/04/19 | 調整事件記錄條件。 | 施雷蜀華 | 周宗亮 |  |
| V2.2 | 2013/05/06 | 因應ISO20000:2011新版條文要求，新增服務請求。 | 施雷蜀華 | 潘靜螢 |  |
| V2.3 | 2014/02/14 | 增訂《SO-18-001-附件A\_事件管理流程圖》 | 施雷蜀華 | 丘建華 |  |
| V2.4 | 2015/12/09 | 調整C、D、E、F級事件定義中的影響範圍 | 施雷蜀華 | 丘建華 |  |
| V2.5 | 2015/12/30 | 調整G級事件中目標處理時間 | 施雷蜀華 | 丘建華 |  |
| V2.6 | 2016/10/13 | 調整D級事件影響範圍 | 施雷蜀華 | 余萬事 |  |
| V2.7 | 2017/05/12 | 1. 第五章第七節，新增「事件呈報人員」 2. 第六章第一節，增加事件通報主管機關機制 3. 新增《SO-18-001-附件B 證券期貨市場資通安全事件通報應變作業注意事項》 | 施雷蜀華 | 周宗亮 |  |
| V2.8 | 2018/08/10 | 修改D級事件影響範圍 | 施雷蜀華 | 余萬事 |  |
| V2.9 | 2020/05/26修訂  2020/07/01發行 | 修改G級事件處理方式 | 施雷蜀華 | 余萬事 |  |
| V3.0 | 2021/04/23 | 配合2020年桌面演練決議，增修資訊安全事件之判定及結束作業。 | 雷惜福 | 周宗亮 |  |
| V3.1 | 2023/12/21 | 修改第六章第三、四、五節 | 吳美慧 | 余萬事 |  |

目錄

[第一章 目的 4](#_Toc382914107)

[第二章 範圍 4](#_Toc382914108)

[第三章 名詞定義 4](#_Toc382914109)

[第四章 相關文件 4](#_Toc382914110)

[第五章 權責 5](#_Toc382914111)

[第一節 通報人 5](#_Toc382914112)

[第二節 通報人部門主管 5](#_Toc382914113)

[第三節 資訊部主管或其指定代理人 5](#_Toc382914114)

[第四節 維運處主管 5](#_Toc382914115)

[第五節 事件管理流程負責人 5](#_Toc382914116)

[第六節 事件管理主管 5](#_Toc382914117)

[第七節 事件處理團隊 5](#_Toc382914118)

[第八節 資訊安全管理流程負責人 6](#_Toc382914119)

[第六章 作業內容 6](#_Toc382914120)

[第一節 事件偵測與記錄 7](#_Toc382914121)

[第二節 事件分類及初步支援 8](#_Toc382914122)

[第三節 事件調查及診斷 11](#_Toc382914123)

[第四節 事件解決、恢復與結束 12](#_Toc382914124)

[第五節 流程監控、檢視與報告 13](#_Toc382914125)

[第七章 輸出文件記錄 13](#_Toc382914126)

# 目的

為建立本公司資訊部（以下簡稱本部）事件管理流程之作業準則，特訂定事件管理程序（以下簡稱本程序），規範事件之記錄、分類、解決、處理、結案，以達成以下目標：

### 確保本部提供資訊服務之各類事件處理，均已書面化以利權責單位依循辦理。

### 確保本部所提供資訊服務，各種造成使用者服務使用不便情形，能確實依據議定之服務水準與公司管理要求，盡速加以排除，並對使用者意見加以記錄處理。

# 範圍

本資訊服務管理體系之實施範圍為本部所提供之資訊服務。

# 名詞定義

### 事件（Incident）：任何造成使用者無法正常使用資訊服務之情況，以及因使用者心理感受而衍生出之意見，均屬之。事件分為系統相關以及非系統相關兩大類，本程序主要規範資訊系統相關之事件：

#### 資訊系統相關之事件，例如軟體與硬體異常所造成的資訊處理錯誤或服務中斷，或因傳輸流量受設備損壞或網路不當使用、或遭受阻絕服務（Denial of service）攻擊而引起的異常情形。

#### 非系統相關之事件，例如使用者之詢問、服務請求、意見反應，公用設施受損（包含水電力中斷等）或實體環境因不可抗力因素而造成資訊資產毀損無法正常營運（包含火警、地震、颱風、水災等），因重大疾病及傳染病之因素造成工作環境或人員必需隔離而影響資訊人員正常執行營運作業。

### 影響範圍（Impact）：造成客戶營運已發生或潛在可能發生損害之程度。

### 緊急程度（Urgency）：客戶對於恢復該資訊服務功能之急迫程度。

### 事件分級（Incident Priority）：依定義好事件分級，帶出相關等級所定義之影響範圍（Impact）與緊急程度（Urgency）。

# 相關文件

### BO-CM-001\_事件通報程序

### ~~SO-13-001\_問題管理程序~~

### SO-15-001\_變更管理程序

### SC-00-016\_企業關係管理要點

### SO-MG-007\_服務報告管理程序

# 權責

## 通報人

公司所有使用者皆應主動通報事件，並協助確認、排除與解決。

## 通報人部門主管

部門主管或其代理人於系統相關之事件發生時，接收通報人之通報。

## 資訊部主管或其指定代理人

經判斷屬A級之事件，應立即向本公司指揮官通報，並進行事件處理。

## 維運處主管

### 屬重大事件，由維運處主管向資訊部主管呈報並通報各業務權責單位主管

### 維運處主管於重大事件期間，於營業上班時間於監控室統籌各項處理情形與回報，例假日及非上班時間緊急通報並協調相關人員處理

## 事件管理流程負責人

### 由維護營運處一科主管擔任

### 負責設計事件管理流程之關鍵績效衡量指標（KPIs）

### 負責事件管理流程管理報表及績效管理指標之檢視及報告

### 負責提出事件管理流程運作之改善建議

## 事件管理主管

### 由維護營運處一科主管擔任

### 確保事件管理依據流程設計要求運作

### 監控事件管理績效評量狀況

### 提出事件管理改善建議

### 事件處理完畢後，確認事件之排除狀況，應向相關人員通報事件處理完畢

## 事件處理團隊

### 事件處理團隊由事件管理人員、事件處理人員、事件呈報人員所組成

### 事件管理人員，其職責如下：

#### 由維護營運處人員擔任；另服務自有資金及非交易部分系統亦可由下列人員擔任

##### 金融系統處：可擔任衍商、風控、會計、財務系統等相關自有資金系統之事件管理人員。

##### 技術研發處：可擔任CIS、CIS人事、CRM、Mail、LCS系統、企金、保金保代、KPI等非交易系統之事件管理人員。

#### 依據事件管理流程，執行各項作業

#### 負責事件生命週期之追蹤，包含事件記錄、分類、初步支援、解決及恢復與結束

#### 將接獲或監控到疑似資訊安全事件之事件通知予資安人員、客服人員及其他相關主管或人員

#### 依據所授權範圍與專業能力，進行事件之處理解決

#### 向使用者說明事件處理情況與服務現況

#### 執行各項改善作業

#### 提供初步資訊安全事件之事件處理措施、情況、結果予資安人員、客服人員及其他相關主管或人員

### 事件處理人員，其職責如下：

#### 由資訊部同仁擔任

#### 負責處理事件管理人員未能處理之事件或足以影響交易的緊急事件，如下述

##### 盤中報價，風控，下單等事件需立即反應，並由事件處理人員共同參與處理，儘速排除異常

##### 未能提供事件管理人員標準處理程序之事件

##### 未曾發生過事件無法判斷原因者

##### 需修改程式及資料庫

### 事件呈報人員，其職責如下：

#### 由策略發展處二科同仁擔任

#### 接獲事件通報(如：監控中心、客服人員、分公司等)，由資安人員判斷是否屬資訊安全事件

#### 依據主管機關要求，經與稽核室及相關主管或人員確認事件等級與通報層級後，負責向主管機關通報資訊安全事件

#### 依據事件處理之結果，經與稽核室及相關主管或人員判斷資安事件結束，通知事件管理人員進行事件結案

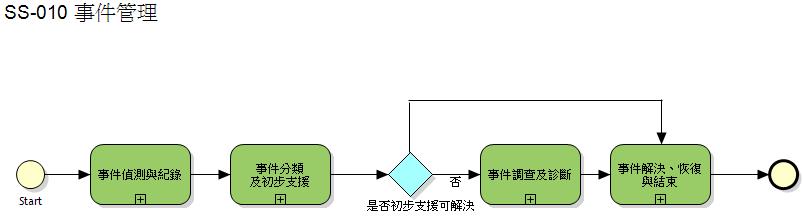
## 資訊安全管理流程負責人

### 由資訊部主管指派資訊安全人員擔任

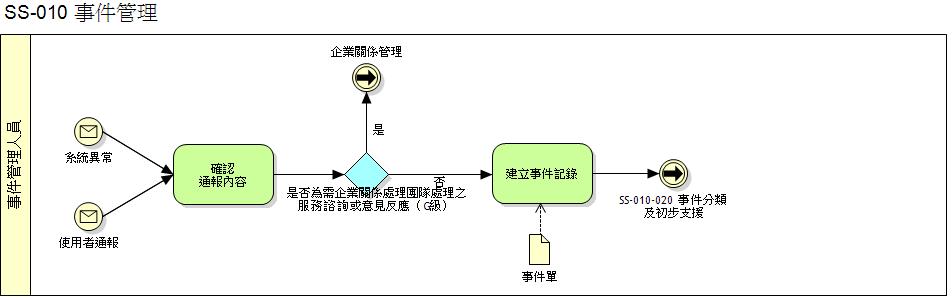
### 參與事件監控、檢視及報告作業活動，並提供事件管理流程之諮詢

# 作業內容

本管理程序之分為事件偵測與紀錄、事件分類及初步支援、事件調查及診斷、事件解決、恢復與結束，共四個作業內容。細節執行步驟流程圖，於各節分述說明。



## 事件偵測與記錄



### 事件通報

#### 所有人員發現（或懷疑發生）任何服務異常事件，應在知會直屬部門主管後，由通報人判斷該事件屬於系統相關或非系統相關之事件，資訊系統類之事件通報應予資訊部監控室~~中心~~。非系統類之事件則應統一通報至部門主管，並依循《BO-CM-001\_事件通報程序》辦理。

#### 監控系統自動通報或經值班人員檢核後判斷其會造成異常現象時，必須通報至資訊部監控室~~中心~~，並立即採取因應的行動措施。

#### 若屬服務請求依據《SO-18-001-F03\_服務請求清單》程序進行事件通報。

### 事件記錄

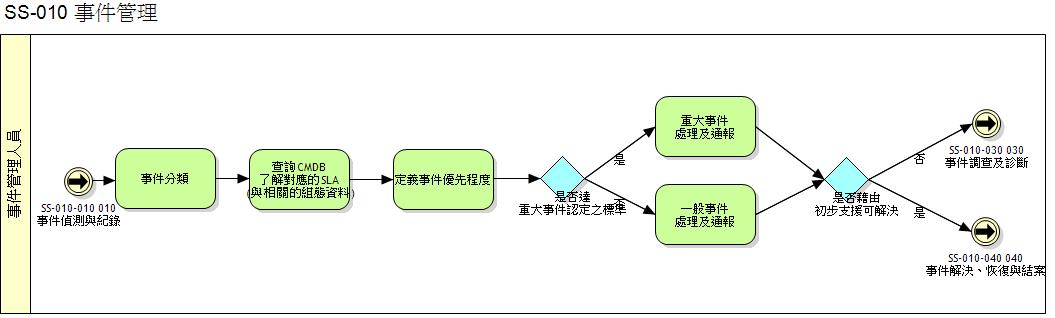
#### 通報人通報事件至資訊部監控室~~中心~~時，事件管理人員應儘速處理，使事件能在最短時間內獲得處理。事件管理人員在事件處理後應於事件管理系統開立《SO-18-001-F02\_事件單》並將記錄處理內容。若使用者通報內容屬於意見反應，由通報人直接通報紀部業務管理處統整後向資訊部提出需求。

#### 由監控系統自動通報後或經由值班人員檢核的異常，若已造成異常或判斷不處理將會造成異常，值班人員應於事件管理系統開立《SO-18-001-F02\_事件單》並由事件管理人員進行後續追蹤。

#### 事件管理人員應於事件結束後儘速完成事件開立及紀錄，並將接受事件通報之時間與事件結束之時間填入《SO-18-001-F02\_事件單》中之『事件發生時間』、『事件結束時間』欄位。

#### 若屬服務請求依據《SO-18-001-F03\_服務請求清單》程序進行事件記錄。

## 事件分類及初步支援



### 事件分類

#### 事件類型：事件管理人員應依據事件的描述，對應下列事件類型之定義，以下各事件類型中提到相關事件分級，各分級的判斷標準將在本章本節中「二、事件分級」中詳述。

##### 服務異常

資訊服務因系統或非系統因素，使得服務提供狀況不符所議定之要求，其對應事件分級為A級～F級。

##### 服務諮詢

使用者對系統使用操作不熟悉及對資訊業務不了解，或屬使用者對於現有服務提供，因個人使用因素而有解釋說明需要，其對應事件分級為F級。

##### 意見反應

功能新增及修改建議，由通報人直接通報紀部業務管理處統整後向資訊部提出需求。

##### 服務請求

使用者對於不需修改程式及異動資料的請求，須提供使用者標準的作業程序，其對應事件分級為R級，並依據《SO-18-001-F03\_服務請求清單》程序進行事件通報、記錄及處理。

#### 服務類別：則在事件管理人員應在接獲事件時由通報人的資訊及觀察到的現象判斷那些服務受到影響，服務類別內容請參考《SC-00-017\_服務水準管理要點》。

#### 系統名稱：由事件管理人員應在接獲事件時，由通報人提供之資訊及觀察到之現象判斷並選擇何為主要受影響系統。並可連結CMDB功能得知目前該異常主要系統或服務之最新狀況及其他可能受影響的相關系統。

### 事件分級

#### 依事件管理人員塡入的事件分級，系統主動帶出緊急程度及影響範圍，另依照事件管理人員填入之「事件發生時間」欄位起算各事件分級之目標處理時間，以協助事件處理團隊瞭解該事件排除之急迫性。

#### 事件分級A至D級定義為重大事件。

#### 資訊安全事件為A至C級之事件以及經資安及相關人員依據資訊或系統遭洩漏、竄改或運作受影響情事判定屬資安事件之事件。

| 事件類型 | 說明 | 事件分級 | 影響範圍 | 緊急程度 | 目標處理時間 |
| --- | --- | --- | --- | --- | --- |
| 服務異常 | 資訊服務因系統或非系統因素，使得服務提供狀況不符所議定之要求。 | A | 全面營運中斷或直接影響商譽 | 高 | 1小時 |
| B | 部分營運中斷 | 高 | 1小時 |
| C | 單一交易系統全面無法正常運作，且異常狀況超過30分鐘仍未能獲得控制 | 中 | 次一營業日前（8:00A.M.）恢復系統正常運作  （事件發生15分鐘內提供替代方案） |
| D | 有以下情況之一成立者：  1.單一交易系統全面無法正常運作，但異常狀況於30分鐘內獲得控制  2.系統功能異常有交易面影響，含下單、行情、帳務(如庫存、未平倉)功能，且該系統無其他替代功能，並受影響客戶達50位(含)以上3.造成公司損失1萬元以上或單一事件申報錯帳人數達3人以上(含3人)。 | 中 | 次一營業日（8:00A.M.）前恢復系統正常運作  （事件發生15分鐘內提供替代方案） |
| E | 有以下情況之一成立者：  1.系統功能異常有交易面影響並影響少數使用者  2.非交易系統功能異常，有帳務作業面影響  3.單一事件，需特別關注追蹤(由事件管理人判斷) | 低 | 次一營業日17:00前 |
| F | 1.系統功能異常，無交易及帳務作業面影響  2.單一事件，不用特別關注追蹤 | 低 | 7天（含假日） |
| 服務諮詢 | 使用者對於現有服務提供，因個人使用因素而有解釋說明需要 |
| 意見反應 | 使用者對於現有服務之建議，或是人員處理過程之態度反應。 | G | N/A | N/A | 功能新增及修改建議，由通報人直接通報紀部業務管理處統整後向資訊部提出需求。 |
| 服務請求 | 使用者對於不需修改式及異動資料的請求。 | R | 單一個人或少數使用者 | 與交易相關則緊急程度高，反之則低 | 依據《SO-18-001-F03\_服務請求清單》內不同種類規範不同目標時間 |

### 各級事件處理程序

各等級事件處理程序如下。各事件等級皆可由事件管理團隊依狀況調整其事件等級，調整後則依各等級進行相關處理程序。

所有資訊系統相關之重大事件皆應透過電子郵件或口頭通報資訊部主管及維運處主管；惟為處理上之即時性，維運處主管於接到通知時，則應立即主動通報資訊部主管及業務權責主管，並於三個工作天內提供重大事件改善報告予業務權責主管。

#### A、B等級事件

##### 經判斷為A級之事件，則應立即通知危機處理小組組長及指揮官，由指揮官視事件狀況決定是否啟動異地辦公室進行業務復原，並授權資訊部主管啟動異地備援機房。

##### 經判斷為B級事件，則交由事件處理團隊進行事件處理並同時回報資訊部部門主管。若B級事件無法於預定時間內進行事件排除時，資訊部部門主管需視情況決定是否將該事件升級為A級事件。

##### 事件處理團隊應隨時記錄與追蹤事件處理過程，並於事件排除後，由維運處主管或其指定代理人確認事件之排除狀況，並通知相關人員問題排除完畢。

##### A或B等級之事件之各項處理之內容或過程與文件必須嚴守機密，所有同仁禁止對外任意談論或傳播，統一由公司發言人對外通報及發言。

#### C或D等級之事件

##### 經事件管理人員協同相關人員判斷為C或D等級之系統相關事件，先回報予資訊部主管或處級主管，由事件管理人員協同事件處理人員負責進行事件排除處理。

##### 事件管理人員應持續追蹤事件處理進度與過程，並於預計處理時間內觀察事件是否已被排除。若異常事件無法於預計時間內排除，則應由事件管理主管協同相關人員訂出事件處理回復措施，通報資訊部主管後經同意後進行。

##### 事件處理團隊應隨時記錄與追蹤事件處理過程，並於事件排除後，由維運處主管或其指定代理人確認事件之排除狀況，並通知相關人員問題排除完畢。

#### E或F等級之事件處理

##### 事件管理人員接獲系統相關之事件通報後，事件管理人員應協同事件處理人員確認事件狀態影響範圍、程度、預計處理時間，通報業務影響之相關人員。

##### 所有事件均應填寫於事件管理系統，切勿延宕或試圖隱瞞，通報內容應說明發生事件原因，事件記錄應包含其通報人、記錄人、發生時間、地點、異常事項、影響範圍…等。

#### G級事件之處理

功能新增及修改建議，由通報人直接通報紀部業務管理處統整後向資訊部提出需求。

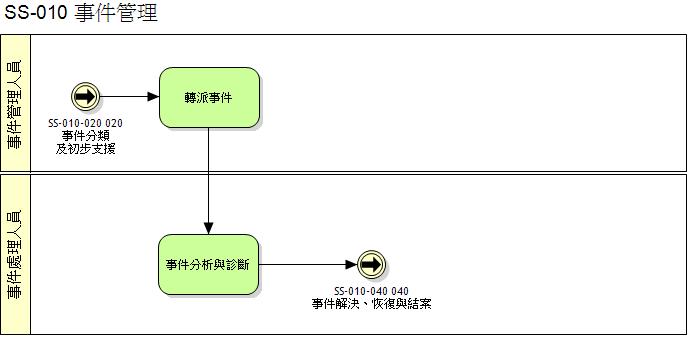
#### R級事件之處理

依據《SO-18-001-F03\_服務請求清單》程序進行事件處理。

#### 資訊安全事件之事件處理

1. 事件管理人員應將接獲或監控到疑似資訊安全事件之事件(參考“事件分級”第三項)通知資安人員及客服人員及其他相關主管或人員。
2. 接獲事件通報(如：監控中心、客服人員、分公司等)，由資安人員判斷是否屬資訊安全事件。
3. 依據《SO-18-001-附件B\_證券期貨市場資通安全事件通報應變作業注意事項》由資安人員或稽核人員進行對主管機關事件通報。

## 事件調查及診斷



### 事件分析與診斷

#### 事件管理人員接獲事件需依標準程序，處理經驗及搜查現有事件處理資料、問題及已知錯誤資料(服務提供者應確保事件和服務請求管理流程的相關人員能存取和使用相關資訊，包括服務請求管理程序、已知錯誤、已解決的問題和組態管理資料庫。另自上線及部署管理流程得到的上線成功或失敗的資訊、預計的上線日期，應可被事件和服務請求管理流程使用)，找出可排除該事件之方式，並將該方式記錄於事件單中，如需支援則將事件反應至事件處理人員接手處理。

#### 事件處理人員應依據事件單內容，利用自身專業能力、問題及已知錯誤資料，找出可排除該事件之方式，並將該方式記錄於事件單中。

#### 為確保事件和服務請求管理流程的相關人員能存取和使用相關資訊，包括服務請求管理程序、已知錯誤、已解決的問題和組態管理資料庫。另自上線及部署管理流程得到的上線成功或失敗的資訊、預計的上線日期，應可被事件和服務請求管理流程使用。

### ~~事件升級成問題~~

#### ~~事件轉成問題的判斷條件：~~

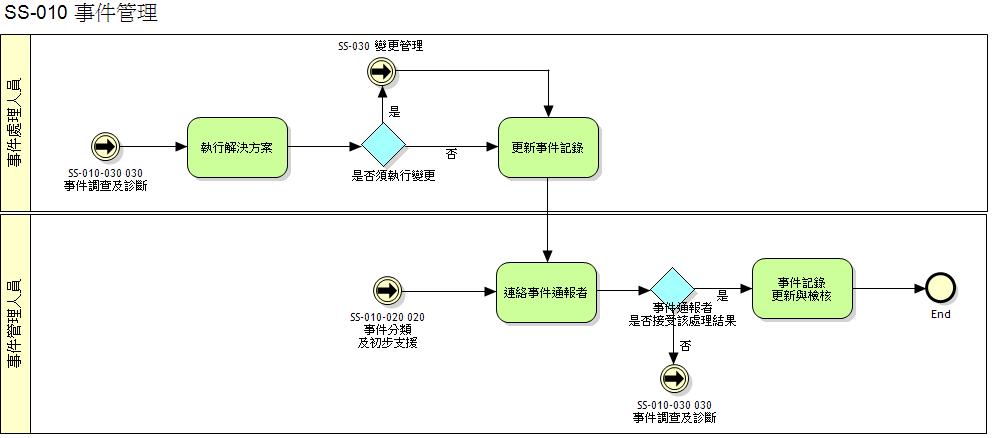
##### ~~事件等級為E級以上且當週無找到根本原因者；~~

##### ~~事件等級為E級以上且已知根本原因但無永久解決方案者或預估若未徹底解決將可能會造成與事件相關系統發生錯帳或直接影響商譽者。~~

~~上述條件若符合其中一項則由事件管理主管勾選轉問題單，並由問題管理主管進一步處理。（詳細內容請參照《SO-13-001\_問題管理程序》）~~

#### ~~如未構成轉問題條件之事件，雖事件已結束但如仍有後續處理動作需進行者，會待後續動作皆完成才會將事件單進行關單動作。~~

## 事件解決、恢復與結束



### 事件排除

#### 事件若已判斷是程式BUG或需修正資料庫，則可由事件處理團隊填寫《SO-08-001-F01\_需求申請單》或《SO-08-001-F06\_資料異動申請書》進行程式修改或資料異動等。（詳細內容請參照《SO-15-001\_變更管理程序》）

#### 盤中發生和交易有關事件須通知系統負責人並報主管並儘速排除。

#### 如影響層面較大則須發出公告或電子郵件給相關使用者並提供使用者應變方式降低事件造成的影響。

#### 非盤中交易時間接獲事件如有標準程序則依其標準程序處理，如無標準程序則尋求事件處理人員支援依事件等級處理程序進行解決。

### 事件結案

#### 如同時接獲多個單位或多位通報人反應，當事件解決後可以用發佈公告方式通知通報人即結案，內容含事件狀況說明及處理方式說明。

#### 如只接獲單一單位或單一通報人反應則以電話、MAIL、OCS等方式回覆處理結果後將其結案。

#### 事件管理人員應於事件結束後通知事件通報人員並填入「事件結束時間」。

#### 事件結案後~~，且不構成問題處理條件者~~，事件處理團隊以及事件管理主管亦可更新事件相關處理內容與結束，進行事件後續追蹤。~~若進一步需要轉為問題者，由事件管理主管會同問題管理主管判斷是否轉問題單。（詳細內容請參照《SO-13-001\_問題管理程序》）~~

#### 若為資訊安全事件，事件管理人員召開事件會議，相關主管及資安人員出席，由事件管理人員提供初步事件處理措施、情況、結果。事件之結案由資安人員經與稽核室及相關主管或人員確認相關處理措施己使資安事件結束並請示相關主管後判斷資安事件結束，對主管機關通報事件結束並通知事件管理人員進行事件結案。

## 流程監控、檢視與報告

### 由事件管理人員記錄後即在目標處理時間內監控及檢視處理進度並協助結案。

### 至少每月由事件管理團隊~~主管~~針對事件~~（問題）~~單產出~~(1)事件（問題）統計表、(2)~~E級以上事件報表及統計表~~、(3)未完成問題追蹤表，於維運處月（週）會或事件檢討會議中提出報告~~。

### 事件管理流程負責人應依據《SO-MG-007\_服務報告作業程序》要求，定義本流程之績效衡量指標及服務報告需求。

### 事件管理流程負責人應針對事件管理流程進行流程監控及檢視，同時針對未能達成之流程關鍵績效指標提出改善計畫。（細節請參照《SO-MG-007\_服務報告作業程序》）

# 輸出文件記錄

### SO-18-001-F02\_事件單

### SO-18-001-F03\_服務請求清單

### SO-18-001-附件A\_事件管理流程圖

### SO-18-001-附件B\_證券期貨市場資通安全事件通報應變作業注意事項