金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

金融資安聯防

金融資安資訊分享與分析中心(F-ISAC)

110年7月

大綱

1 金融資安聯防體系

2 金融資安資訊分享與分析中心營運成果

3 強化資安聯防重點工作

金融資安聯防體系

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

事前防患未然

F-ISAC彙整分析全球資安事件情資，發布駭客威脅預警，並培育資安專業人員，讓金融業者得以事先防範。

事中防微杜漸

F-SOC關聯分析金融業者回傳之事件資訊，探究潛在之可疑行為與攻擊風險，結合情資分享平台強化聯防監控體系。

事後降低傷害

F-CERT協同資安廠商提供應變處理服務，協助金融業者進行損害控制，期能降低損害，儘早恢復金融服務。

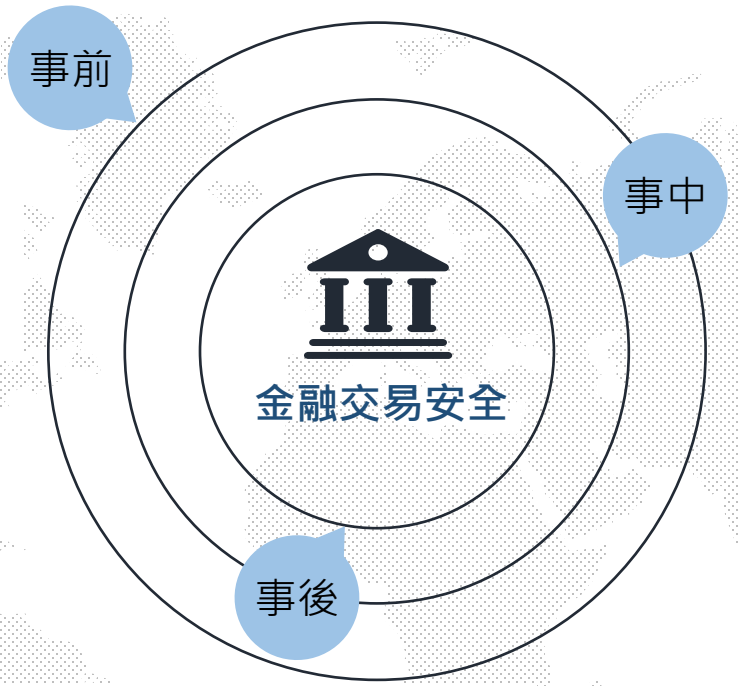
TLP:GREEN

金融資安聯防體系主要服務

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

F-ISAC
金融資安情資分析與分享

- 發布威脅情資或報告
- 舉辦研討會及教育訓練
- 參與國際交流



F-SOC
二線金融資安聯防監控

- 維運並推動資安聯防監控機制
- 與國家資安監控中心(N-SOC)分享資安事件情資

F-CERT
二線金融電腦緊急應變處理

- 資安防護諮詢
- 資安事件應變協處
- 資安攻防演練

TLP:GREEN

金融資安資訊分享與分析中心營運成果

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

金融資安資訊分享與分析中心(106年12月成立)
Financial Information Sharing and Analysis Center

會員數338家

建立國際ISACs情資交流

- FS-ISAC 美國FS-ISAC (108年3月)
- enisa 歐盟FI-ISAC (108年5月)
- Financials ISAC Japan 日本F-ISAC (108年10月)
- CERT-IL 以色列CERT-IL
- 금융보안원 FINANCIAL SECURITY INSTITUTE 韓國FSI

防患未然 F-ISAC事前預防 → **防微杜漸** F-SOC事中監控 → **降低傷害** F-CERT事後復原

威脅預警

- 建置F-ISAC金融資安情資分享平台
- F-ISAC發布威脅警訊計1101則
- 推動會員情資分享計548則

人才培育

- 資安研討會24場
- 資安防護實作課程20梯次
- 資安職能認證課程2梯次

資安演練

- 13家銀行參加行政院跨國攻防演練(CODE2019)
- 辦理「金融DDoS攻防演練」計22家金融業者參演

聯防監控

- 建置F-SOC二線金融資安聯防監控平台
- 制定資安事件聯防監控規則

事件處理

- 建置F-CERT二線金融電腦緊急應變小組
- 109年協助會員處理勒索軟體攻擊事件。
- 110年協助會員處理偽冒網站及詐騙簡訊事件。

TLP:GREEN

金融資安資訊分享與分析中心營運成果

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

近期資安聯防重大成效

發布駭客組織針對我國金融機構發動DDoS攻擊勒索警訊，並與國際ISAC組織情資分享。

協助金融業者處理加密勒索攻擊，清查遭駭範圍、採集可疑程式樣本、分析攻擊手法並提供防護改善建議。

針對Zerologon、SolarWinds Orion IT管理平台等重大安全漏洞發布情資示警，並配合金管會調查金融業者防護現況。

我國關鍵基礎設施遭勒索軟體攻擊之24小時內發布情資示警，讓金融機構得以預先防範，免遭同類型攻擊威脅。

重要專案及連假期間，彙整分析資安監控事件，穩固金融資安聯防監控體系。

協助金融業者處理偽冒簡訊及偽冒網站，彙整分析協請刑事局打詐中心及法務部調查局資通安全處協助封鎖及關閉。

TLP:GREEN

金融資安資訊分享與分析中心營運成果

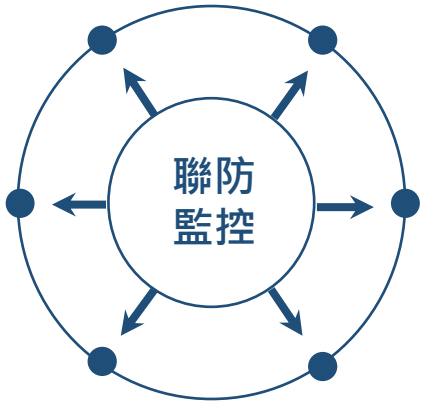
金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

金融資安聯防監控

- 金融資安聯防監控中心(F-SOC)為金融領域二線SOC，收集彙整各金融單位發生之資安事件資訊，做為威脅示警、關聯分析及歷史資料查詢之用。
- 金融業者可藉由**F-SOC提供之95項監控規則**進行資安防護盤點，確認可辨識資安威脅。F-SOC藉由金融業回傳之事件情資，比對、分析可疑攻擊來源，了解金融業目前所面臨之威脅狀態。

F-SOC

- 建立資安監控記錄接收/上傳機制
- 收容金融業者資安監控記錄
- 分析、審核及追蹤資安監控記錄
- 掌握金融領域整體資安現況及威脅
- 跨業別資安聯防分析與情資回饋



金融業者

- 回報資安監控記錄
- 強化事件蒐集與事件分析能量

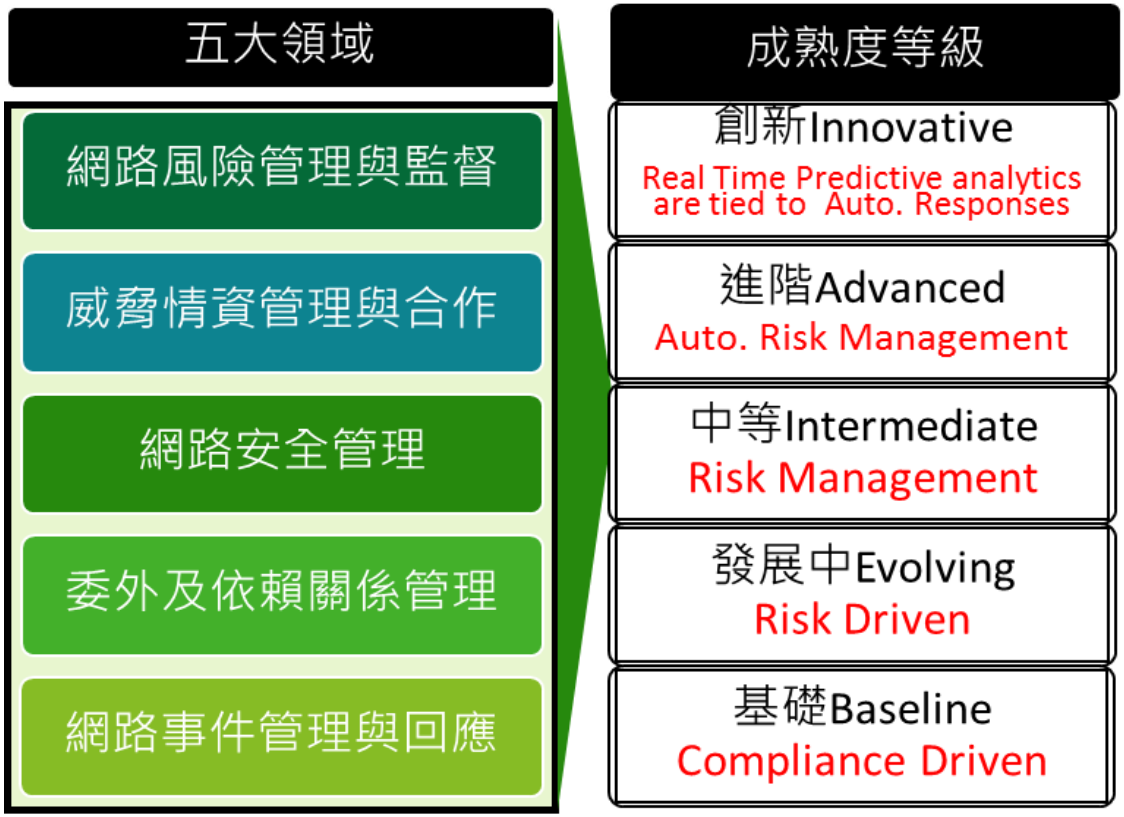
TLP:GREEN

金融資安資訊分享與分析中心營運成果

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

協助推動資安治理成熟度評估

- 設計網路安全評估工具，以**固有風險**普查及**網路安全成熟度**自評兩個面向，協助**金融業者(109年銀行業、110年保險業、111年證券業)**自我評估資安風險與配當之資安治理成熟度。
- 規劃建置符合我國金融產業規模，且可**重複衡量之金融資安治理成熟度評估機制**，以協助金融機構識別組織固有風險，進而瞭解其資訊安全準備情形。



TLP:GREEN

強化資安聯防重點工作(1/6)

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

承辦「強化金融機構資安韌性計畫委外案」

- 金融機構資安監控組態基準及作業指引
- 金融資安攻防演練
- 資料保全運作機制
- 金融業者網際網路服務安全檢測

強化資安聯防

提升資安服務

提升F-ISAC/F-SOC/F-CERT服務

- 金融偽冒網站偵測服務
- 金融資安治理成熟度評估機制
- 資安事件緊急應變服務
- 會員服務單一入口網站
- 自動化監控分析機制
- 資安防護實作課程

TLP:GREEN

強化資安聯防重點工作(2/6)

訂定資通安全防護基準

參考行政院國家資通安全會報技術服務中心發布之共通規範及政府組態基準等相關文件，研擬金融業電腦系統組態基準、資訊系統安全軟體開發生命週期及網路架構規劃等參考指引。包含：

1. Windows伺服器作業系統(3個版本)。
2. Red Hat Linux(1個版本)。

強化資安聯防重點工作(3/6)

建立資安情資關聯分析平台

建立情資關聯分析機制，有效整合外部情資與我國金融機構分享之情資，及時掌握威脅，提供金融機構早期預警及防護建議。本年度執行重點摘錄如下：

1. 外部情資：**維持外部情資來源**(包含ISAC、CERT、資安公司、社群及媒體等)。
2. 我國金融機構分享情資：**金融機構分享情資，經彙整分析後發布比例達5成以上**。
3. 規劃導入資安情資關聯分析平台概念性驗證作業，並**研擬標準交換格式及內容，與F-SOC情資進行介接**。

TLP:GREEN

強化資安聯防重點工作(4/6)

加強金融資安國際合作

掌握國際金融資安情勢並觀摩其服務運作情形，配合國際組織會議時程，參與國際組織會議，並持續加強與國際金融機構合作事宜。

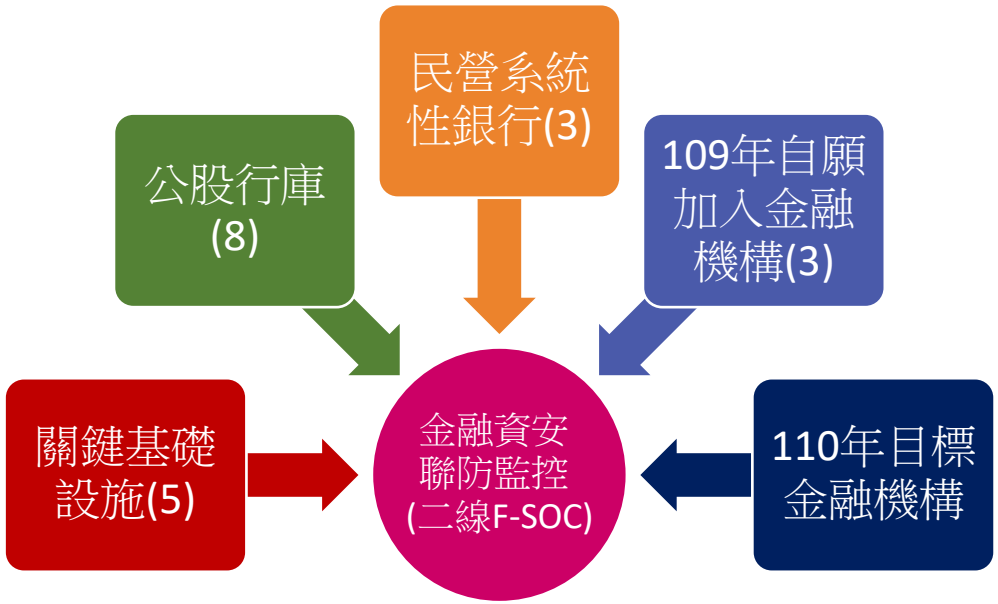
1. **持續參與國際ISAC/CERT組織會議**。
2. **加強與國際金融資安機構合作**(例如：新南向政策之國家、澳洲或紐西蘭等)，並積極參與相關機構之實體或線上會議。

強化資安聯防重點工作(5/6)

推動金融機構SOC與F-SOC協同運作

考量SOC建置成本及推動F-SOC對資安聯防之效益，將循序漸進邀請主要金融機構參與F-SOC運作。

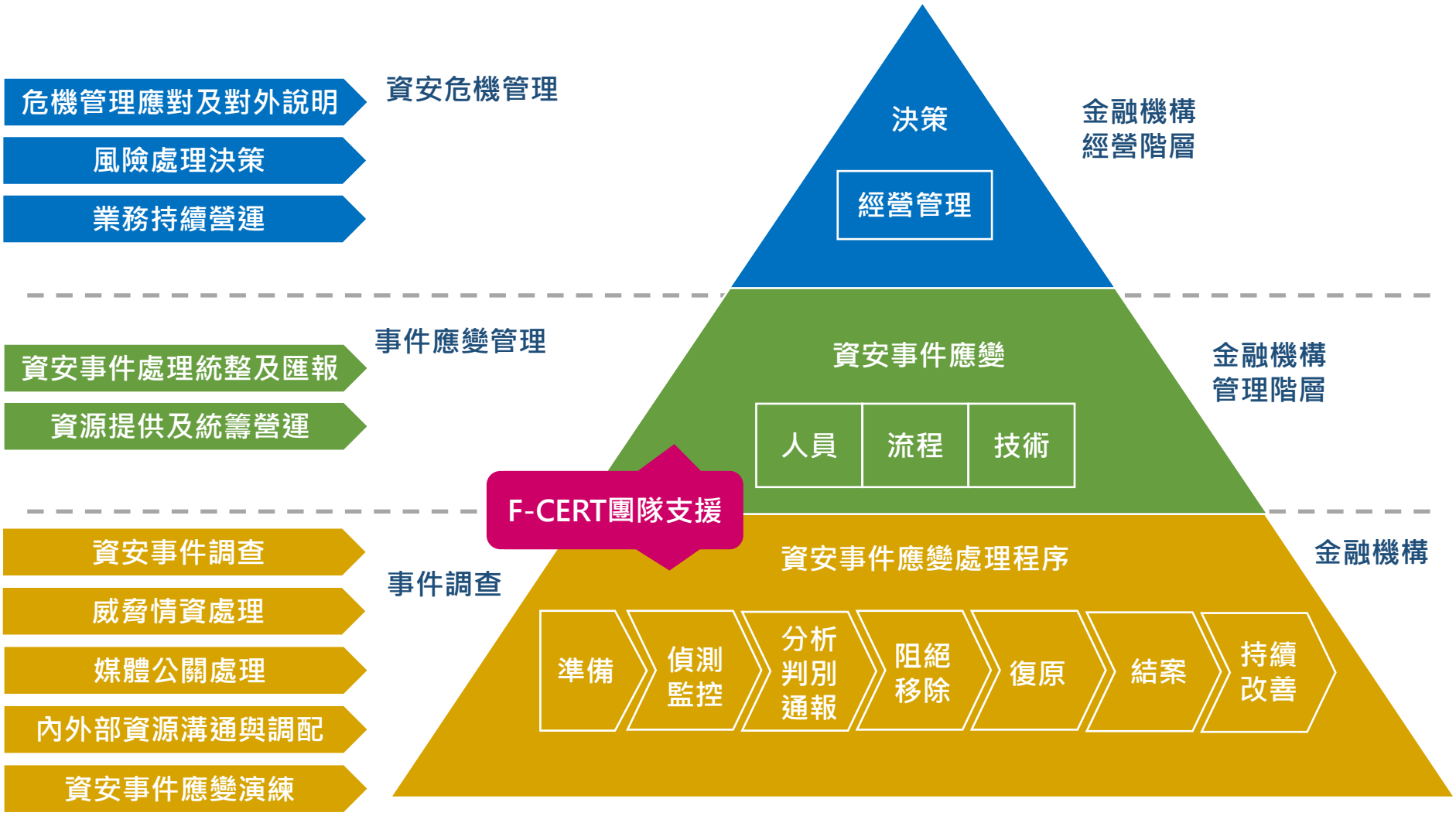
109年度已有關鍵基礎設施、公股、民營系統性銀行及重點金融機構加入F-SOC二線資安聯防監控，**110年持續邀請金融機構參與，並每季產製F-SOC監控分析報告**。



強化資安聯防重點工作(6/6)

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

支援金融資安事件應變體系



TLP:GREEN

以情資驅動的資安防護

強化金融交易安全

金融資安資訊分享與分析中心(F-ISAC)
www.fisac.tw
service@fisac.tw
(02)2655-7077