金融監督管理委員會
Financial Supervisory Commission

金融資安 NEXT

金融監督管理委員會
資訊服務處 林裕泰
111年9月22日

金融資安行動方案-(2010.8)

願景

追求安全便利不中斷的金融服務

目標

- 建立業者重視資安的組織文化
- 提升業者資安治理能力與水準
- 確保系統持續營運與資料安全

推動策略

強化資安監理	深化資安治理	精實金融韌性	發揮資安聯防

具體措施

強化資安監理	深化資安治理	精實金融韌性	發揮資安聯防
1. 型塑金融機構重視資安的組織文化 2. 完備資安規範 3. 強化資安監理職能 4. 加強金融資安檢查	1. 加強資安管理 2. 強化資安監控 3. 加強資安人才培育	1. 增進營運持續管理量能 2. 加強資安演練 3. 建構資料保全避風港	1. 資安情資分享與合作 2. 建立金融資安事件應變體系 3. 建立金融資安事件監控體系

What's Happened ?

疫情

- 資安疆界的改變
- 數位轉型

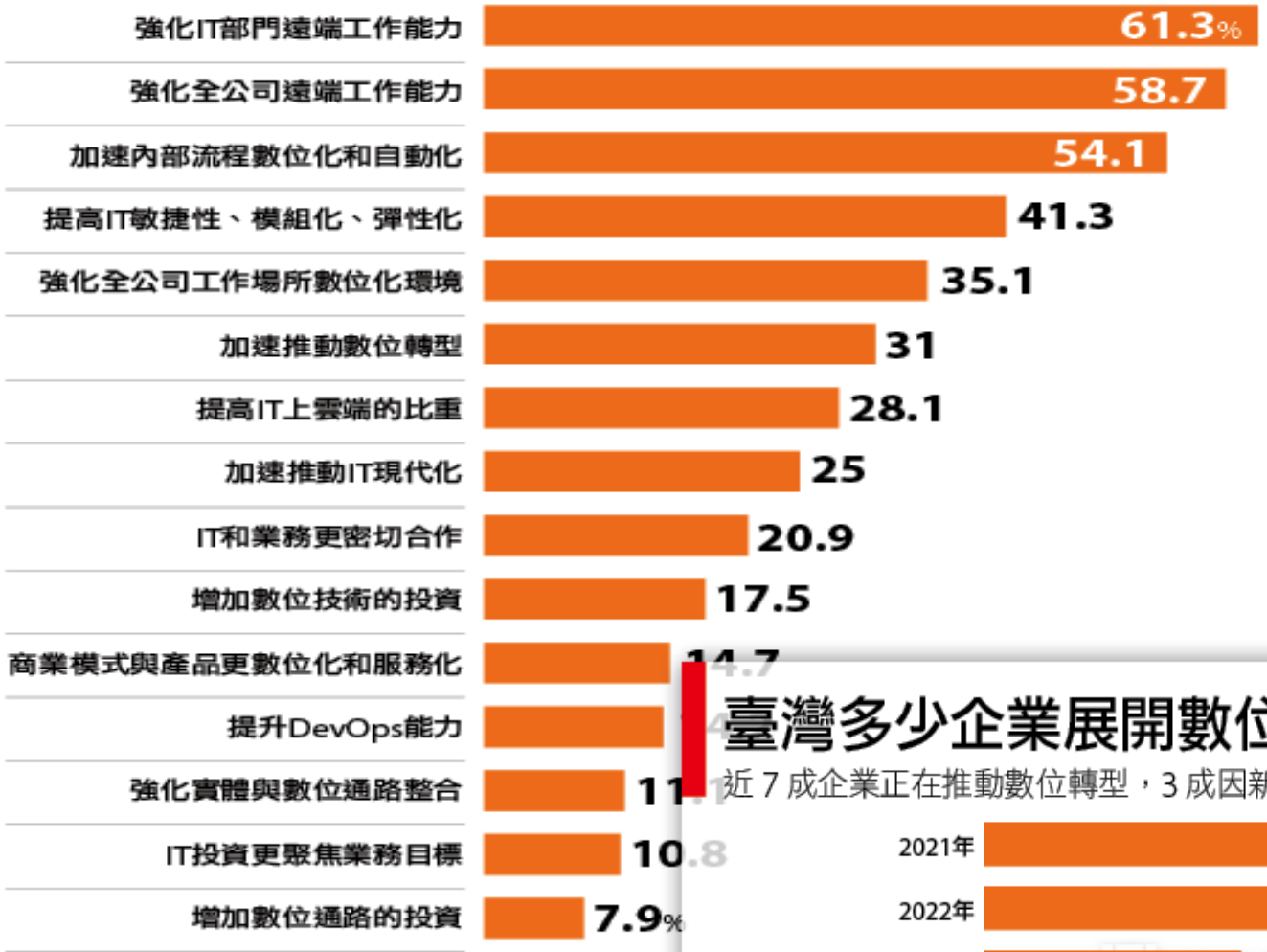
俄烏戰爭

- 實體戰爭的前哨站
- 數位韌性

資料來源：2022 iThome CIO大調查，2022年8月

2022 年因應新常態的 IT 對策 Top 15

遠端工作能力和流程數位化已是企業數位韌性的基本能力



資料來源：2022 iThome CIO大調查，2022年8月

臺灣多少企業展開數位轉型？

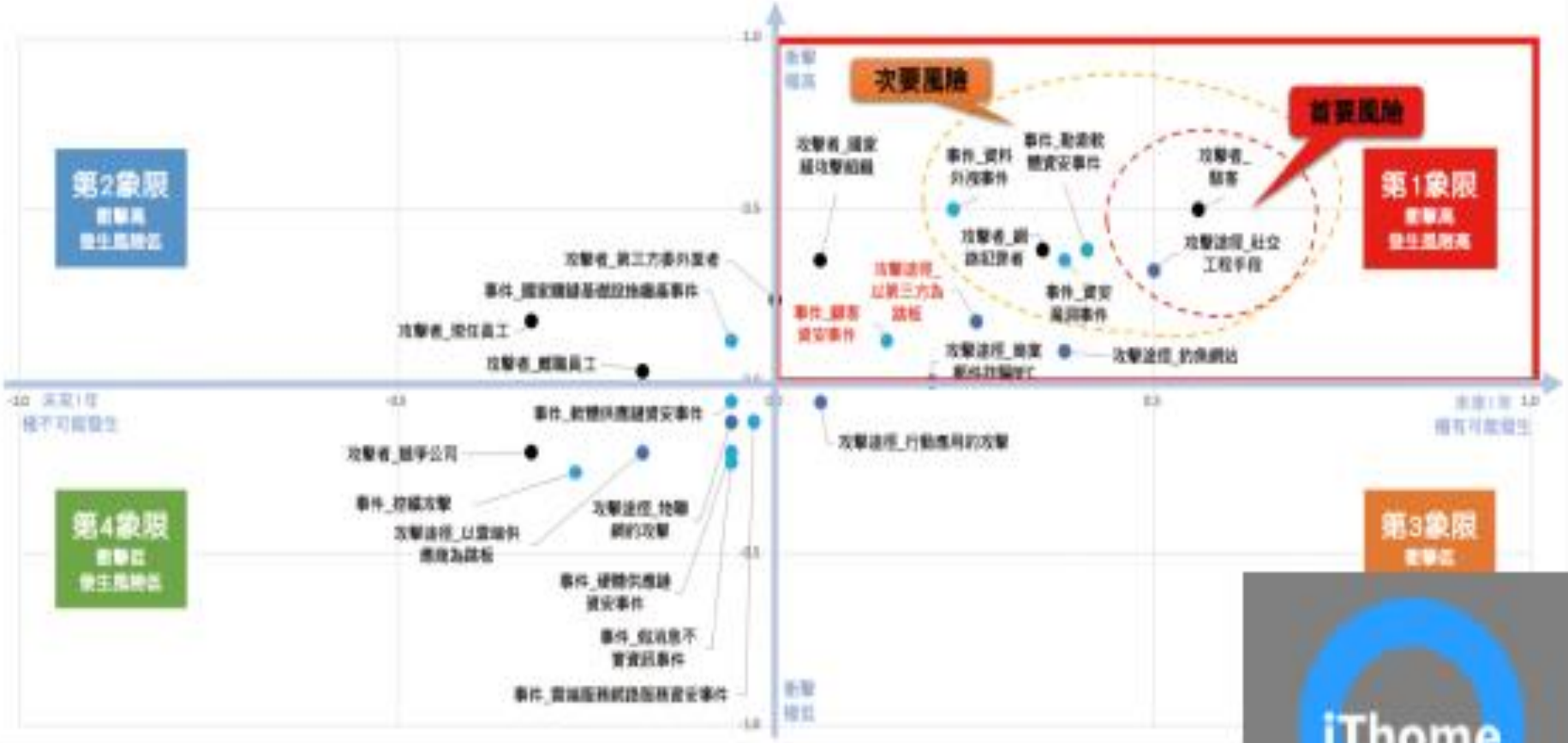
近 7 成企業正在推動數位轉型，3 成因新常態今年加速轉型

資料來源：2022 iThome CIO大調查，2022年8月

iThome

金融業企業資安風險圖（未來一年）

駭客和社交工程手段的威脅，是金融業者在 2022 年的兩大首要風險，又以駭客攻擊的衝擊最大，未來一年也最可能發生。其次，也得留意多項次要風險，包括勒索軟體、資安漏洞、網路犯罪者和資料外洩。顧客資安事件和以第三方發動的攻擊是今年突然竄起的風險

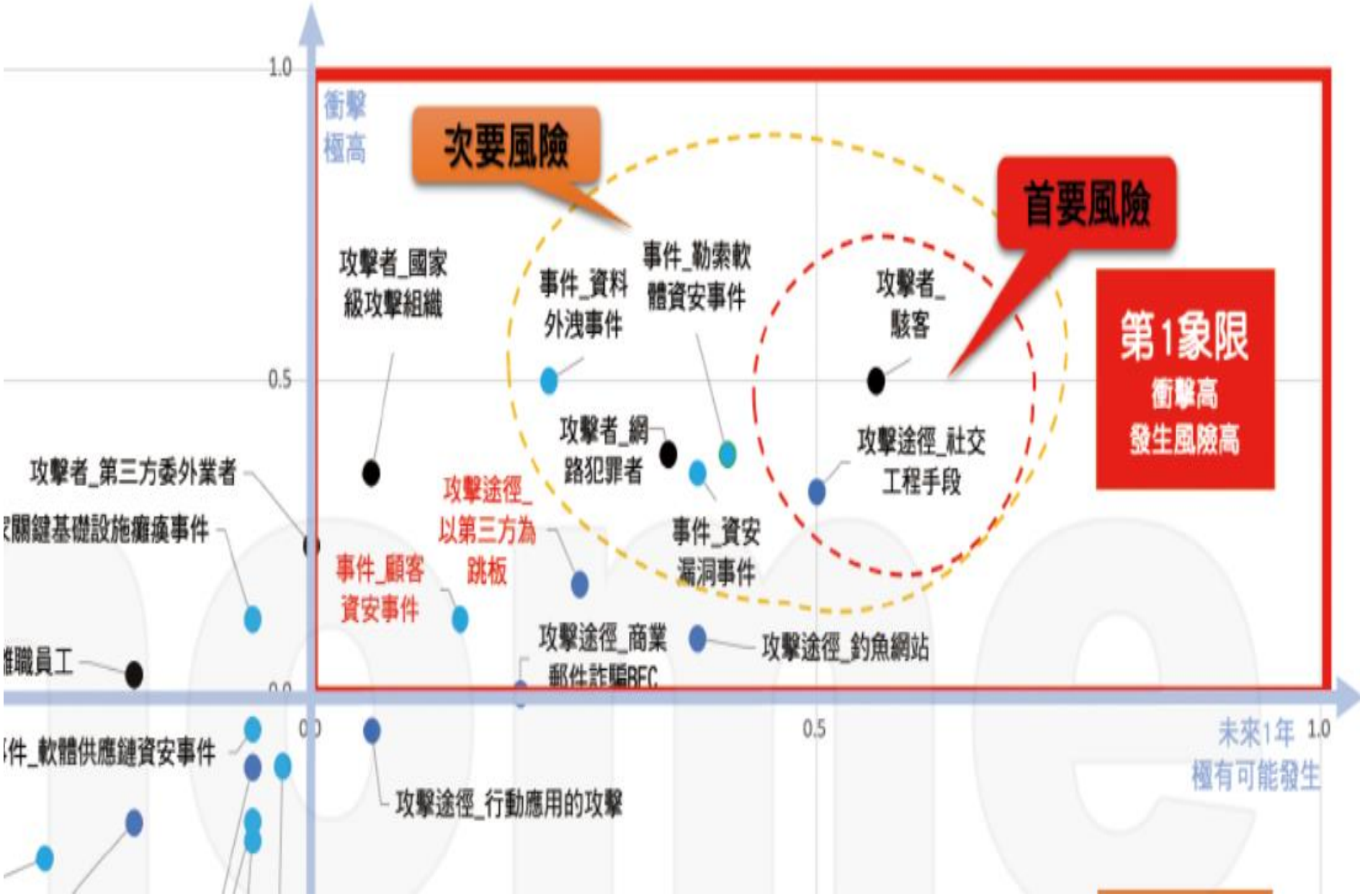


企業資安風險圖製作說明：

在iThome 2022年CIO暨資安大調查中，由企業自評為資安項目的兩項指標，一項是該項目對企業資安的衝擊程度（衝擊極高和衝擊極低），另一項是該項目未來1年的發生風險（極可能發生與極不可能發生）。橫直軸是該項目對企業的衝擊，位置越往上代表衝擊越大，水平軸是企業未來1年發生該項目的風險，位置越右，代表可能性越大，紅色文字的項目為今年發生風險明顯較高者。【問卷說明】本調查對象為企業CIO大調查企業，由資訊管理和大學的IT與資安主管，進行線上問卷，有效問卷416份，其中61.9%填答者為企業資安最高主管

資料來源：2022 iThome CIO大調查，2022年6月

iThome

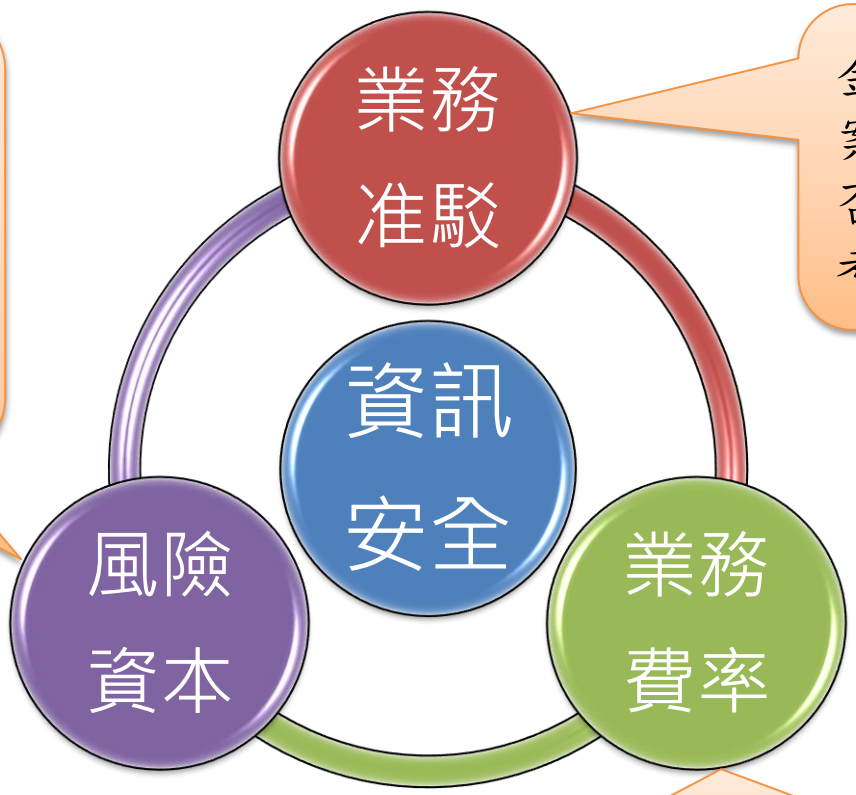

1.0
衝擊
極高
次要風險
首要風險
第1象限
衝擊高
發生風險高
攻擊者_國家
級攻擊組織
事件_資料
外洩事件
事件_勒索軟
體資安事件
攻擊者_
駭客
0.5
攻擊者_網
路犯罪者
攻擊途徑_社交
工程手段
攻擊者_第三方委外業者
關鍵基礎設施癱瘓事件
攻擊途徑_
以第三方為
跳板
事件_資安
漏洞事件
事件_顧客
資安事件
攻擊途徑_商業
郵件詐騙BEC
攻擊途徑_釣魚網站
職員工
0.0
0.0
0.5
1.0
未來1年
極有可能發生
件_軟體供應鏈資安事件
攻擊途徑_行動應用的攻擊

金融資安行動方案重點

- 結合監理工具提供激勵誘因
- 以戰代訓-強化資安演練廣度與深度
- 型塑金融機構重視資安的組織文化
- 金融資安聯防 F-ISAC/F-SOC
- 強化新興科技的資安防護
- 建構資源共享的資安應變機制
- 系統化培育金融資安專業人才
- 落實災害應變復原運作機制

(一)結合監理工具提供激勵誘因

未落實資訊安全之金融機構，提高其作業風險法定資本之計提



金融業者申請開辦業務案件，資訊安全管理是否落實，作為本會准駁考量因素之一

資訊安全執行較好金融機構，適用較低費率：

- 存款保險
- 保險安定基金

(二)型塑重視資安的組織文化

執行措施

- 推動一定規模金融機構或純網銀設置副總經理層級之資安長
- 鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組
- 設置資安專責單位、主管及人員，並採差異化監理措施

執行成效(111.6)

- 已於110年9月完成修法，要求設置副總層級資安長，計有40家銀行、11家保險公司、22家券商設置
- 已有58家金融機構遴聘具資安背景之董事、顧問或設置資安諮詢小組

上市櫃公司設置資安長

設置資安長、資安專責單位及資安人員(內控準則第9條之1)

第一級公司

111年底前設置資安長、資安專責單位(含資安主管及至少2名專責人員)

- 資本額100億元以上
- 台灣五十成分股公司
- 主要經濟活動以電子方式媒介商品或服務者

第二級公司

112年底前配置資安主管及至少1名專責人員

- 第一級以外的上市(櫃)公司
- 最近未連續3年虧損且每股淨值未低於面額

第三級公司

鼓勵配置至少1名專責人員

- 第一級以外的上市(櫃)公司
- 最近連續3年虧損或每股淨值低於面額

(三)強化新興科技的資安防護

兼顧服務創新與安全

金融機構運用新興科技發展創新業務，
亦須預先考量相關資安風險因子

＋

因應委外及跨業合作

強化金融供應鏈體系風險評估與
管理，降低體系風險

→

增修訂資安自律規範

APP
雲端服務
開放銀行
網路身分驗證
供應鏈風險評估

攻擊樣態與事件

零信任戰略

世界重要國家政府推動規劃

- 零信任已從概念探討階段進入實務部署規劃，世界重要國家之政府紛紛建立國家零信任網路安全戰略

美國

具體規劃2024年前聯邦網路完成初步遷移。

歐盟

2020年建立歐盟網安戰略，提出標準框架，協助成員國轉型。

中國

發布國家級標準，建立「零信任聯盟」規劃轉型。

新加坡

2021年10月網路安全戰略，定為國家網安框架。

資料來源：國家安全局

多元金融身分驗證框架及標準

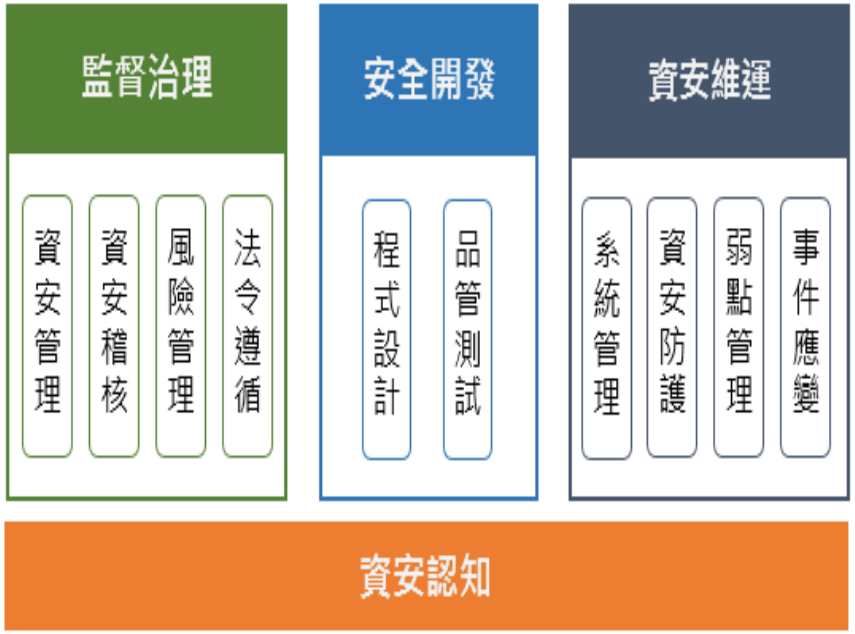
國際標準化組織, ISO
(International Organization for Standardization)

(四)系統化培育金融資安專業人才

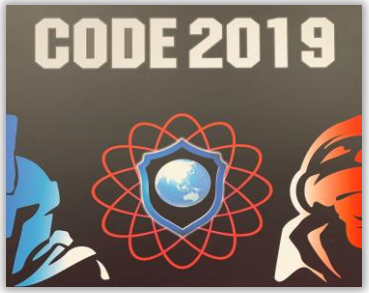
職能布陣 → 職涯發展

- 訂定**人才培訓地圖**，強化金融資安人才能力建構
- 開設**金融資安人才養成專班**，結合科技公司，充實師資及課程
- 透過產學合作、跨業合作，**培育跨領域人才**
- 鼓勵資安人員**取得國際資安證照**，以提升專業能力

金融產業資安人才培訓架構

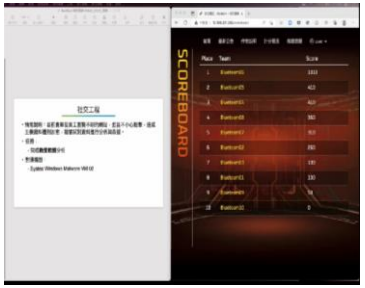


(五)以戰代訓-強化資安演練廣度與深度



跨國攻防演練
(模擬金融)

金融資安攻防演練
(紅藍對抗)



金融資安攻防演練
(技術演練)

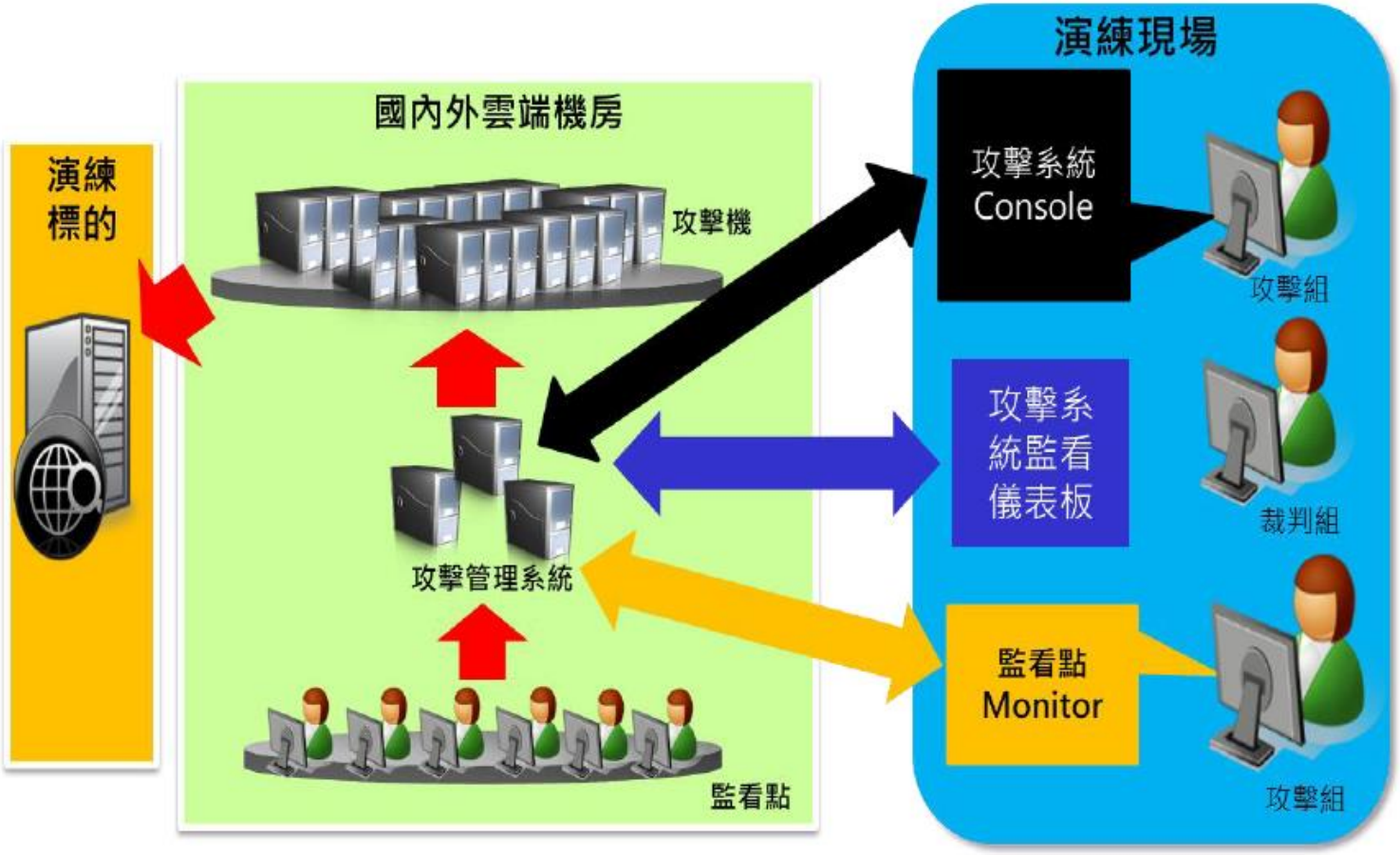
2018 2019 2020 2021 2022

金融DDoS演練

金融BAS演練

MITRE ATT&CK™ Breach & Attack Simulation

DDoS演練

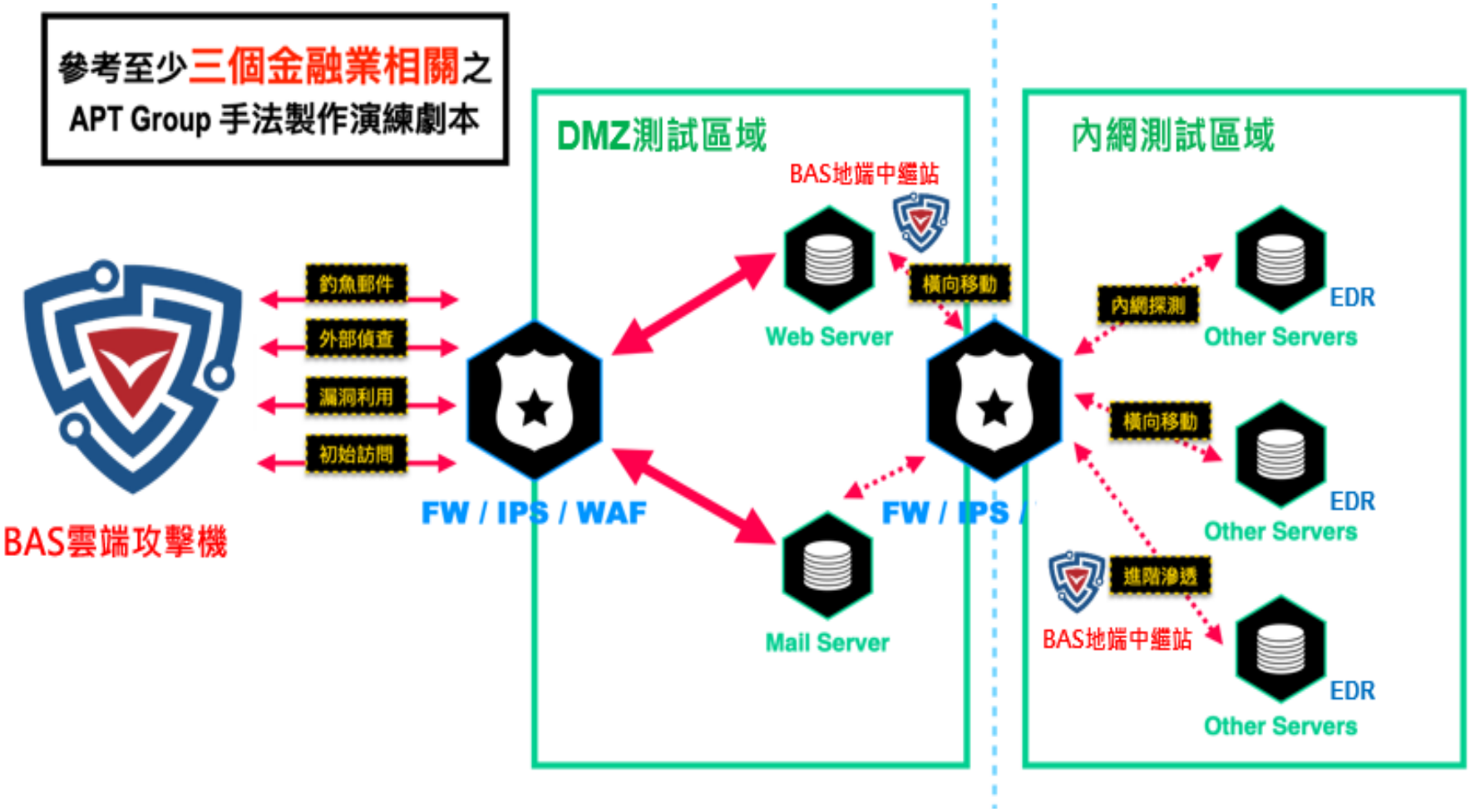

演練現場
國內外雲端機房
演練
標的
攻擊機
攻擊系統
Console
攻擊組
攻擊系
統監看
儀表板
裁判組
攻擊管理系統
監看點
Monitor
攻擊組
監看點

網路攻防演訓

- ✓ 情境腳本自動化攻擊(包含SQL Injection、木馬、勒索軟體)
- ✓ 透過模擬演練學習MITRE ATT&CK攻擊鏈知識
- ✓ 強化金融機構資安人員處理資安事件之應變能力
- ✓ 提升資安人才培育容量
- ✓ **跨機構技術交流與人才庫**

入侵與攻擊模擬演練(BAS)

參考至少三個金融業相關之
APT Group 手法製作演練劇本



重大事件應變情境演練

- 策略推演
  - 簡報式推演
  - 決策模擬推演
    - 連續式推演
    - 階段式推演
    - 特定功能推演
    - 複合型態
- 技術操演
  - 真實環境
    - 社交工程演練
    - 紅/紫隊演練
    - DDoS演練
    - 滲透測試
  - 模擬環境
    - 網路攻防演練
    - CTF競賽
    - 威脅獵捕競賽

Coming Soon.....

(六)金融資安聯防 F-ISAC

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

建立國際
ISACs
情資交流

- 美國FS-ISAC (108.03)
- 日本F-ISAC (108.10)
- 泰國TB-CERT (110.11)
- 美國FIRST (111.1)

- 歐盟FI-ISAC
- 以色列CERT-IL
- 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

- 維運F-ISAC金融資安情資分享平台
- 發布威脅警訊
- 推動會員情資分享
- 偽冒網站偵測
- 研析資安技術

人才培育

- 資安研討會、說明會
- 資安技術實務課程
- 協同金融領域教育訓練機構推動資安訓練

聯防監控

- 維運F-SOC二線金融資安聯防監控平台
- 研訂資安事件聯防監控規則、監控組態基準與作業指引

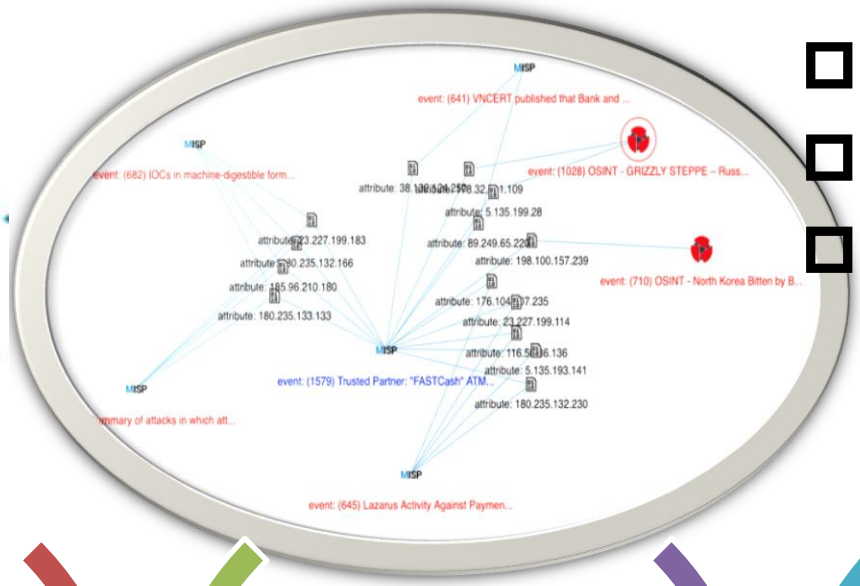
資安演練

- 參與主管機關演練計畫
- 辦理金融領域DDoS攻防演練
- 辦理金融領域網路攻防競賽

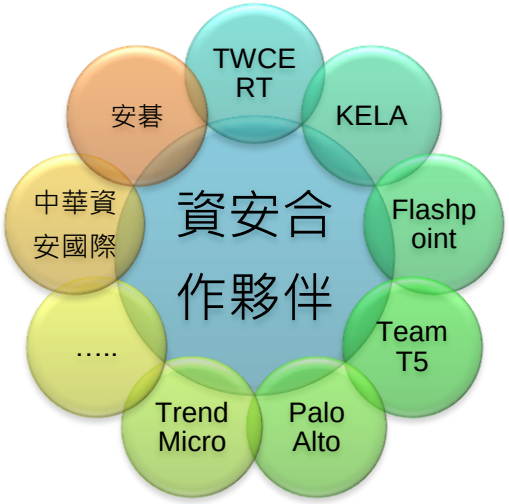
事件處理

- 維運F-CERT二線金融電腦緊急應變小組
- 提供資安事件應處服務

資安情資分享與合作

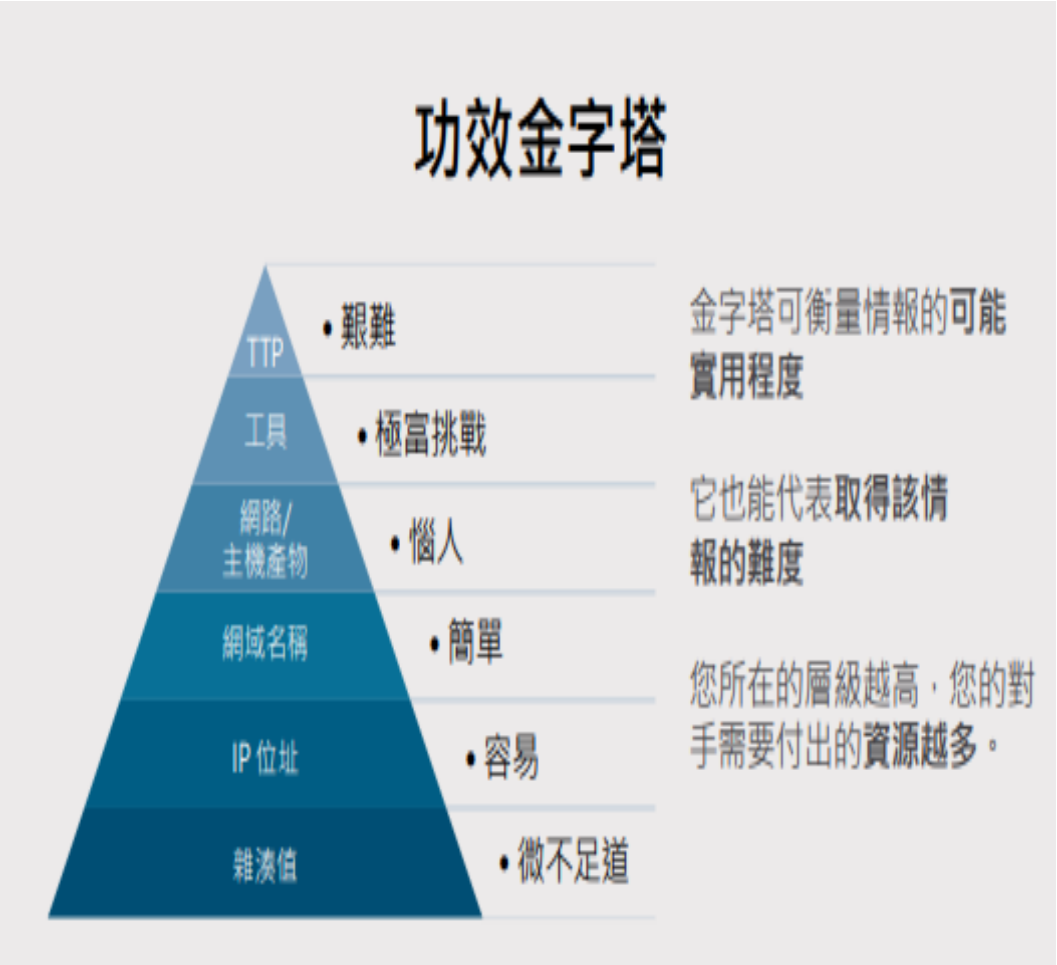


- 多元化情資來源
- 智能化情資分析
- 國際化情資合作



會員分享

提升情資分享動能



Ref: https://www.fireeye.com/content/dam/fireeye-www/regional/zh_TW/solutions/pdfs/wp-siem-to-esm.pdf

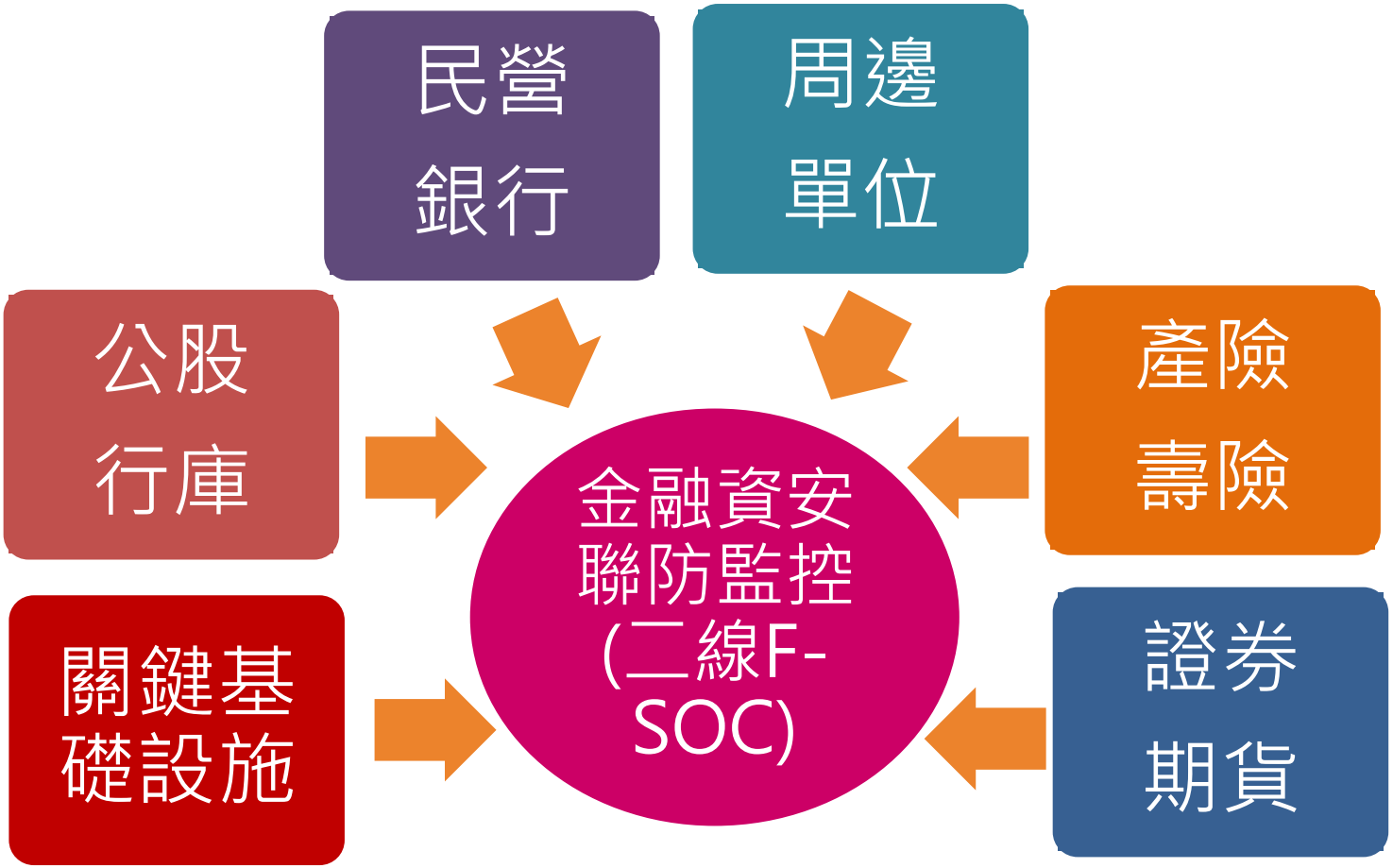
情資分享計分標準

分數	項目	說明
1 分	雜湊值	檔案之 MD5、SHA1、SHA256 等
1 分	IP	IP 位址
1 分	DN/URL	網域名稱或網址
1 分	漏洞名稱	與特定漏洞有關之威脅
4 分	網路產物	HTTP Header 或 Mail Header 分析資訊
4 分	主機產物	攻擊者於主機留下特定字串或值，如登錄機碼、可辨識特定種類惡意程式字串等
5 分	攻擊工具	使用特定駭客工具進行攻擊
6 分	攻擊手法	攻擊各階段之手法

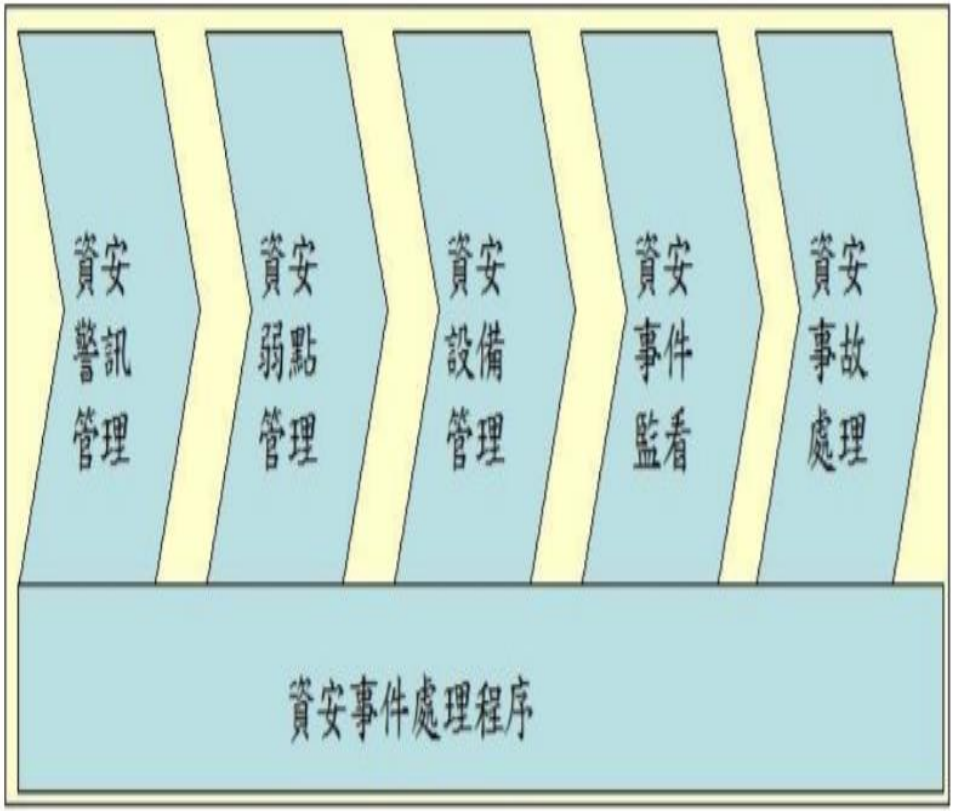
×

影響等級分數	項目		
	資安漏洞 CVSS 3.0	攻擊活動	資安事件
4	Critical	極高	4 級事件
3	High	高	3 級事件
2	Medium	中	2 級事件
1	Low	低	1 級事件

(七)金融資安聯防 F-SOC

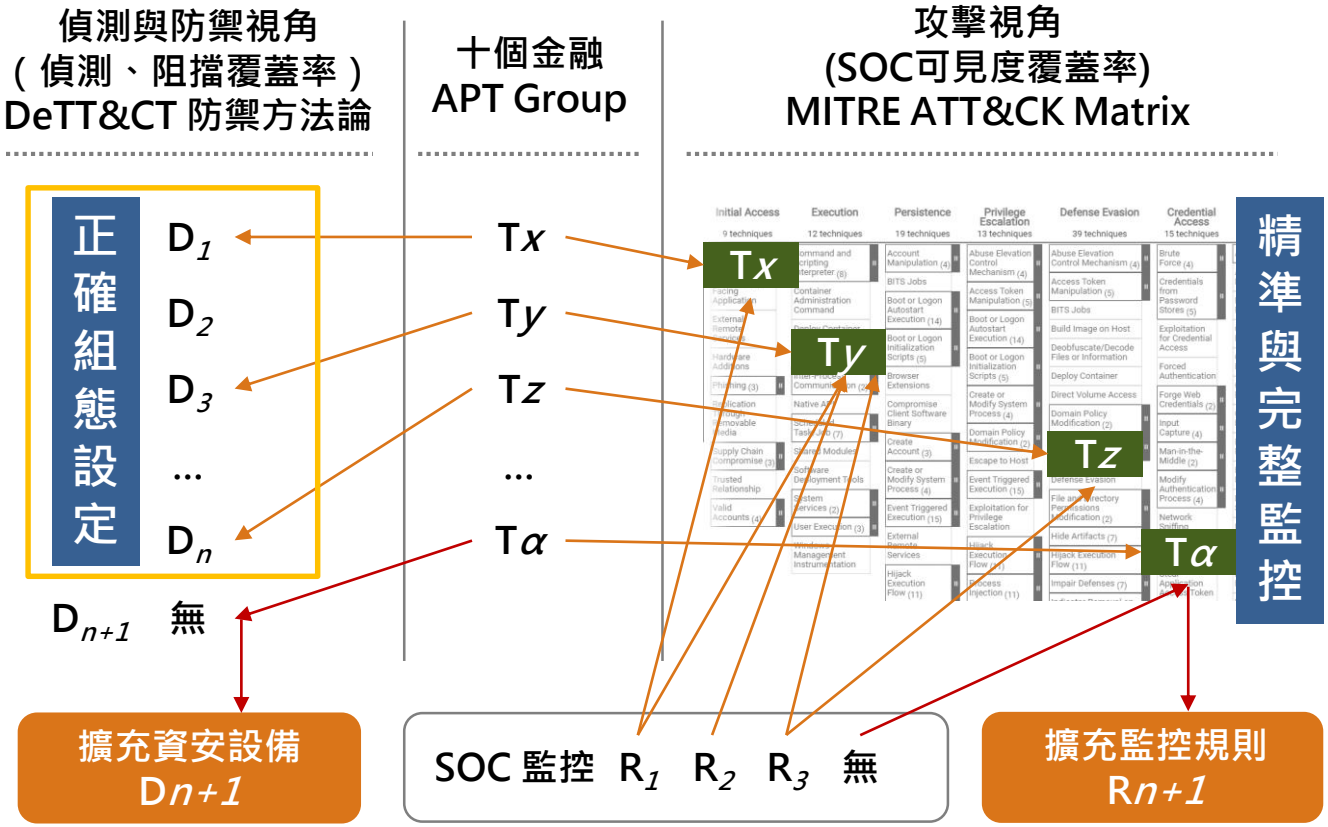


鼓勵建立資安監控機制(SOC)



Cyber Kill Chain, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

發展資安監控組態基準



- 運用 DeTT&CT 防禦方法論，將金融機構常用之資安、網路、應用系統等設備，映射至前項步驟蒐整的 118 個駭客攻擊手法，針對所對應到的駭客攻擊技術，研析其特徵與手法，產出相對應之SIEM平台的金融機構資安監控規則（SIEM Rules）

(八)建構資源共享的資安應變機制

因應資安事件應變處理具高度時效要求，單一機構資源有其限制，建立資源共享的資安應變機制

- 金控集團應變小組
- 周邊單位及公會支援小組
- F-ISAC/F-CERT應變體系

(九)落實災害應變復原運作機制

沒有100%的資訊安全 - 建立平時及終極防護能量

營運持續管理

- 識別核心業務
- 訂定最大可容忍中斷時間
- 演練、壓力測試

備援環境實作驗證

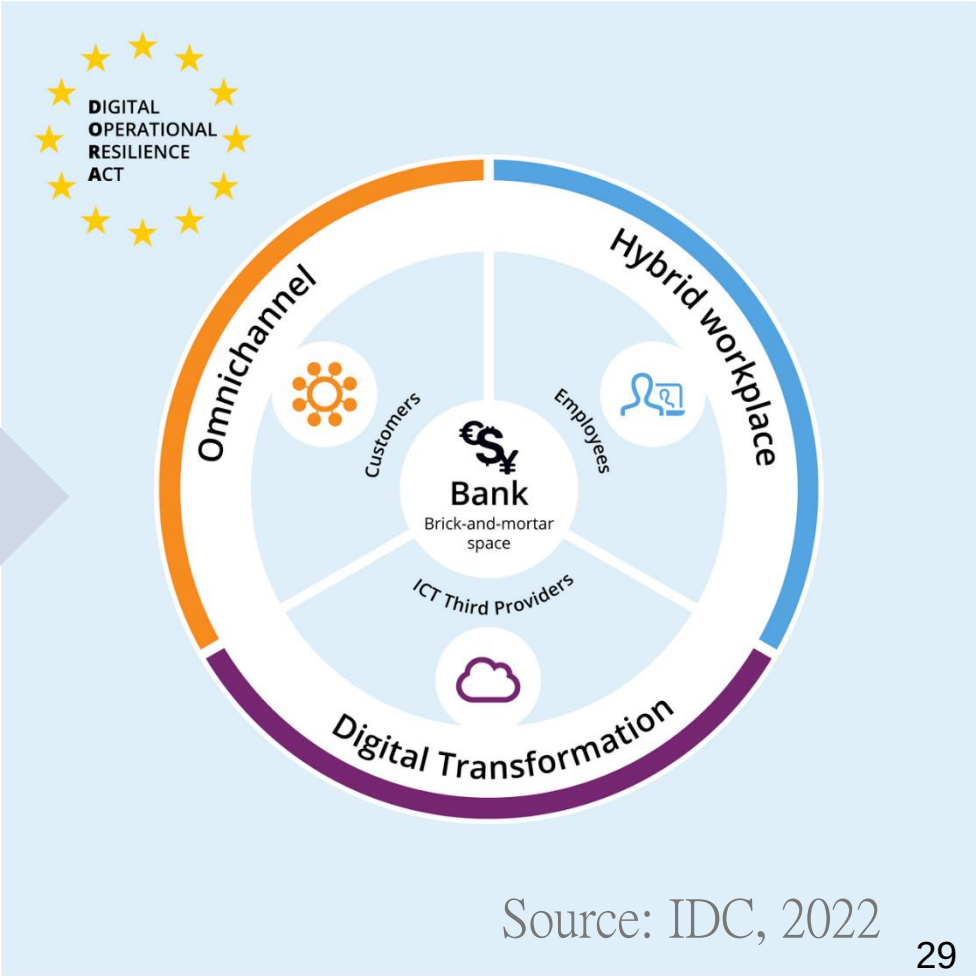
- 復原能力實證
  - 本地備援
  - 異地備援
- 實際業務運作驗證

關鍵資料保全

- 資料保護
- 資料可移性
- 資料復原性
- 關鍵服務持續性

數位韌性

- 風險管理
- 事件通報
- 韌性測試
- 第三方供應商風險監控



Source: IDC, 2022

(十)金融資安治理成熟度評估

五大領域
網路風險管理與監督
威脅情資管理與合作
網路安全管理
委外及依賴關係管理
網路事件管理與回應

成熟度等級
創新Innovative Real Time Predictive analytics are tied to Auto. Responses
進階Advanced Auto. Risk Management
中等Intermediate Risk Management
發展中Evolving Risk Driven
基礎Baseline Compliance Driven

- 109年度-銀行業
- 110年度-保險業
- 111年度-證券業

5大控制領域
494題

鼓勵導入資安國際標準

- 鼓勵金融機構導入國際資安管理標準及國際營運持續管理標準，並取得相關驗證，透過第三方獨立機構檢視管理制度及持續營運之有效性。

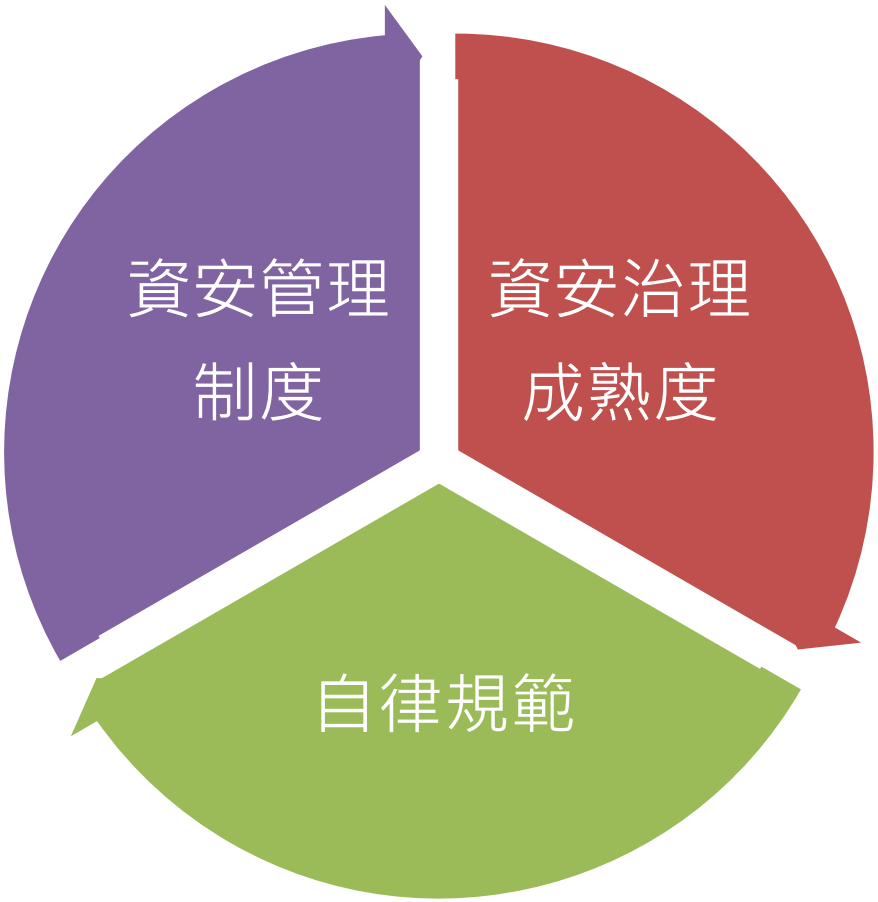
國際資安管理標準(ISO27001)

- 為健全金融機構資訊安全管理制度，鼓勵業者導入國際資安管理標準。
- 截至110年6月底，已取得驗證者有銀行業32家、保險業38家、證券業25家。

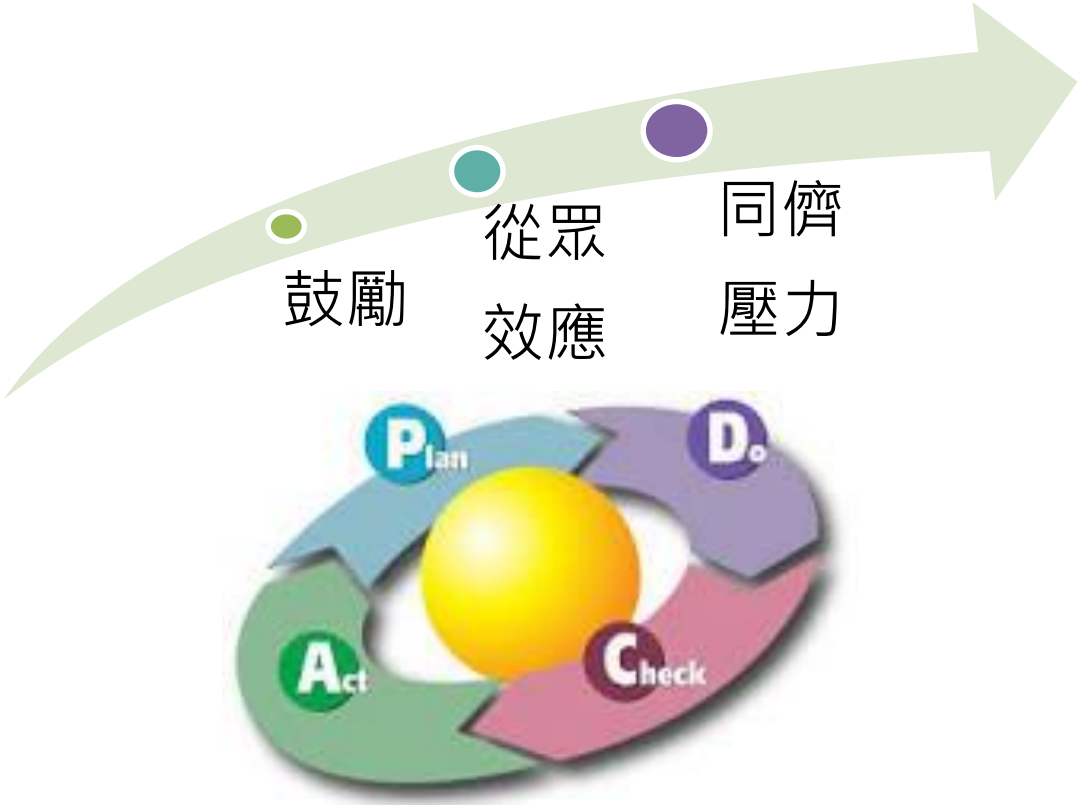
國際持續營運管理標準(ISO22301)

- 為確保金融服務不中斷，鼓勵業者導入國際持續營運管理標準。
- 截至111年6月底，已取得驗證者有銀行業10家、證券業5家、保險業5家。

五大領域	成熟度等級
網路風險管理與監督 威脅情資管理與合作 網路安全管理 委外及依賴關係管理 網路事件管理與回應	創新Innovative Real Time Predictive analytics are tied to Auto. Responses 進階Advanced Auto. Risk Management 中等Intermediate Risk Management 發展中Evolving Risk Driven 基礎Baseline Compliance Driven



從共通基準邁向策略目標



簡報完畢
敬請指教