臺灣證券交易所
TAIWAN STOCK EXCHANGE
流通證券・活絡經濟

竭誠為您服務

106年度證券期貨市場資安報告

107年6月

企業籌資更便捷 大眾投資更穩當 ・ 企業資訊更透明 交易機制更公正 金融商品更多元

辦理依據

「106年度第2次證券期貨市場資通安全會議」決議

- **為瞭解證券期貨市場之資安情形及未來展望，提供主管機關資安政策之推動及業者資安防護之參考**，有關證券期貨市場年度資安報告，請證交所邀集相關周邊單位討論報告之撰寫，並可請相關公會等提供意見，於每年3月底前函報

「107年度第1次證券期貨市場資通安全會議」決議

- 請就報告內容擇要可適當公開部分，提供證券期貨業者參考，以強化資安防護

大綱

- 年度資安事件回顧
- 證券商資通安全防護規範
- 證券商資安防護現況
- 證券商資安防護強化作為
- 結論

年度資安事件回顧

DDoS勒索攻擊

SEC EDGAR遭駭

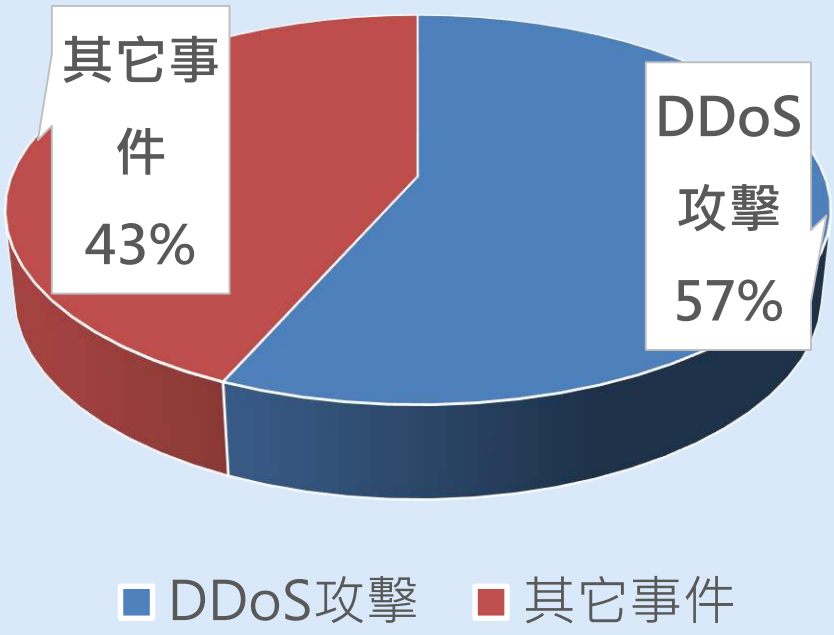
Wanna Cry

遠銀Swift遭駭

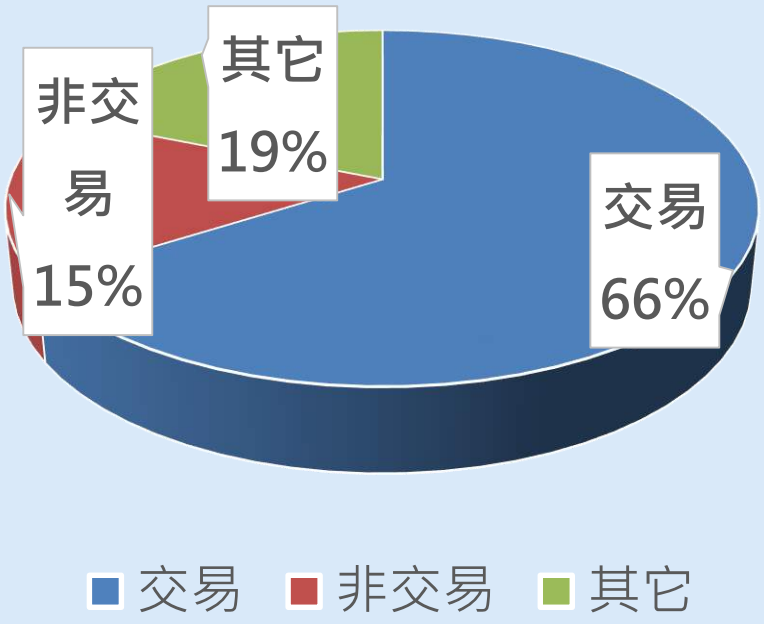
106年度證券商通報事件

通報事件數：53件

事件類型



影響範圍



證券商資通安全防護規範

建立證券商資通安全檢查機制

年度資安查核

專案查核

參考 ISO27001資訊安全管理系統

資訊安全自律規範

社群媒體

行動安全
(含BYOD)

雲端安全

證券暨期貨市場各服務事業建立內部控制制度處理準則(107.5.30修訂)

- **應配置適當資安人力及設備**
  (主管機關得視服務事業規模、業務性質及組織特性，命令設置資安專責單位、主管及人員)
  (107年6月8日金管證券字第1070320242號)

- **資安主管、董事長、總經理、稽核主管聯名出具資安執行情形聲明書，於會計年度終了後三個月內提報董事會**

- **資安主管及人員，每年至少接受十五小時以上資安專業課程訓練或職能訓練**

- **其他使用資訊系統之從業人員，每年至少接受三小時以上資安宣導課程**

- **公會應訂定並定期檢討資安自律規範**

證券商資通安全防護現況

證券期貨商資訊安全防護標準研究報告符合度

註：106年4月參照「政府機關（構）資通安全責任等級分級作業規定」，並搭配市場特性設計資安防護成熟度問卷

證券商分級

方案	第一級	第二級	第三級	第四級
資本額(指撥營運資金)	達100億以上	40億至100億	40億以下	• 非金控子公司 • 網路下單(含API)占公司成交比率小於30% • 未開辦保管客戶資產相關業務者
金控子公司	隸屬金控子公司者至少列為第二級			
符合券商數	9	11	24	30

第一級：資本額(指撥營運資金)達100億元以上之業者；
第二級：資本額(指撥營運資金)介於40億元以上到未達100億元之業者；
第三級：資本額(指撥營運資金)未達40億元之業者，但為金融控股公司之子公司證券商者，列為第二級。
第四級:非金融控股公司之子公司證券商符合以下條件證券商，逕行列入第四級。
近2年網路下單(含API)占公司成交比率小於30%，且未開辦保管客戶資產相關業務者(如：自辦信用交易、證券業務借貸款項、不限用途款項借貸、辦理有價證券借貸、定期定額財富管理等)。

證券商分級列表

第一級(9家)	第二級(11家)	第三級(24家)		第四級(30家)		
日盛	合庫	大展	致和	宏遠	永興	法銀巴黎
統一	*臺銀	土銀	石橋	港商麥格理	光隆	香港上海匯豐
元富	亞東	台灣企銀	金港	台灣匯立	日茂	
兆豐	第一金	彰銀	北城	美林	永全	
群益	中國信託	大慶	中農	台灣摩根士丹利	福邦	
凱基	國票	高橋	新光	高盛亞洲	全泰	
富邦	台新	日進	聯邦銀行	瑞士信貸	福勝	
元大	康和	盈溢	陽信	港商德意志	信富	
永豐金	玉山	犇亞	大鼎	香港商野村	豐農	
	國泰	台中銀	鑫豐	港商法國興業	安泰	
	華南永昌	新百王		花旗環球	摩根大通	
		光和		瑞銀	萬泰	
		大昌		富隆	萬通	
		德信		寶盛	大和國泰	

*低於40億但隸屬於金控

資訊系統分類分級

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
資訊系統分類分級 (原僅適用網際網路下單業者)	V	V	V	V

現況	證券商							
是否針對資訊系統進行分級管理?	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	9	2	21	3	28	2
	100%		81.82%		87.5%		93.33%	

ISMS推動

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
關鍵資訊系統導入ISMS	V	V		

現況	證券商							
關鍵資訊系統是否導入ISO27001資訊安全管理系統(ISMS)？	第一級		第二級		第三級		第四級	
	是	否	是	否	-	-	-	-
	7	2	5	6	-	-	-	-
	77.78%		45.45%		-		-	

內控稽核

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
每年至少辦理一次資訊安全查核作業	V	V	V	V

現況	證券商							
是否每年執行內部稽核？(至少1次以上)	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	11	0	24	0	30	0
	100%		100%		100%		100%	

業務持續運作

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
訂定故障復原程序及營運持續計畫	V	V	V	V
每年至少辦理1次演練(含事件通報演練)	V	V	V	V

現況	證券商							
是否每年辦理核心資訊系統持續運作演練？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	11	0	19	5	28	2
	100%		100%		79.17%		93.33%	

防護縱深(防毒)

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
防毒設備	V	V	V	V

現況	證券商							
是否導入防毒設備？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	11	0	24	0	30	0
	100%		100%		100%		100%	

防護縱深(防火牆)

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
防火牆設備	V	V	V	V

現況	證券商							
是否導入防火牆設備？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	11	0	23	1	28	2
	100%		100%		95.83%		93.33%	

防護縱深(郵件過濾)

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
郵件過濾機制	V	V	V	V

現況	證券商							
是否導入郵件過濾機制？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	10	1	16	8	20	10
	100%		90.91%		66.67%		33.33%	

防護縱深(Web 應用程式弱點防禦)

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
網際網路下單業者，Web 應用程式弱點防禦機制	V	V	V	V

現況	證券商							
網際網路下單業者，是否導入網頁應用程式防火牆(Web Application Firewall, WAF)？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	3	6	2	9	9	15	1	11
	33.33%		18.18%		37.5%		8.33%	

防護縱深(DDoS防護)

竭誠為您服務

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
網際網路下單業者，流量清洗或流量分流機制	V	V	V	V

現況	證券商							
網際網路下單業者，是否導入流量清洗(clean pipe)或流量分流(content delivery network)機制？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	11	0	24	0	14	0
	100%		100%		100%		100%	

監控管理(導入SOC)

竭誠為您服務

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
建立SOC監控關鍵系統	V			
監控關鍵系統安全機制，識別異常並警示		V		
網際網路下單業者，定期檢查網路下單系統功能，並留存紀錄			V	V

現況	證券商							
第一級業者，是否導入資訊安全監控中心(SOC)監控機制？	第一級		第二級		第三級		第四級	
	是	否	-	-	-	-	-	-
	5	4	-	-	-	-	-	-
	55.56%		-		-		-	

弱點掃描

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
每年至少辦理2次關鍵系統弱點檢測(原僅適用網際網路下單業者)	V	V	V	V

現況	證券商							
是否每年辦理網站安全弱點檢測次數？(2次以上)	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	8	3	10	14	9	21
	100%		72.72%		41.67%		30%	

滲透測試

證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
辦理對外服務關鍵系統滲透測試	每年	每2年	每2年	

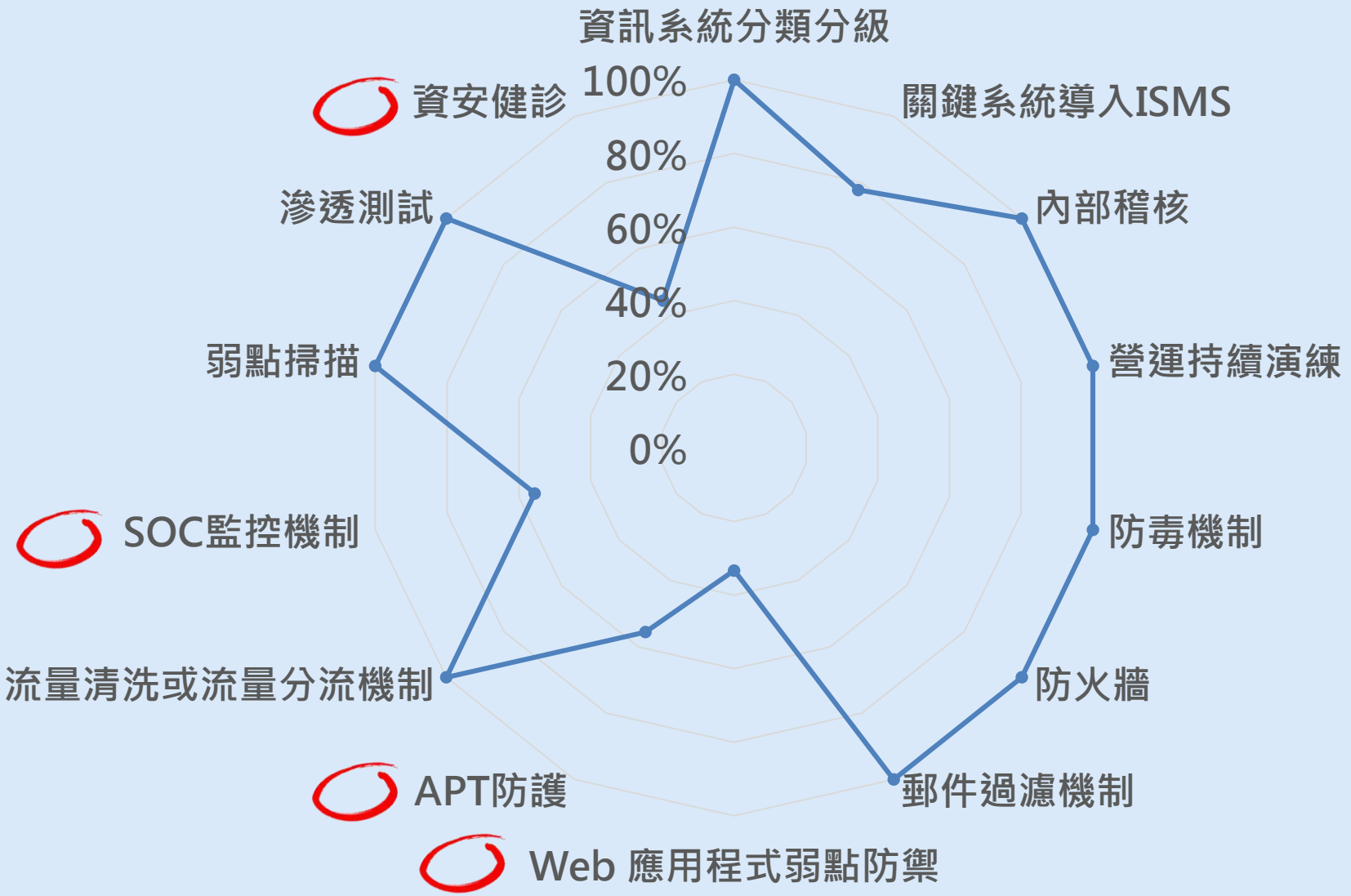
現況	證券商							
是否每年辦理系統滲透測試？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	9	0	4	7	10	14	-	-
	100%		36.36%		41.67%		-	

資安健診

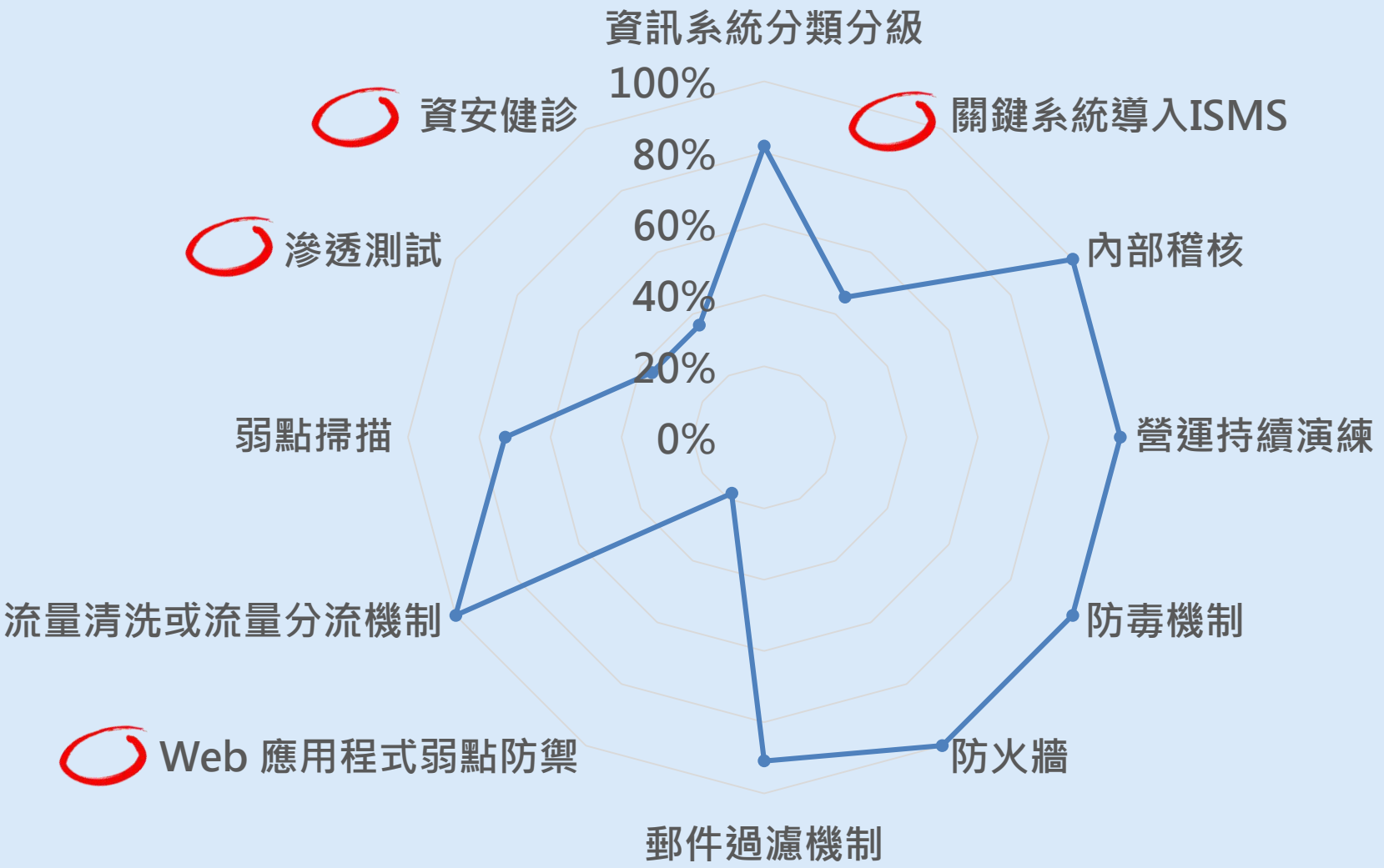
證券期貨商資訊安全防護標準研究報告	第一級	第二級	第三級	第四級
辦理資安健診	每2年	每2年		

現況	證券商							
是否每年辦理資安健診？	第一級		第二級		第三級		第四級	
	是	否	是	否	是	否	是	否
	4	5	4	7	-	-	-	-
	44.44%		36.36%		-		-	

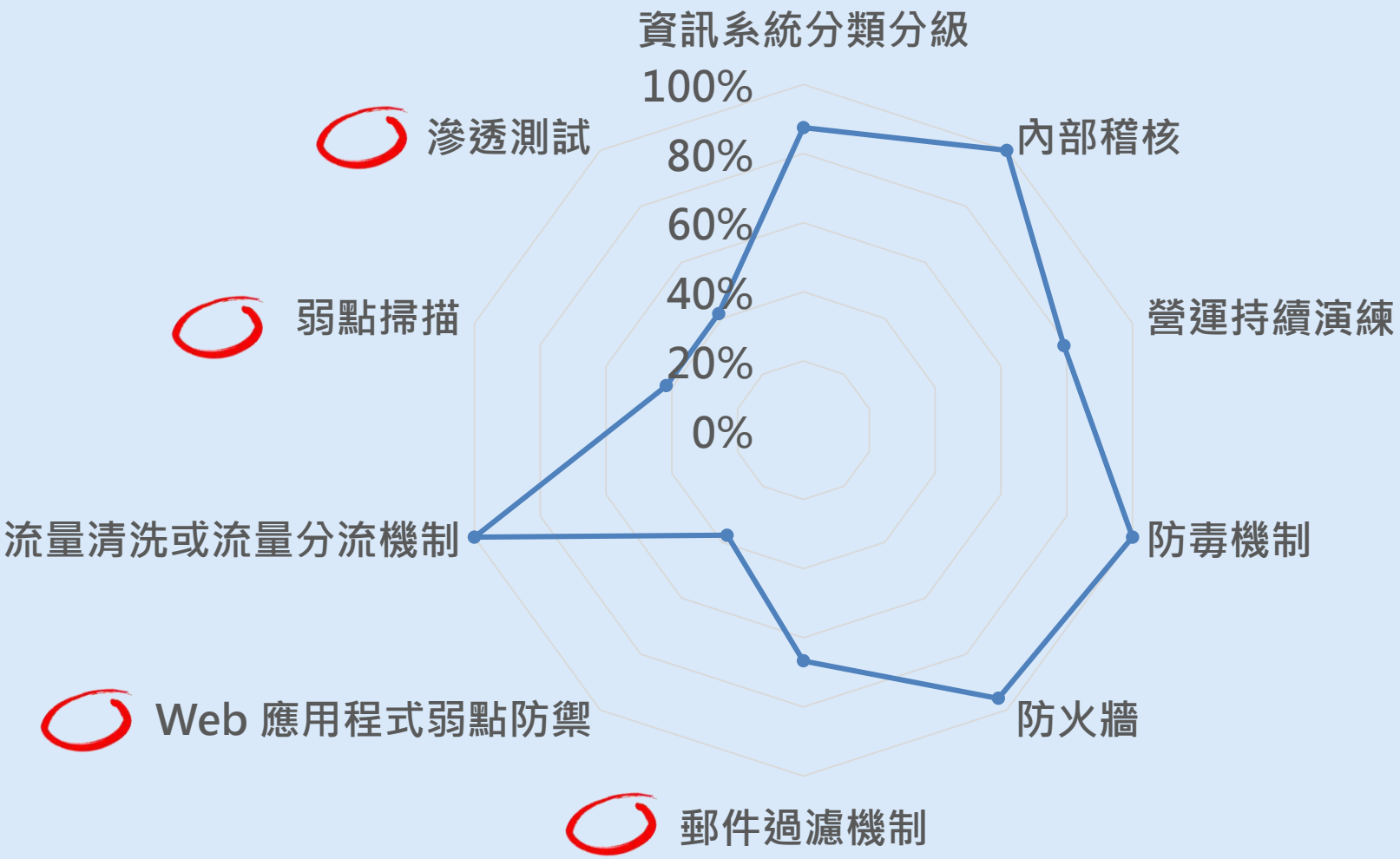
一級證券商符合度


資訊系統分類分級
關鍵系統導入ISMS
內部稽核
營運持續演練
防毒機制
防火牆
郵件過濾機制
Web 應用程式弱點防禦
APT防護
流量清洗或流量分流機制
SOC監控機制
弱點掃描
滲透測試
資安健診
100%
80%
60%
40%
20%
0%

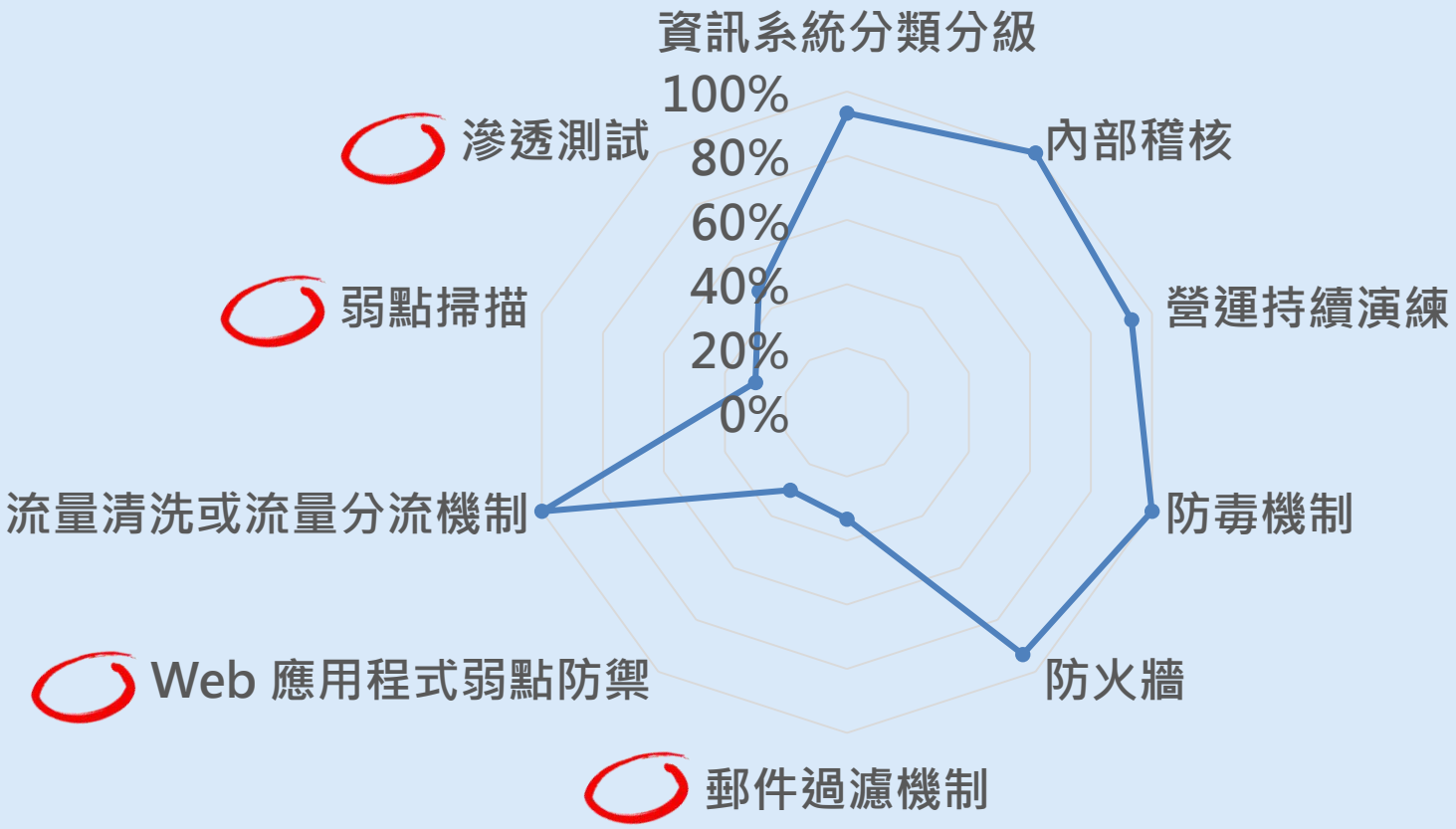
二級證券商符合度


資訊系統分類分級
100%
80%
60%
40%
20%
0%
資安健診
關鍵系統導入ISMS
滲透測試
內部稽核
弱點掃描
營運持續演練
流量清洗或流量分流機制
防毒機制
Web 應用程式弱點防禦
防火牆
郵件過濾機制

三級證券商符合度


資訊系統分類分級
100%
80%
60%
40%
20%
0%
內部稽核
營運持續演練
防毒機制
防火牆
郵件過濾機制
Web 應用程式弱點防禦
流量清洗或流量分流機制
弱點掃描
滲透測試

四級證券商符合度


資訊系統分類分級
100%
80%
60%
40%
20%
0%
內部稽核
營運持續演練
防毒機制
防火牆
郵件過濾機制
Web 應用程式弱點防禦
流量清洗或流量分流機制
弱點掃描
滲透測試

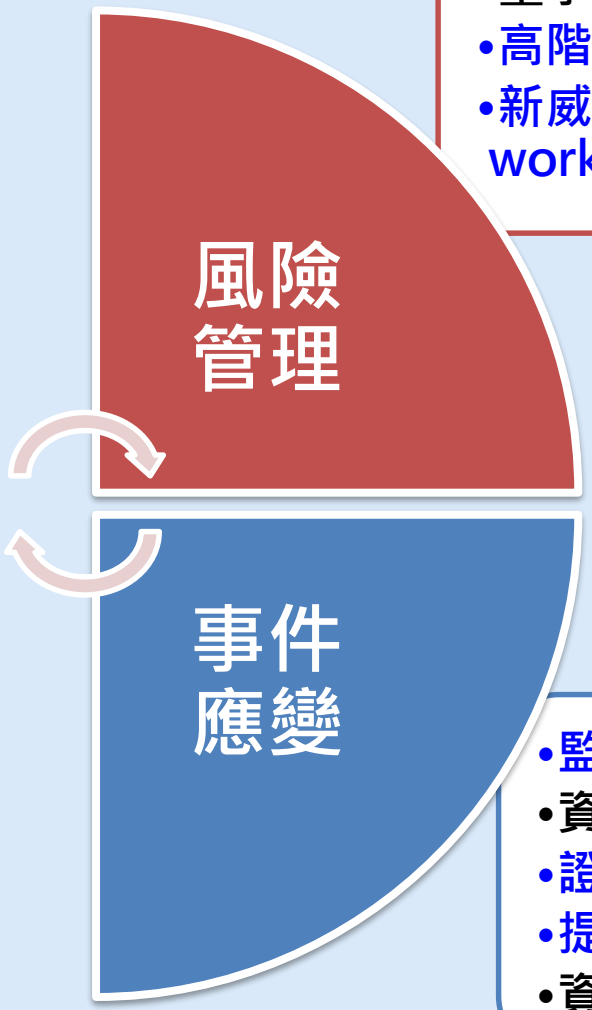
證券商資安防護強化作為

證券商資安防護強化作為

風險管理

- 證券期貨市場資安會議
- 董事會報告資安執行情形
- 高階主管資安宣導
- 新威脅與資訊科技發展 workshop

證券商資安防護強化作為



- 證券期貨市場資安會議
- 董事會報告資安執行情形
- 高階主管資安宣導
- 新威脅與資訊科技發展workshop

- 監控業者資訊服務
- 資安通報系統
- 證券期貨業緊急應變小組
- 提供業者技術支援
- 資安資訊分享平台

證券期貨市場資通安全事件通報應變作業注意事項

初步通報

知悉事件30分鐘內辦理

正式通報

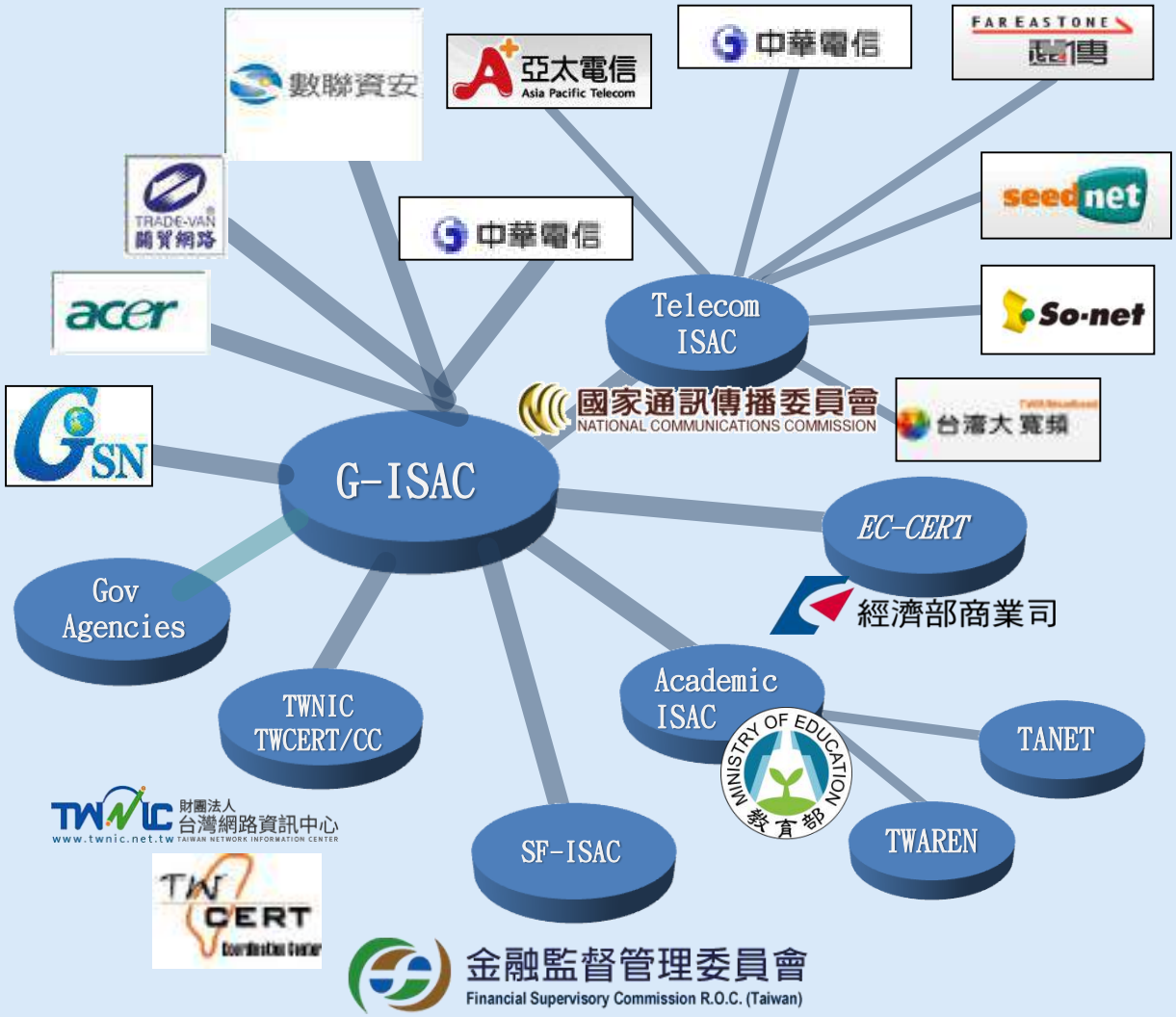
於查明事件後儘速辦理

解除通報

事件處理完成後

資安資訊分享與分析中心

竭誠為您服務



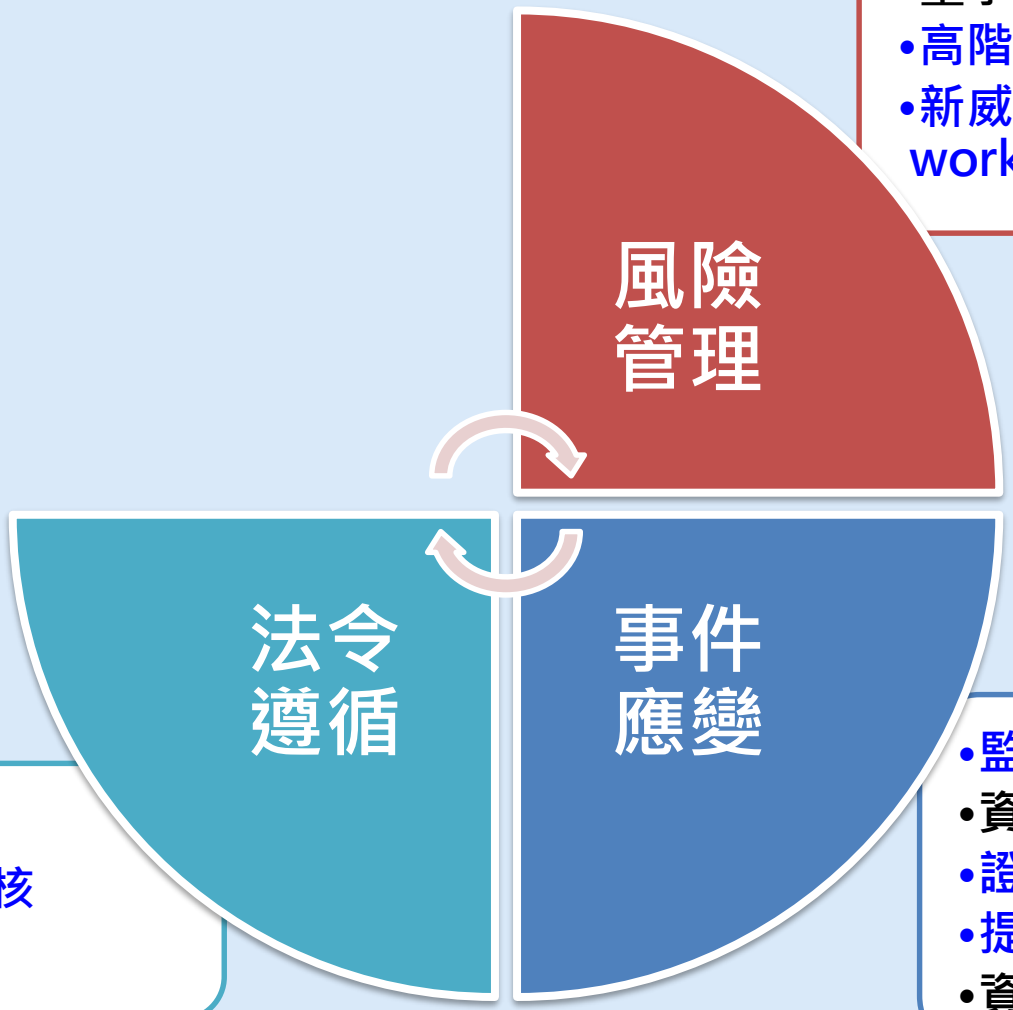
105年推動金管會所屬機關構、證期業者加入

106-107年建置金融資安資訊分享與分析中心(F-ISAC)

107年建置金融網路危機處理中心(F-CERT)

證券商資安防護強化作為

- 證券期貨市場資安會議
- 董事會報告資安執行情形
- 高階主管資安宣導
- 新威脅與資訊科技發展 workshop



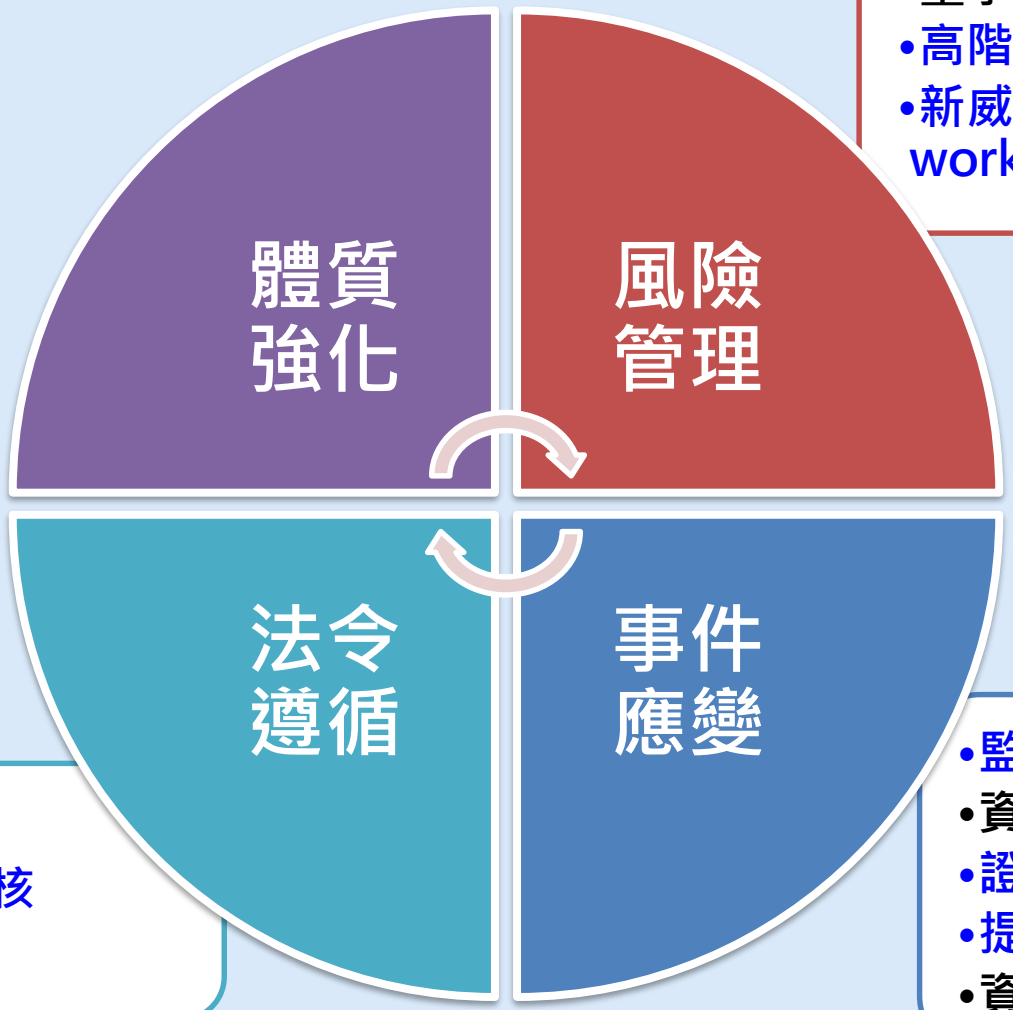
- 業者資安查核

- 監控業者資訊服務
- 資安通報系統
- 證券期貨業緊急應變小組
- 提供業者技術支援
- 資安資訊分享平台

證券商資安防護強化作為

竭誠為您服務

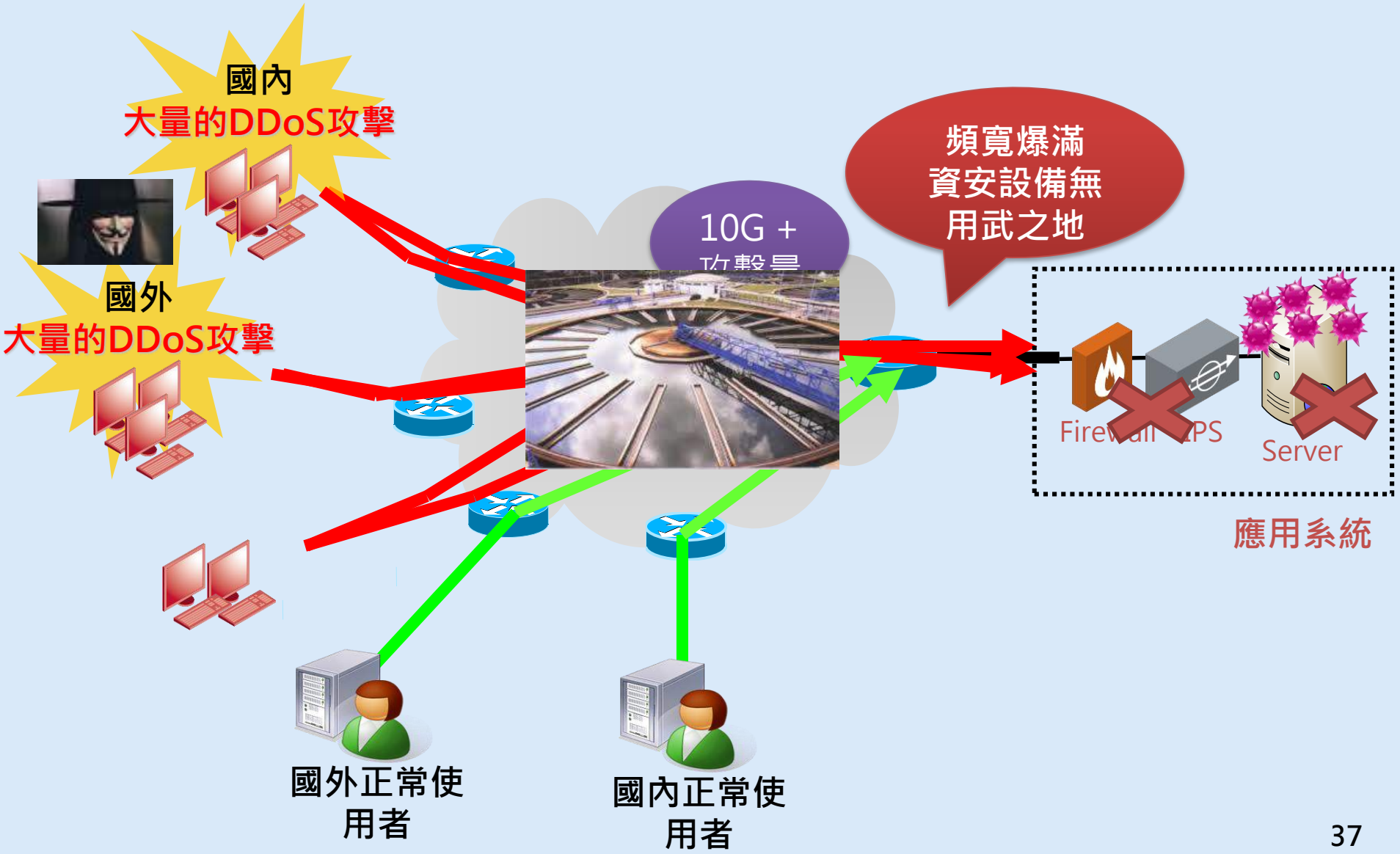
- 證券期貨市場資安會議
- 董事會報告資安執行情形
- 高階主管資安宣導
- 新威脅與資訊科技發展 workshop



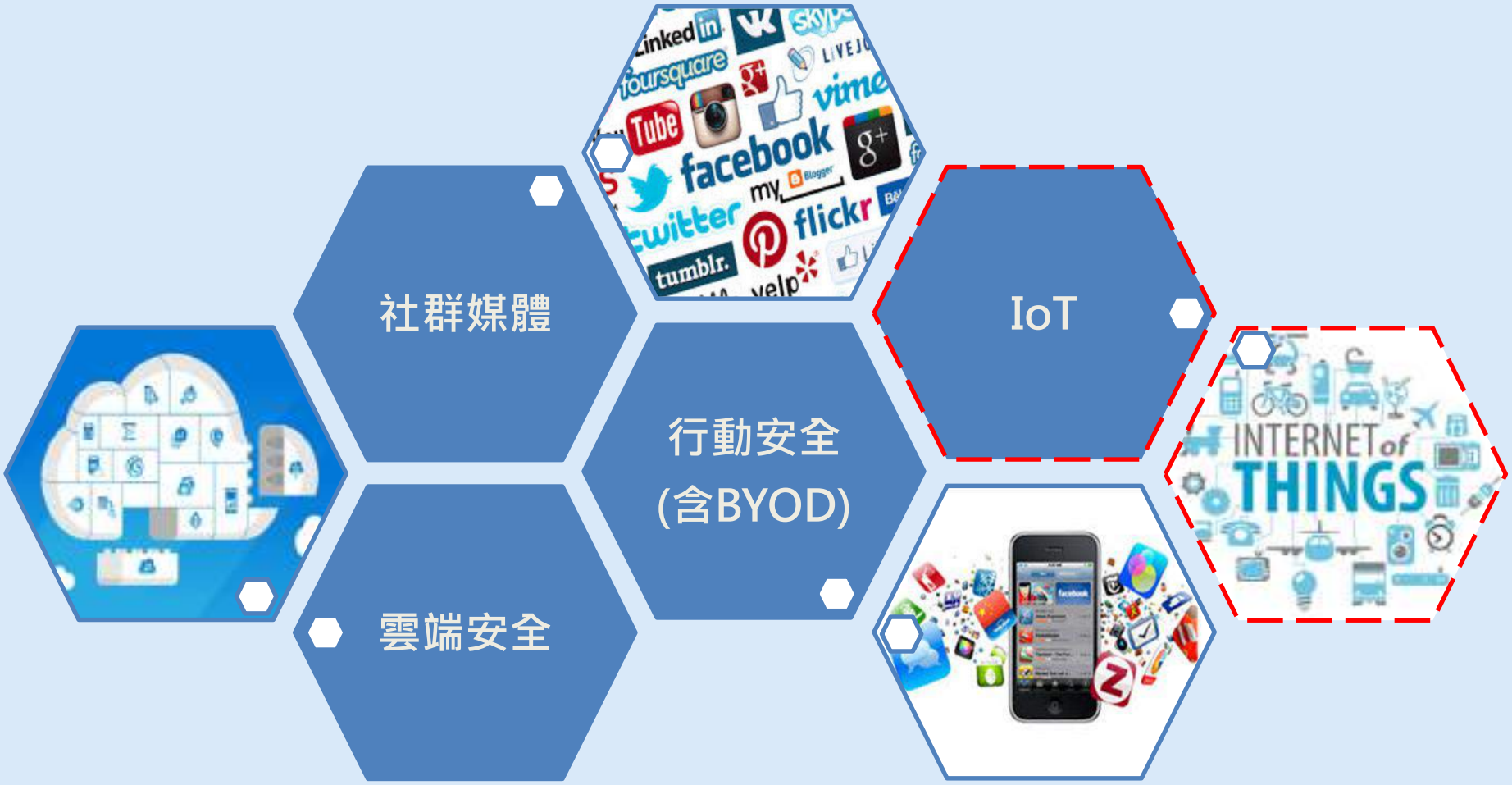
- 業者資安查核

- 監控業者資訊服務
- 資安通報系統
- 證券期貨業緊急應變小組
- 提供業者技術支援
- 資安資訊分享平台

DDoS攻擊防護


國內
大量的DDoS攻擊
國外
大量的DDoS攻擊
10G +
頻寬爆滿
資安設備無
用武之地
Firewall
IPS
Server
應用系統
國外正常使
用者
國內正常使
用者

物聯網(IoT)控管指引

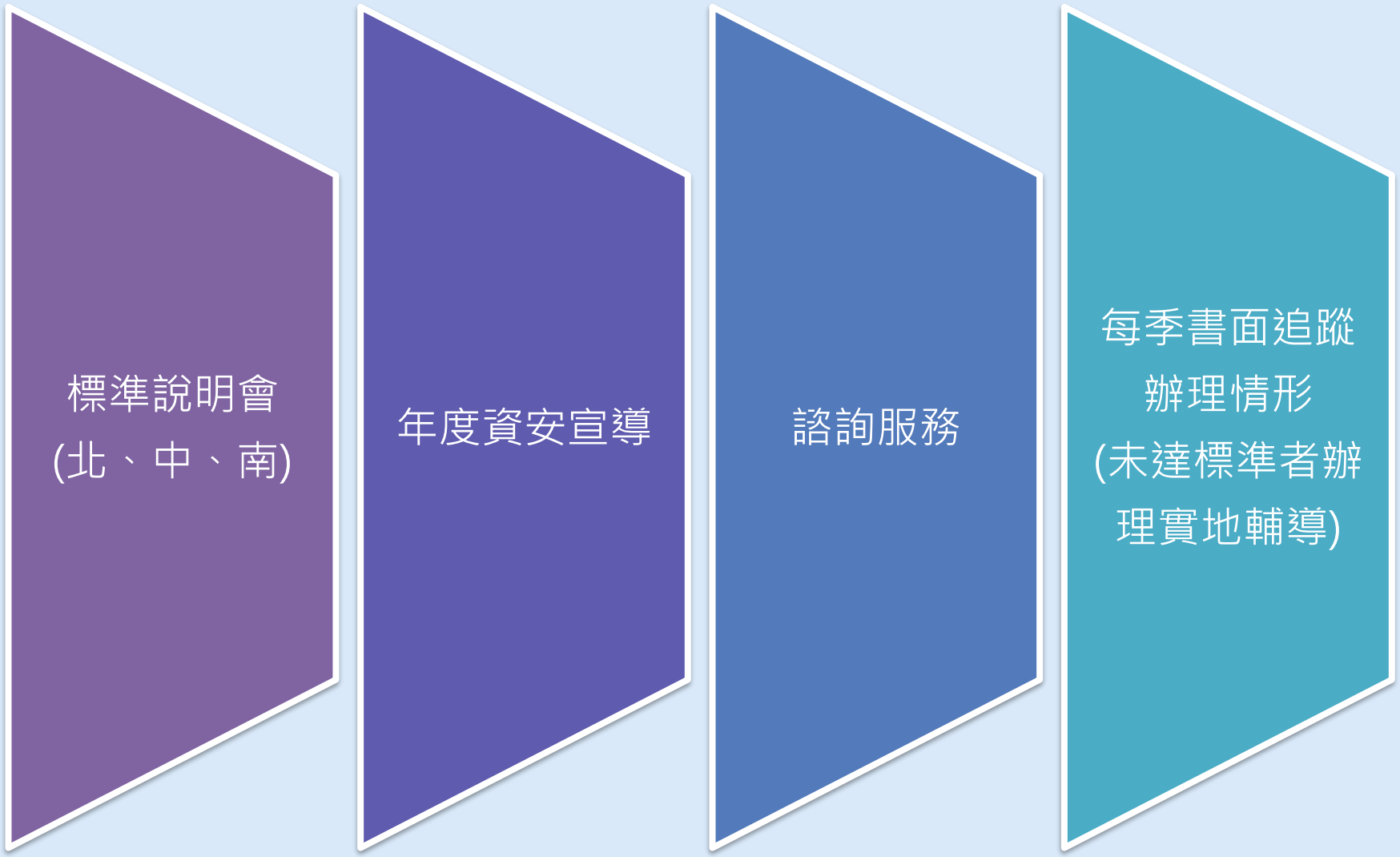


證券期貨業者資通安全防護標準研究報告

依不同等級建立應遵循之
資訊安全管理標準

證券期貨業者資通
安全防護標準

推動「資安防護標準」

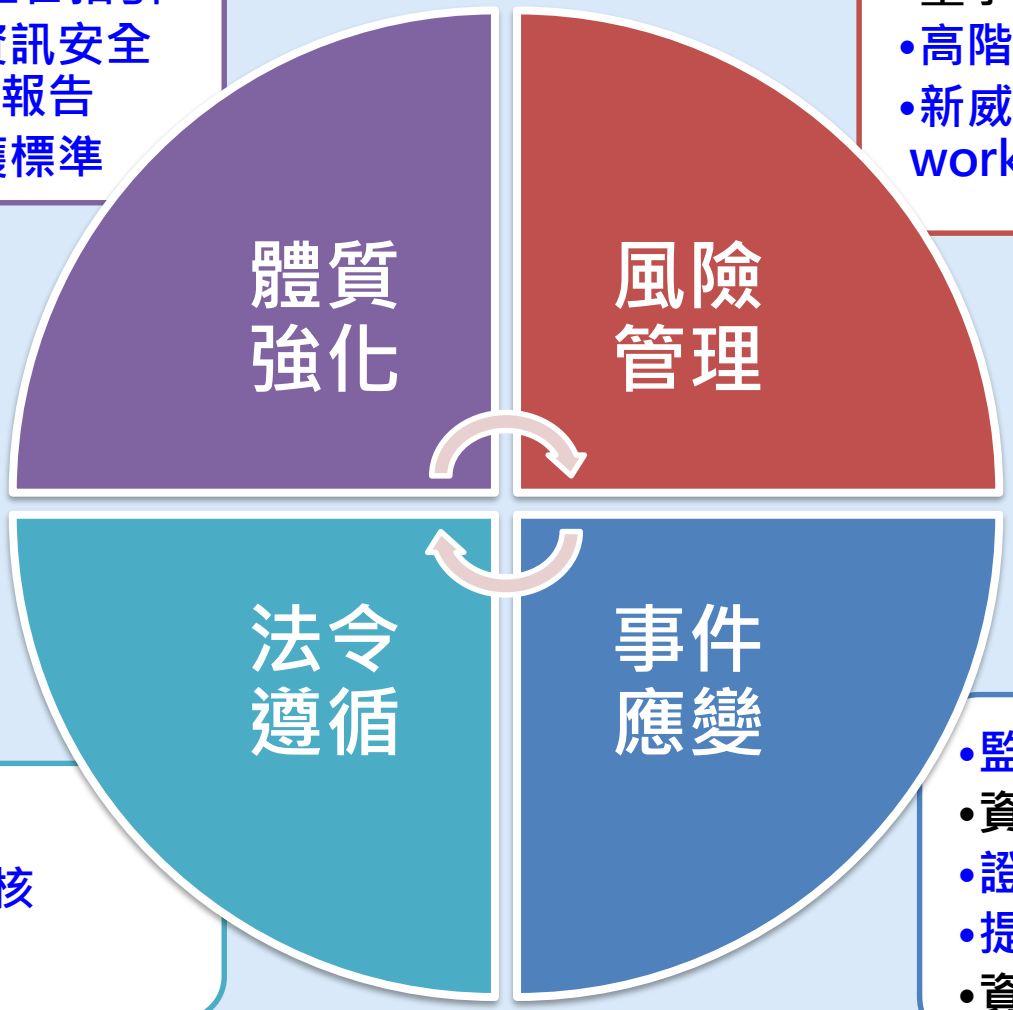


證券商資安防護強化作為

竭誠為您服務

- DDoS攻擊防護
- 物聯網(IoT)控管指引
- 證券期貨商資訊安全防護標準研究報告
- 推動資安防護標準

- 證券期貨市場資安會議
- 董事會報告資安執行情形
- 高階主管資安宣導
- 新威脅與資訊科技發展workshop



- 業者資安查核

- 監控業者資訊服務
- 資安通報系統
- 證券期貨業緊急應變小組
- 提供業者技術支援
- 資安資訊分享平台

簡報完畢