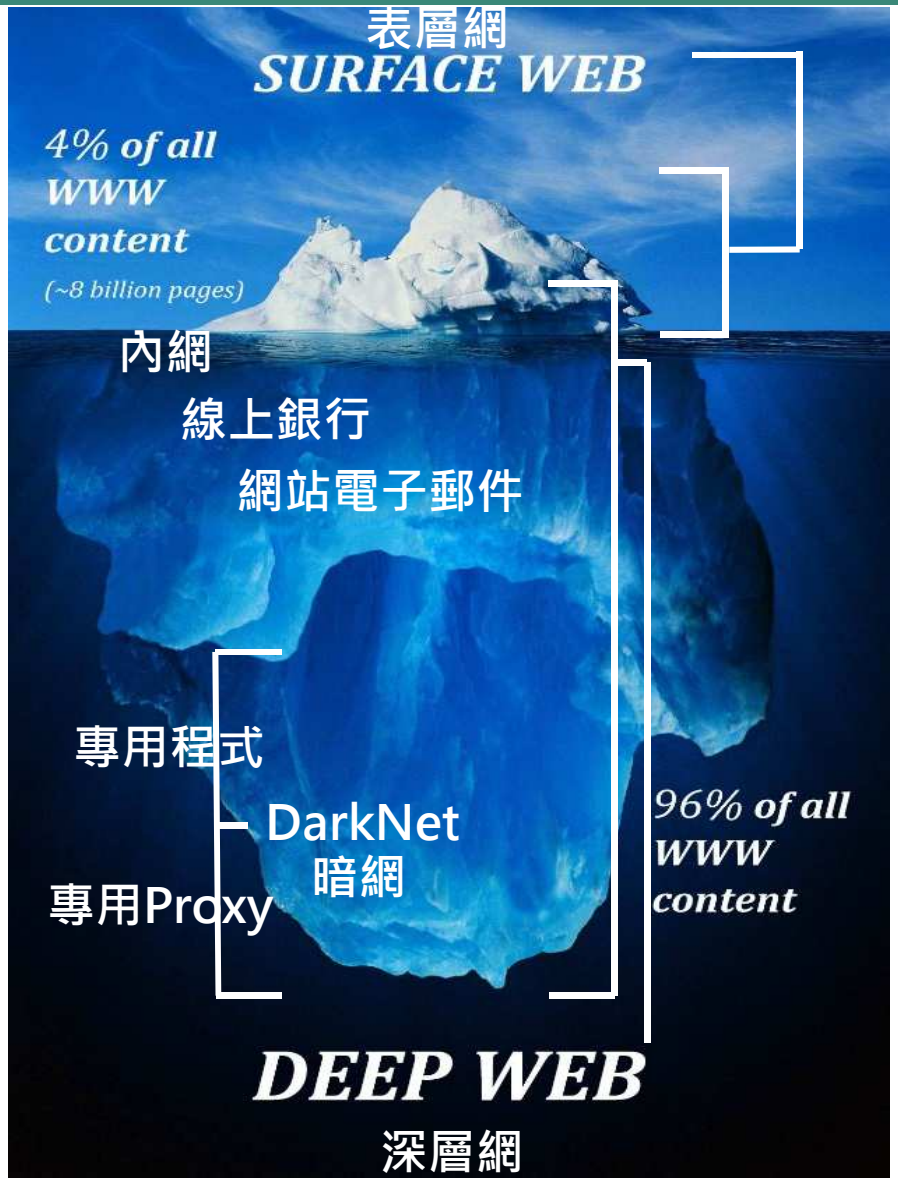
大吉大利話資安

howard@ey.gov.tw

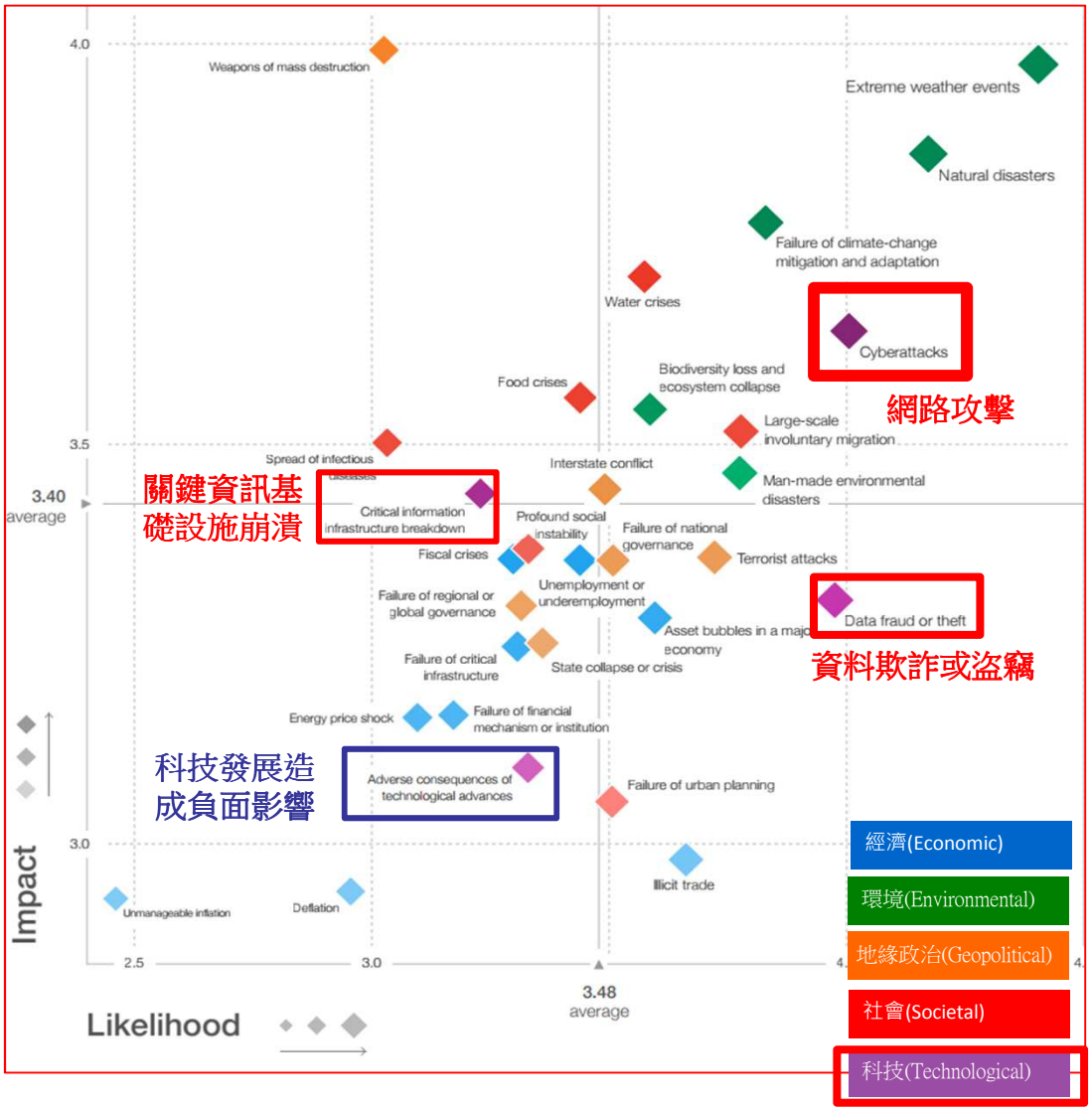
107年7月27日

- 面臨的環境
- 怎麼想?怎麼做?
- 產業的機會在哪?

Deep Web


表層網
SURFACE WEB
4% of all WWW content
(~8 billion pages)
內網
線上銀行
網站電子郵件
專用程式
DarkNet
暗網
專用Proxy
96% of all WWW content
DEEP WEB
深層網

世界經濟論壇2018全球風險調查報告



10大可能風險

1. 極端氣侯
2. 自然災害
3. 網路攻擊(同時為第6大影響風險、2017年排名第6)
4. 資料欺詐或盜竊(2017年排名第5)
5. 氣候變化調節與適應機制失效
6. 大規模非自願移民
7. 人為環境災害
8. 恐怖攻擊
9. 非法貿易
10. 主要經濟體的資產泡沫化

全球資安威脅趨勢

進階持續威脅攻擊竊取機密資料

分散式阻斷服務攻擊癱瘓網路運作

物聯網設備資安弱點威脅升高

關鍵資訊基礎設施資安風險倍增

網路與經濟罪犯影響電子商務與金融運作

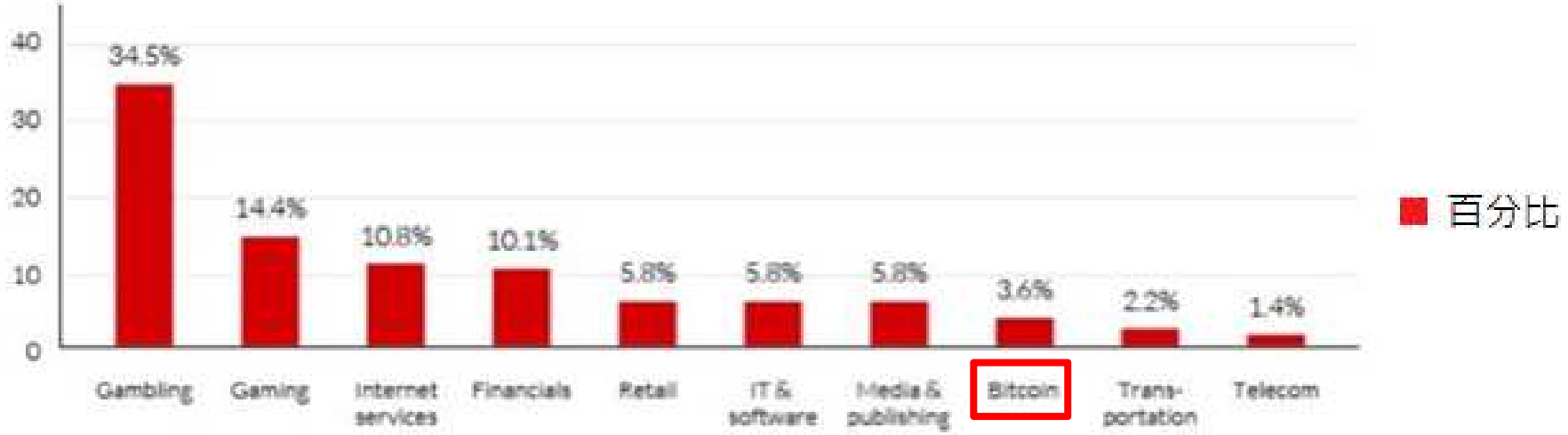
資安(訊)供應商持續遭駭破壞供應鏈安全

進階持續威脅攻擊竊取機密資料

竊走孟加拉央行26億　駭客入侵SWIFT金融軟體

出版時間：2016/04/25 16:28

分散式阻斷服務攻擊癱瘓網路運作

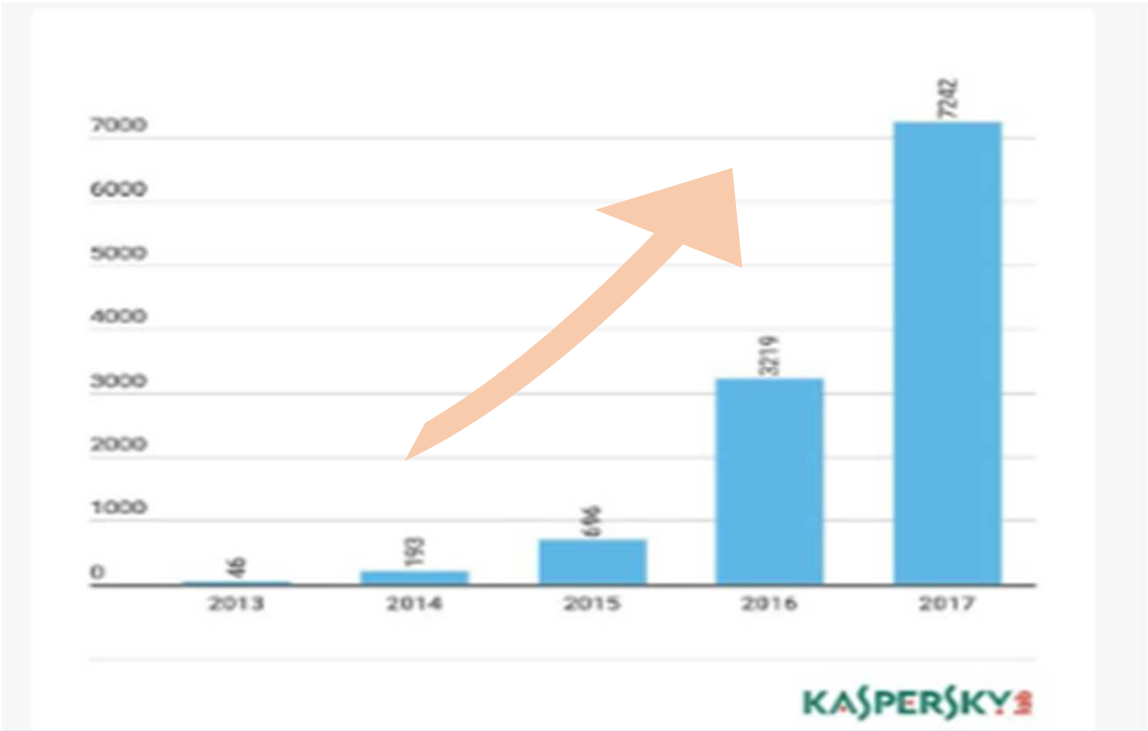


前十大DDoS攻擊產業目標

資料來源：IMPERVA

物聯網設備資安弱點威脅升高

IoT惡意程式數量



資料來源：KASPERSKY LAB

關鍵資訊基礎設施資安風險倍增

世界首例，烏克蘭大停電證實是遭駭客入侵

作者 藍 弋丰 | 發布日期 2016 年 01 月 11 日 7:42 | 分類 網路, 能源科技, 資訊安全 Follow G+ 讚 1,830 分享

烏克蘭電力系統遭駭原因是網路釣魚，如何加強資安防護引討論

作者 藍 弋丰 | 發布日期 2016 年 04 月 26 日 15:13 | 分類 能源科技, 資訊安全 Follow G+ 讚 86 分享

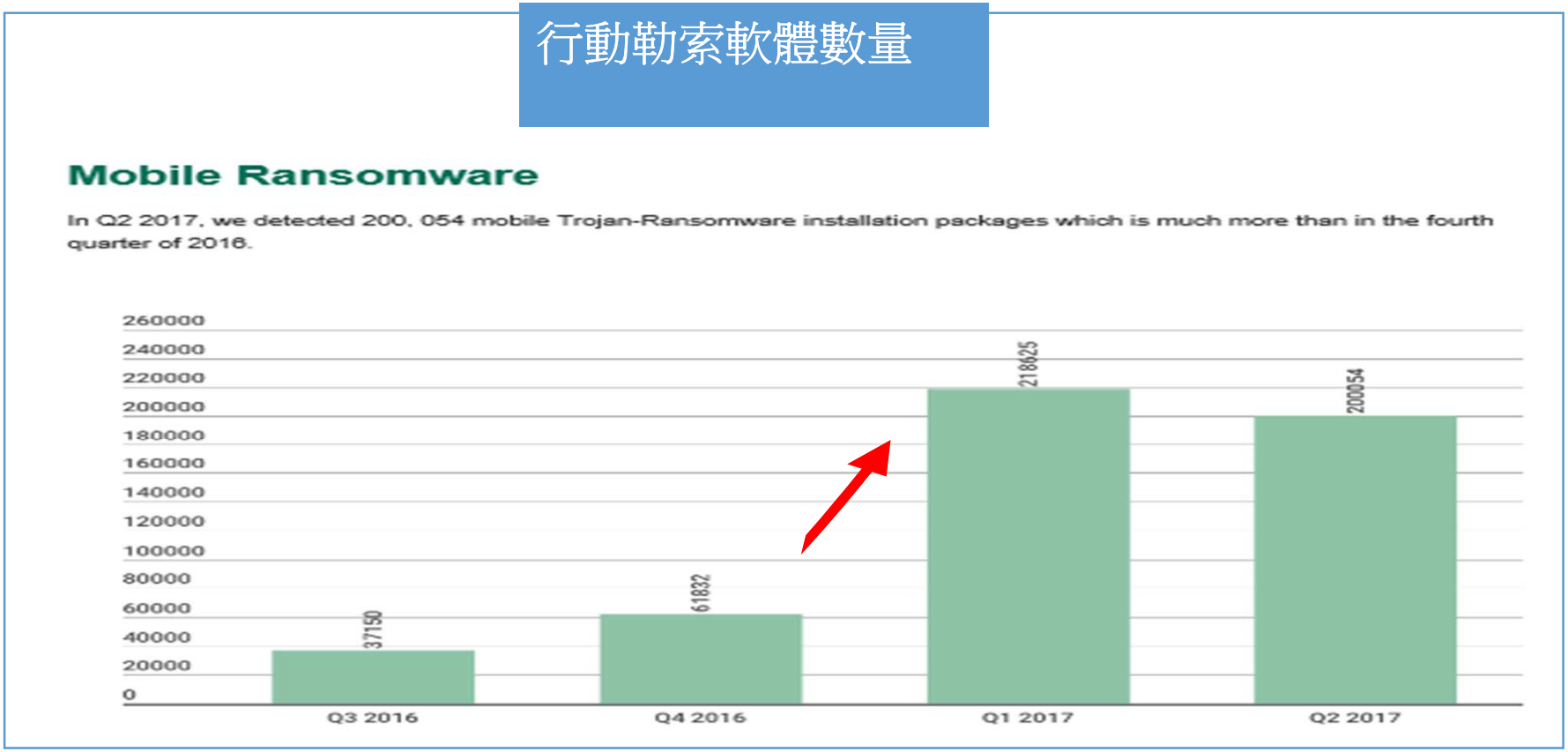
CI安全警報再次響起! FireEye：駭客入侵電廠意外觸發系統中斷供電，疑國家級駭客所為

駭客攻擊電廠卻意外觸發工業安全系統中斷程序，除未造成任何實體損害，資安廠商FireEye表示，這是一個國家級的攻擊，而且下一次可能沒這麼幸運，

文/ 李建興 | 2017-12-18 發表 讚 4.7萬 按讚加入iThome粉絲團 讚 174 分享 G+

網路與經濟罪犯影響電子商務與金融運作

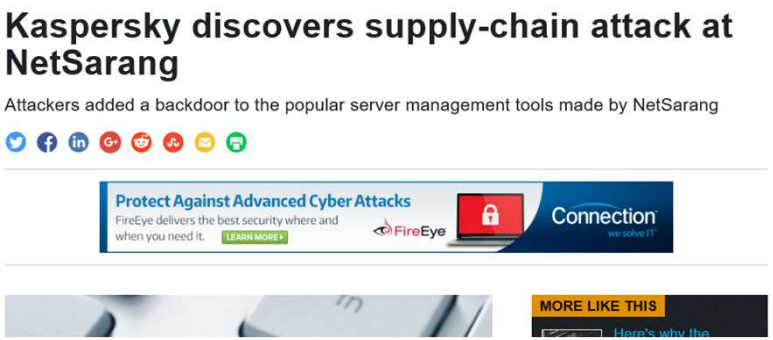
行動勒索軟體數量



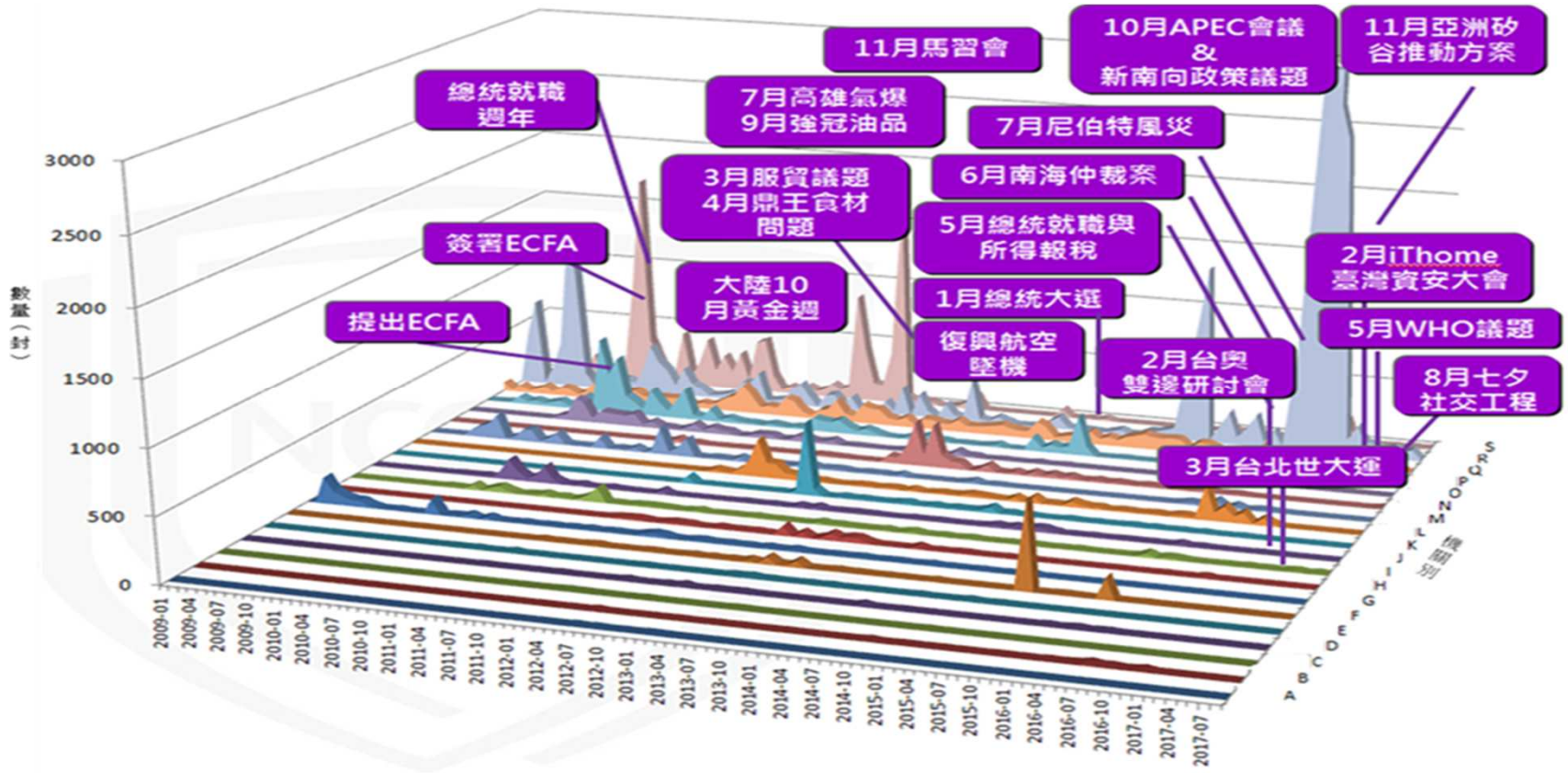
資料來源：KASPERSKY LAB

資安(訊)供應商持續遭駭破壞供應鏈安全

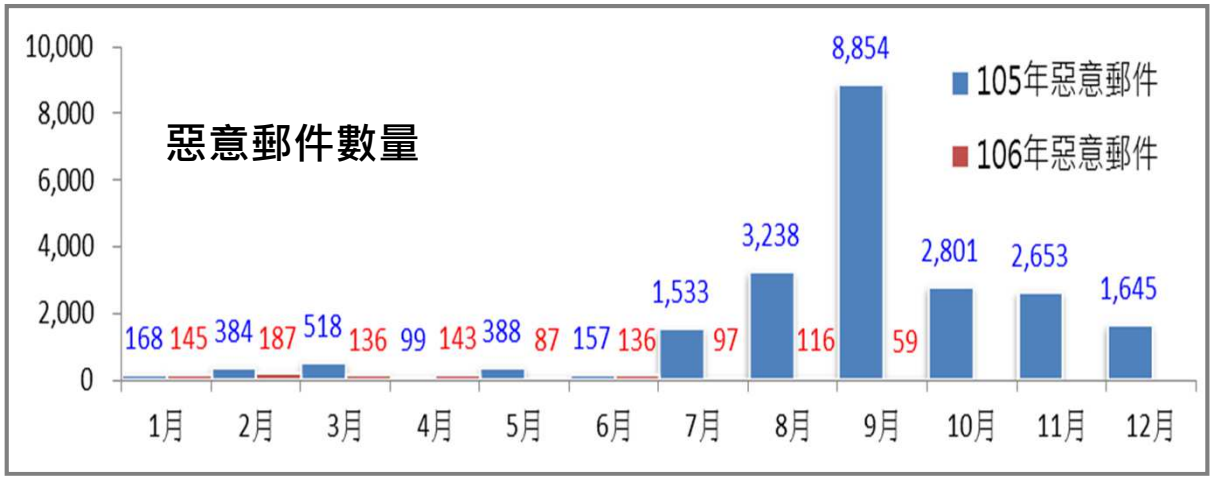
供應鏈攻擊警告：知名清理軟體CCleaner被惡意軟體感染，官網下載也得當心！

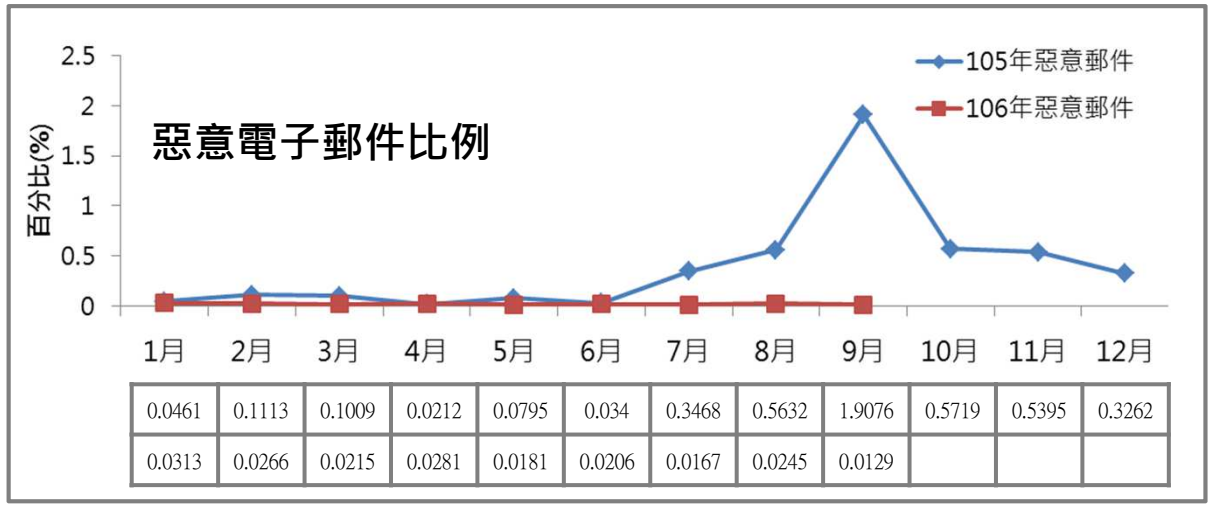


進階持續性威脅(APT)攻擊手法



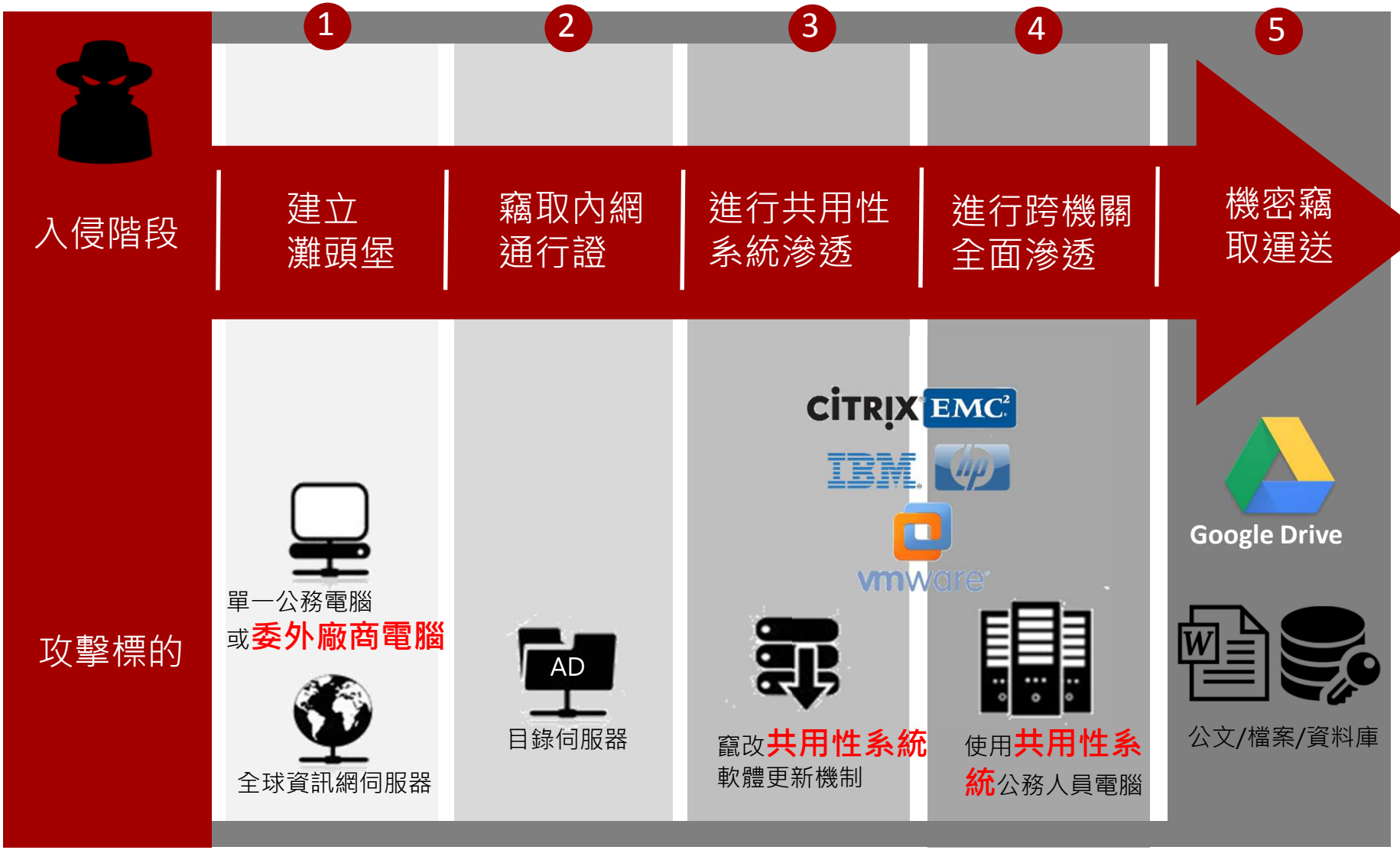
進階持續性威脅(APT)攻擊仍在



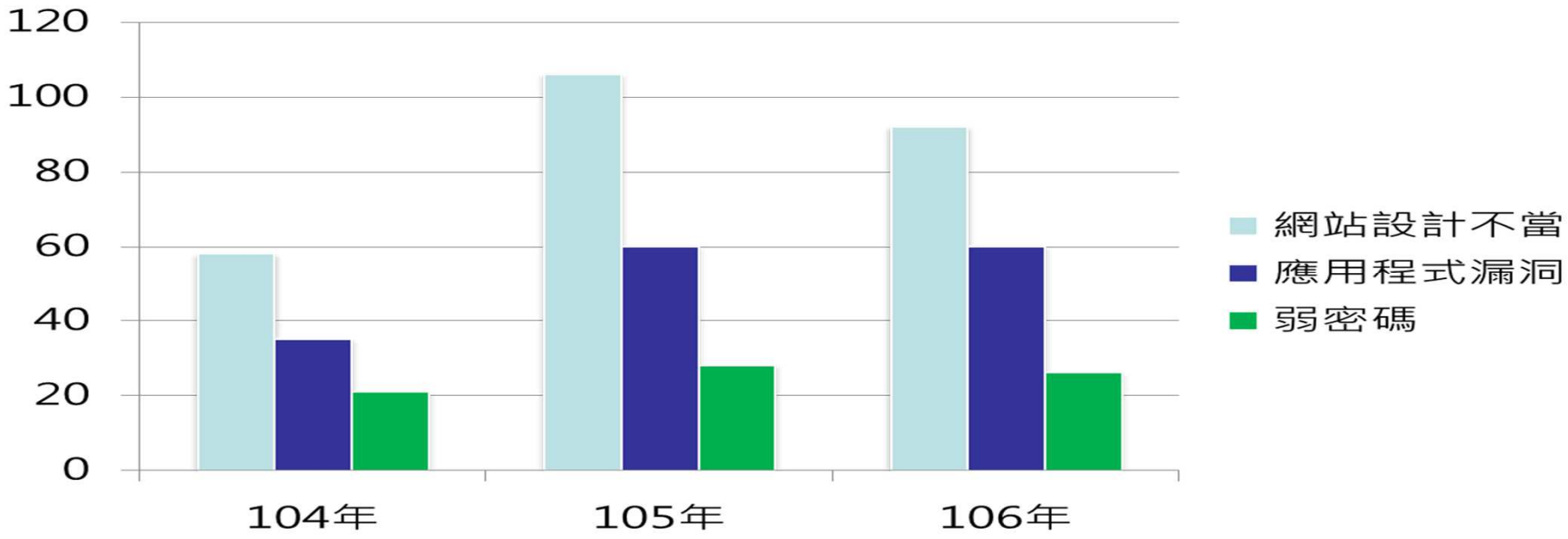


0.0461	0.1113	0.1009	0.0212	0.0795	0.034	0.3468	0.5632	1.9076	0.5719	0.5395	0.3262
0.0313	0.0266	0.0215	0.0281	0.0181	0.0206	0.0167	0.0245	0.0129			

共用性系統與雲端服務遭利用

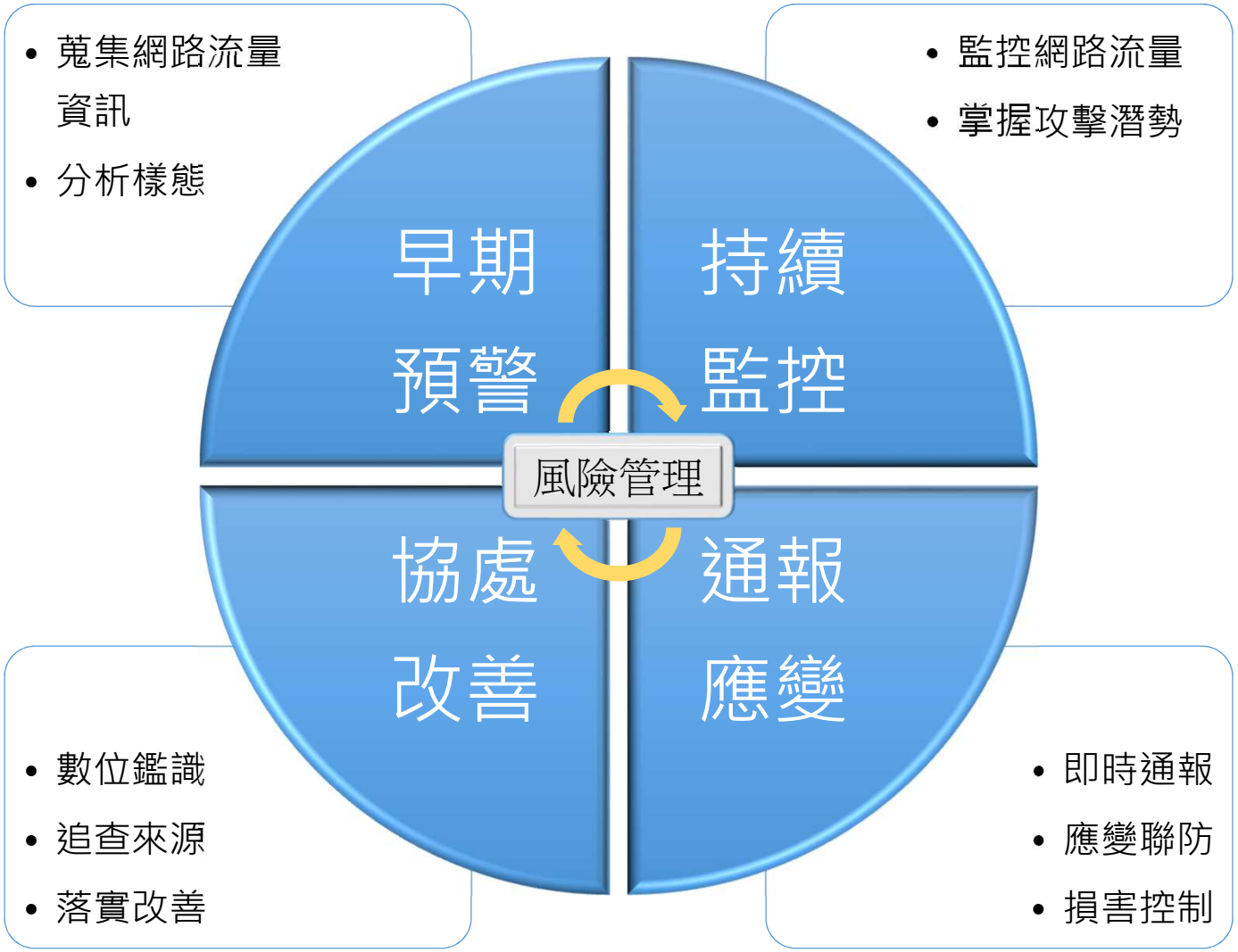


政府機關資安事件發生原因

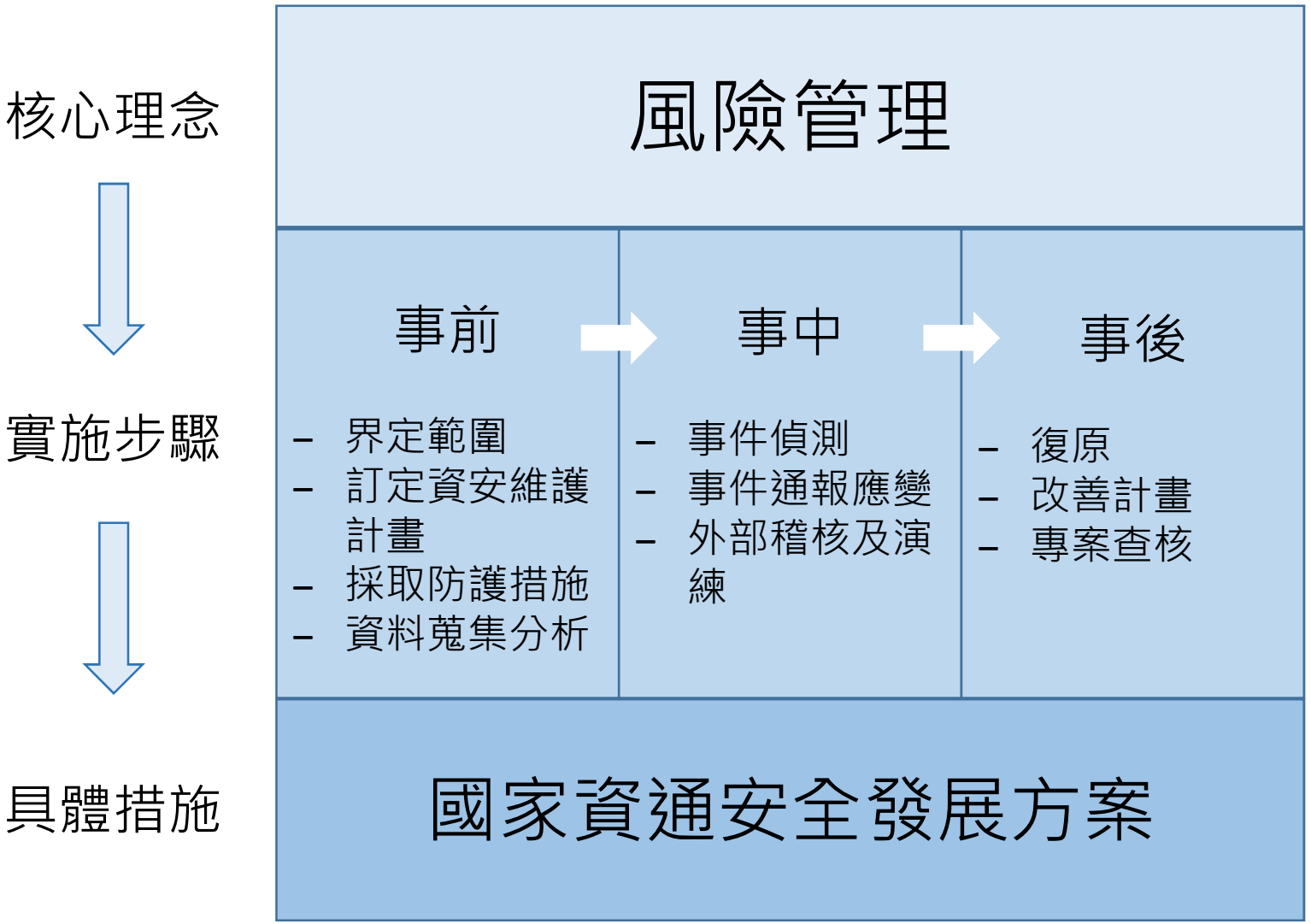


- 我們面臨的環境
- 怎麼想?怎麼做?
- 產業的機會在哪?

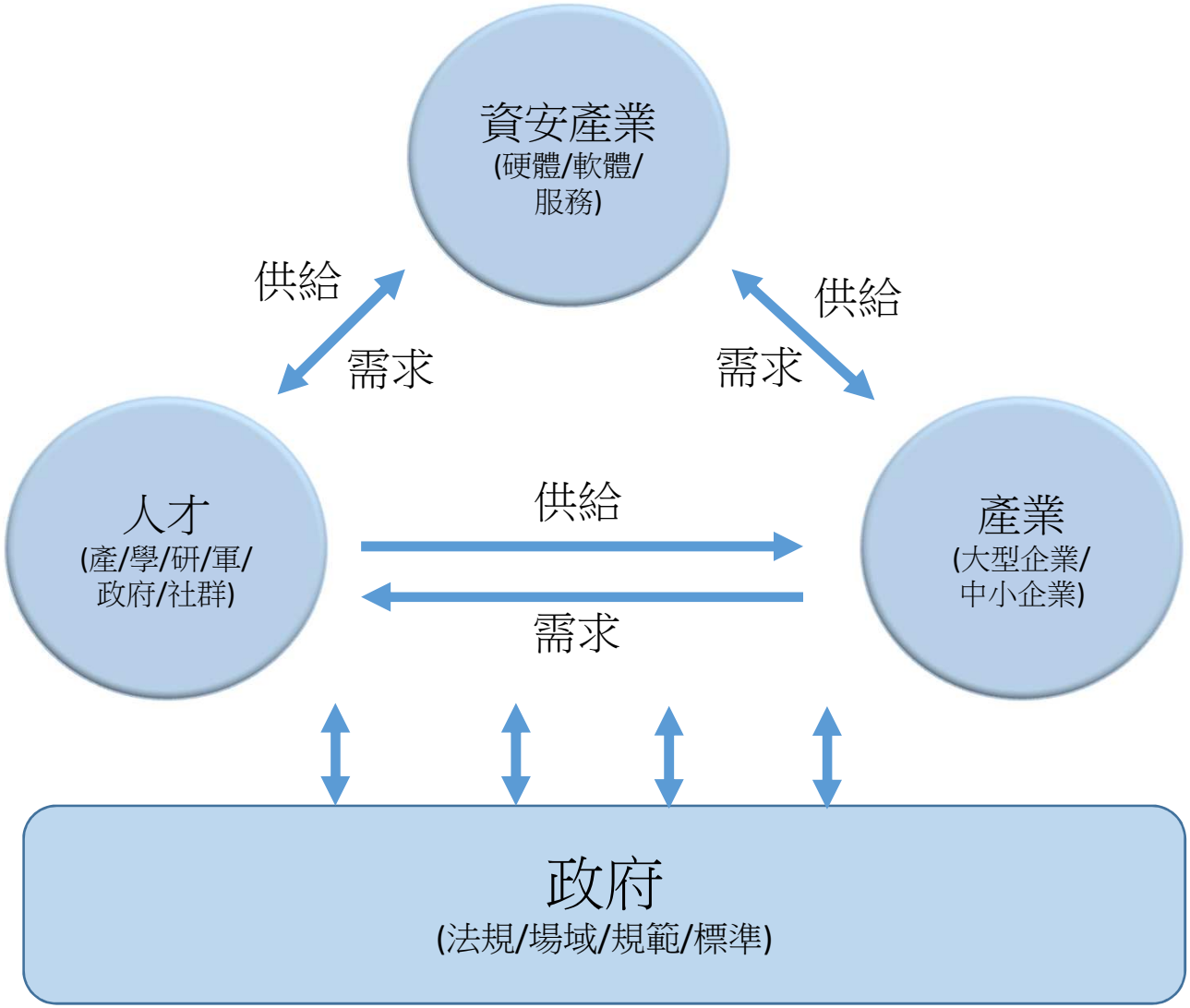
以風險管理為核心的資安防護



資通安全實施架構


核心理念
實施步驟
具體措施
風險管理
事前
事中
事後
界定範圍
訂定資安維護計畫
採取防護措施
資料蒐集分析
事件偵測
事件通報應變
外部稽核及演練
復原
改善計畫
專案查核
國家資通安全發展方案

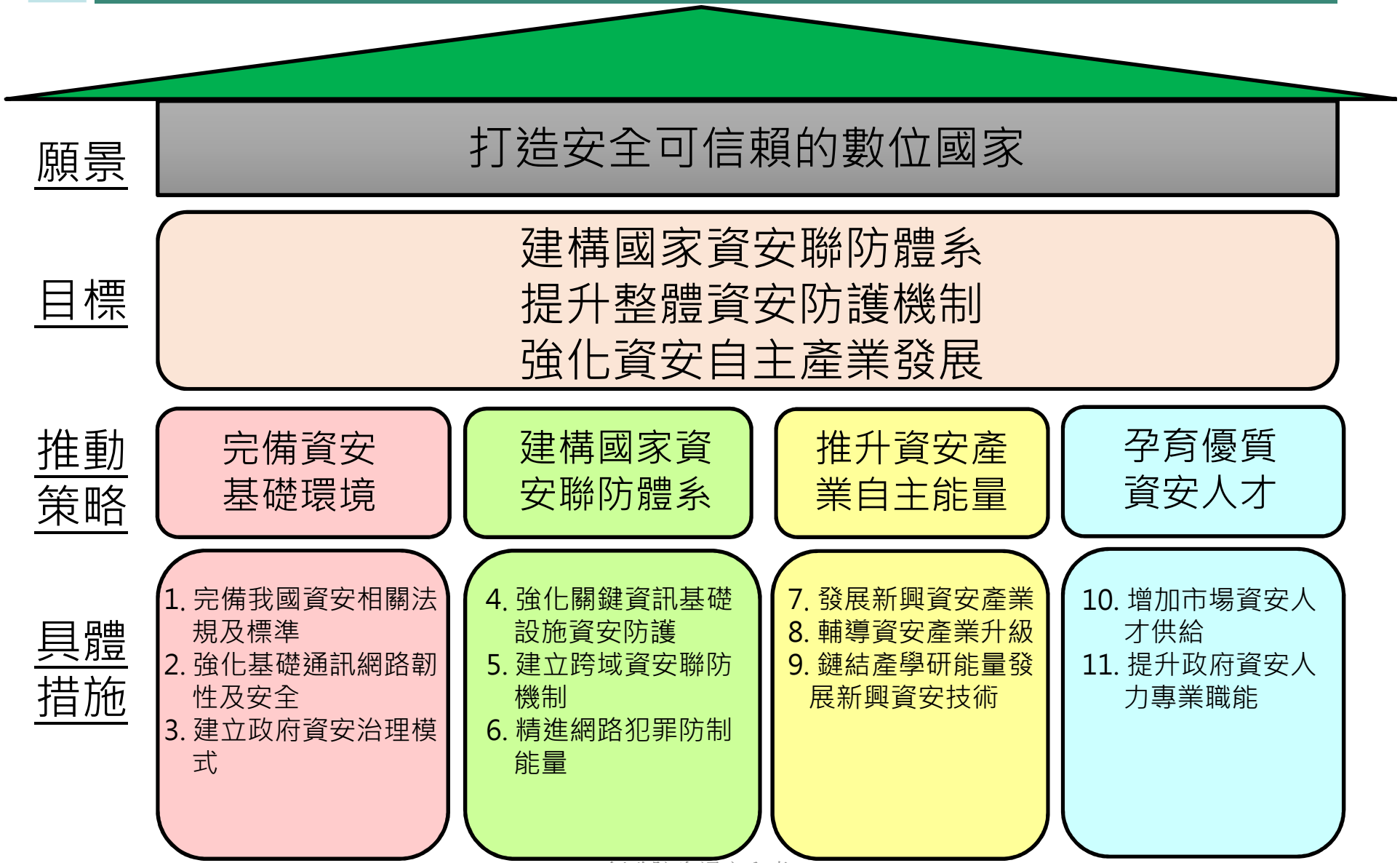
建構資安生態系


資安產業
(硬體/軟體/
服務)
供給
需求
供給
需求
人才
(產/學/研/軍/
政府/社群)
供給
需求
產業
(大型企業/
中小企業)
政府
(法規/場域/規範/標準)

資安人才培育


政策推動
在學
高中職、大專以上
• 建構實務研習環境
• 建立資安道德意識
• 尋覓潛才專案培育
各級學校
• 建立資安意識觀念
• 推動資安認知教育
社群團體
• 強化社群互動交流挖掘/培育人才
• 推動社課社師交流引導
在職
政府機關
• 推動資安專職專才
• 強化核心領域職能
• 多元轉任/多元進用
產業人員
• 產業資安人才職訓/進修
• 跨域研發人才培育
• 培養前瞻技術能力
• CIIP領域專才培訓
在營
資通電軍
• 提升現有軍種資安能力
• 強化資通電軍專業能力與實戰操演技能

資安發展藍圖


願景
打造安全可信賴的數位國家
目標
建構國家資安聯防體系
提升整體資安防護機制
強化資安自主產業發展
推動策略
完備資安基礎環境
建構國家資安聯防體系
推升資安產業自主能量
孕育優質資安人才
具體措施
1. 完備我國資安相關法規及標準
2. 強化基礎通訊網路韌性及安全
3. 建立政府資安治理模式
4. 強化關鍵資訊基礎設施資安防護
5. 建立跨域資安聯防機制
6. 精進網路犯罪防制能量
7. 發展新興資安產業
8. 輔導資安產業升級
9. 鏈結產學研能量發展新興資安技術
10. 增加市場資安人才供給
11. 提升政府資安人力專業職能

法案結構

- 行政院、委託或委任單位、各公務機關
- 中央目的事業主管機關權責
- 權限委託

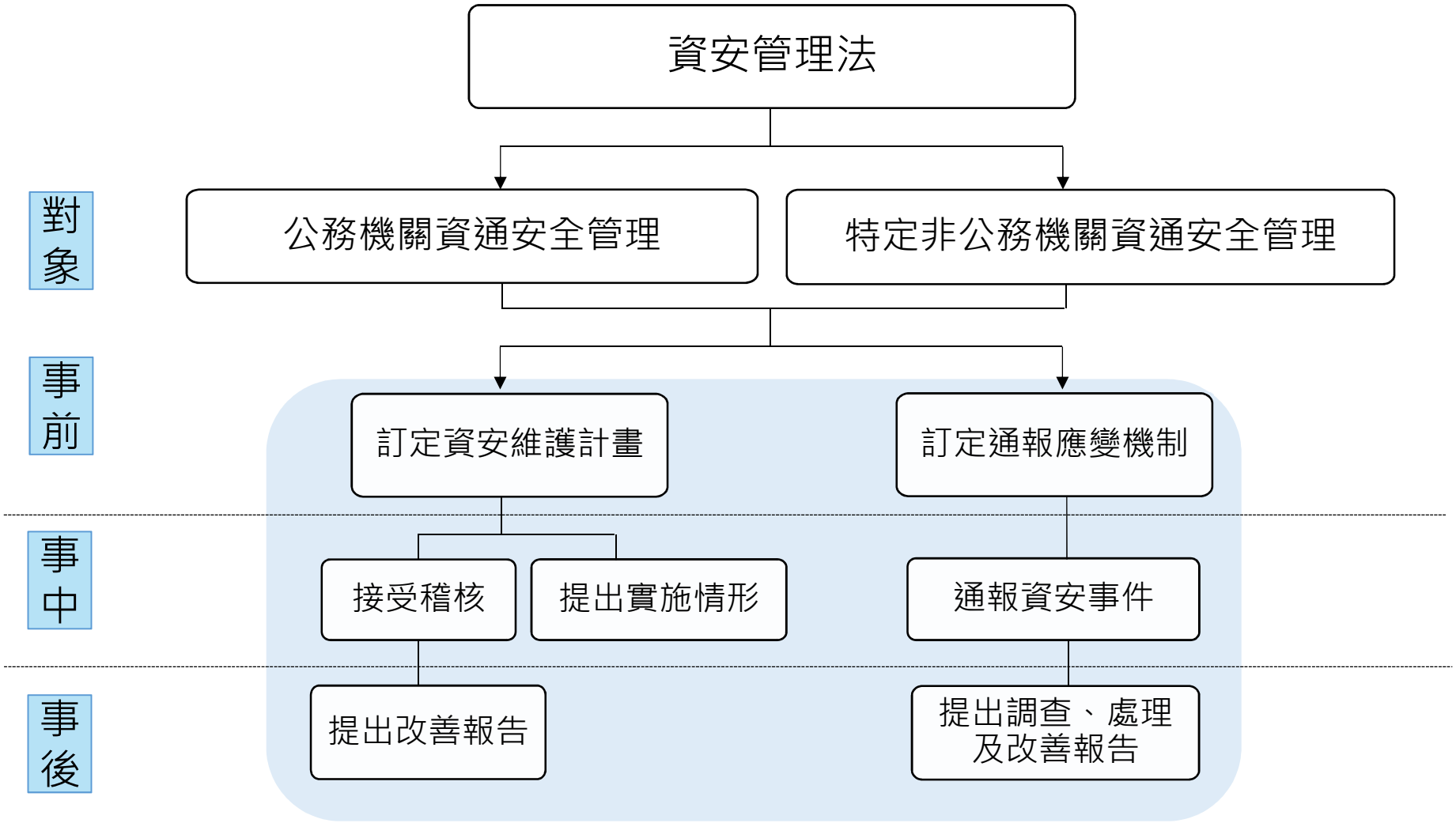
- 資安責任等級分級
- 資安維護計畫之制定與實施
- 年度資安維護計畫實施情形提出
- 資安稽核
- 資安事件通報應變
- 改善報告
- 公告
- 定期公布國家資通安全情勢報告及資通安全發展方案
- 建立情資分享機制

- 公務機關人員獎懲標準
- 通報義務
- 資安維護計畫實施
- 改善報告
- 應變機制

- 資安責任等級分級
- 資安維護計畫之制定與實施
- 資安長設置
- 年度資安維護計畫實施情形提出
- 資安稽核
- 改善報告
- 資安事件通報應變
- 公務機關人員獎懲標準

- 資安責任等級分級
- 資安維護計畫之制定與實施
- 年度資安維護計畫實施情形提出
- 資安稽核
- 資安事件通報應變
- 改善報告
- 公告
- 罰則

資安管理法架構


資安管理法
對象
公務機關資通安全管理
特定非公務機關資通安全管理
事前
訂定資安維護計畫
訂定通報應變機制
事中
接受稽核
提出實施情形
通報資安事件
事後
提出改善報告
提出調查、處理及改善報告

立法目的及規範對象

➢ 立法目的

為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。

➢ 規範對象

以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

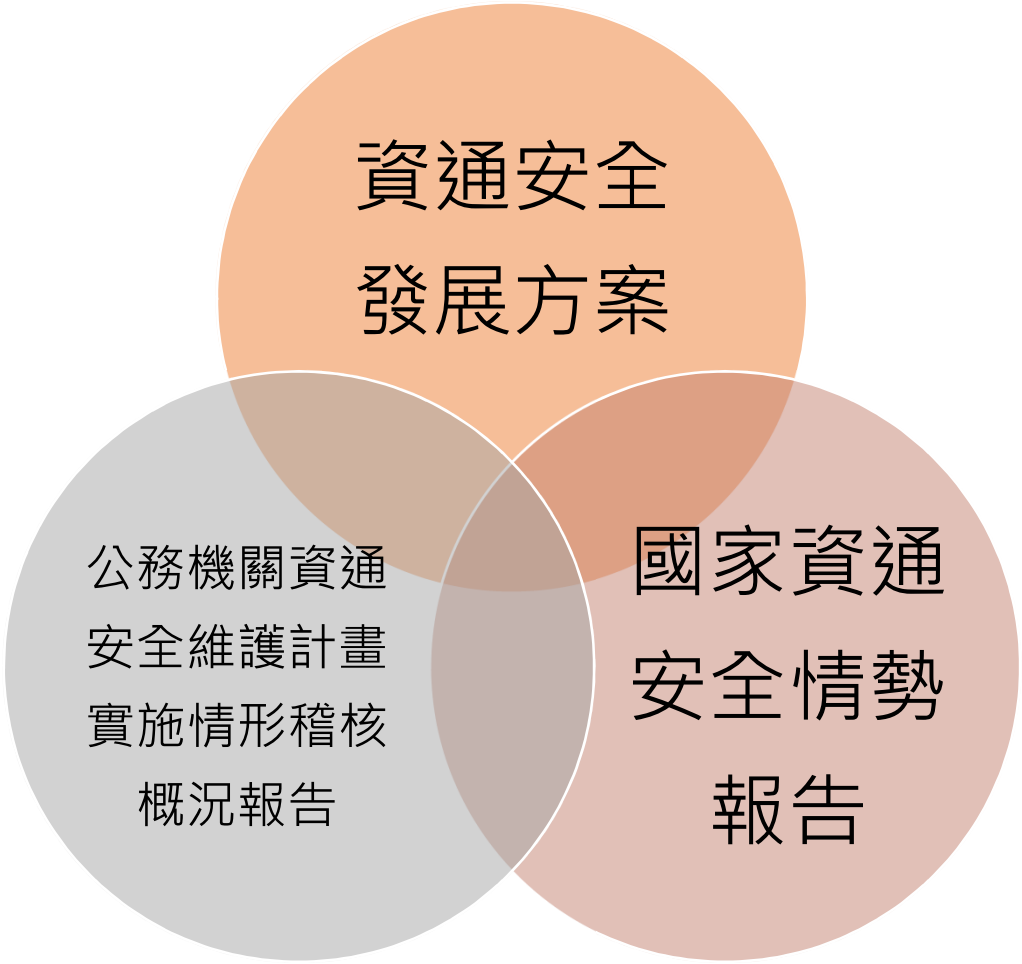
公務機關

- 中央與地方機關(構)
- 公法人

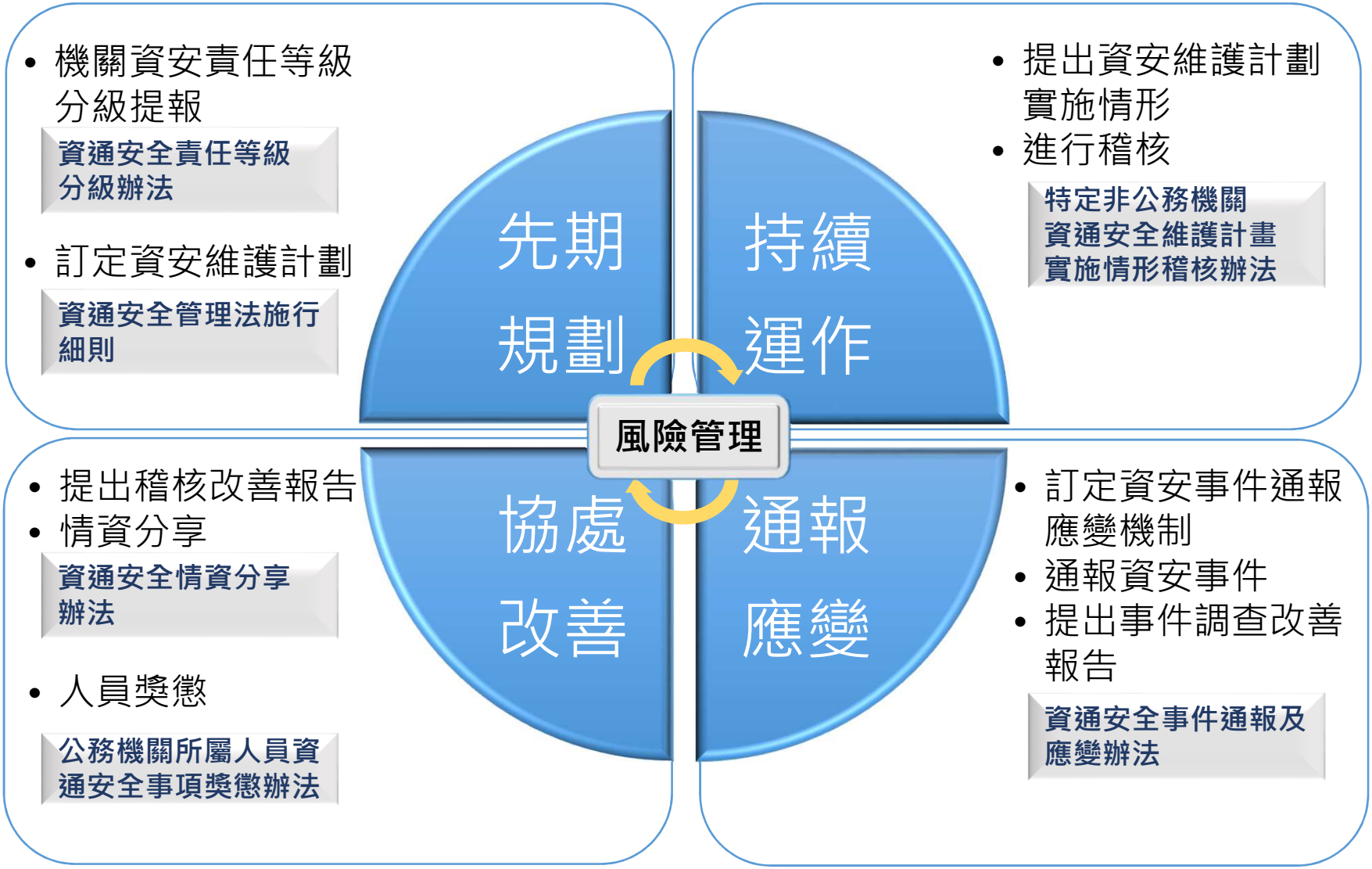
特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

送立法院備查文件

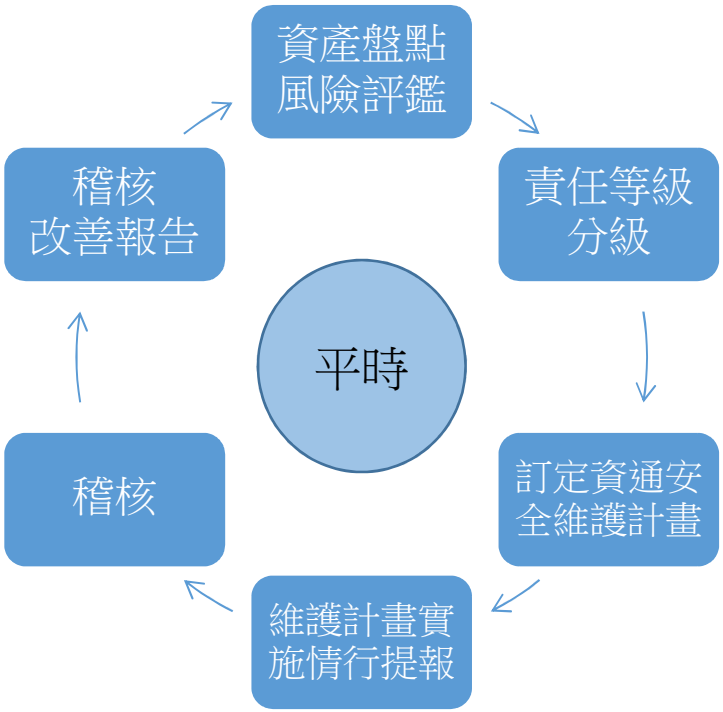


資安管理子法架構

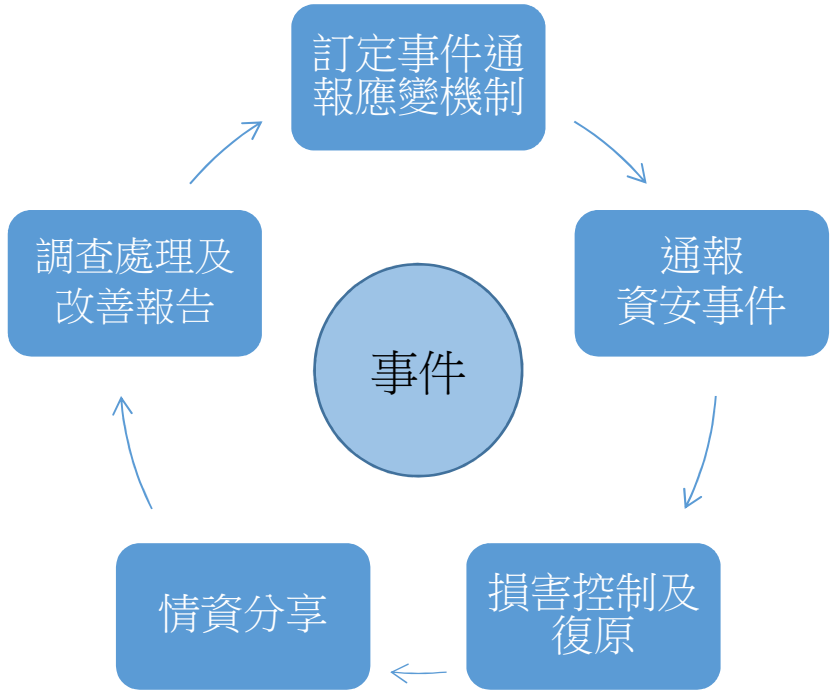

先期規劃
持續運作
協處改善
通報應變
風險管理
• 機關資安責任等級分級提報
資通安全責任等級分級辦法
• 訂定資安維護計劃
資通安全管理法施行細則
• 提出資安維護計劃實施情形
• 進行稽核
特定非公務機關資通安全維護計畫實施情形稽核辦法
• 提出稽核改善報告
• 情資分享
資通安全情資分享辦法
• 人員獎懲
公務機關所屬人員資通安全事項獎懲辦法
• 訂定資安事件通報應變機制
• 通報資安事件
• 提出事件調查改善報告
資通安全事件通報及應變辦法

本法資安管理事項

資通安全責任等級分級辦法



資通安全事件通報應變辦法



特定非公務機關資通安全維護計畫實施情形稽核辦法

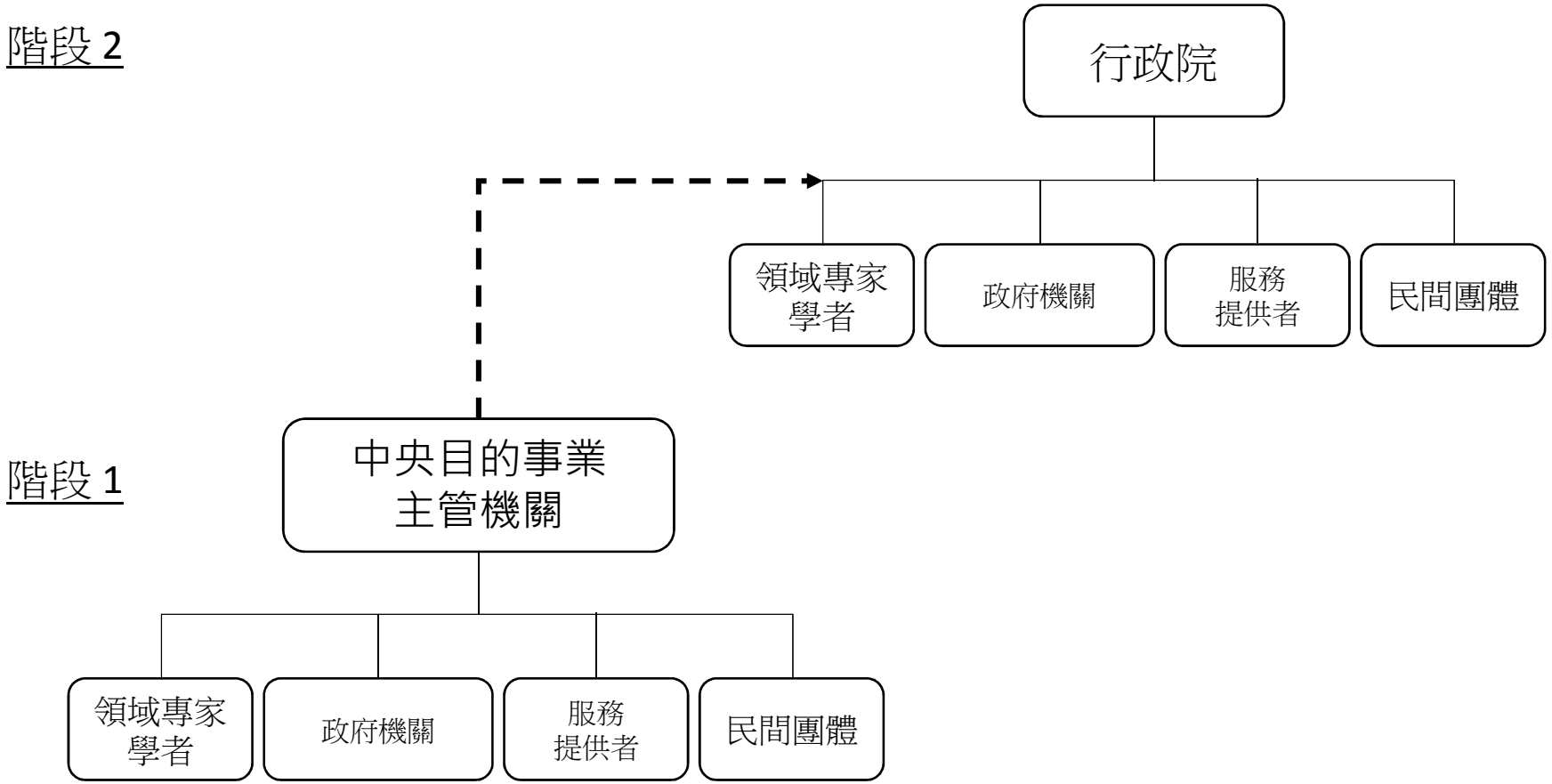
資通安全情資分享辦法

公務機關所屬人員資通安全事項獎懲辦法

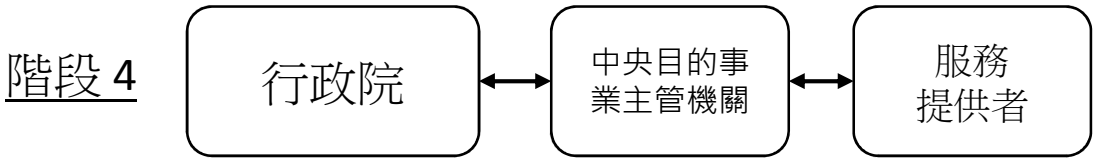
資通安全管理法施行細則

關鍵基礎設施(CI)

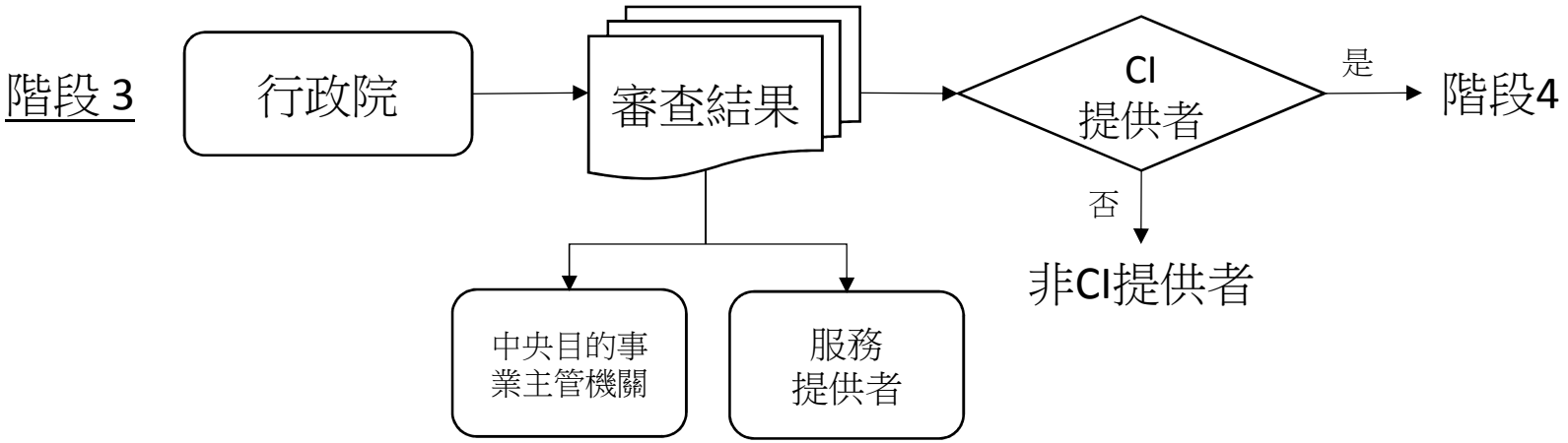
CI提供者指定程序(1/2)



CI提供者指定程序(2/2)



資通安全維護計畫實施情形



情資分享之內容

情資定義

情資分享例外

涉及營業秘密、侵害權利或正當利益(不含但書)

依法令規定應秘密或限制、禁止公開

分享情資

- 我們面臨的環境
- 怎麼想?怎麼做?
- 產業的機會在哪?

臺灣資安產業發展現況

終端與行動裝置防護

2017年產值：新臺幣98.7億元
參與廠商：43家

身份驗證、存取控制、防毒/惡意程式防護...

網路與閘道安全

2017年產值：新臺幣104.4億元
參與廠商：39家

防火牆, IDS/IPS,UTM, APT防護,...

資安營運管理服務

2017年產值：新臺幣63.5億元
參與廠商：12家

SOC監控服務、ISAC服務、雲端資產管理...

資安系統整合

2017年產值：新臺幣77.6億元
參與廠商：121家

資安系統整合、經銷服務...

物聯網安全

2017年產值：新臺幣0.04億元
參與廠商： 9 家

IOT加密模組、ICS Gateway、IC PUF...

WEB與內容應用安全

2017年產值：新臺幣9.5億元
參與廠商：14家

Email安全、WAF設備、內容過濾軟體、資料庫安全...

資安檢測/顧問服務

2017年產值：新臺幣31.8億元
參與廠商：41家

資安顧問、資安驗證、稽核鑑識、資安檢測...

資安支援服務

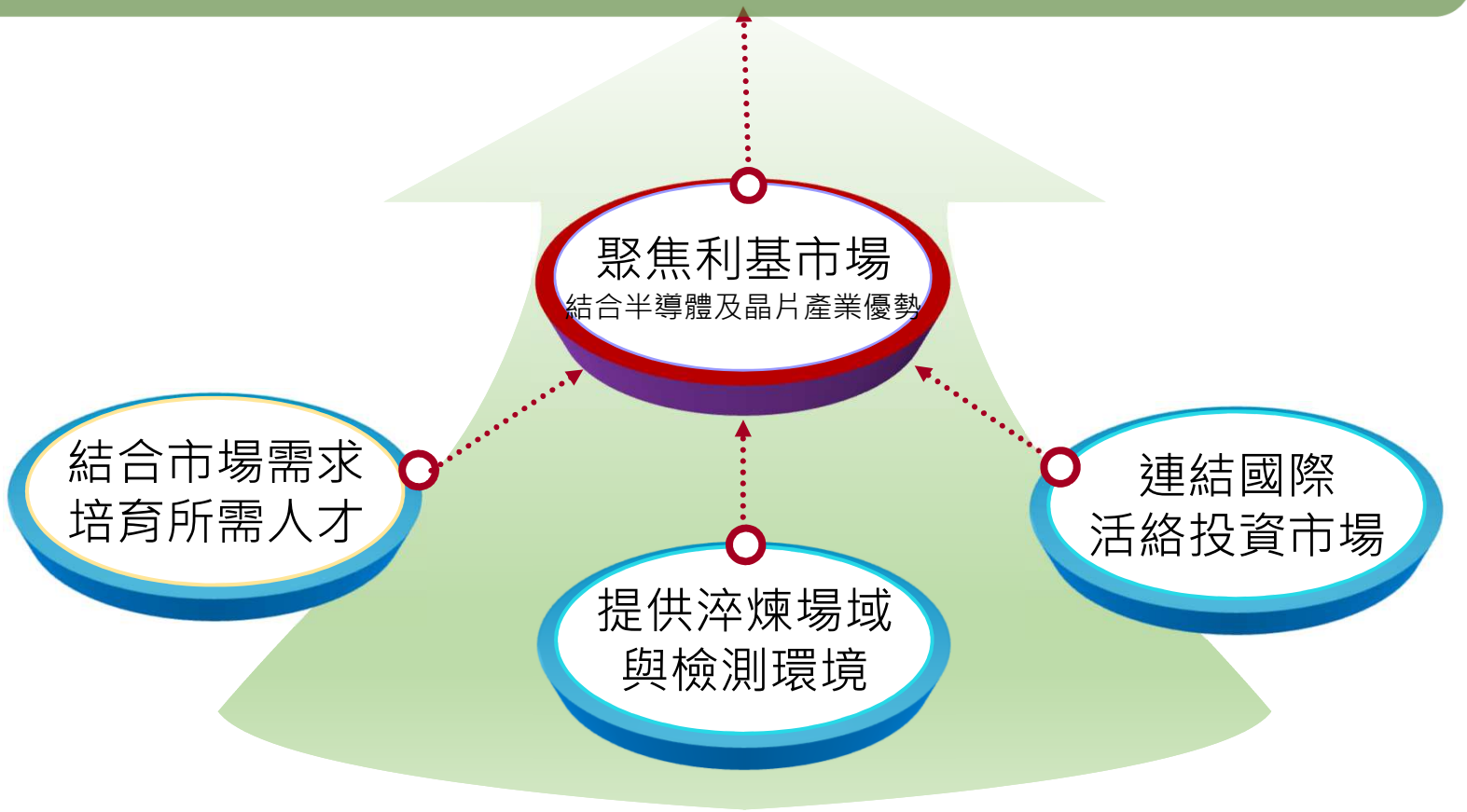
2017年產值：新臺幣2.1億元
參與廠商：15家

資安教育訓練、資安保險服務...

資料來源：工業技術研究院

願景

建立全球資安產業創業基地
打造臺灣產業優質安全品牌



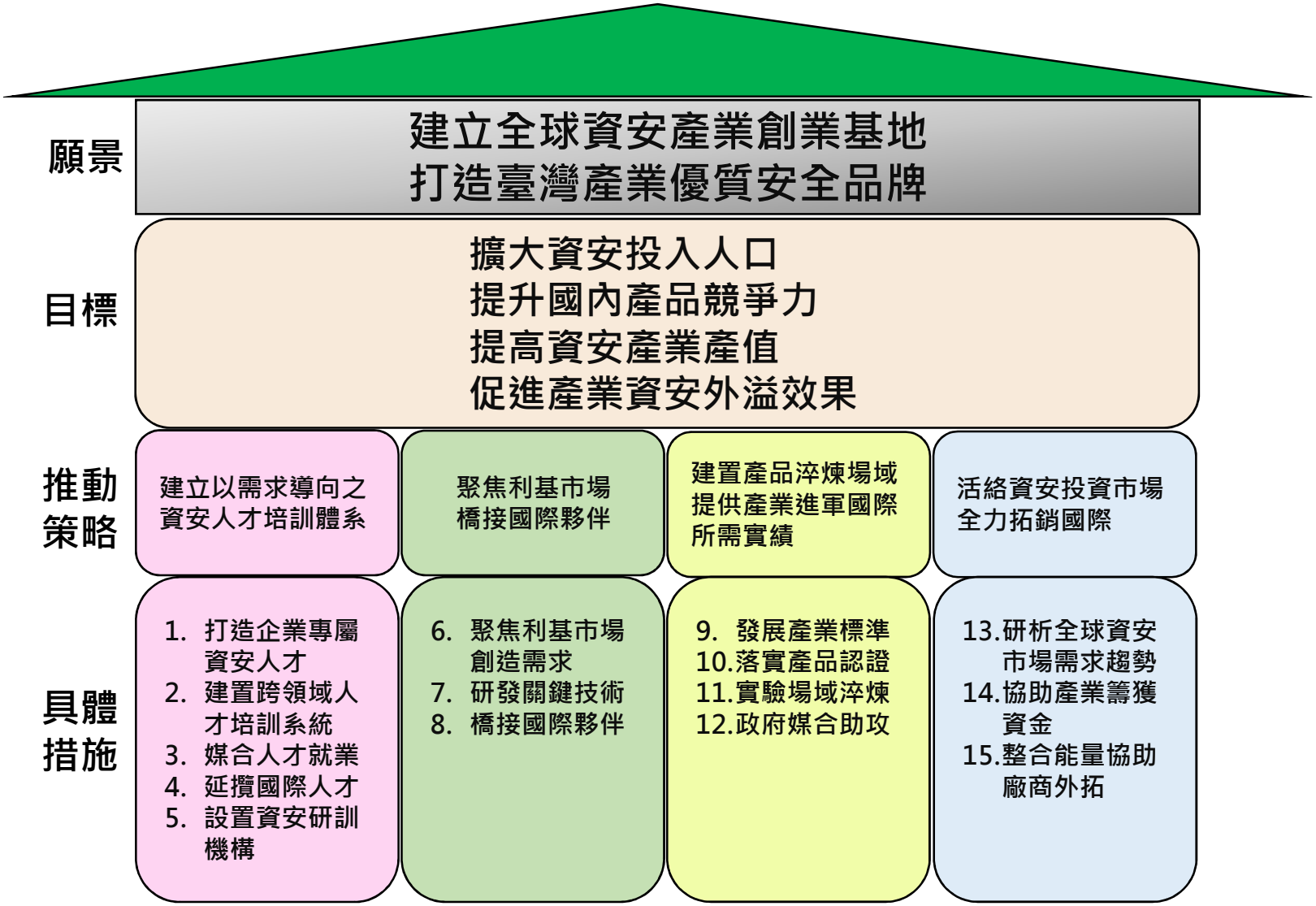
目標

目標1 擴大資安投入人口	目標2 提升國內產品競爭力	目標3 提高資安產業產值		目標4 促進產業資安外溢效果
~2020年				
資安投入人口數由現行8,500人成長5%	增修我國具優勢資通產品資安檢測驗證累計達9項	扶植新創公司累計達20家	資安產值550億	通過我國資安檢測驗證之產業產品，銷售額成長5%
~2025年				
資安投入人口數達萬人	增修我國具優勢資通產品資安檢測驗證累計達21項	扶植新創公司累計達40家	資安產值780億(8年double)	通過我國資安檢測驗證之產業產品，銷售額成長7%

建立全球資安產業創業基地

打造臺灣產業優質安全品牌

資安產業發展藍圖


願景
建立全球資安產業創業基地
打造臺灣產業優質安全品牌
目標
擴大資安投入人口
提升國內產品競爭力
提高資安產業產值
促進產業資安外溢效果
推動策略
建立以需求導向之資安人才培訓體系
聚焦利基市場橋接國際夥伴
建置產品淬煉場域提供產業進軍國際所需實績
活絡資安投資市場全力拓銷國際
具體措施
1. 打造企業專屬資安人才
2. 建置跨領域人才培訓系統
3. 媒合人才就業
4. 延攬國際人才
5. 設置資安研訓機構
6. 聚焦利基市場創造需求
7. 研發關鍵技術
8. 橋接國際夥伴
9. 發展產業標準
10. 落實產品認證
11. 實驗場域淬煉
12. 政府媒合助攻
13. 研析全球資安市場需求趨勢
14. 協助產業籌獲資金
15. 整合能量協助廠商外拓

策略一：建立以需求導向之資安人才培訓體系

具體措施

一、打造企業專屬資安人才

準確協助個別企業培育人才，立即達成企業及人才雙贏目標

二、建置跨領域人才培訓系統

培訓系統範圍涵蓋從通才到專才、校園到企業、政府到民間
系統內涵包括學習地圖、教材、師資、認證等

三、媒合人才就業

提供資安人才投入市場誘因，含興趣(社群競賽)、媒合機制等

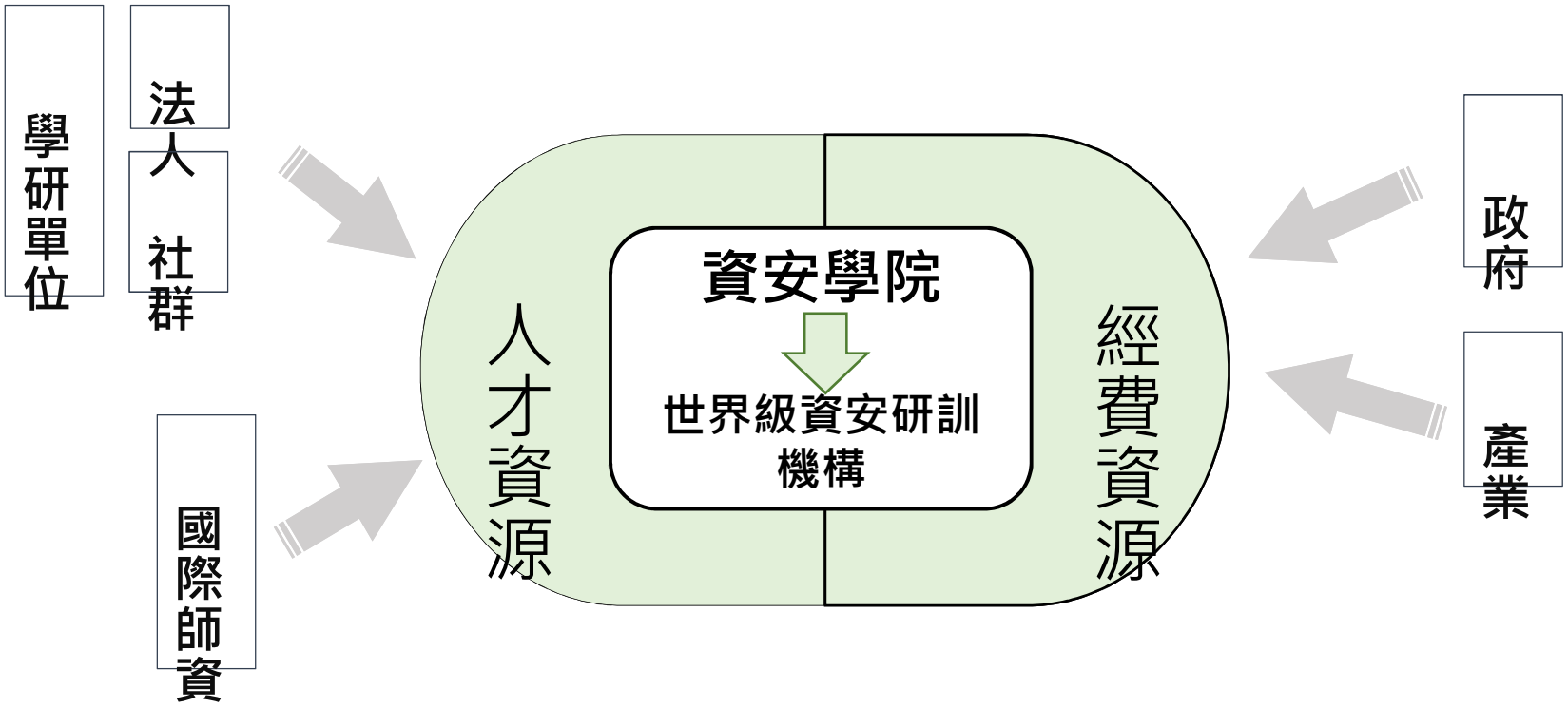
四、延攬國際人才

快速引入國際人才資源並製造產業國際合作機會

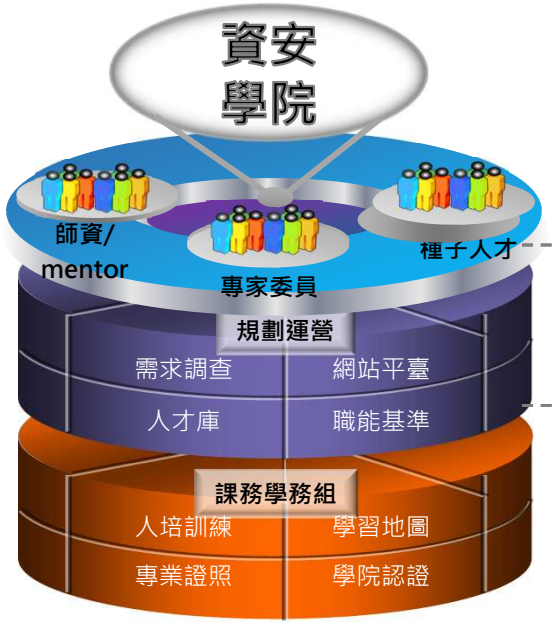
五、設置資安研訓機構

直接促成產官學研人才培育合作，繼而產業攜手並打入國際市場

成立資安學院



學院架構



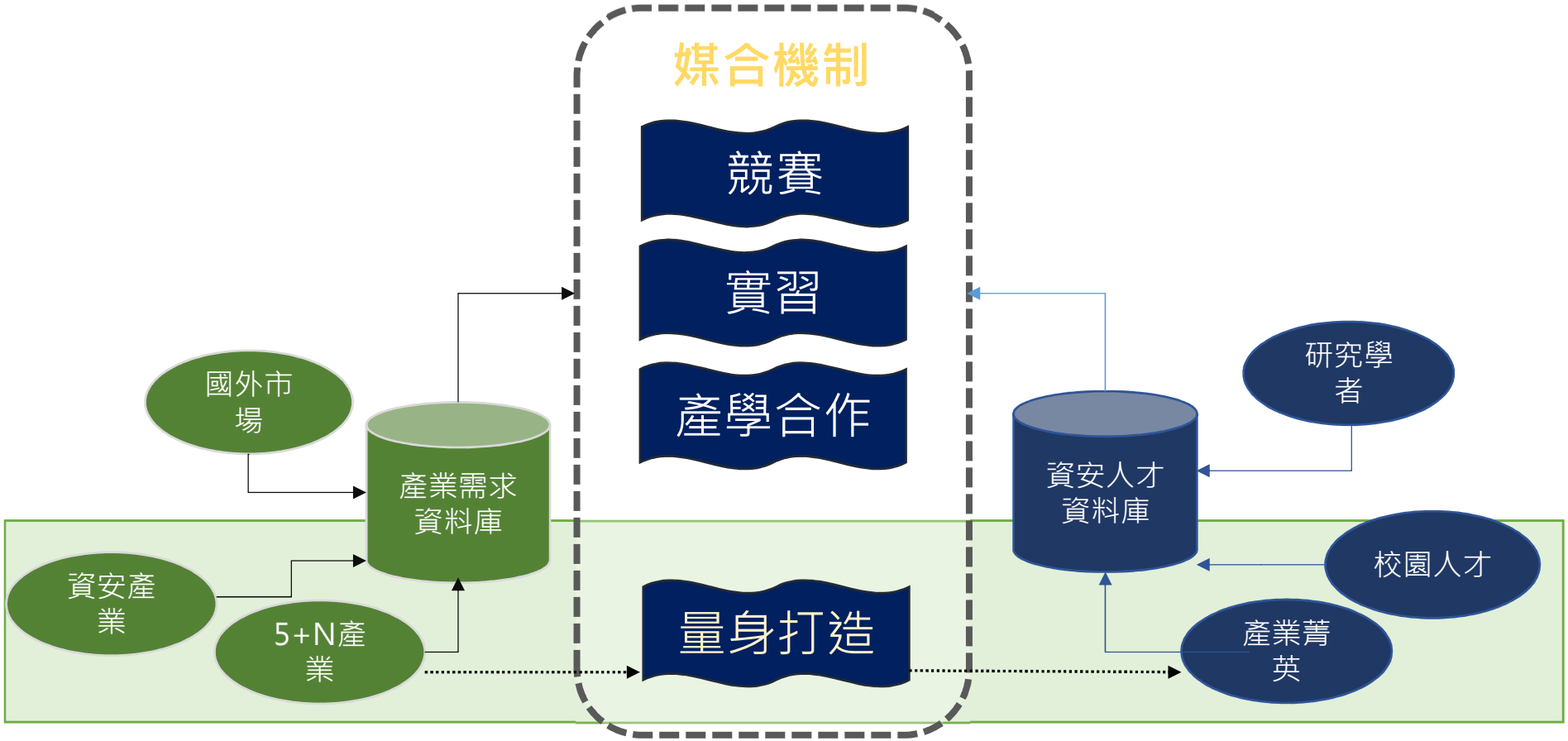
行政能量支援

- 認證機制
- 產業資安調查
- 網站地圖
- 人才資料庫

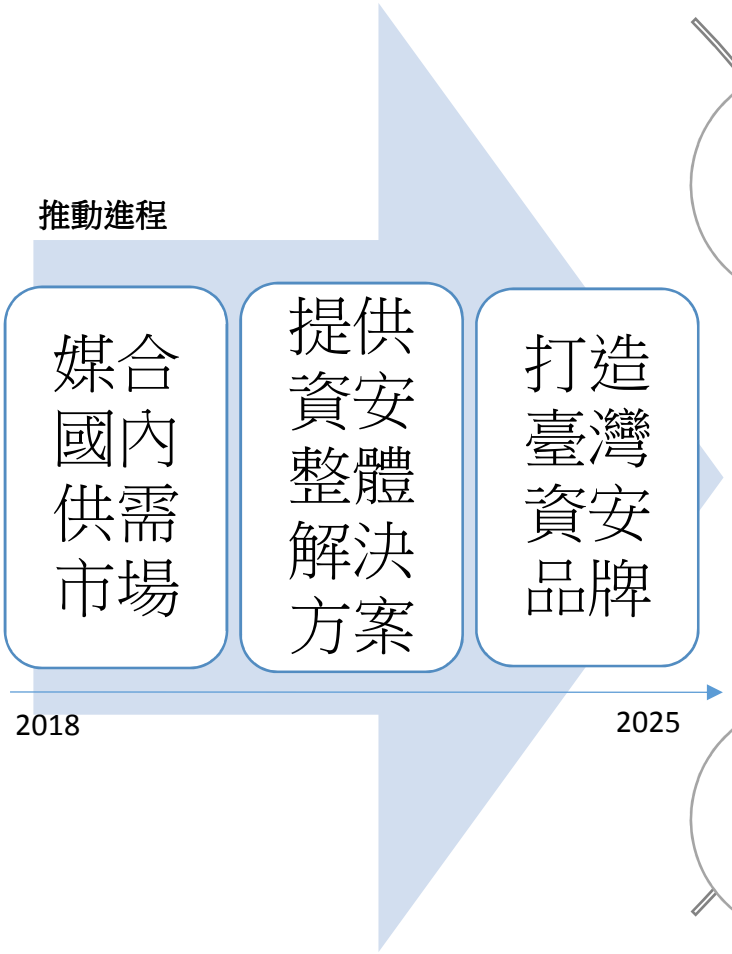
人才培育藍圖

- 資安學習地圖
- 論壇講座
- 國際活動
- 就業媒合

人才媒合機制


媒合機制
競賽
實習
產學合作
量身打造
國外市場
產業需求資料庫
資安產業
5+N產業
資安人才資料庫
研究學者
校園人才
產業菁英

策略二：聚焦利基市場並橋接國際夥伴



具體措施

一、聚焦利基市場 創造需求

結合我國半導體、晶片、資通訊產業優勢，聚焦5+2產業創新(含物聯網)資安需求，促進資安產業與晶片產業的連結引導政府機關、國營企業、關鍵基礎設施等，所採購的資訊資安軟硬體，應採適當措施，提高國內自主率。

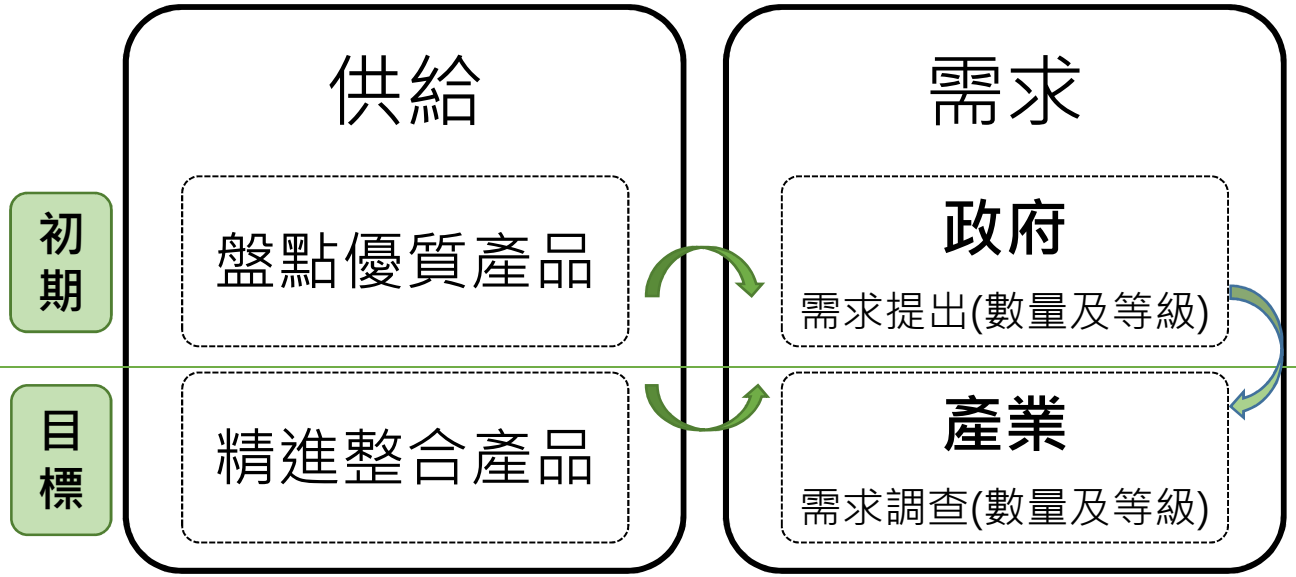
二、研發關鍵技術

引導政府計畫投資前瞻及可產品化之資安相關技術
善用國際級加速器扶植資安新創投入資安技術研發

三、 橋接國際夥伴

引導跨國及跨域合作以提供國內外產業資安市場整體解決方案

媒合國內供需市場



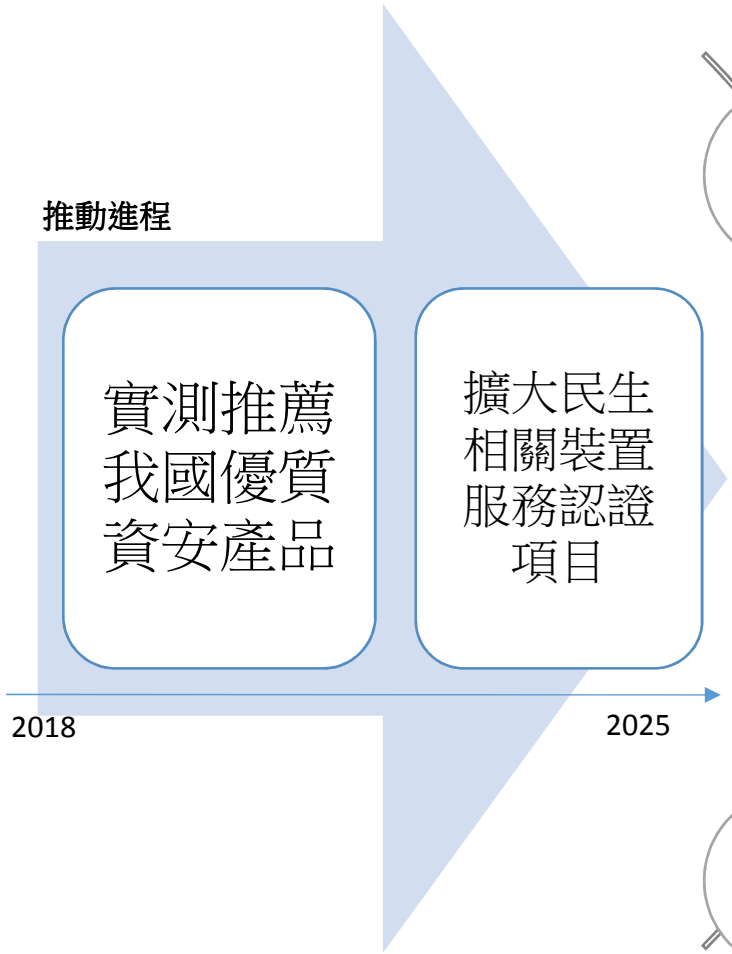
採購案需求說明書訂定**採用自主性產品優先規範**

5+2產業創新、前瞻、旗艦等計畫辦理資通安設備採購案時**80%**招標文件訂定

共同供應契約**資安產品上架數**

每年輔導**15**家廠商產品上架

策略三-建置產品淬煉場域，提供產業進軍國際所需實績



具體措施

一、發展產業標準

導入國際標準並發展國家標準產業規範，推動如物聯網之相關系統、設備、裝置逐步建立分級資安檢測與認證機制

二、落實產品驗證

推動並落實產業標準規範及認證，協助中小企業導入資安管理

三、實驗場域淬煉

逐步建立可持續營運之實驗場域，強化我國產業安全強度

四、政府媒合助攻

透過政策法規製造政府或相關機關使用我國產品機會，以協助我國廠商取得實績，進軍國際

實測推薦我國資安優質產品-淬鍊場域

實驗場域	實驗項目	主責機關
地方及中央機關資通訊建設	資通訊及資安產品	地方及中央機關
關鍵資訊基礎設施	資通訊及資安產品工控系統資安模組	關鍵基礎設施提供者
物聯網(含智慧城鄉)	產品資安模組	地方及中央機關

機制

鼓勵主責機關實測我國優質產品

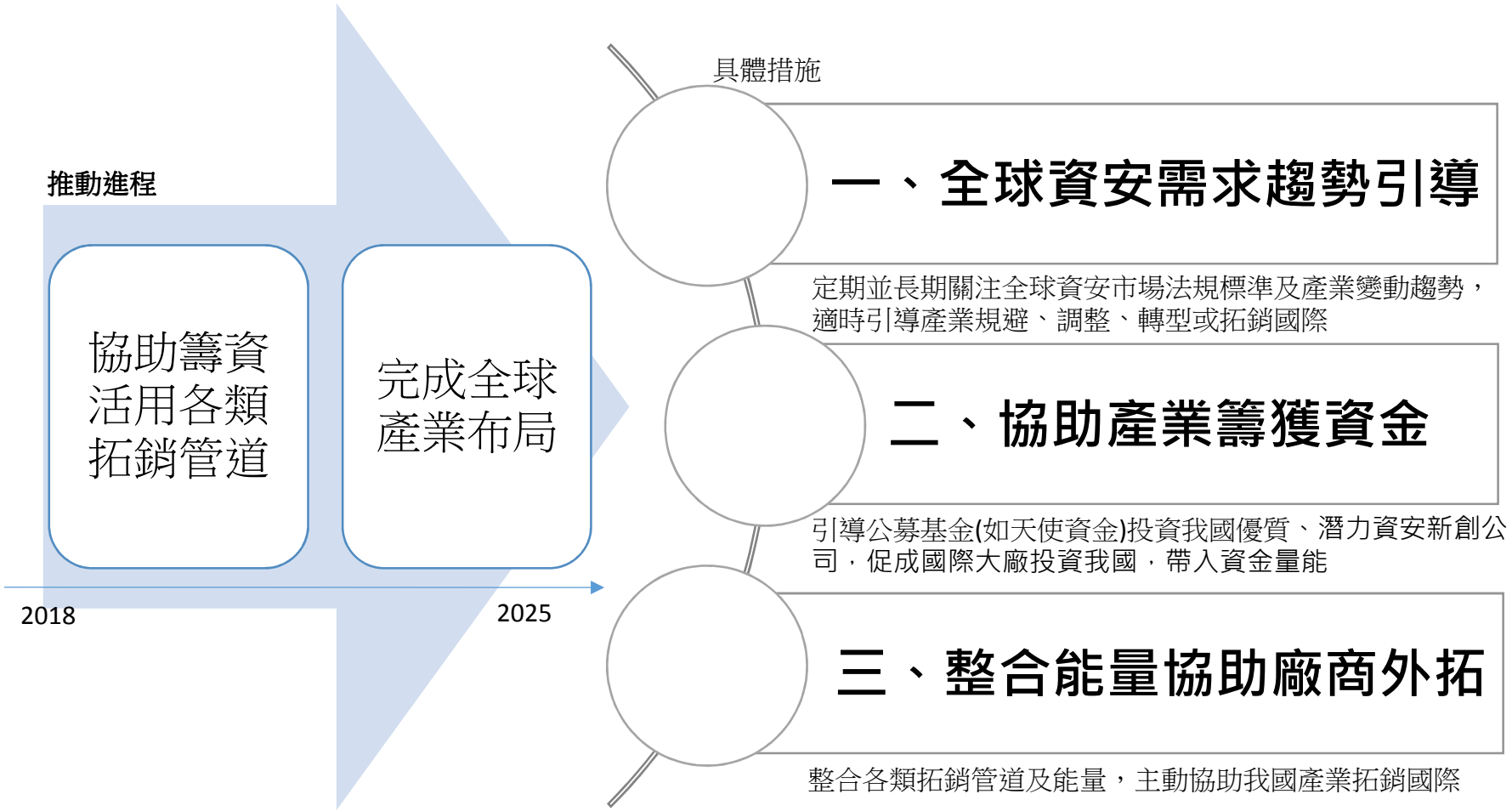
地方、中央機關及關鍵基礎設施提供者
每年各推薦1項我國產品

每年**10**項優質產品

機制

建置可持續性營運之淬鍊場域

策略四-活絡資安投資市場並全力拓銷國際



活用各類拓銷管道

國　際

- 資安國際合作
- 國際產業合作
- 國際角色擔當

國　內

- 技術生根
- 各界交流
- 民眾聚焦
- 凝聚共識

外交體系支援

每年提供10家廠商於海外市場拓展時所需支援

國際拓銷露出

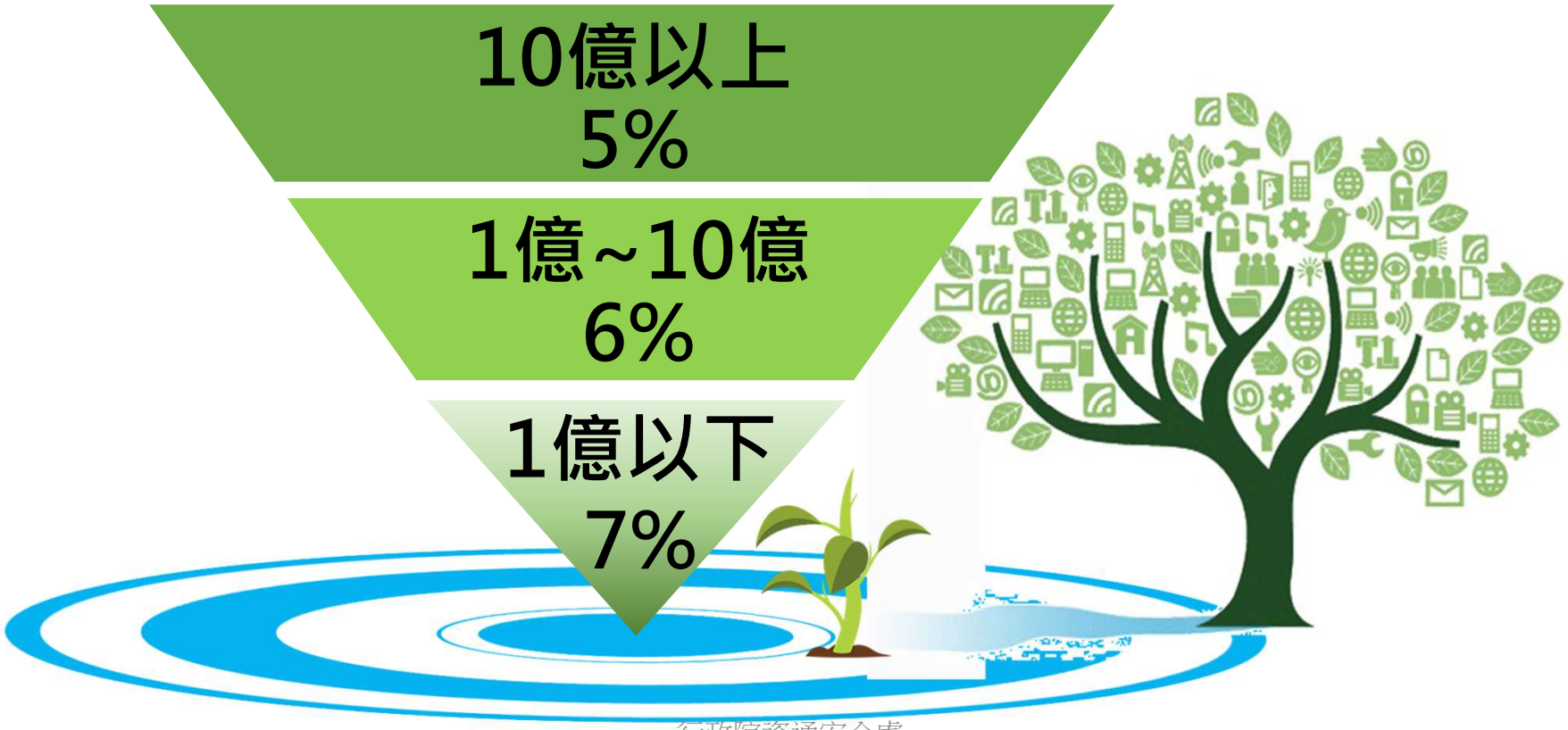
舉辦國際考察團或出國展覽，每年6次以上

國內研討

每年舉辦國內大型研討會2次

投入經費

- 106~109年透過資安旗艦計畫、前瞻基礎建設計畫(數位建設)等投入資安經費約110億元。
- 後續將協調5+2產業創新及政府各相關計畫，依經費規模級距，訂定相對應之資安經費投入比例。



資安是持續精進的風險管理