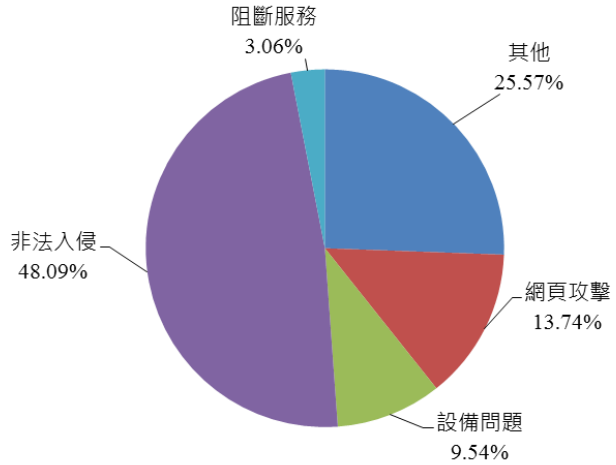
資通安全管理法
資安事件通報機制

行政院資通安全處
howard@ey.gov.tw
108年10月8日

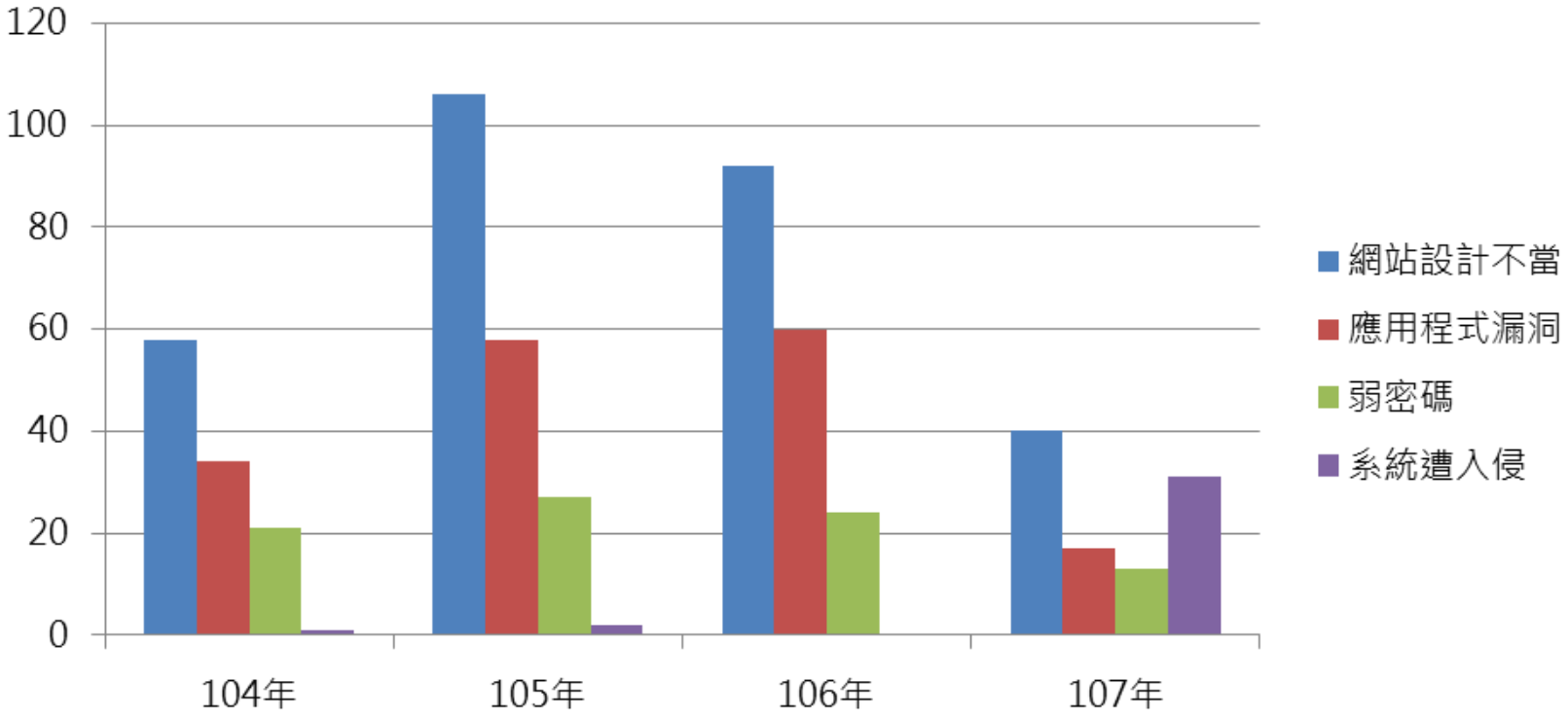
107年政府機關資安事件通報統計

- 107年共接獲262件資安事件通報，其中44.27%(116件)為政府機關接獲資安警訊通告後所進行之通報案件，55.73%(146件)為政府機關主動偵測發現之通報案件
- 通報之資安事件等級
  - 4級事件：0件
  - 3級事件：6件
  - 2級事件：43件
  - 1級事件：213件



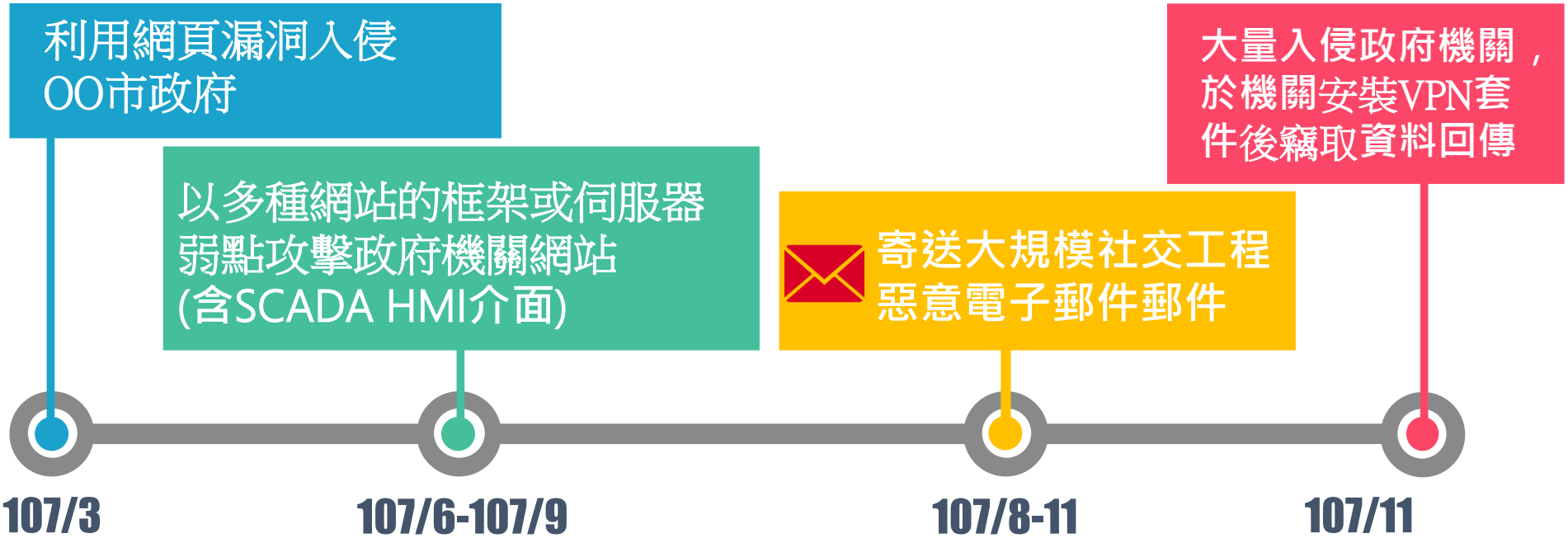
- 歸納通報3級事件類型
  - 機敏資料外洩(如OO市政府衛生局民眾個資外洩等)
  - 核心業務系統或資料遭嚴重竄改(如OO院資訊設備遭植入勒索病毒等)
  - 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作(如OO公司主機異常，導致ATM跨行業務無法正常運作等)

政府機關資安事件主要發生原因



資安事件關聯綜覽

- 經分析發現，近期社交工程電子郵件攻擊與107年其他資安事件關聯，近期駭客改以透過VPN竊取機關資料



攻擊流程

01

公開資訊蒐集

利用政府電子採購網、台灣採購公報網查詢委外系統建置案，鎖定外包商為第一階段攻擊目標

02

弱點偵查掃描

針對特定、影響範圍廣的作業系統或網頁套件弱點，如MS-17010、S2-045等，利用工具進行掃描，鎖定未更新的主機進行攻擊

03

網頁後門植入

利用漏洞將網頁型後門植入受害主機中，建立控制端與受害端之間的連線，繞過防護機制，存取受害主機上的服務

04

內部橫向控制

以該受害主機為基礎，掃描內部其他主機弱點，嘗試取得主機帳密，橫向控制其他內部主機

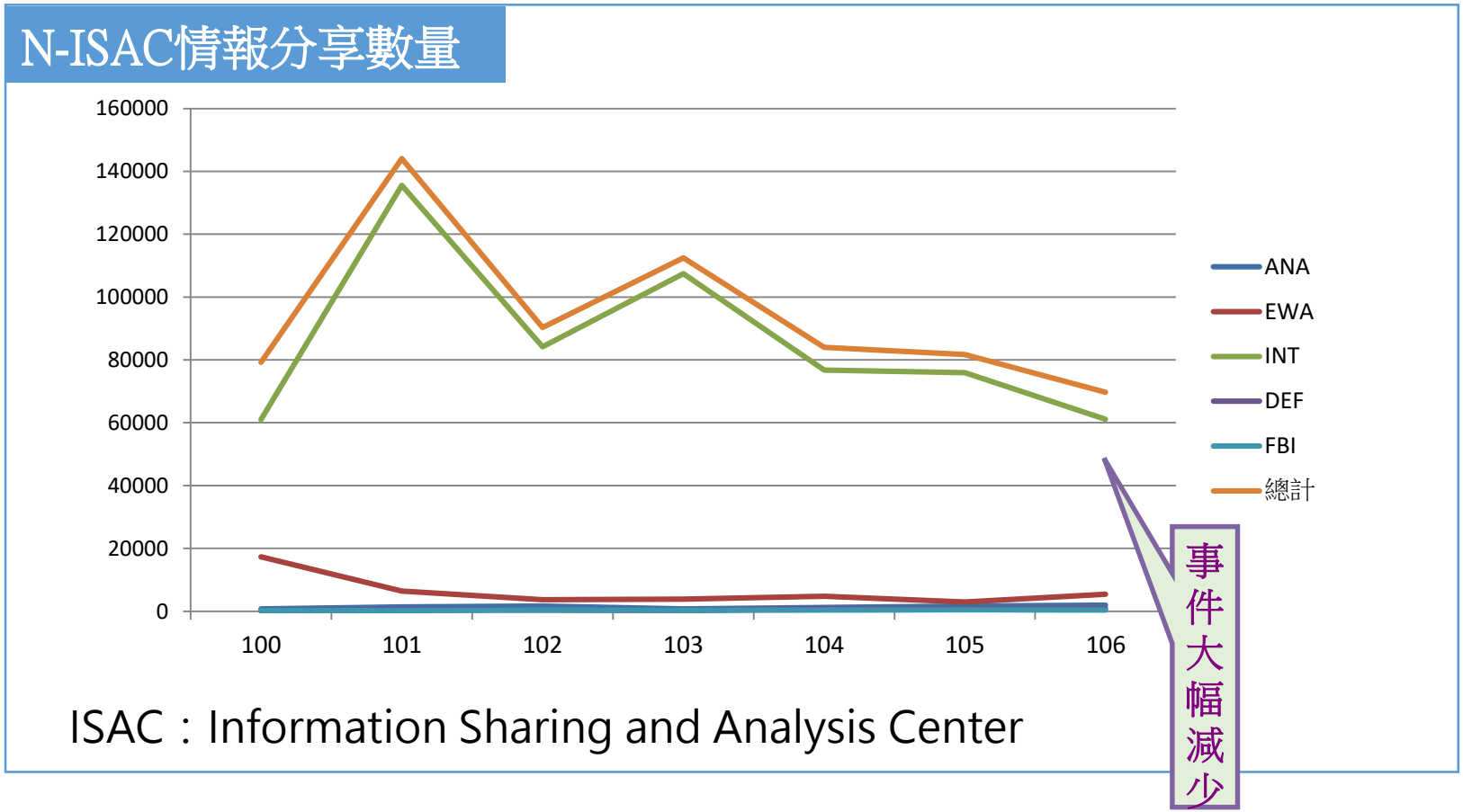
05

外部擴散攻擊

將該受害主機做為跳板，掃描外部單位弱點，植入網頁後門餅登入存取其他外部受害主機

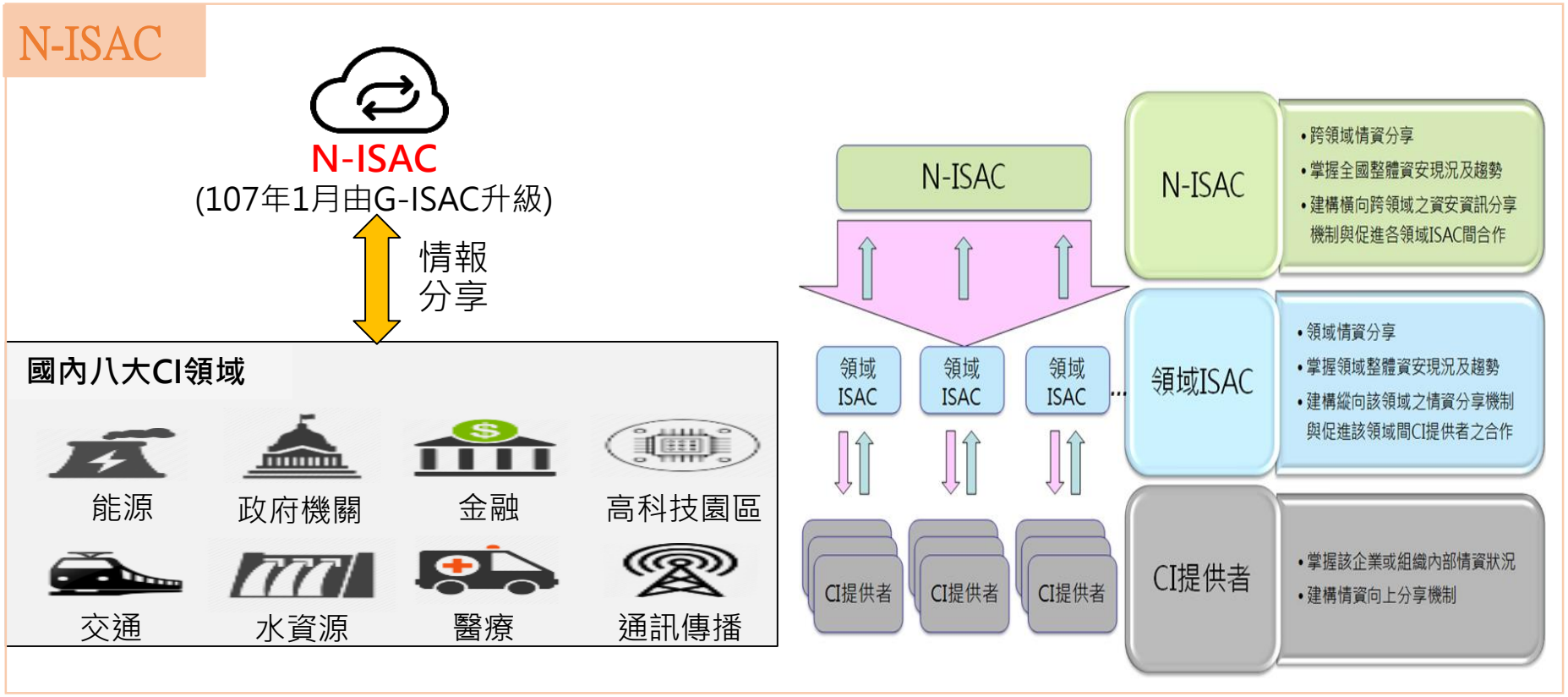
情資分享(1/2)

- 透過**資安資訊分享與交流**，彙整**資安訊息情報**與**跨組織情資**分享，以掌握資安威脅現況，降低資安事件可能造成損害



情資分享(2/2)

- 鑒於國內外資安情資來源漸趨多元，跨領域情資日益增加，需建立更有效之**國家層級的N-ISAC**(National ISAC)運作機制，打造**資安情資聯防網路**



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

資安法施行後之變革


適用範圍面
納管對象擴大
特定非公務
機關
管理面
維護計畫、
專職(責)人力
技術面
明定應辦
事項及控制
措施
政策及整合面
明定資通
安全推動事項
及情資分享
規範面
資安管理
規定位階提
升為法令
資安法

資通安全管理法摘要

- 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
- 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
- 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

- 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

- 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

公務機關之資通安全管理

✓ 應訂定、修正及實施資通安全維護計畫§10
✓ 應訂定通報及應變機制§14 I

行政院

- 擘劃並推動國家資通安全政策
- 資通安全科技發展
- 國際交流合作及資通安全整體防護
- 定期公布國家資安情勢報告及資通安全發展方案

訂定

- 應提出年度資通安全維護計畫之實施情形§12
- 應提出改善報告§13 II
- 應通報資通安全事件§14 II
- 應提出資通安全事件之調查、處理及改善報告§14 III

上級或監督機關 ⇄ 下級或受監督機關

- 應稽核資通安全維護計畫實施情形§13 I

總統府、立法院、司法院、考試院、監察院、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會

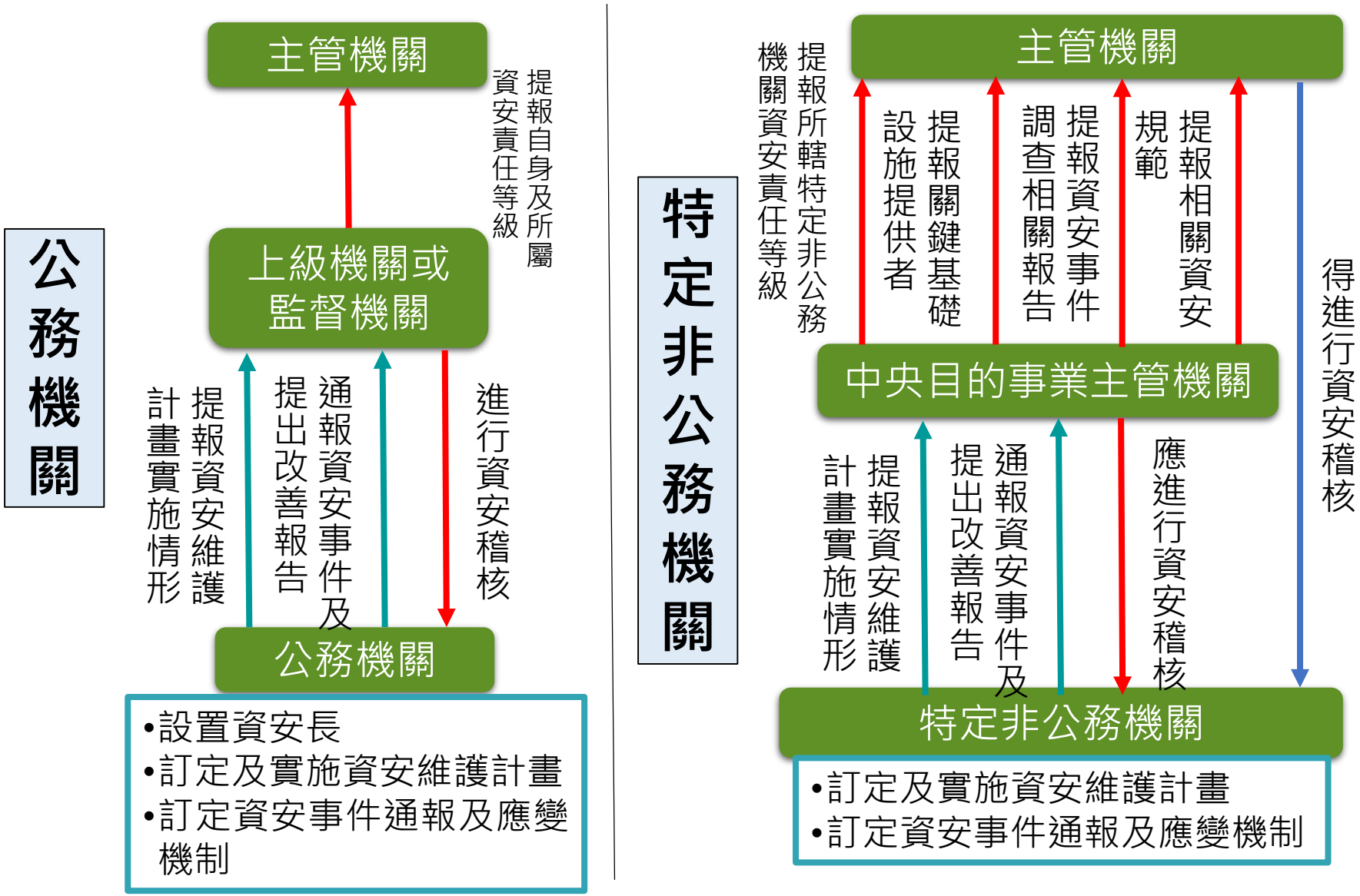
設置資通安全長§11

- ✓資安管理法施行細則§22
- ✓資安責任等級分級辦法§7
- ✓資安事件通報及應變辦法§14、18
- ✓維護計畫實施情形稽核辦法§7、13
- ✓資安情資分享辦法§8
- ✓公務人員獎懲標準§15、§19

特定非公務機關之資通安全管理

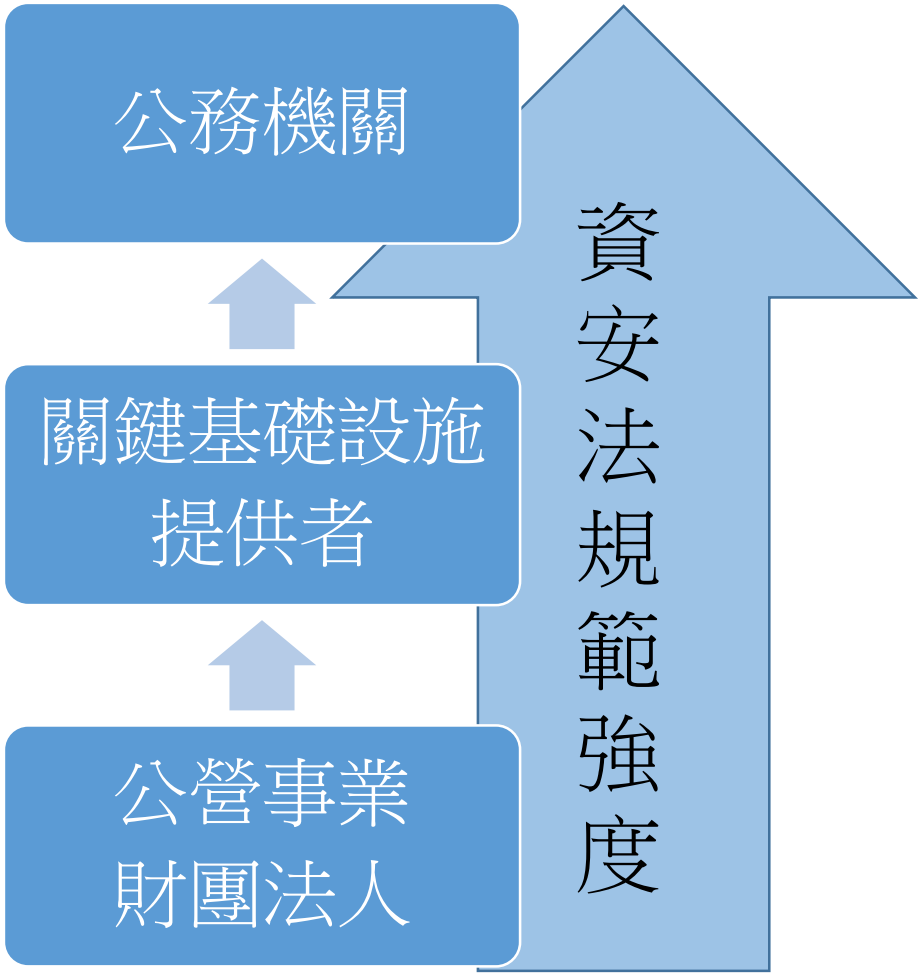
	關鍵基礎設施提供者	公營事業、政府捐助之財團法人
資通安全維護計畫	①應訂定、修正及實施資通安全維護計畫§16 ②應提出資通安全維護計畫之實施情形§16 ③應提出資通安全維護計畫之改善報告§16	①應訂定、修正及實施資通安全維護計畫§17 ②得提出資通安全維護計畫之實施情形§17 ③應提出資通安全維護計畫之改善報告§17
通報應變	④應訂定通報及應變機制§18 ⑤應通報資安事件，並提出調查、處理及改善報告§18	
罰則 §20~§21		

各機關間之角色與權責

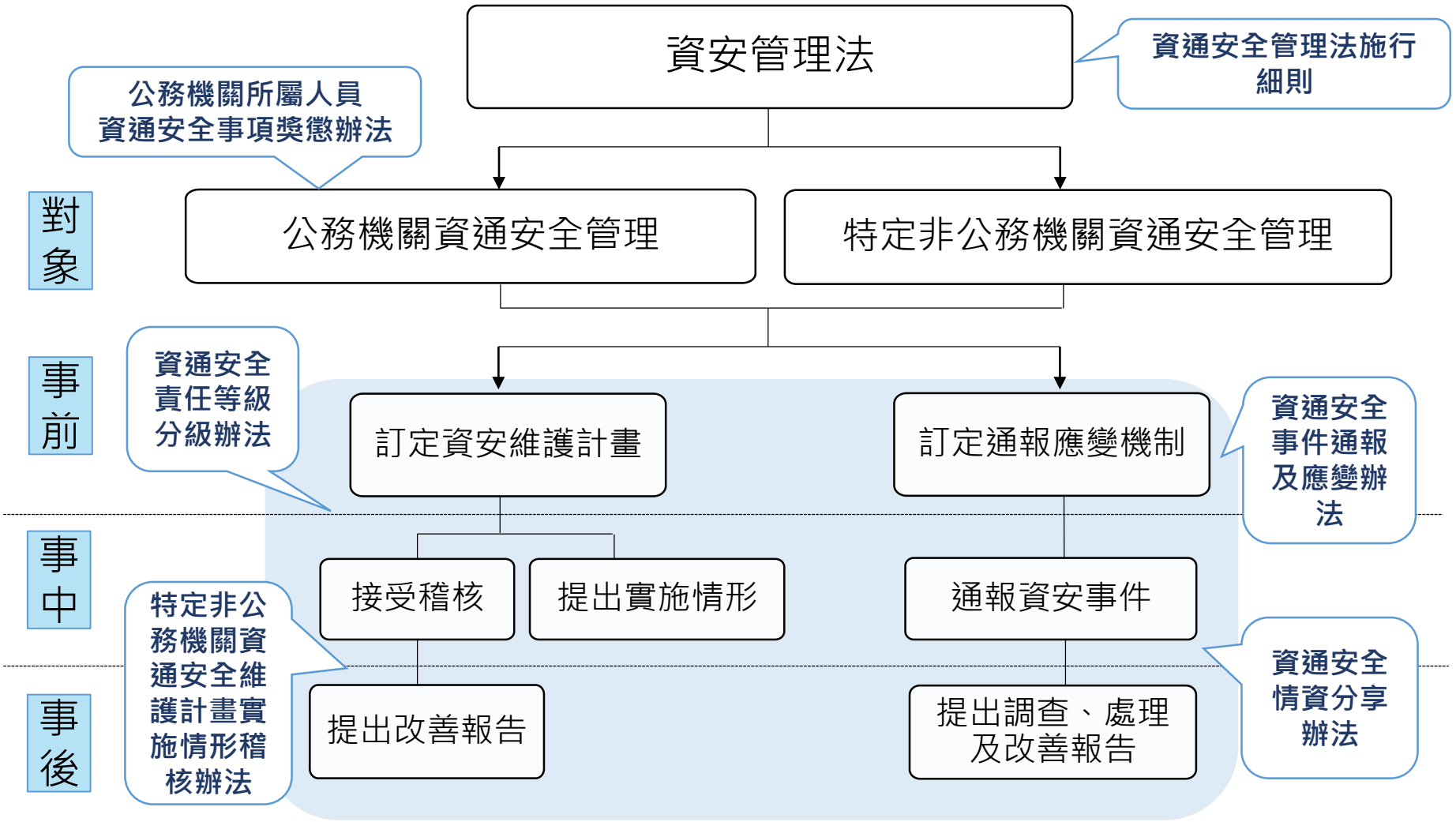

公務機關
主管機關
提報自身及所屬資安責任等級
上級機關或監督機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
進行資安稽核
公務機關
•設置資安長
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制
特定非公務機關
主管機關
提報所轄特定非公務機關資安責任等級
提報關鍵基礎設施提供者
提報資安事件調查相關報告
提報相關資安規範
得進行資安稽核
中央目的事業主管機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
應進行資安稽核
特定非公務機關
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制

本法規範適用先後

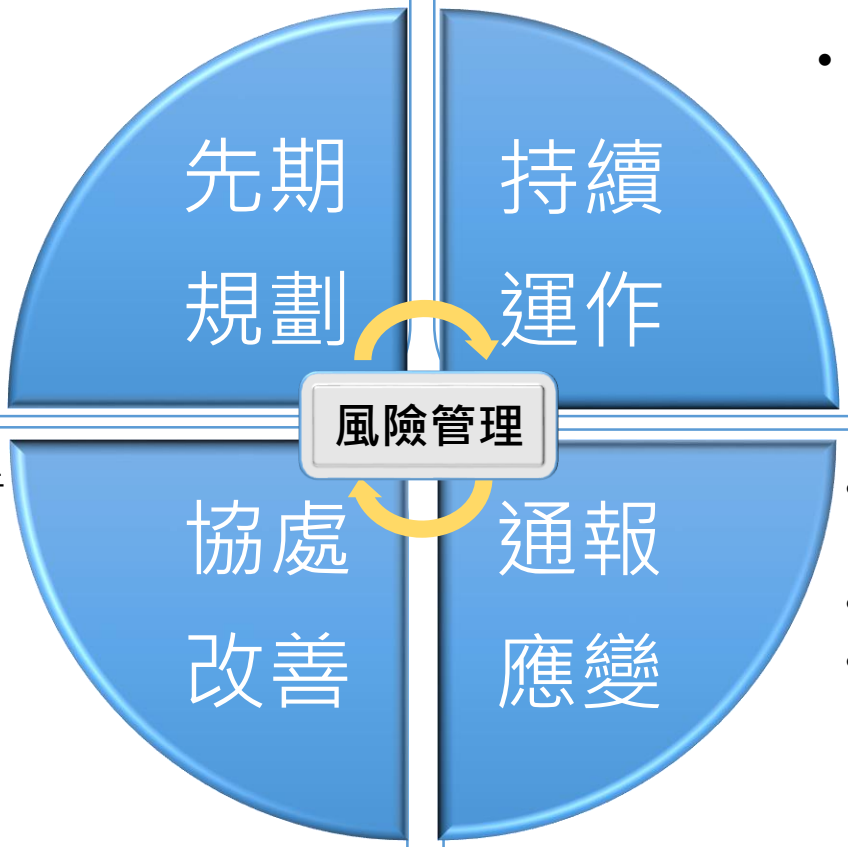
- 同時是公務機關及CI提供者
  - 優先適用公務機關之規定
- 同時是公營事業/財團法人及CI提供者
  - 優先適用CI提供者之規定



資安管理架構


資安管理法
資通安全管理法施行細則
公務機關所屬人員資通安全事項獎懲辦法
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
資通安全責任等級分級辦法
訂定資安維護計畫
訂定通報應變機制
資通安全事件通報及應變辦法
事中
接受稽核
提出實施情形
通報資安事件
特定非公務機關資通安全維護計畫實施情形稽核辦法
事後
提出改善報告
提出調查、處理及改善報告
資通安全情資分享辦法

資安管理子法架構



- 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

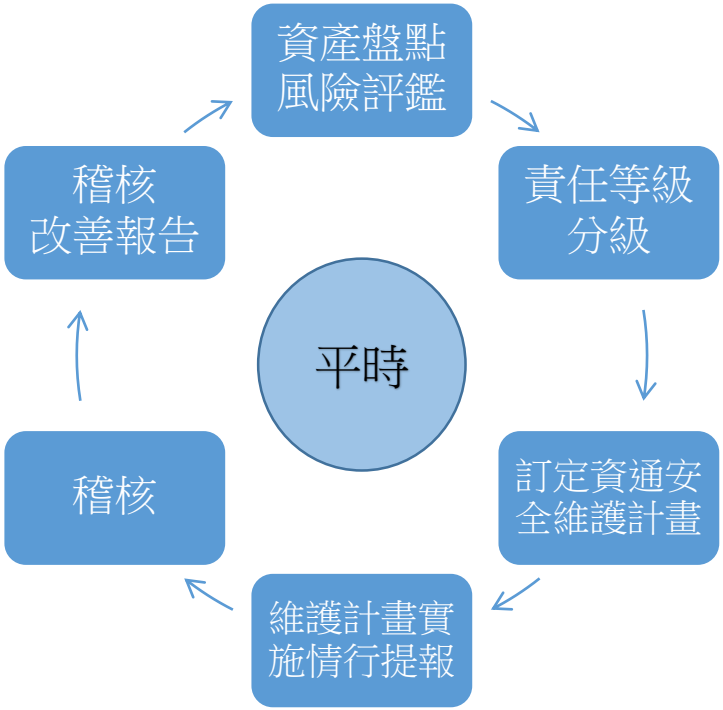
公務機關所屬人員資通安全事項獎懲辦法

- 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

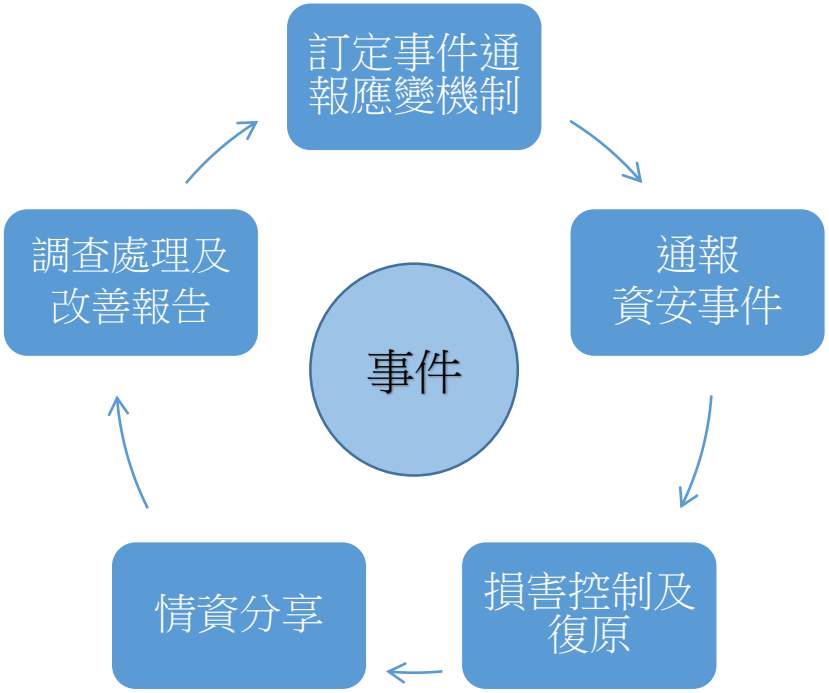
資通安全事件通報及應變辦法

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

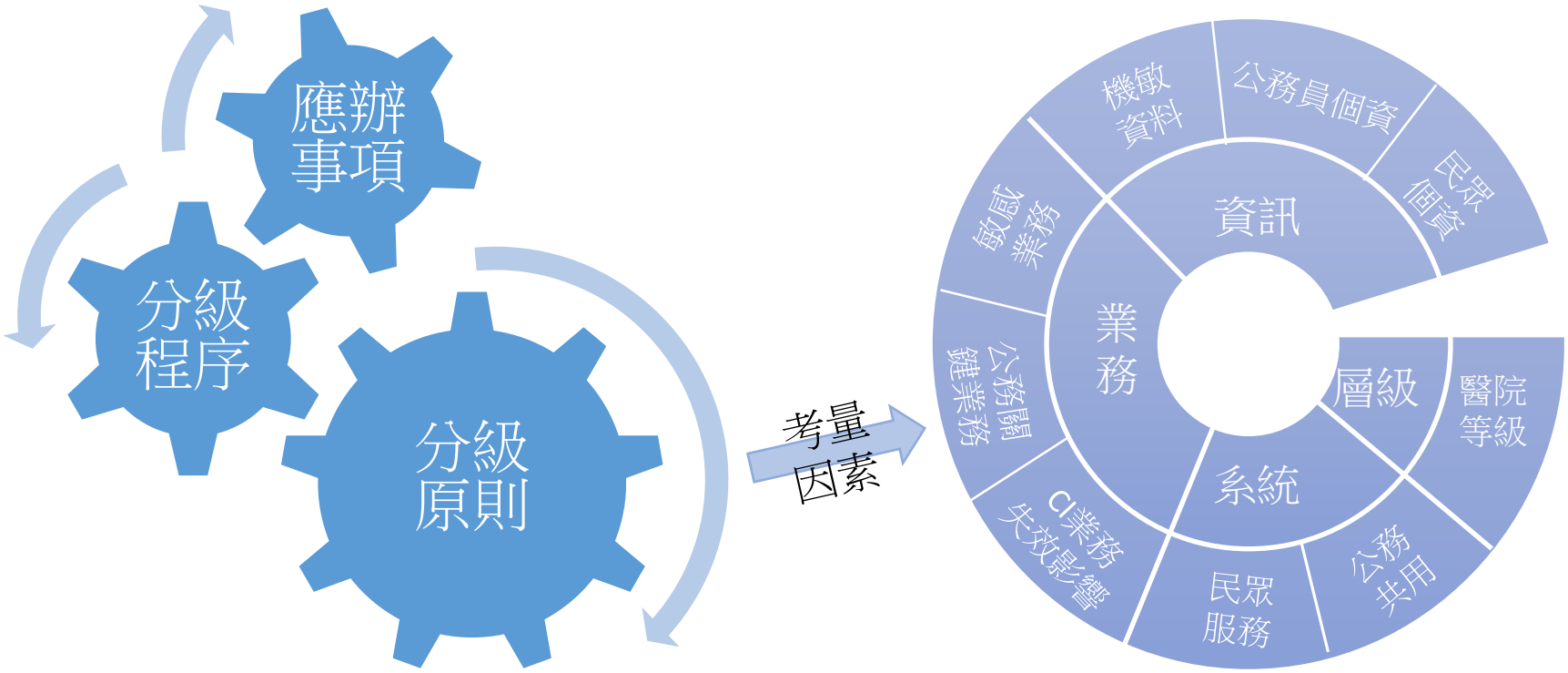
資通安全情資分享辦法

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

資通安全責任等級分級辦法

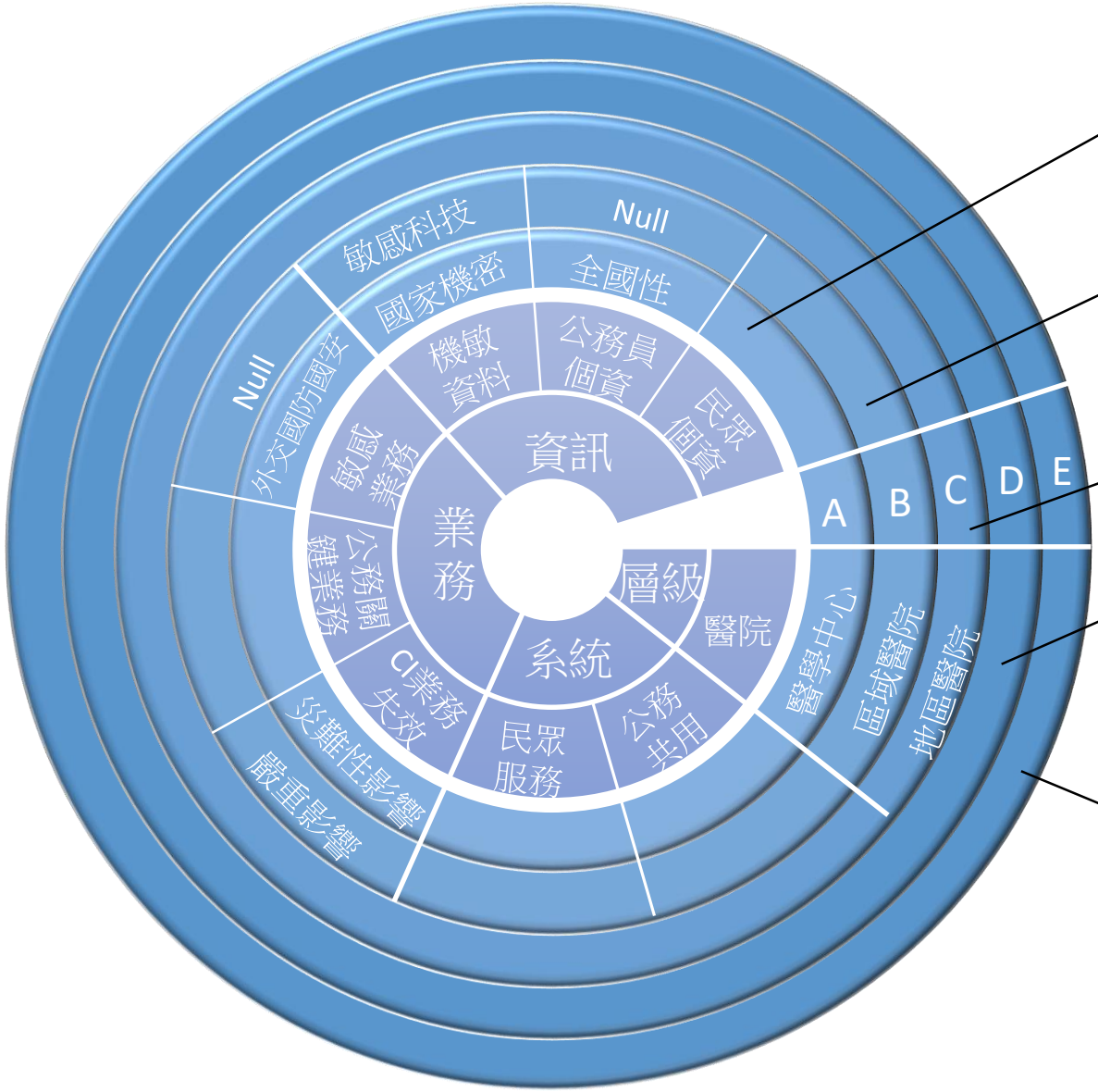
- 機關應考量其業務、資訊、系統、機關層級等因素訂定機關資安責任等級。
- 後續依該責任等級辦理相對應之應辦事項



資通安全責任等級分級辦法

- **法令遵循義務重點**
  - 各機關應提報或核定責任等級（第3條）
  - 各機關應依附表規定辦理其資通安全責任等級應辦事項。（第11條）
    - 附表1至附表8：各等級機關應辦事項
    - 附表9：資通系統防護需求分級原則
    - 附表10：資通系統防護基準

資通安全責任等級分級原則



A級:全國性

B級：區域或地區性

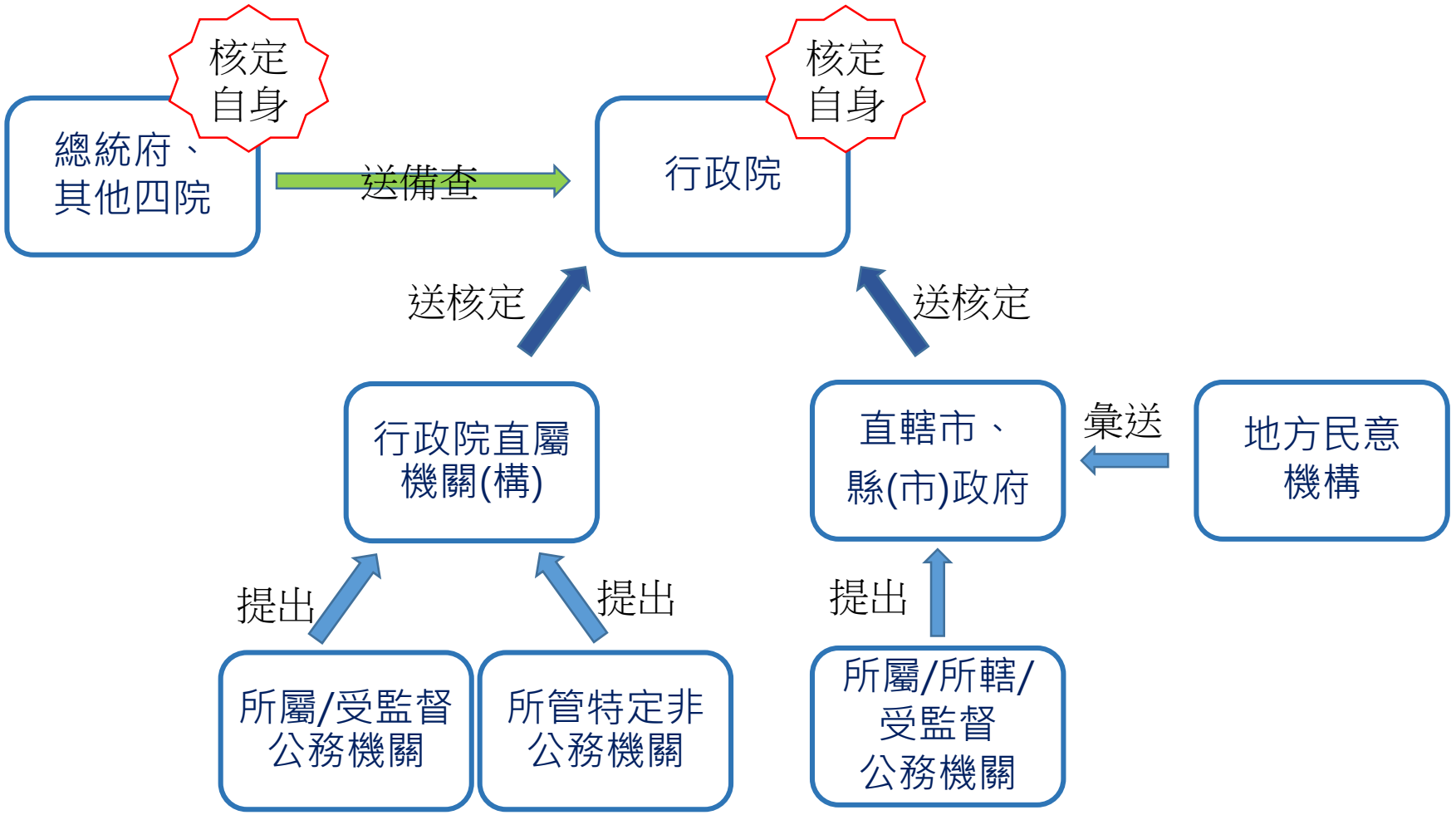
C級：有自行或委外發資訊系統，並設置伺服器者

D級：未自行或委外開發資訊系統，未設置伺服器

E級：全部資訊業務由其他機關兼辦或代辦

§10：各機關得考慮其對國家安全、社會公益或人民之影響，彈性調整其等級

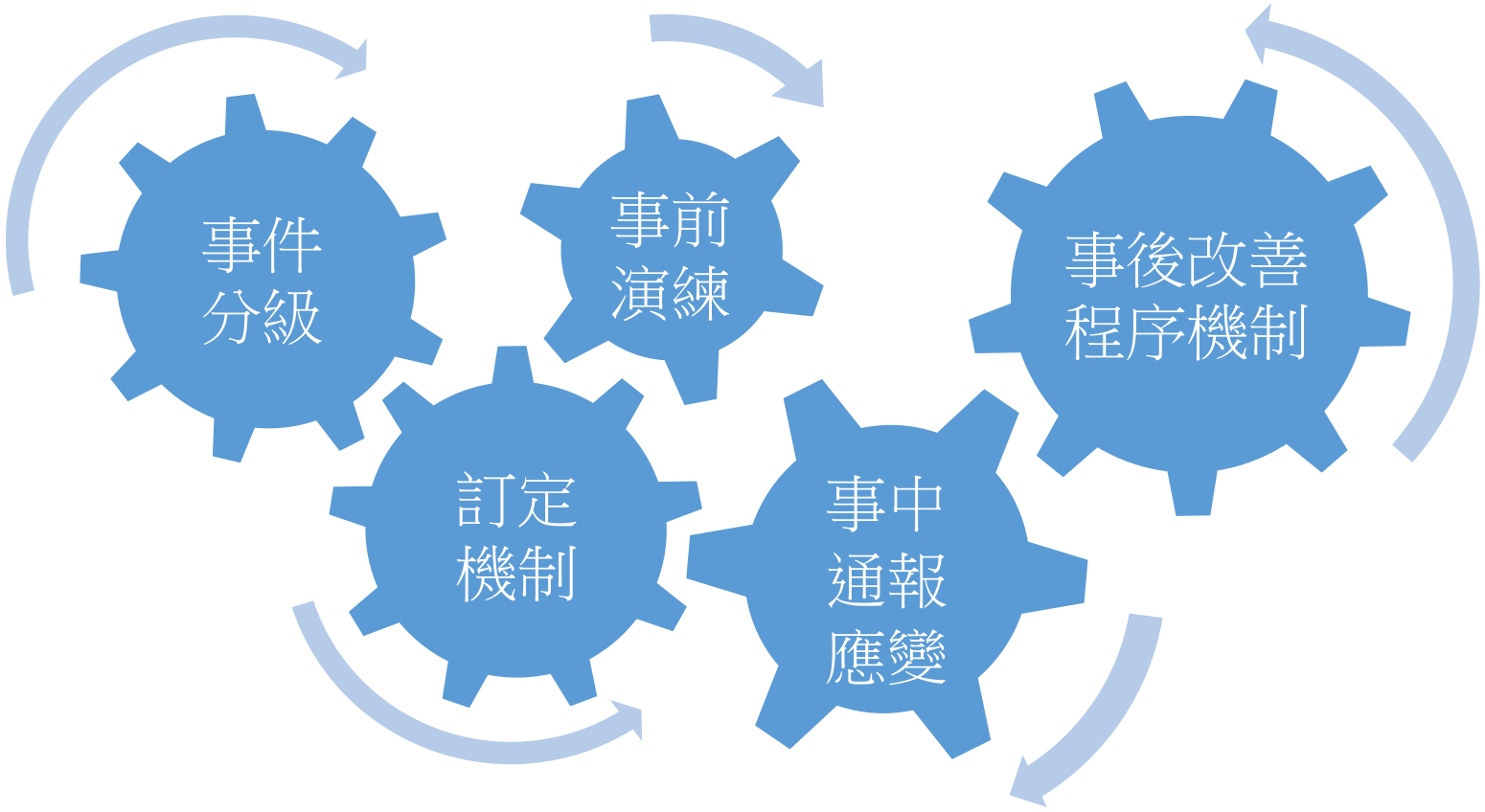
資通安全責任等級分級程序



一般機關：每2年核定一次
新設或職務調整機關：立即辦理等級辦更

資通安全事件通報及應變辦法

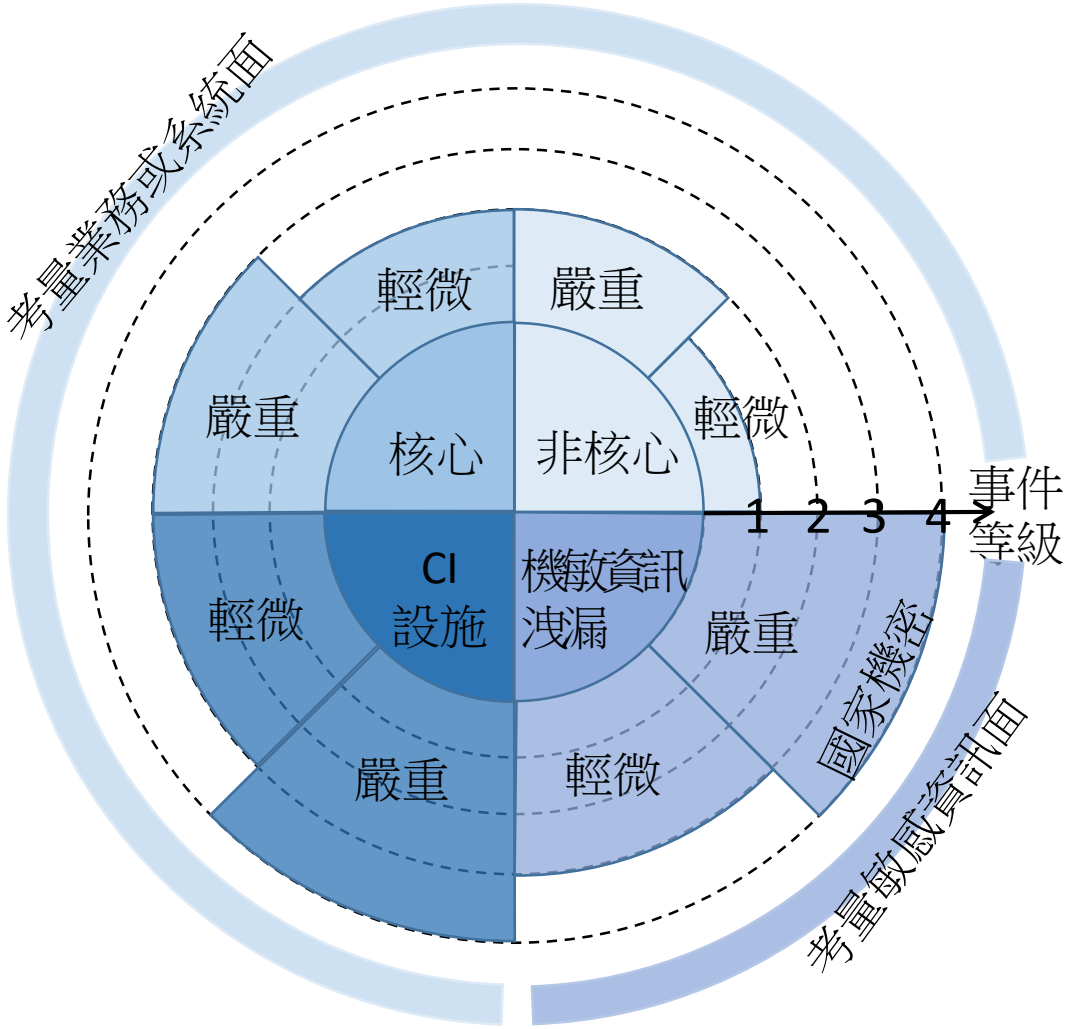
- 為強化各機關之資安事件之因應。
- 規範事件之分級、事前演練、事中通報及應變，以及事後改善之程序、機制。



資通安全事件通報及應變辦法

- **法令遵循義務重點**
  - 資通安全事件之通報方式、時限及程序（第4條、第11條）
  - 資通安全事件等級之審核、時限及程序（第5條、第12條）
  - 資通安全事件之應變方式、時限及程序（第6條、第13條）
  - 機關應就資通安全事件之通報與應變訂定作業規範及其應包括事項（第9、10條、第18、19條）
  - 公務機關資通安全演練作業之規劃、辦理 及其內容（第8條）

資通安全事件分級

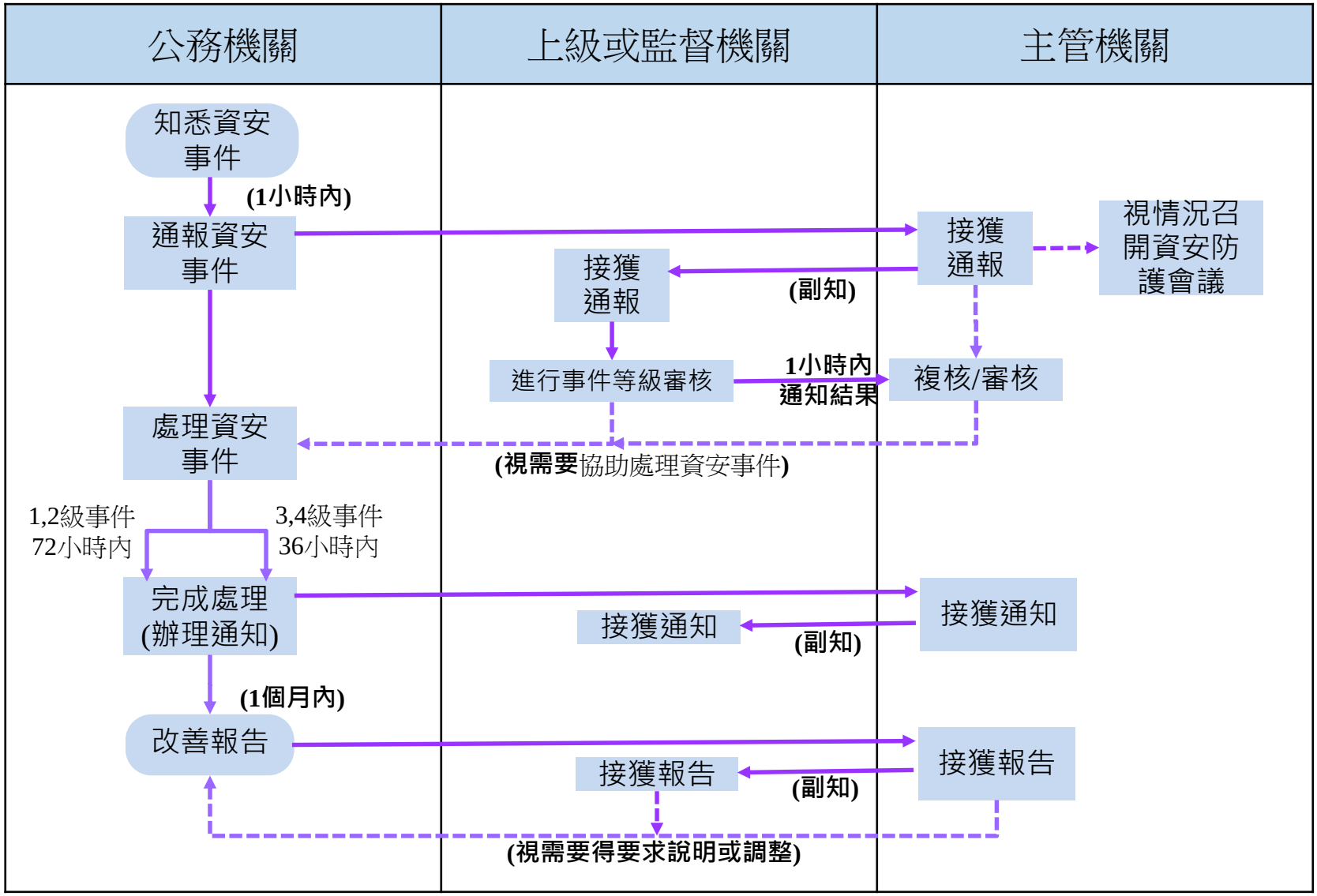


事件輕微或嚴重-考慮C,I,A三面向

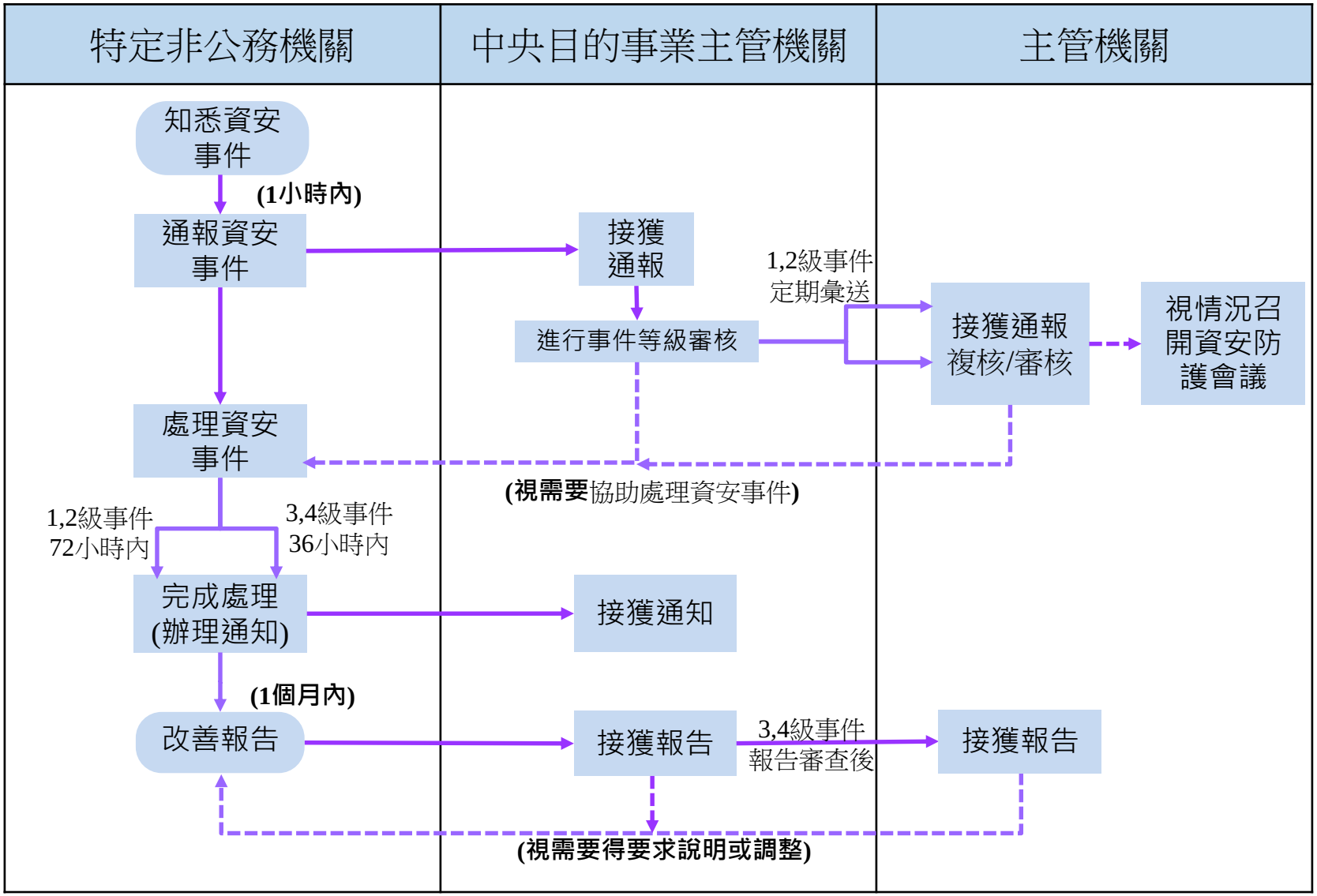
- 機密性
  - 業務資訊遭洩漏
- 完整性
  - 業務資訊遭竄改
  - 資通系統遭竄改
- 可用性
  - 資訊系統受影響或停頓，是否於可接受時間內回復

同一資安事件影響二個以上機關，等級向上提升一級

事件通報流程-公務機關

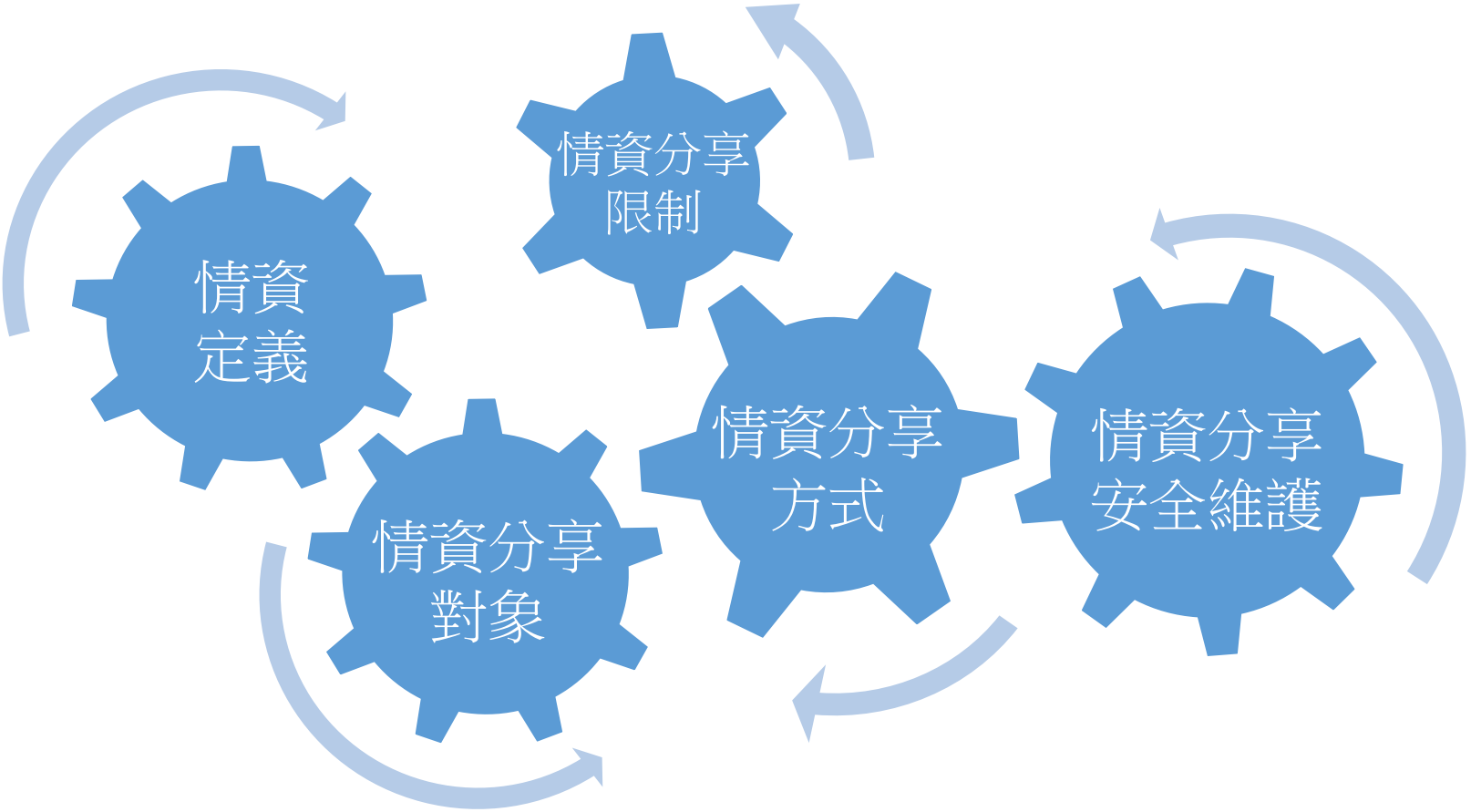

公務機關
上級或監督機關
主管機關
知悉資安事件
(1小時內)
通報資安事件
接獲通報
(副知)
接獲通報
視情況召開資安防護會議
進行事件等級審核
1小時內通知結果
複核/審核
處理資安事件
(視需要協助處理資安事件)
1,2級事件 72小時內
3,4級事件 36小時內
完成處理(辦理通知)
接獲通知
(副知)
接獲通知
(1個月內)
改善報告
接獲報告
(副知)
接獲報告
(視需要得要求說明或調整)

事件通報流程-特定非公務機關



資通安全情資分享辦法

- 提升各機關對於資安之預警能力，強化資安相關資訊之交流。



資通安全情資分享辦法

- **法令遵循義務重點**
  - 進行資通安全情資分享之對象及義務（第3條）
  - 分享及接收資通安全情資之注意事項及安全維護之規定。（第5條及第8條）
  - 資通安全情資分析及整合之規定。(第6條及第7條)

情資分享之內容

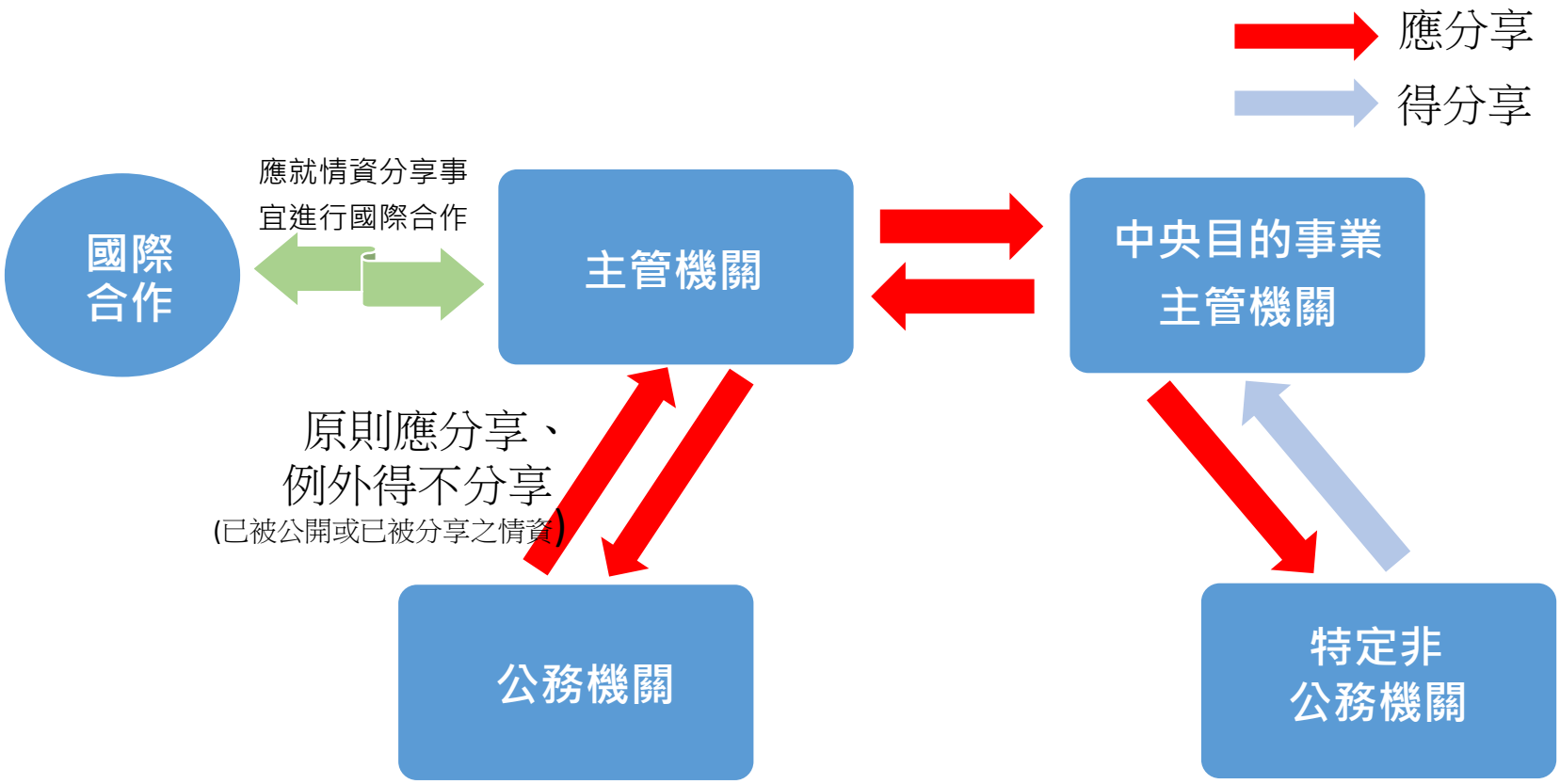
情資定義

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

情資分享之對象



非本法納管對象(§8)；得經主管機關或中央目的事業主管機關同意後，與其進行情資分享

資安是持續精進的風險管理