資通安全法與子法

行政院資通安全處
howard@ey.gov.tw
107年10月3日

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

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

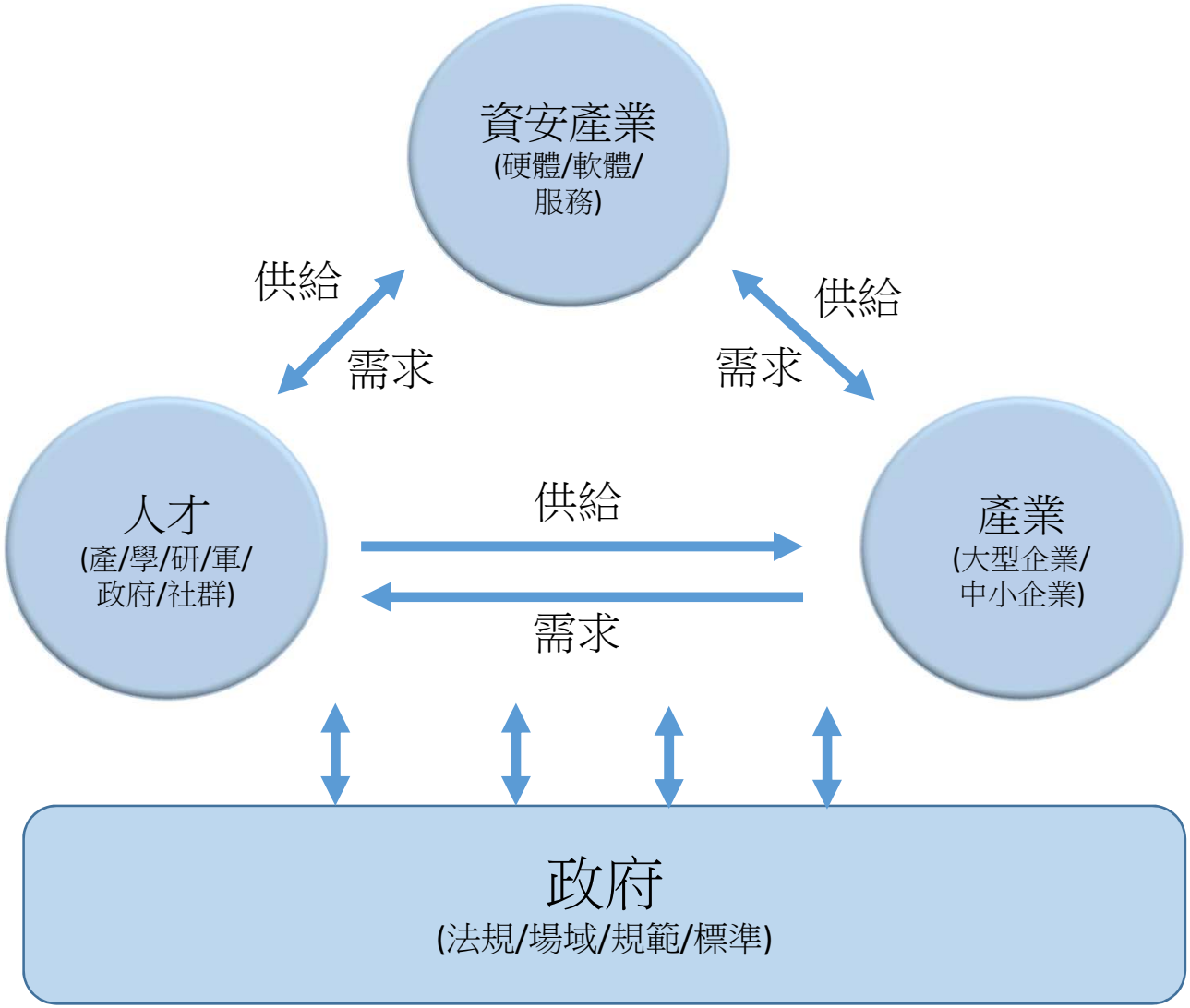
作者 藍 弋丰 | 發布日期 2016 年 04 月 26 日 15:13 | 分類 能源科技, 資訊安全 Follow G+ 讚 86 分享

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+

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)

資通安全管理法

立法歷程

106/4 本院完成審查並將法案函送立法院審查

106/5 於立法院第九屆第三會期完成一讀程序並交付司法及法制委員會審查

107/3-5 研擬子法草案並召開分區座談會

107.5.11 立法院第九屆第五會期二、三讀通過立法

107.6.6 總統令公布

107.7.9 子法進行預告

107/7-8 決定施行日期

D day 正式施行

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

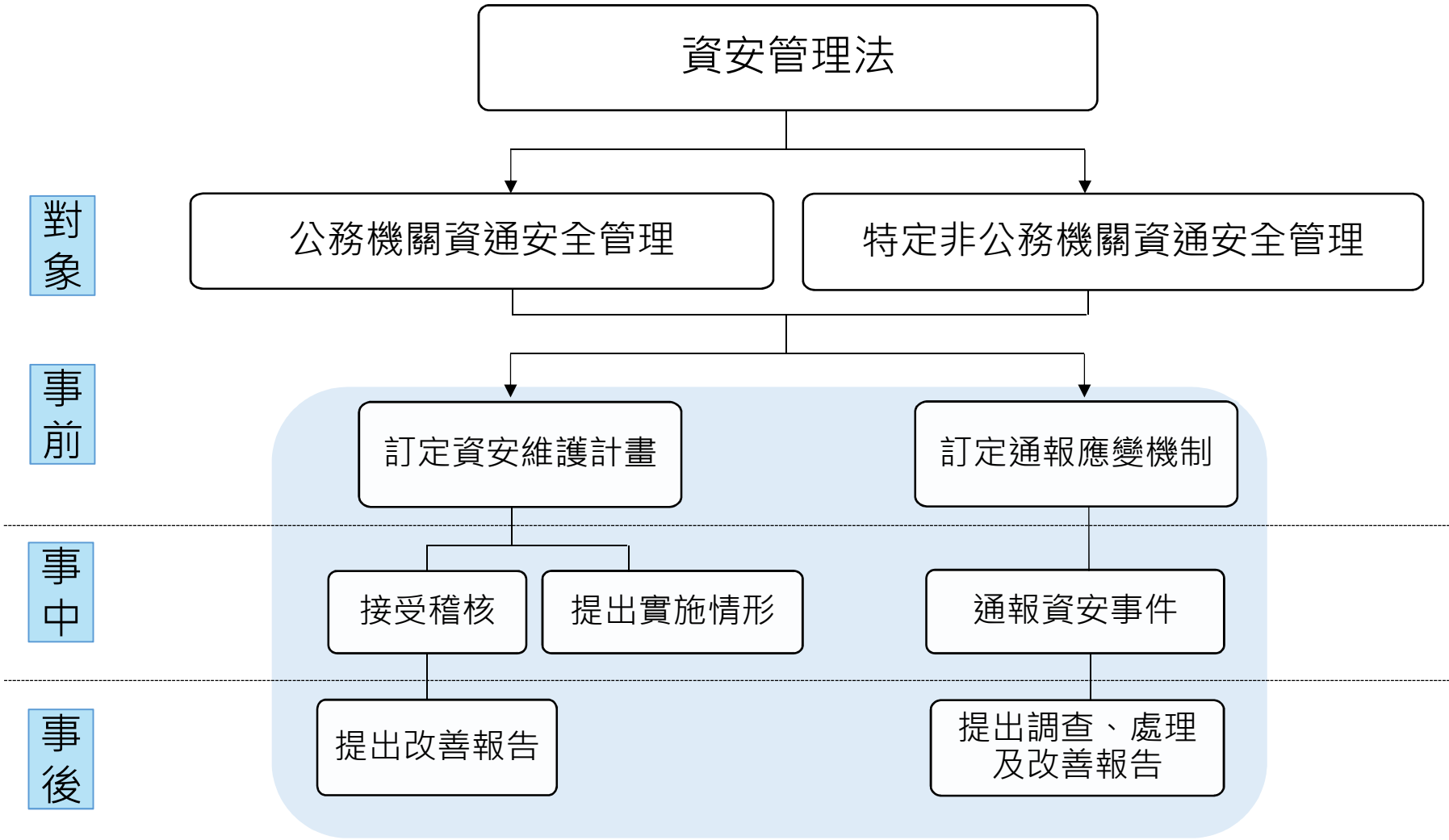
- 資安責任等級分級
- 資安維護計畫之制定與實施
- 資安長設置
- 年度資安維護計畫實施情形提出
- 資安稽核
- 改善報告
- 資安事件通報應變
- 公務機關人員獎懲標準

- 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

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

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

- 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§14II
- 應提出資通安全事件之調查、處理及改善報告§14III

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

- 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

- ✓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

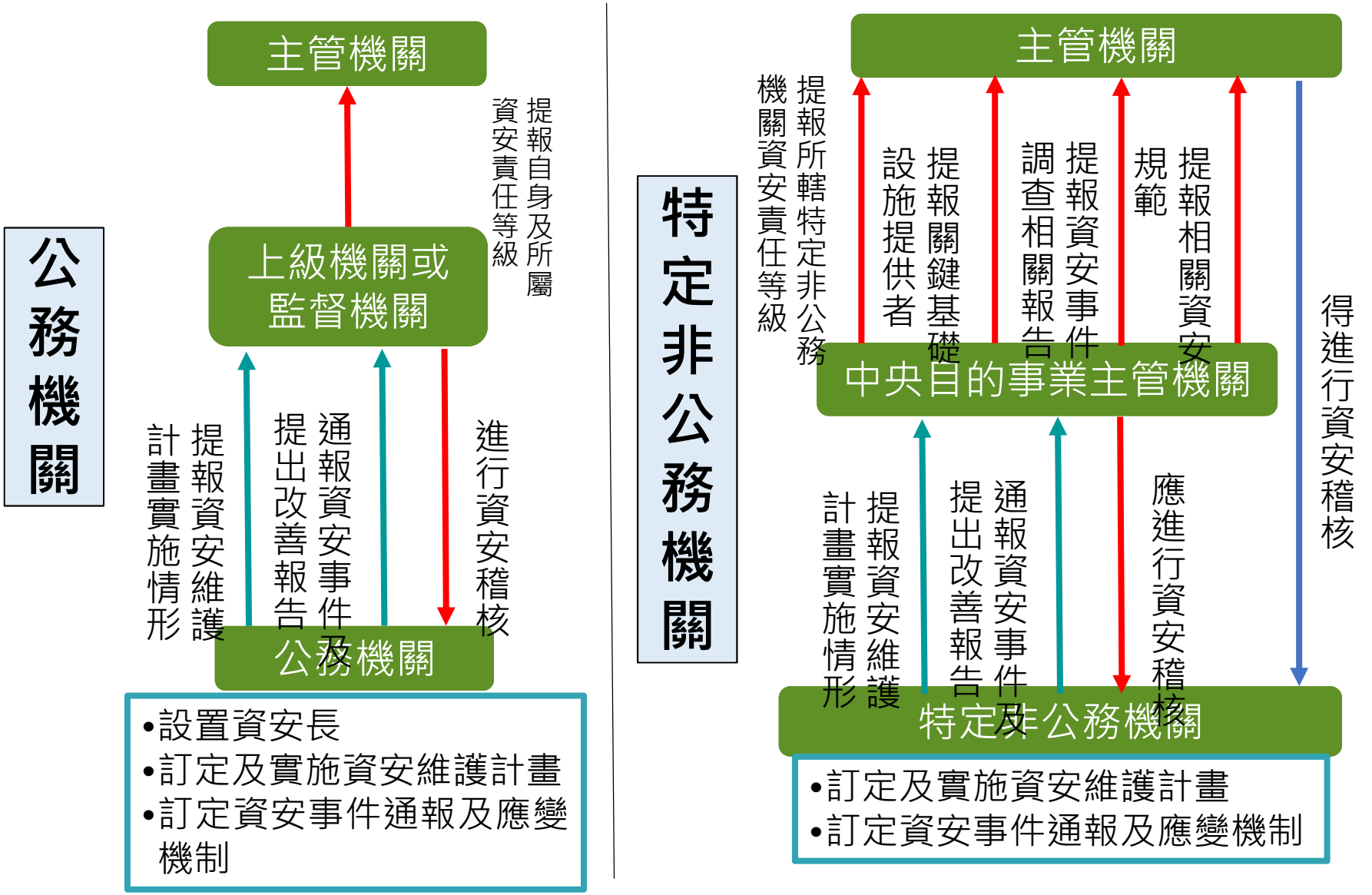
總統府、立法院、司法院、考試院、監察院、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會

設置資通安全長§11

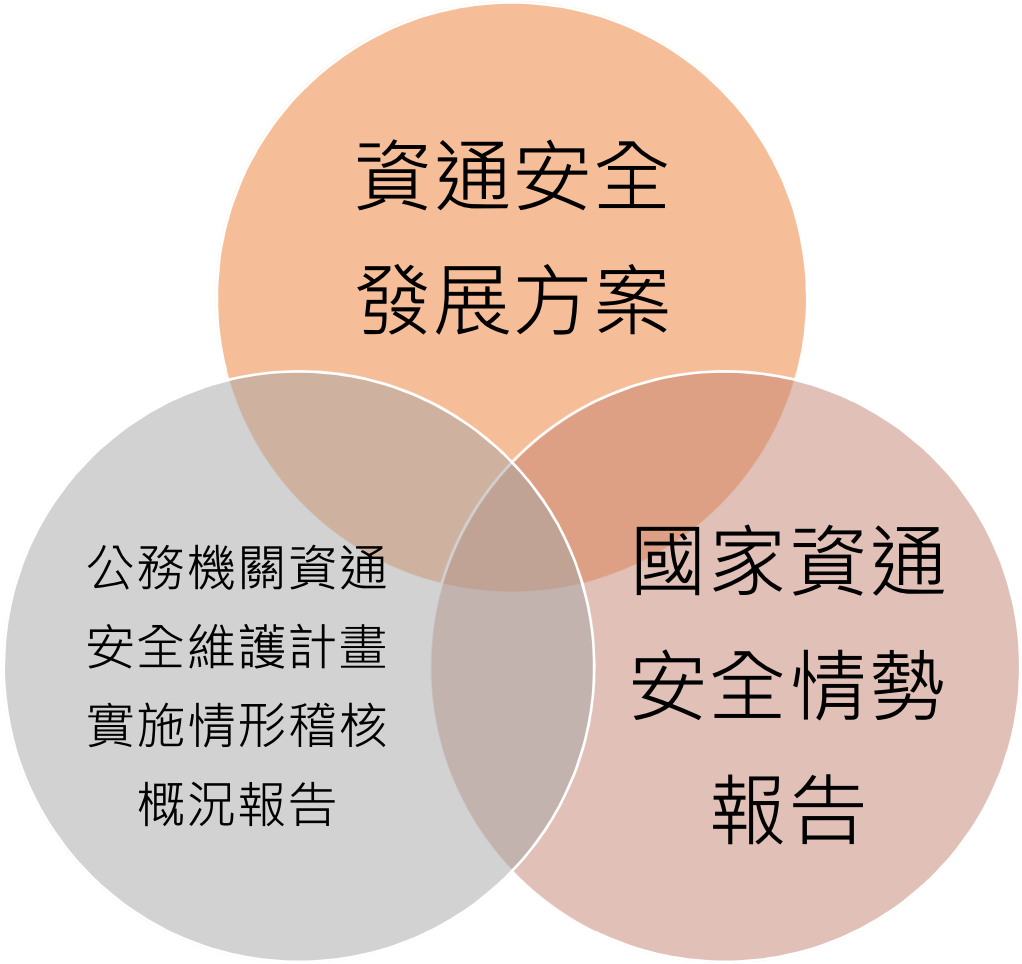
特定非公務機關之資通安全管理

	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

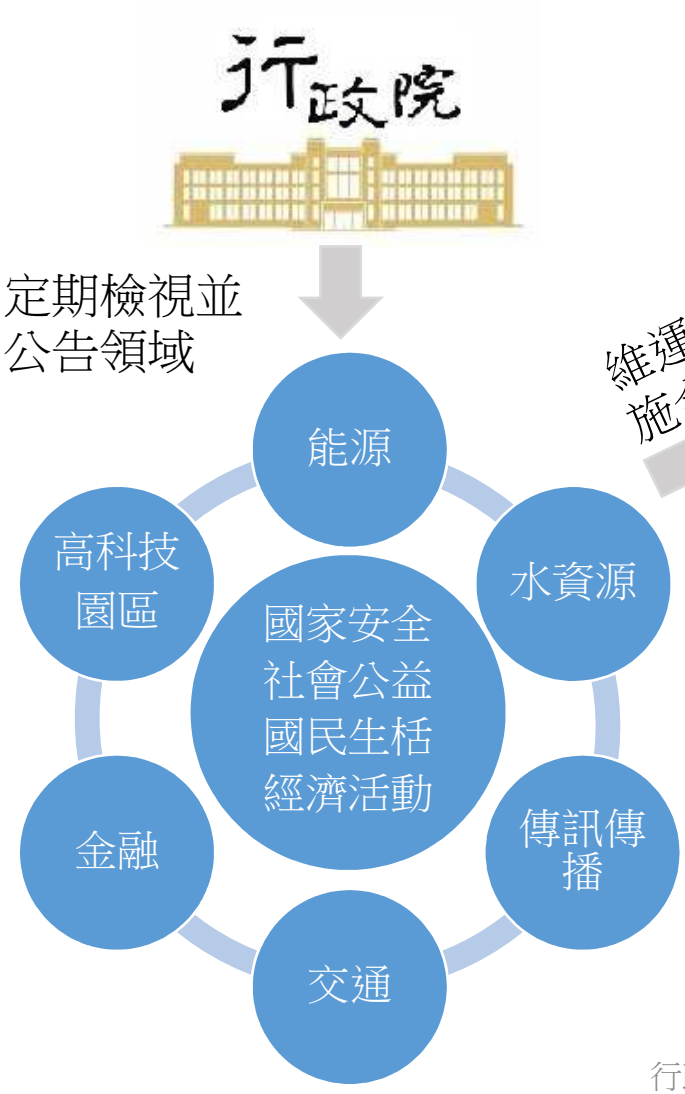

公務機關
主管機關
提報自身及所屬資安責任等級
上級機關或監督機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
進行資安稽核
公務機關
•設置資安長
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制
特定非公務機關
主管機關
提報所轄特定非公務機關資安責任等級
提報關鍵基礎設施提供者
提報資安事件調查相關報告
提報相關資安規範
得進行資安稽核
中央目的事業主管機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
應進行資安稽核
特定非公務機關
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制

送立法院備查文件

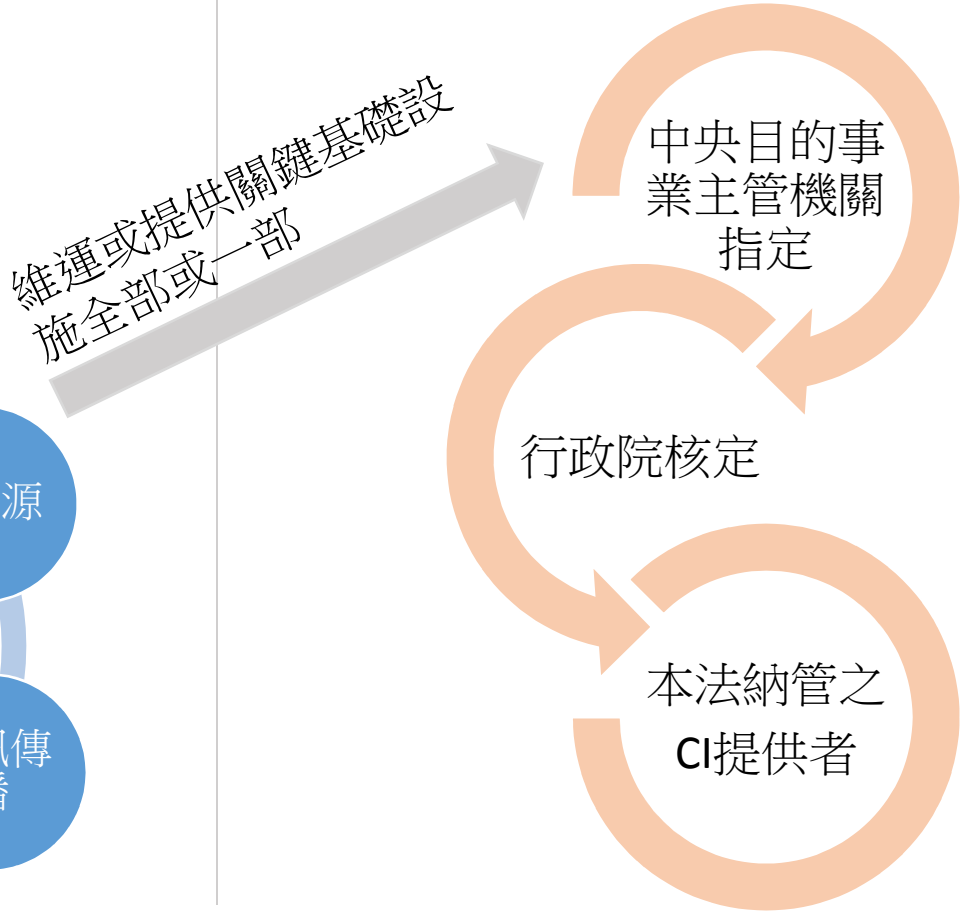


關鍵基礎設施(CI)

關鍵基礎設施(CI)



關鍵基礎設施(CI)提供者核定程序



關鍵基礎設施(CI)

CI提供者盤點作業

關鍵基礎設施

行政院國土安全辦公室

維運或提供關鍵基礎設施全部或一部

匯整

中央目的事業主管機關

關鍵基礎設施提供者

行政院資通安全處

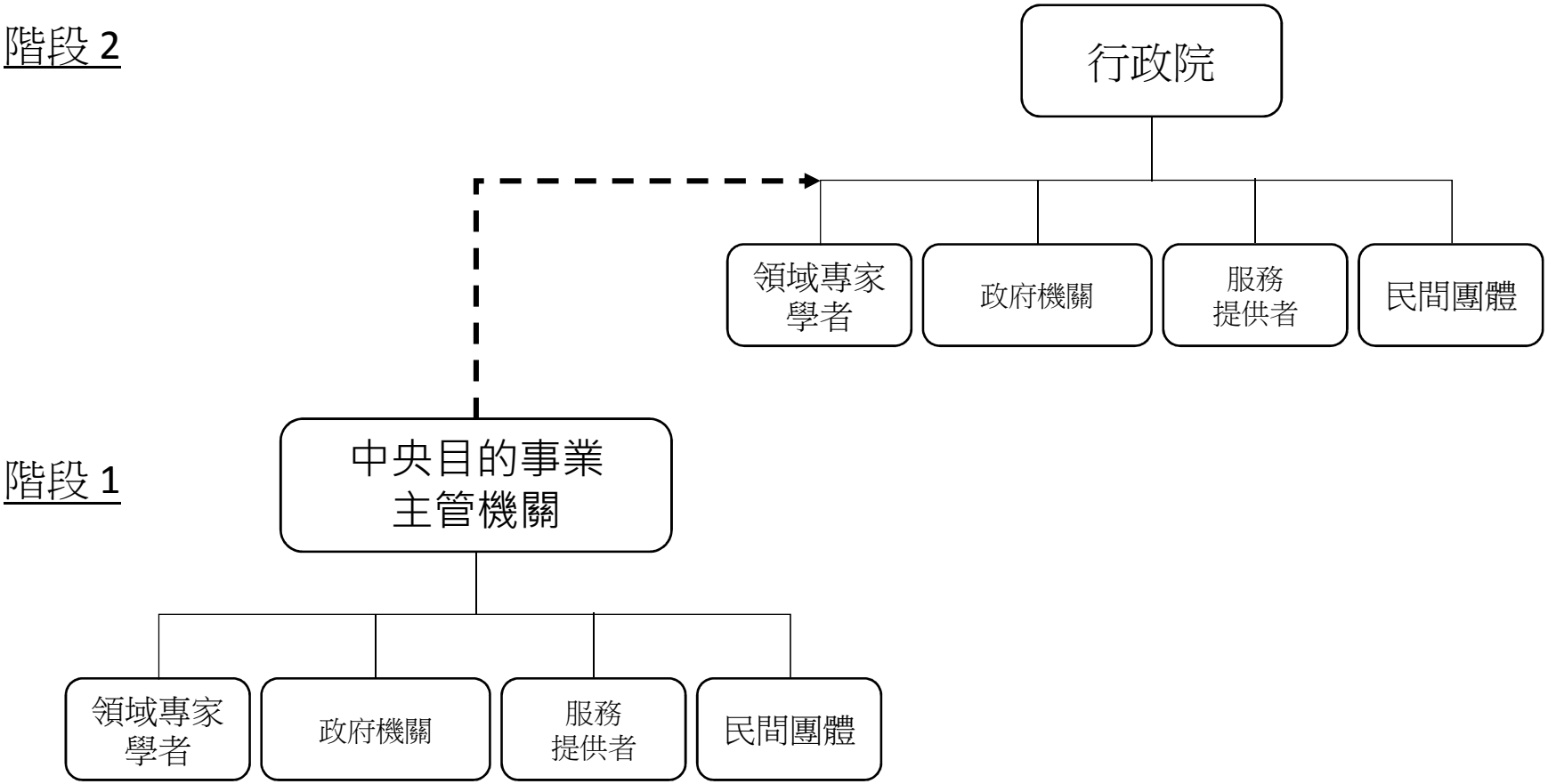
盤點

關鍵基礎設施提供者

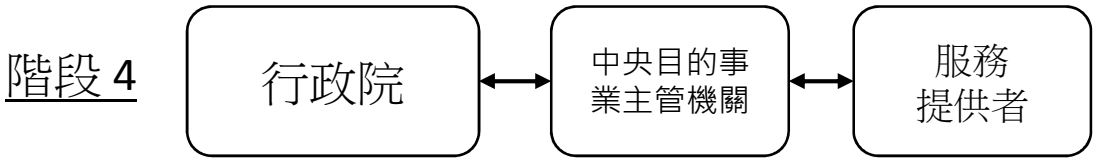
關鍵資訊基礎設施

行政院資通安全處

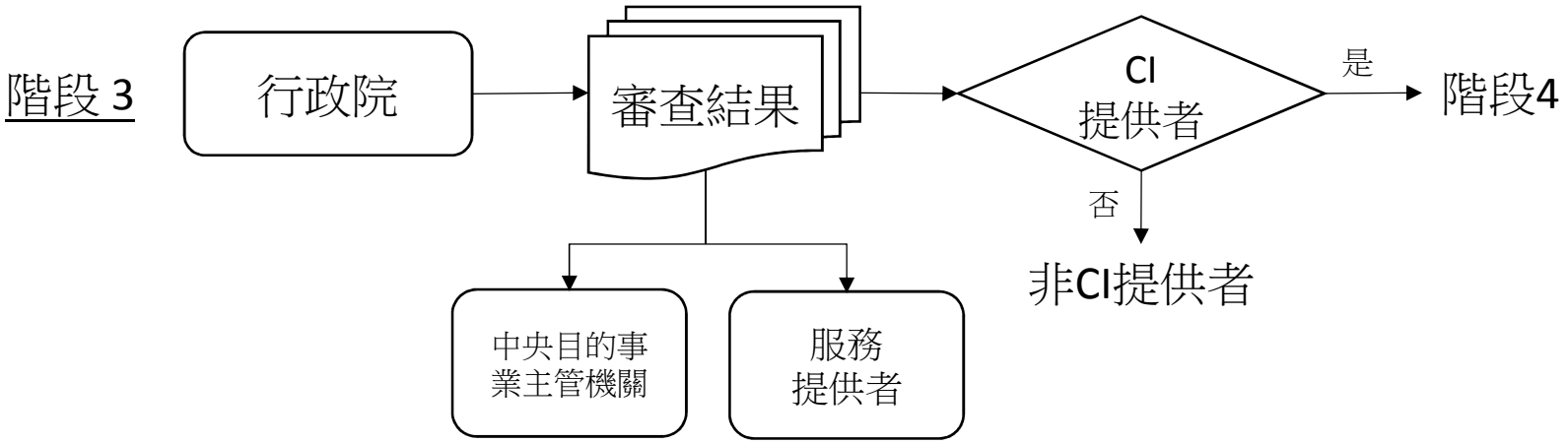
CI提供者指定程序(1/2)



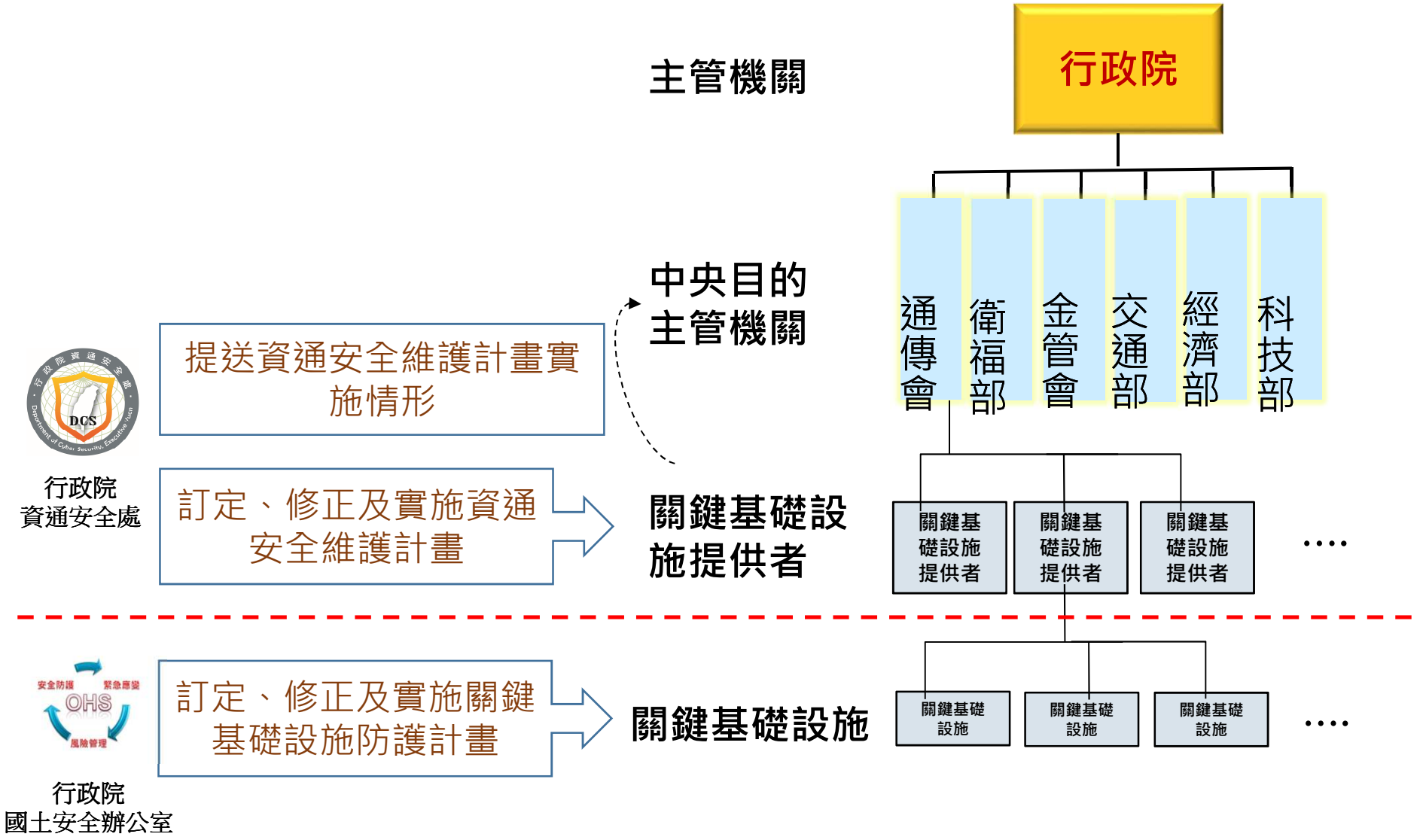
CI提供者指定程序(2/2)



資通安全維護計畫實施情形

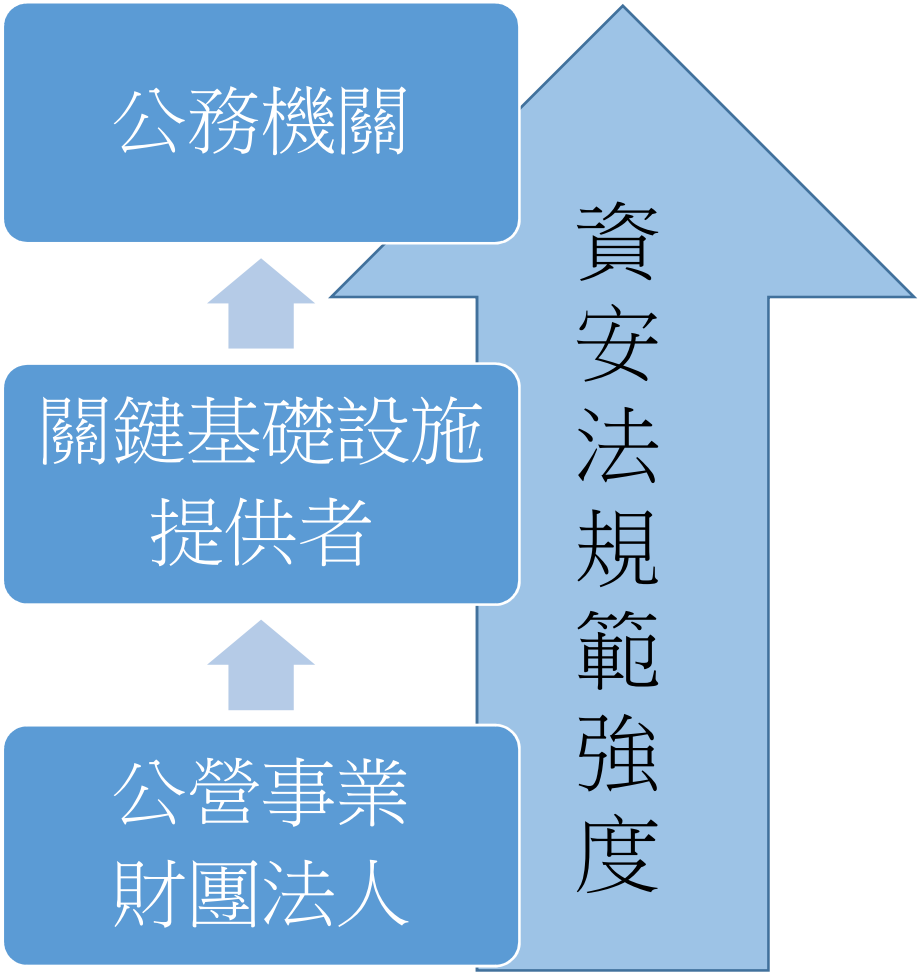


防護計畫

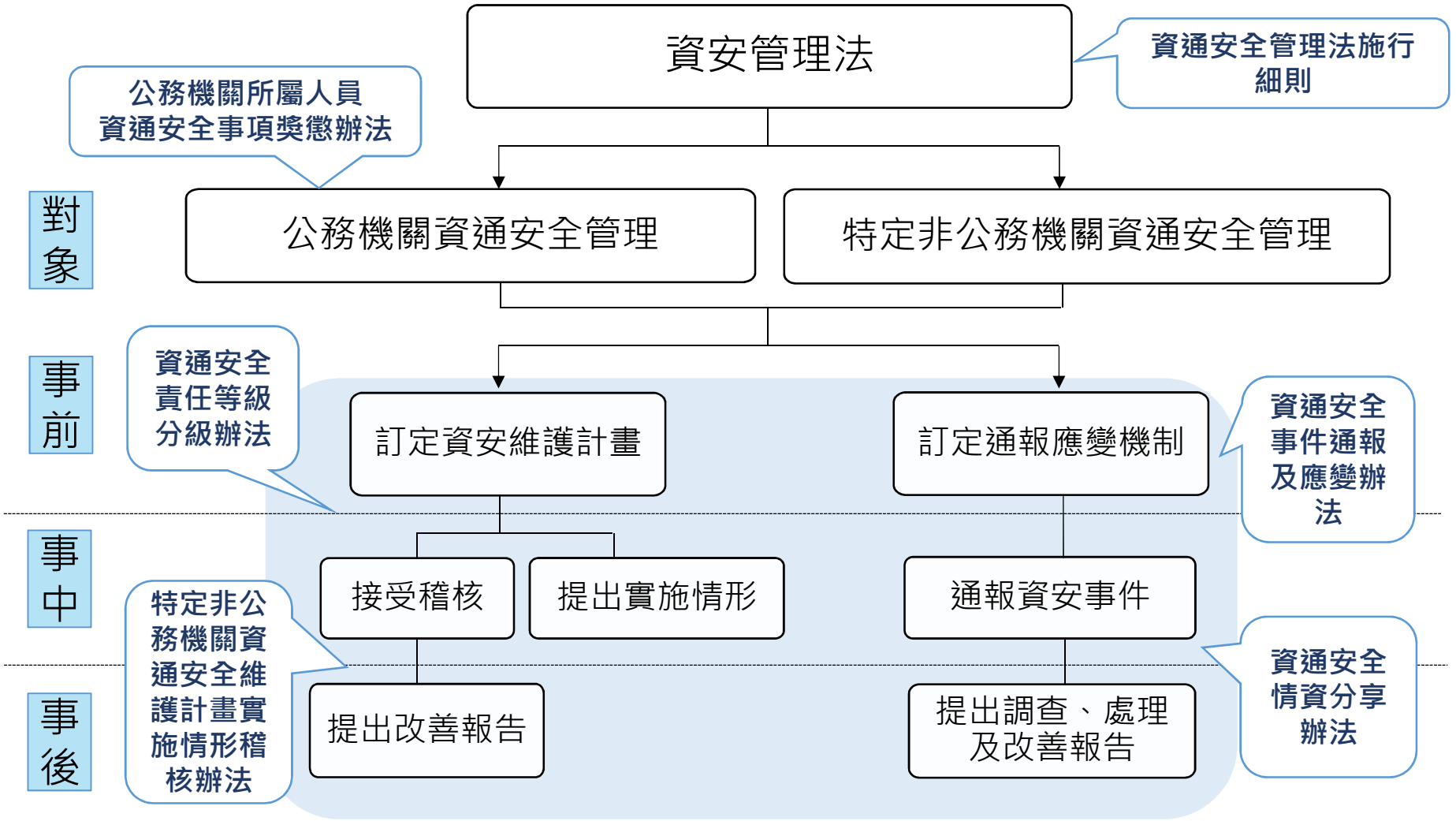

主管機關
行政院
通傳會
衛福部
金管會
交通部
經濟部
科技部
中央目的主管機關
提送資通安全維護計畫實施情形
行政院
資通安全處
訂定、修正及實施資通安全維護計畫
關鍵基礎設施提供者
關鍵基礎設施提供者
關鍵基礎設施提供者
關鍵基礎設施提供者
....
訂定、修正及實施關鍵基礎設施防護計畫
關鍵基礎設施
關鍵基礎設施
關鍵基礎設施
關鍵基礎設施
....
行政院
國土安全辦公室

本法規範適用先後

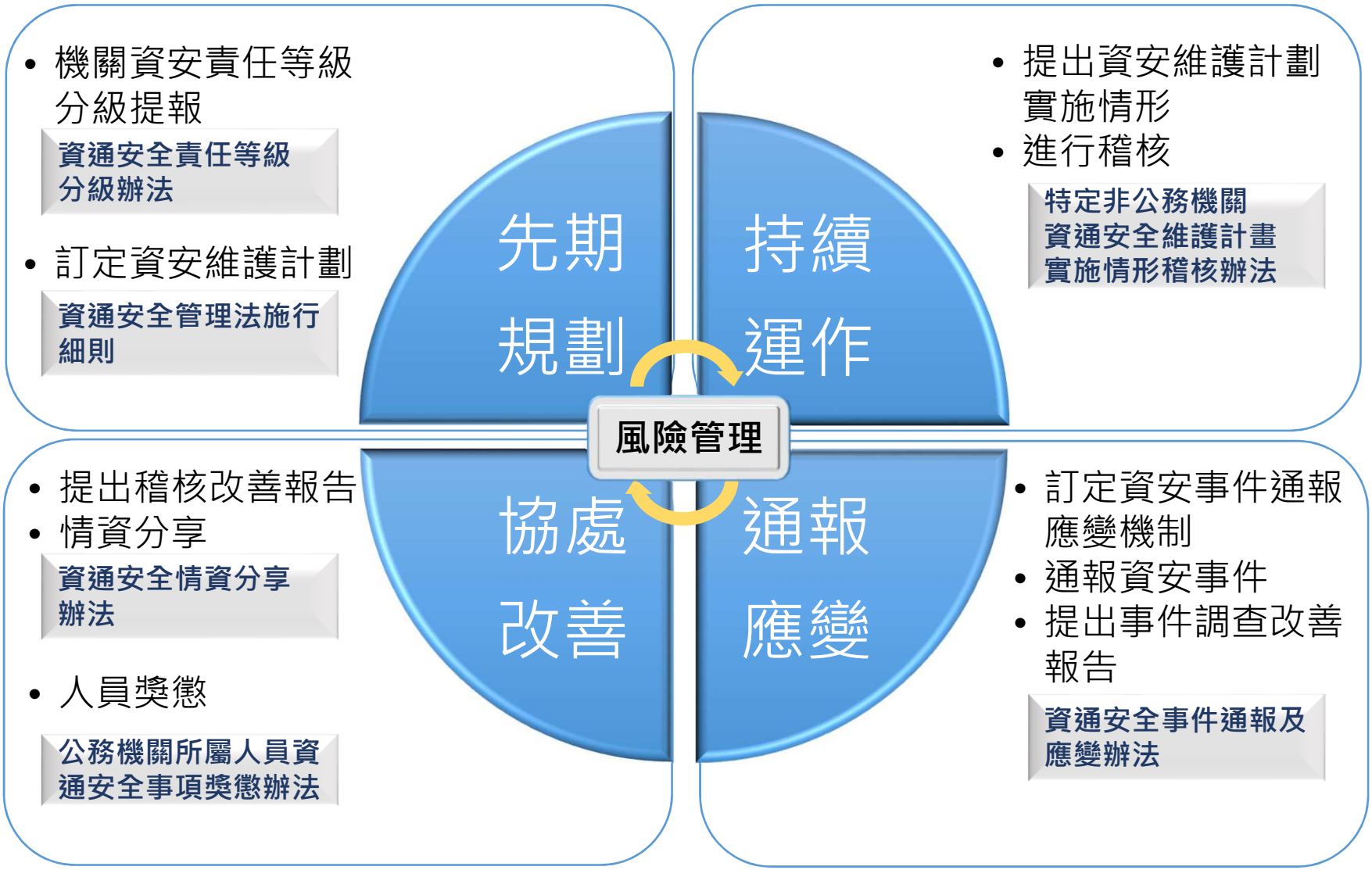
- 同時是公務機關及CI提供者
  - 優先適用公務機關之規定
- 同時是公營事業/財團法人及CI提供者
  - 優先適用CI提供者之規定



資安管理架構

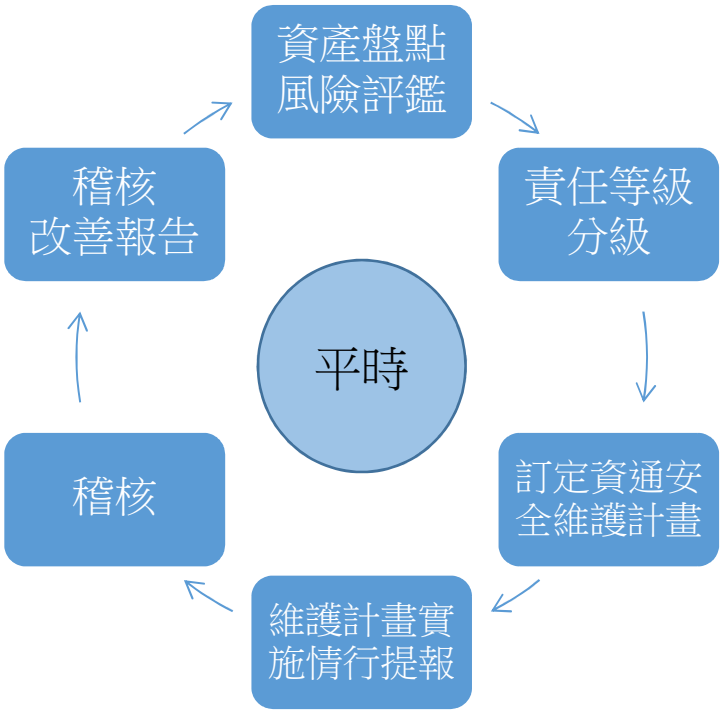

資安管理法
資通安全管理法施行細則
公務機關所屬人員資通安全事項獎懲辦法
對象
公務機關資通安全管理
特定非公務機關資通安全管理
事前
資通安全責任等級分級辦法
訂定資安維護計畫
訂定通報應變機制
資通安全事件通報及應變辦法
事中
接受稽核
提出實施情形
通報資安事件
特定非公務機關資通安全維護計畫實施情形稽核辦法
事後
提出改善報告
提出調查、處理及改善報告
資通安全情資分享辦法

資安管理子法架構

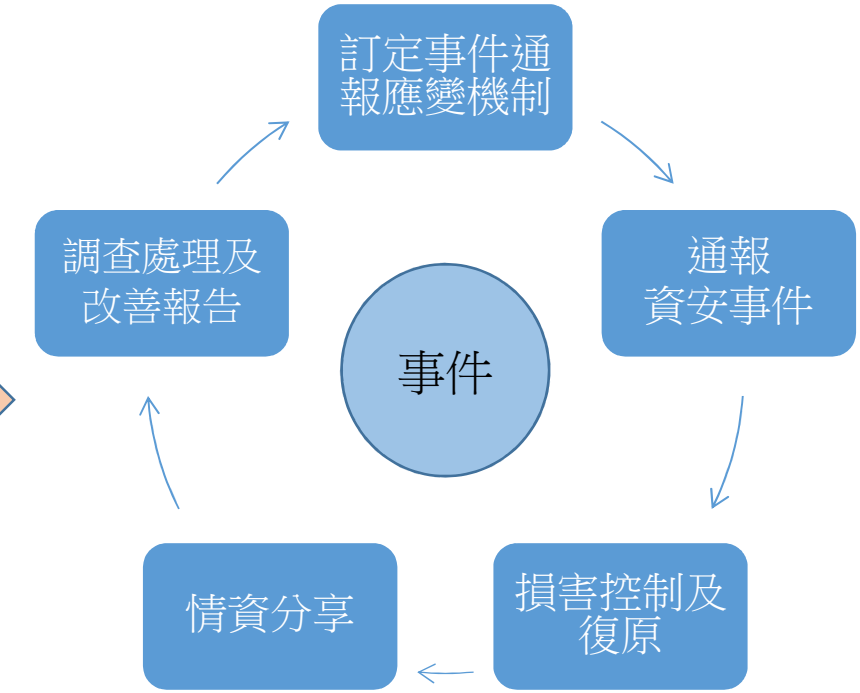

先期規劃
持續運作
協處改善
通報應變
風險管理
• 機關資安責任等級分級提報
資通安全責任等級分級辦法
• 訂定資安維護計劃
資通安全管理法施行細則
• 提出資安維護計劃實施情形
• 進行稽核
特定非公務機關資通安全維護計畫實施情形稽核辦法
• 提出稽核改善報告
• 情資分享
資通安全情資分享辦法
• 人員獎懲
公務機關所屬人員資通安全事項獎懲辦法
• 訂定資安事件通報應變機制
• 通報資安事件
• 提出事件調查改善報告
資通安全事件通報及應變辦法

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

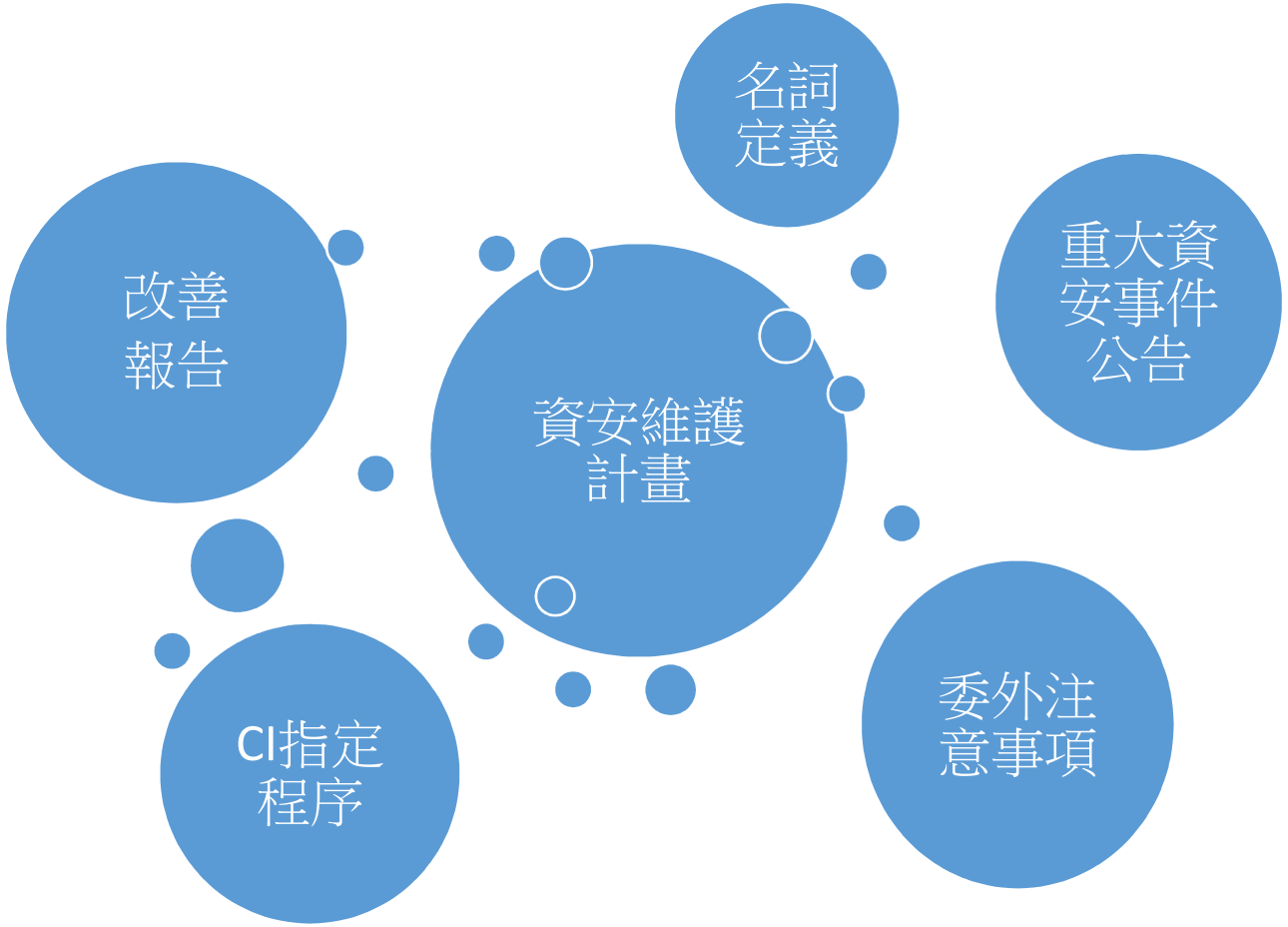
資通安全情資分享辦法

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

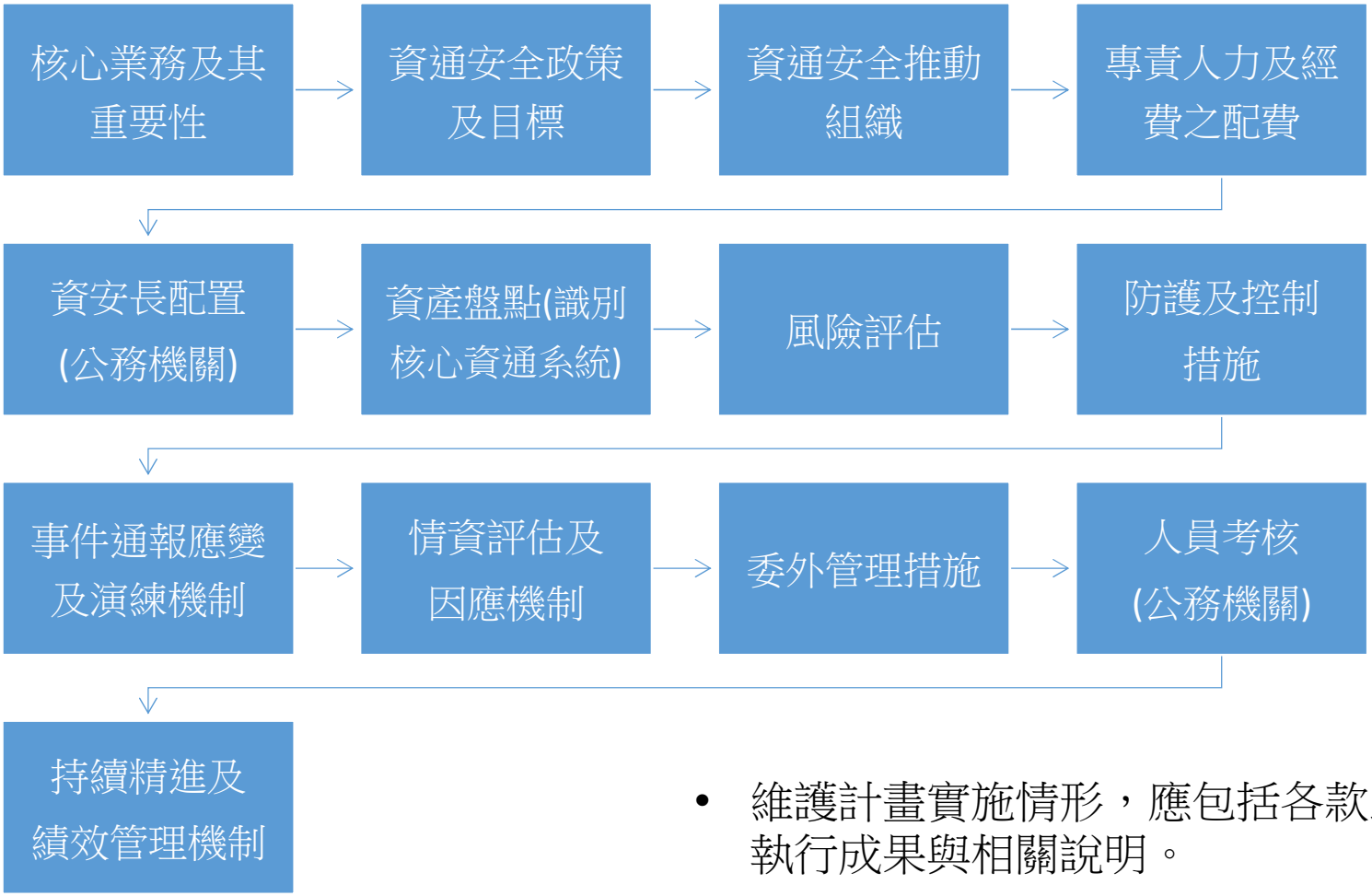
資通安全管理法施行細則

➢為施行資安法，訂定細節、技術性規範。



資通安全維護計畫內容

- 基於風險管理之基礎，包含下列內容



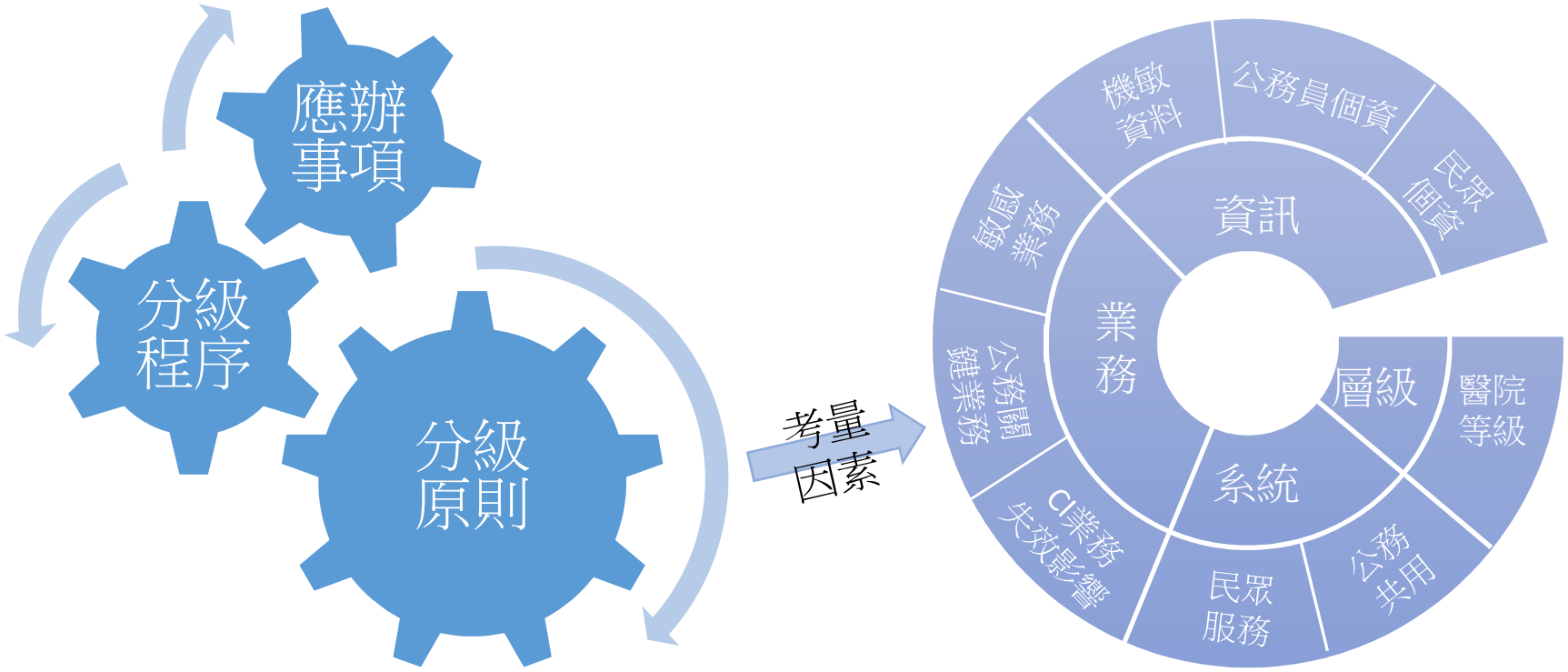
- 維護計畫實施情形，應包括各款之執行成果與相關說明。

改善報告內容要求

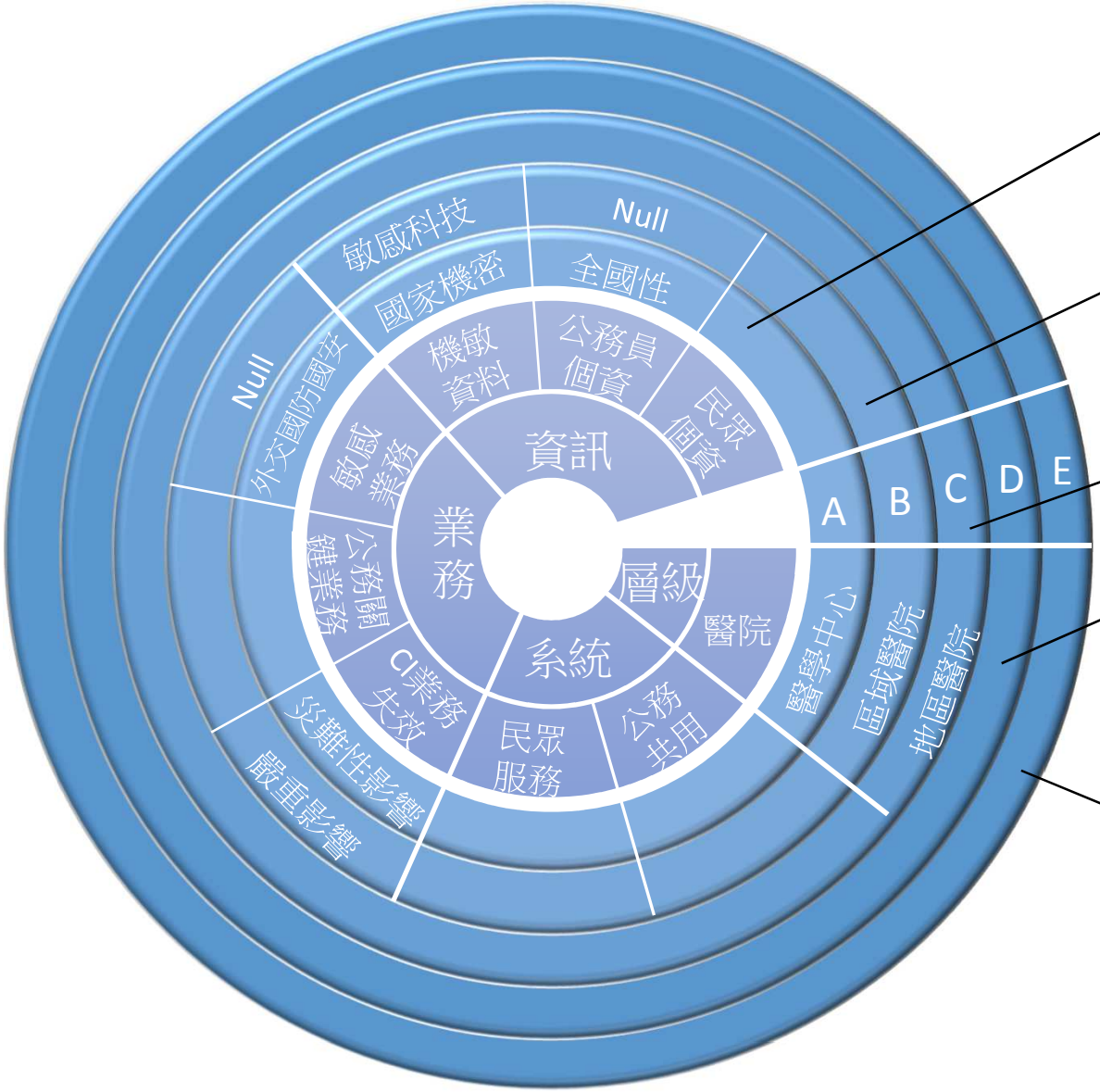
稽核改善報告(§3)	缺失或待改善之項目與內容
	發生原因
	所採取管理、技術、人力或資源等層面之措施
	預定完成時程及執行進度之追蹤
事件調查處理改善報告(§8)	事件發生、完成損害控制或復原作業之時間
	損害控制及復原作業之歷程
	事件調查及處理作業之歷程
	防範再次發生所採取之管理、技術、人力或資源等層面之措施
	預定完成時程及成效追蹤機制

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

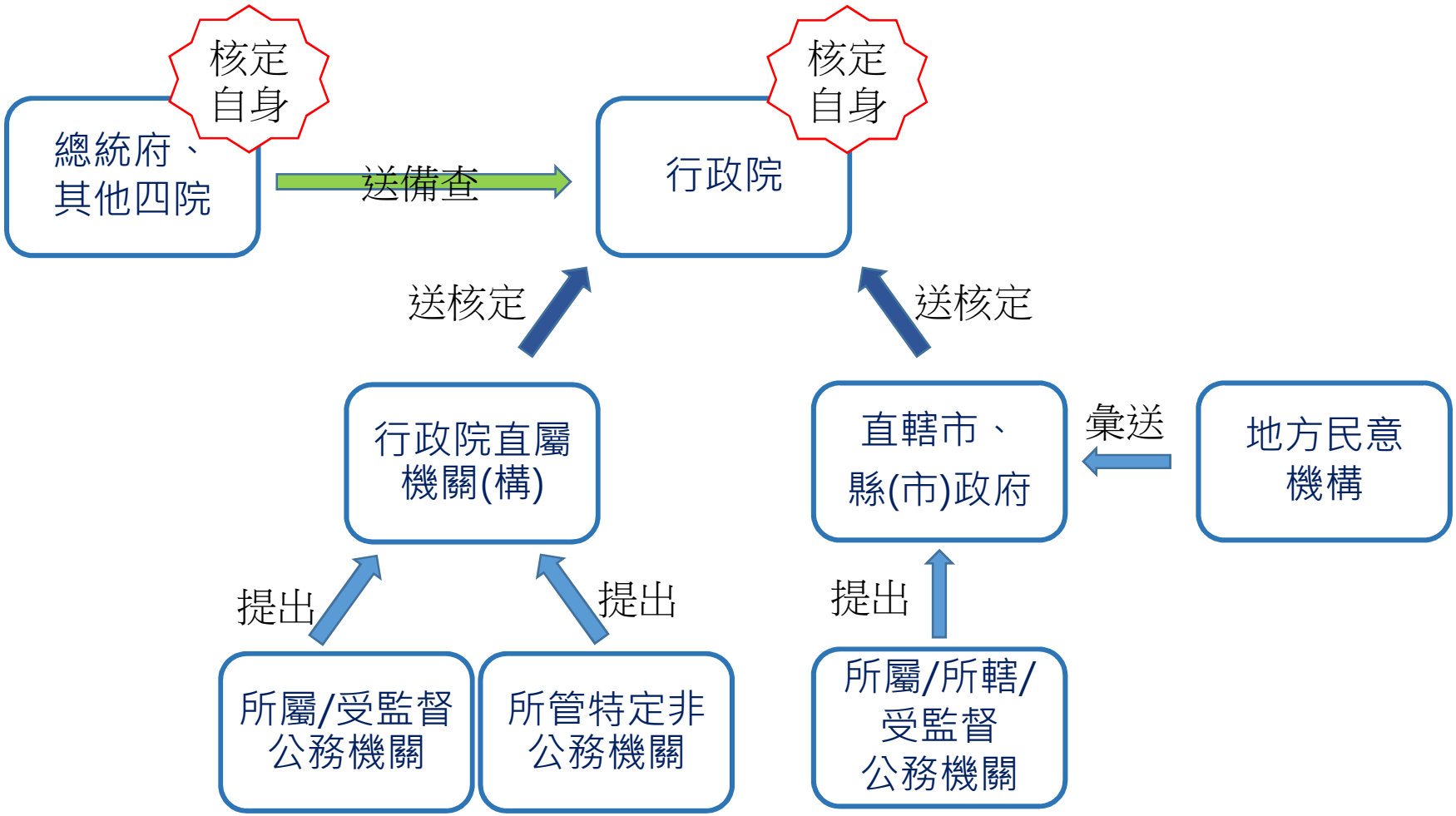
C級：有自行或委外發資訊系統，並設置伺服器者

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

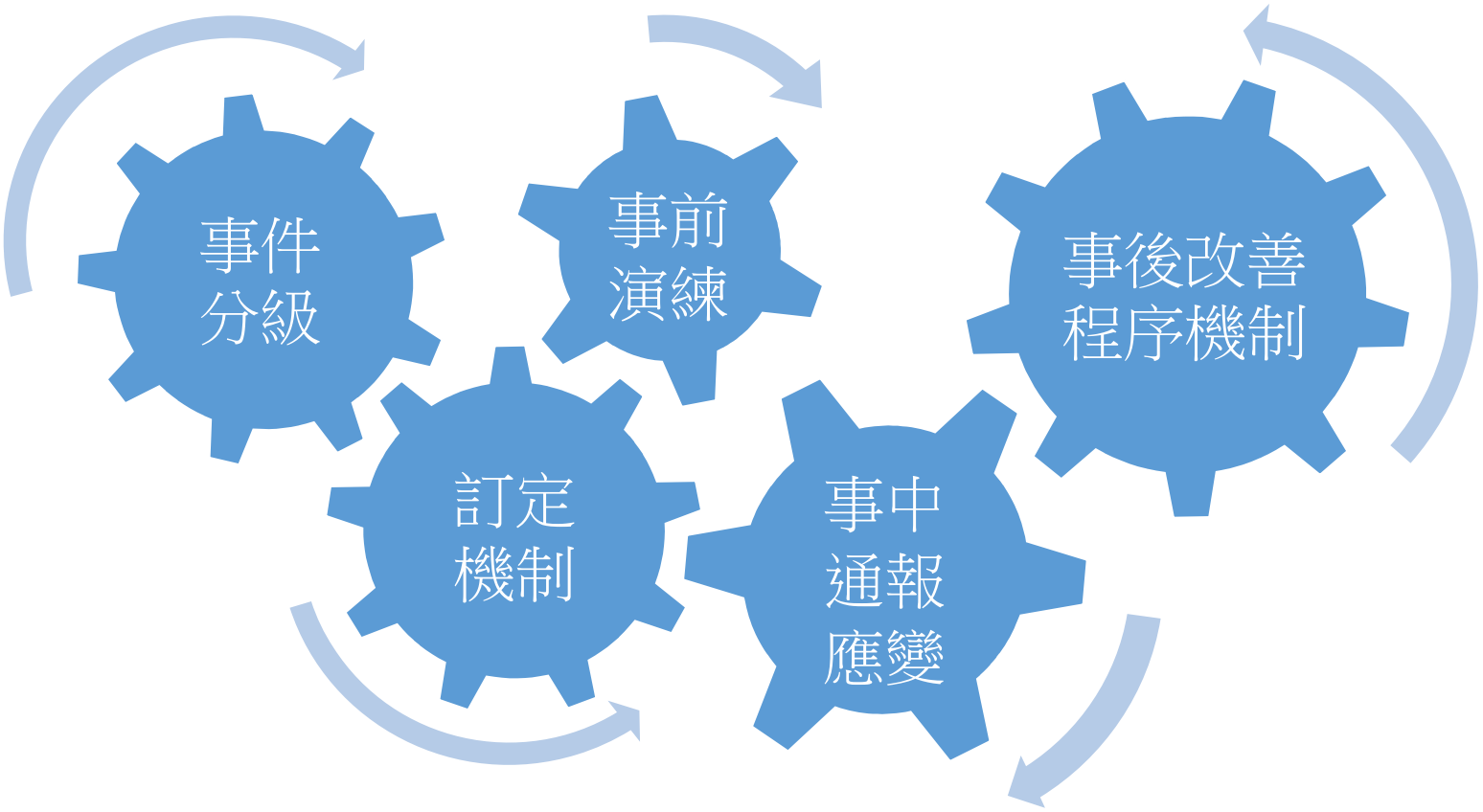
資通安全責任等級分級程序



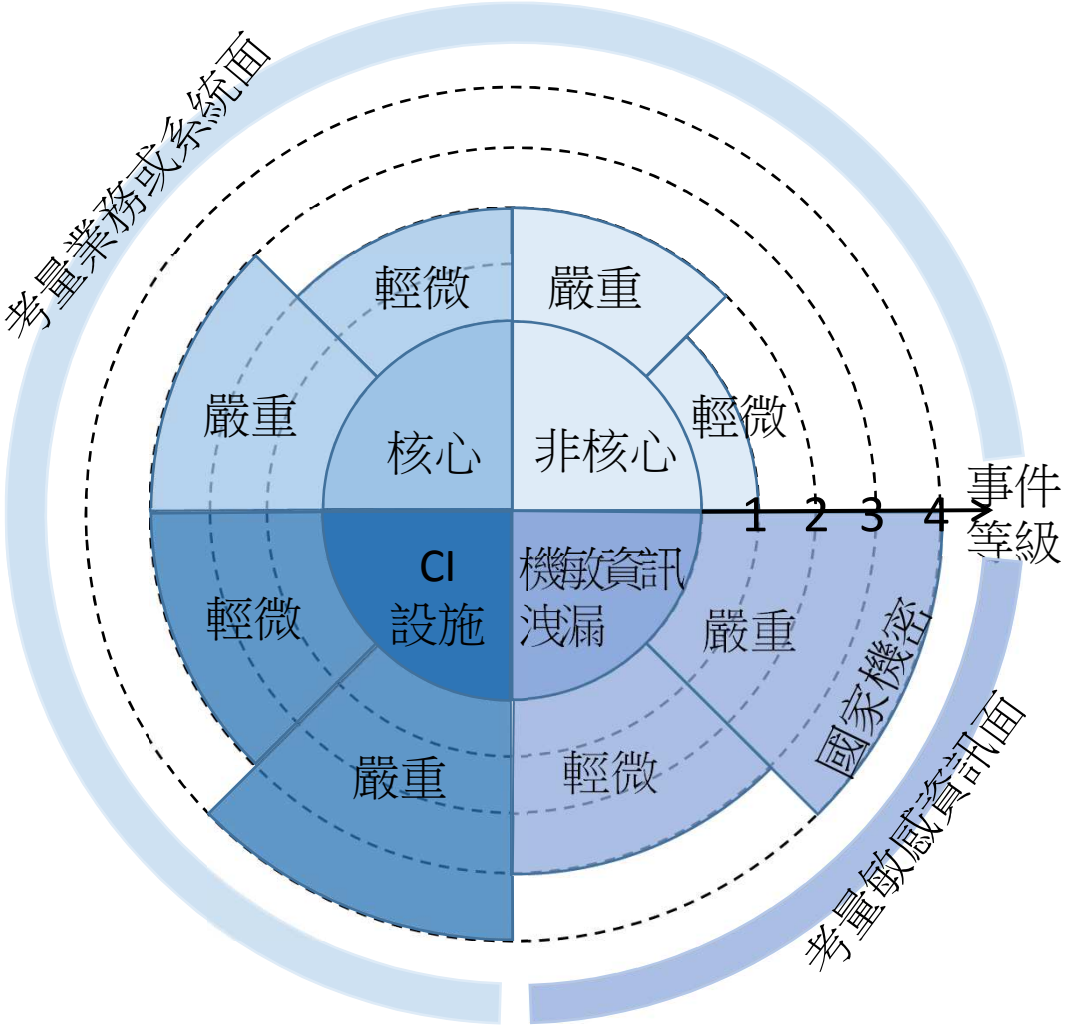
一般機關：每2年核定一次
新設或職務調整機關：立即辦理等級辦更

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

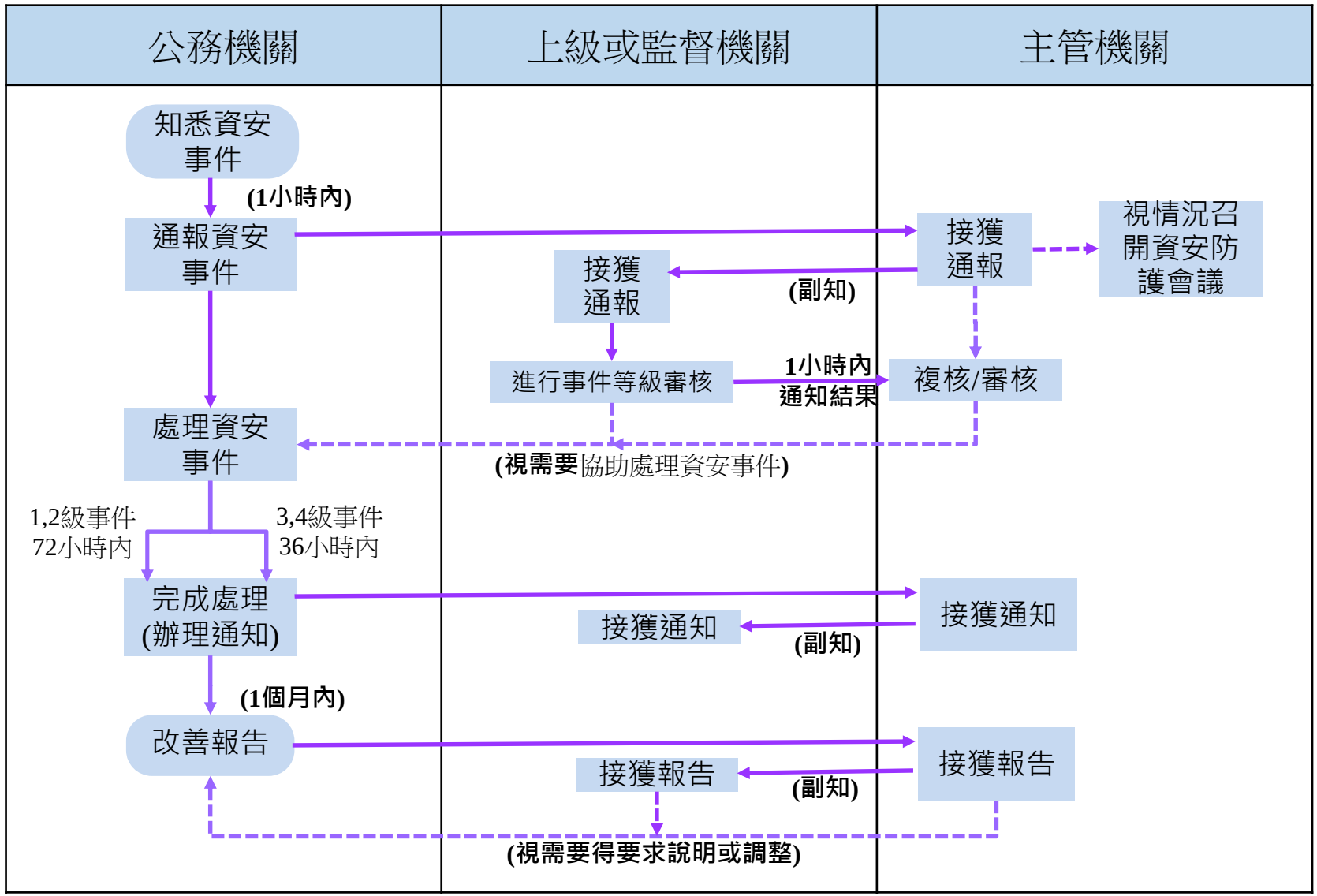


事件輕微或嚴重-考慮C,I,A三面向

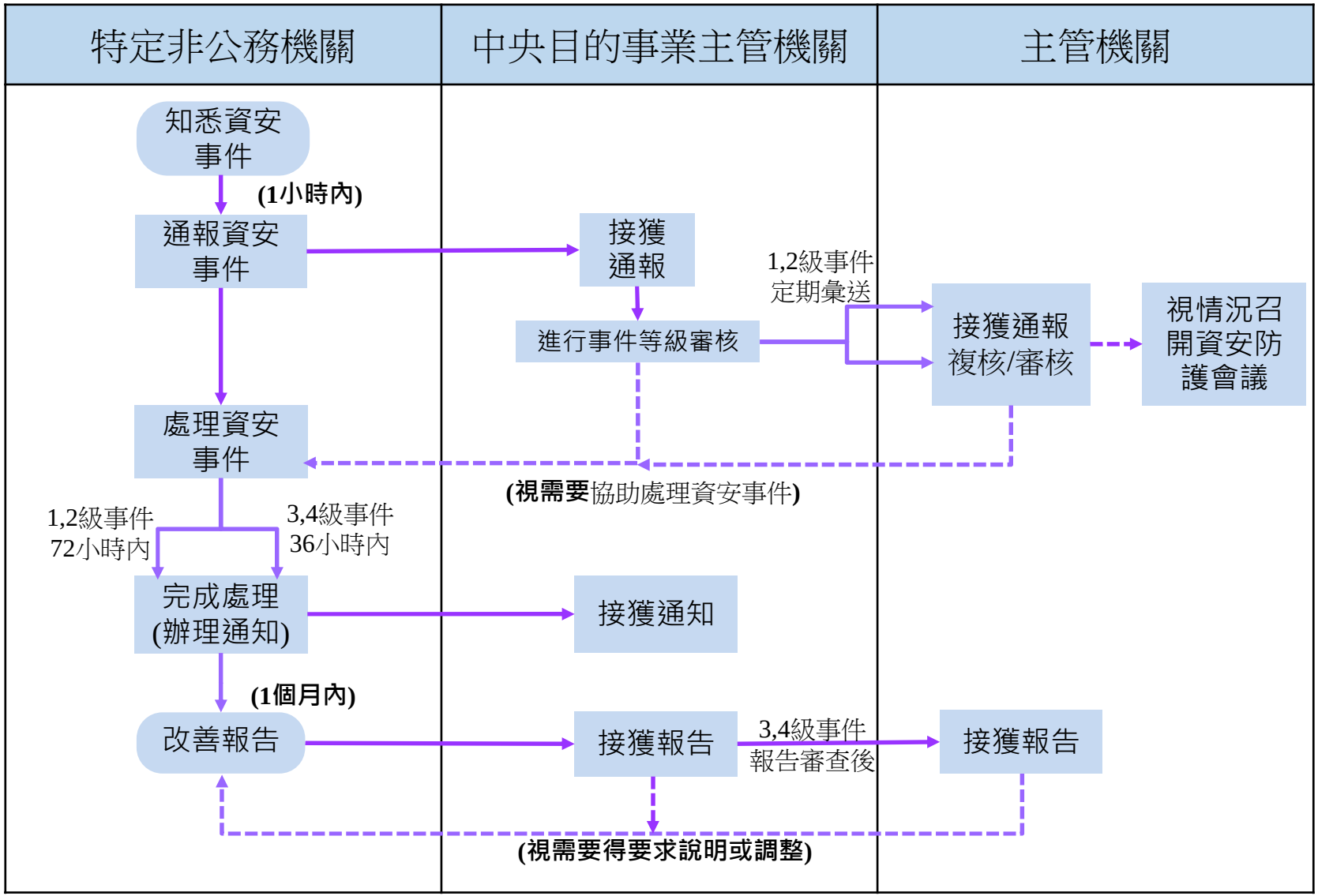
- 機密性
  - 業務資訊遭洩漏
- 完整性
  - 業務資訊遭竄改
  - 資通系統遭竄改
- 可用性
  - 資訊系統受影響或停頓，是否於可接受時間內回復

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

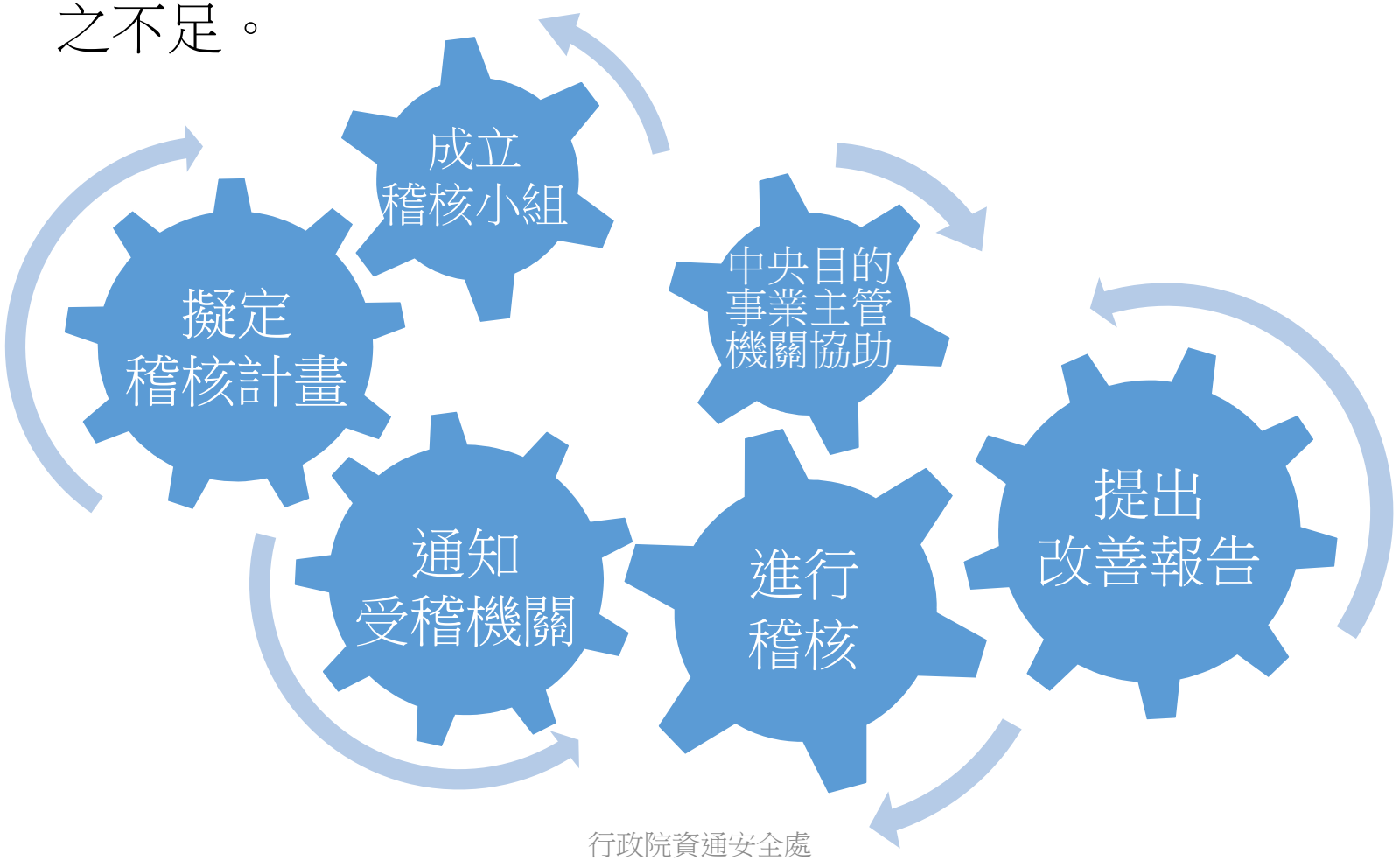

公務機關
上級或監督機關
主管機關
知悉資安事件
(1小時內)
通報資安事件
接獲通報
(副知)
接獲通報
視情況召開資安防護會議
進行事件等級審核
1小時內通知結果
複核/審核
處理資安事件
(視需要協助處理資安事件)
1,2級事件 72小時內
3,4級事件 36小時內
完成處理(辦理通知)
接獲通知
(副知)
接獲通知
(1個月內)
改善報告
接獲報告
(副知)
接獲報告
(視需要得要求說明或調整)

事件通報流程-特定非公務機關

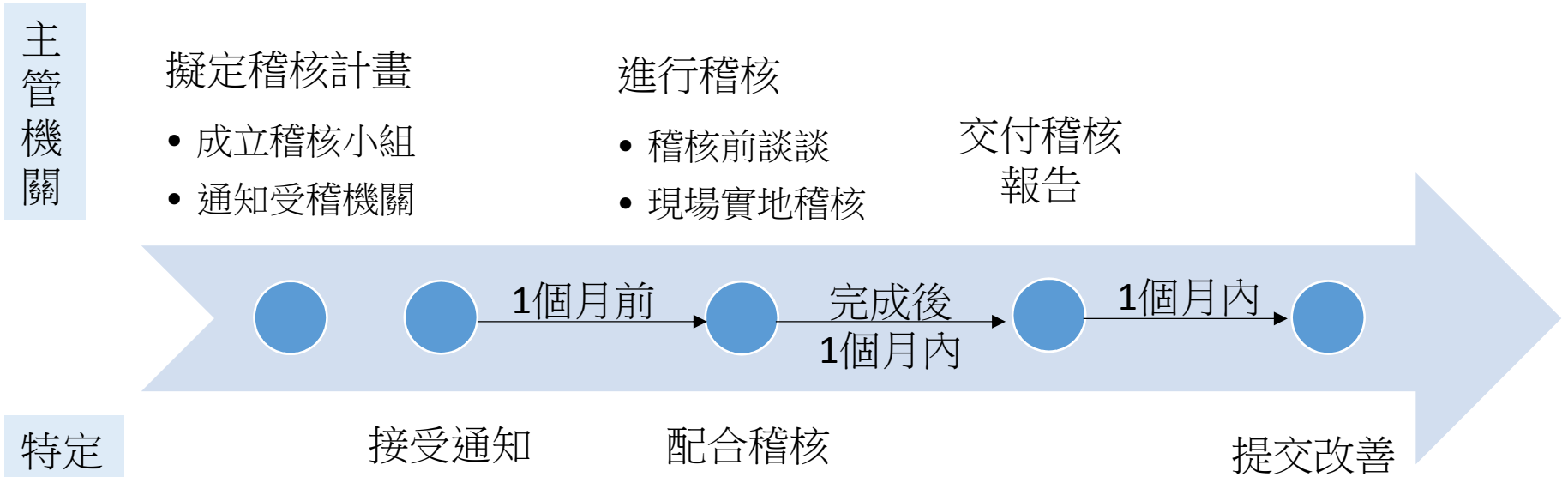


特定非公務機關資通安全維護計畫稽核辦法

- 主管機關對特定非公務機關進行稽核之辦法。
- 敦促實施資安維護計畫，協助其發現該計畫內容或實施之不足。

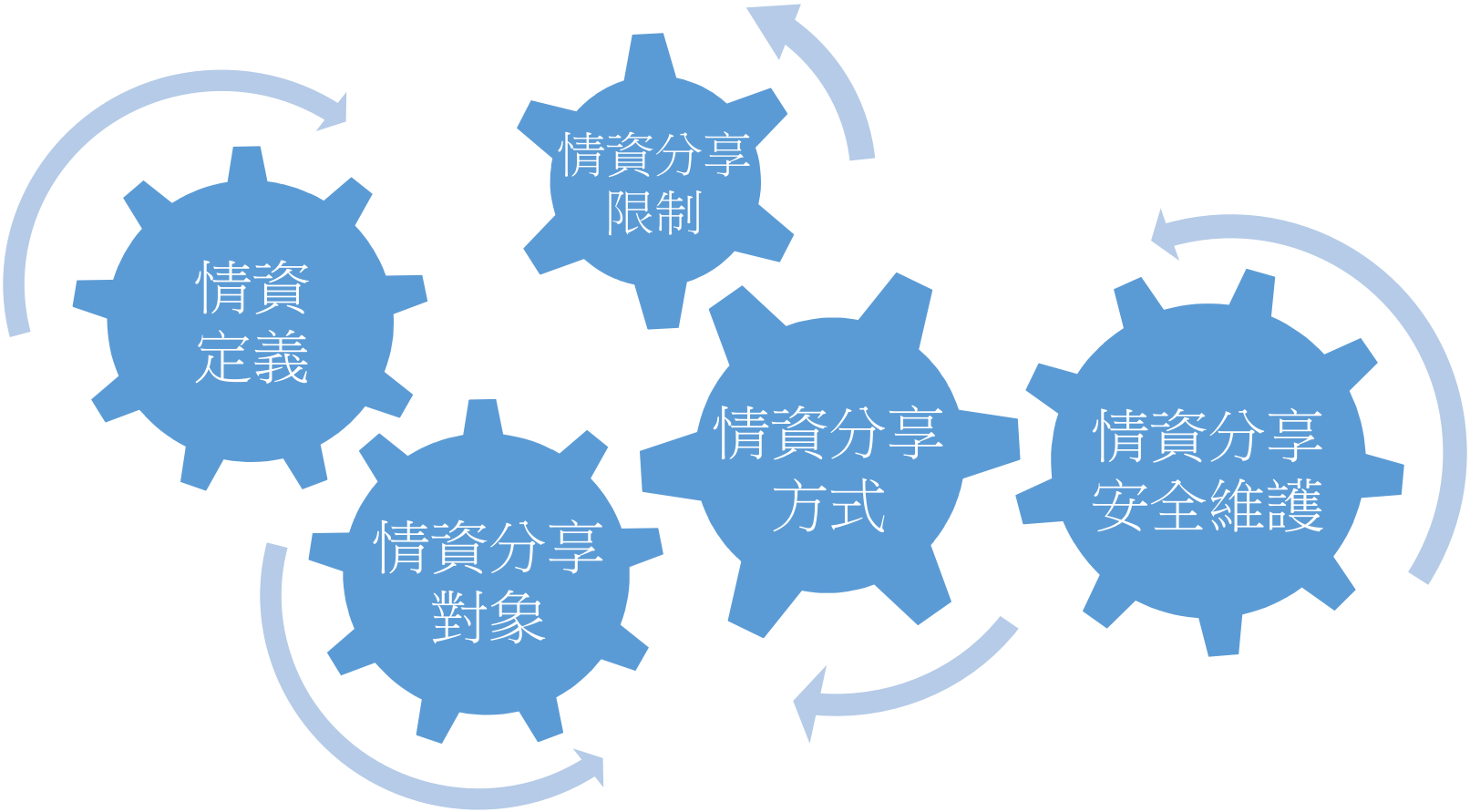


稽核程序


主管機關
擬定稽核計畫
• 成立稽核小組
• 通知受稽機關
進行稽核
• 稽核前談談
• 現場實地稽核
交付稽核報告
1個月前
完成後1個月內
1個月內
特定非公務機關
接受通知
• 有正當理由可調整日期
配合稽核
提交改善報告
中央目的事業主管機關
視主管機關需求派員為必要協助

資通安全情資分享辦法

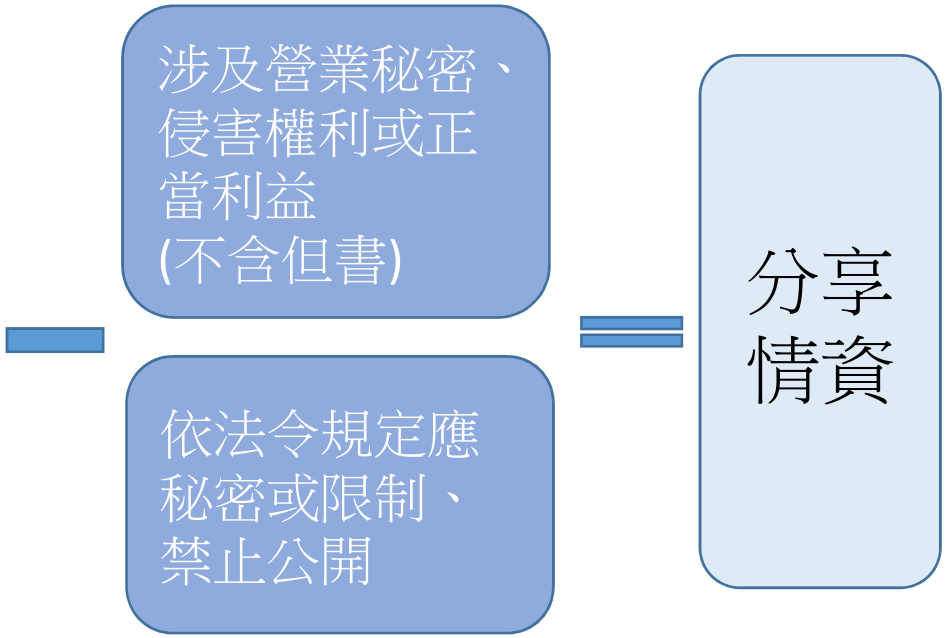
- 提升各機關對於資安之預警能力，強化資安相關資訊之交流。



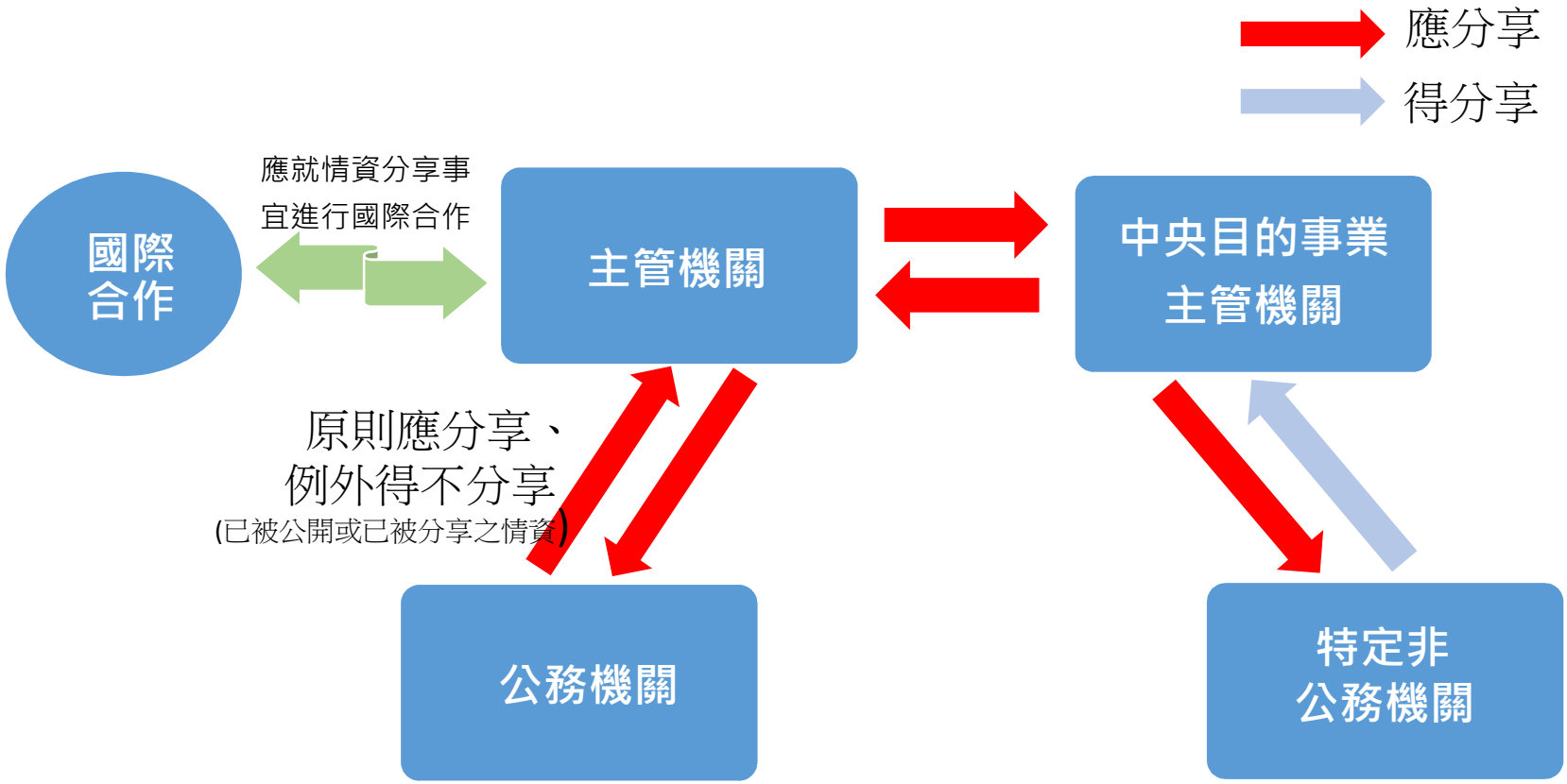
情資分享之內容

情資定義

情資分享例外



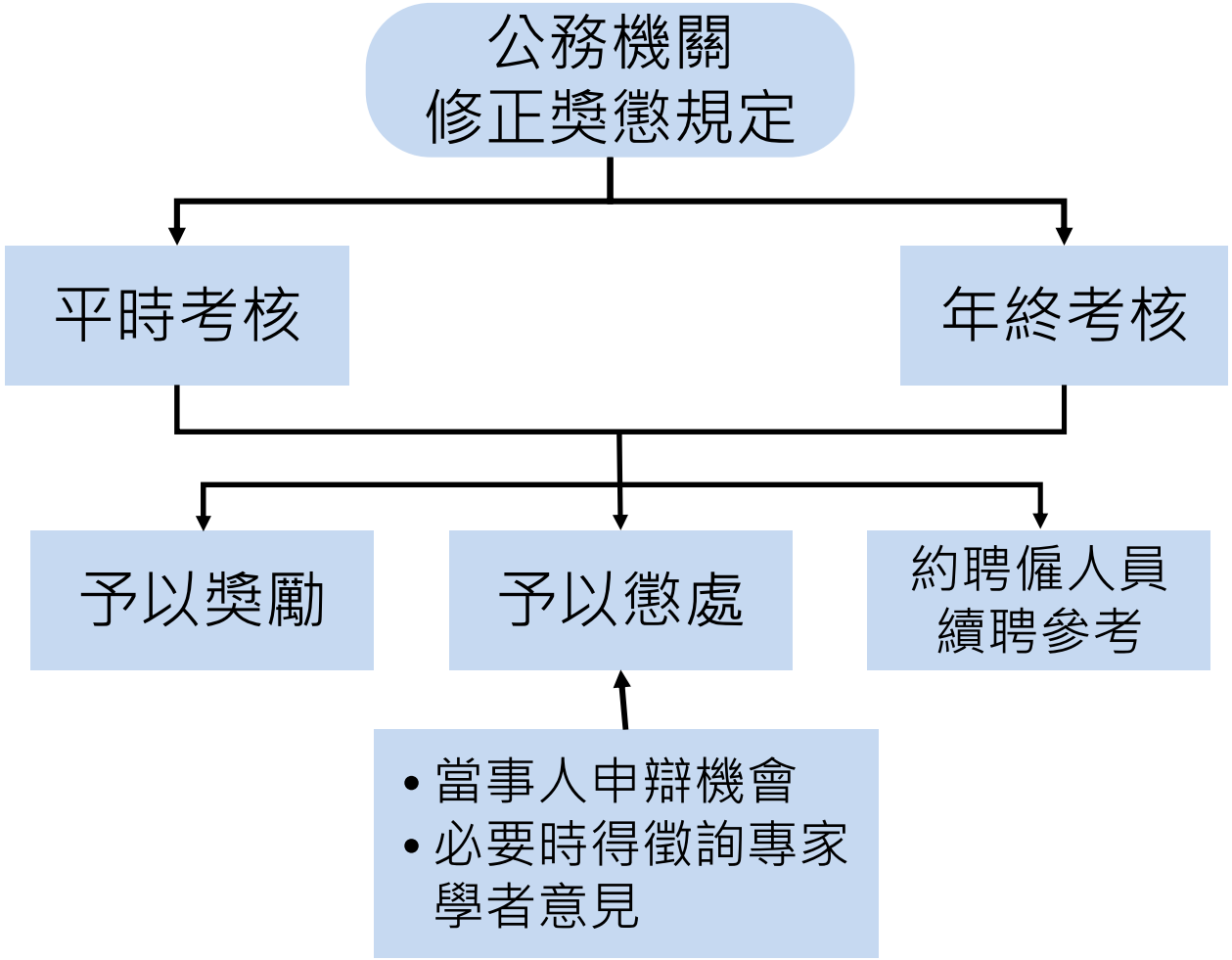
情資分享之對象



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

公務機關所屬人員資通安全事項獎懲辦法

➢ 敦促公務機關所屬人員執行資通安全維護事務



資安是持續精進的風險管理