資通安全管理法
子法草案分區座談會

行政院資通安全處

107年8月

大綱

一、資通安全管理法架構

二、子法草案規範內容

三、整備作業

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

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

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

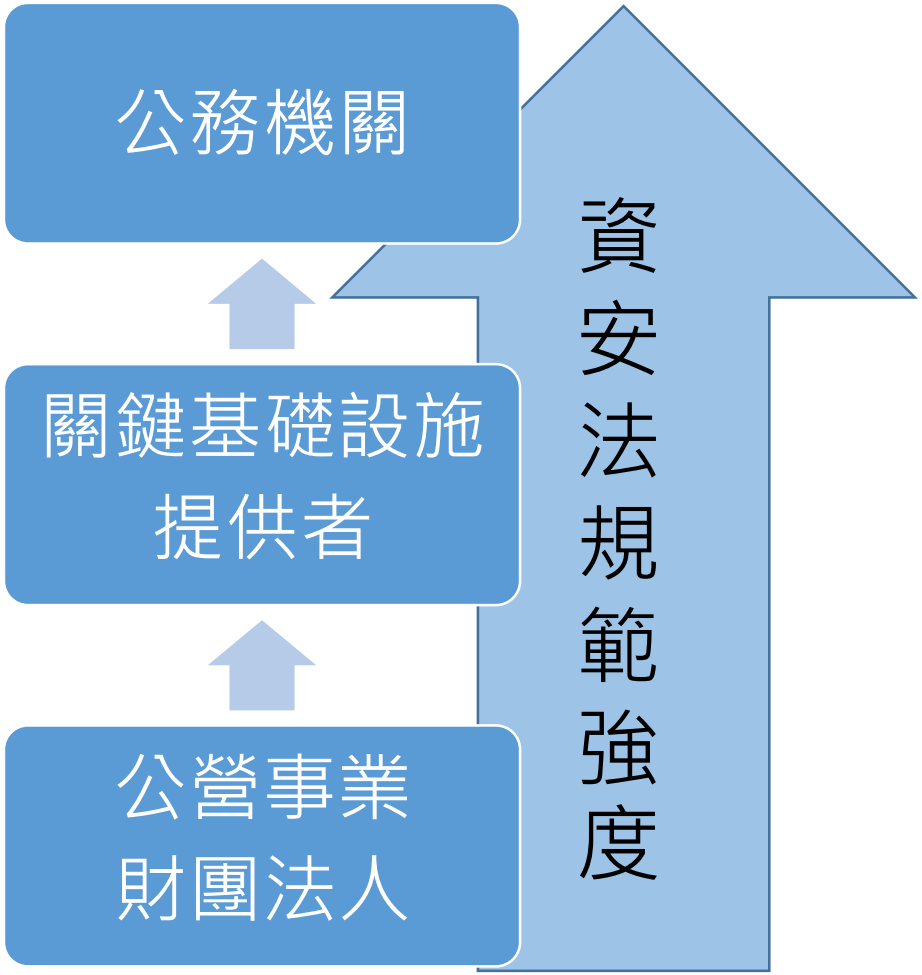
*資安管理法第三條第五款
公務機關：指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。

*資安管理法施行細則第二條
所稱軍事機關，指國防部及其所屬機關(構)、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款規定之機關。

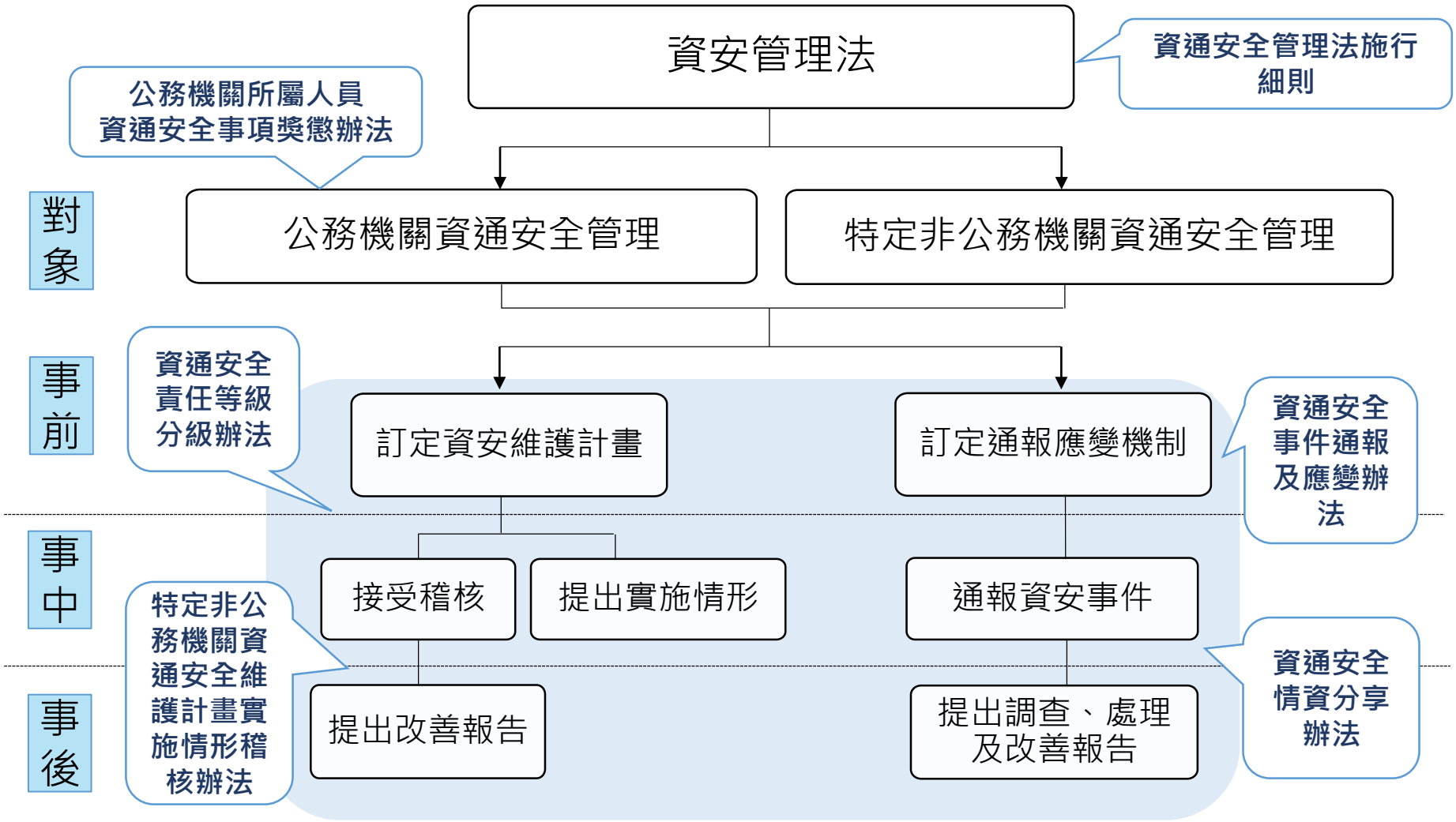
關鍵基礎設施(CI)

本法規範適用先後

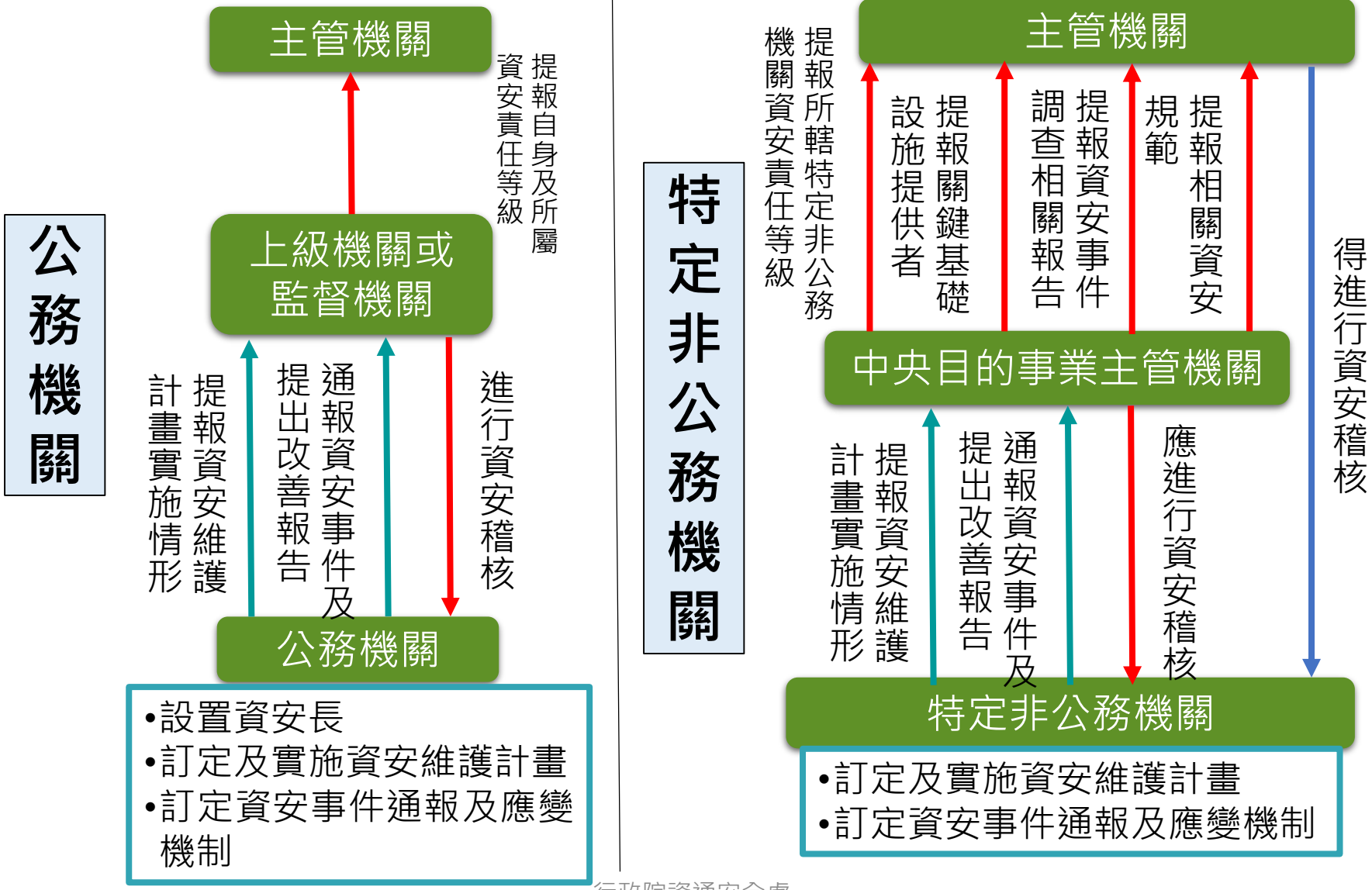
- 兼具公務機關及CI提供者
  - 優先適用公務機關之規定
  - 如：飛航服務總台
- 兼具公營事業/財團法人及CI提供者
  - 優先適用CI提供者之規定
  - 如：台電、中油



資安管理法架構


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

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

大綱

一、資通安全管理法架構

二、子法草案規範內容

三、整備作業

資安管理法子法架構

- 機關資安責任等級分級提報

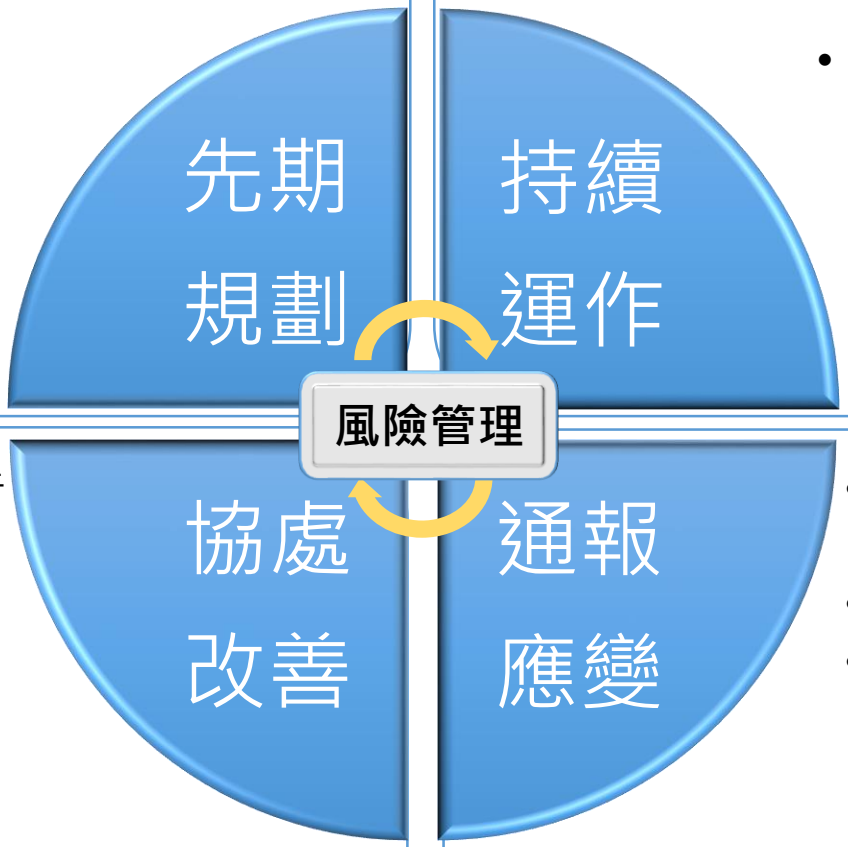
資通安全責任等級分級辦法

- 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

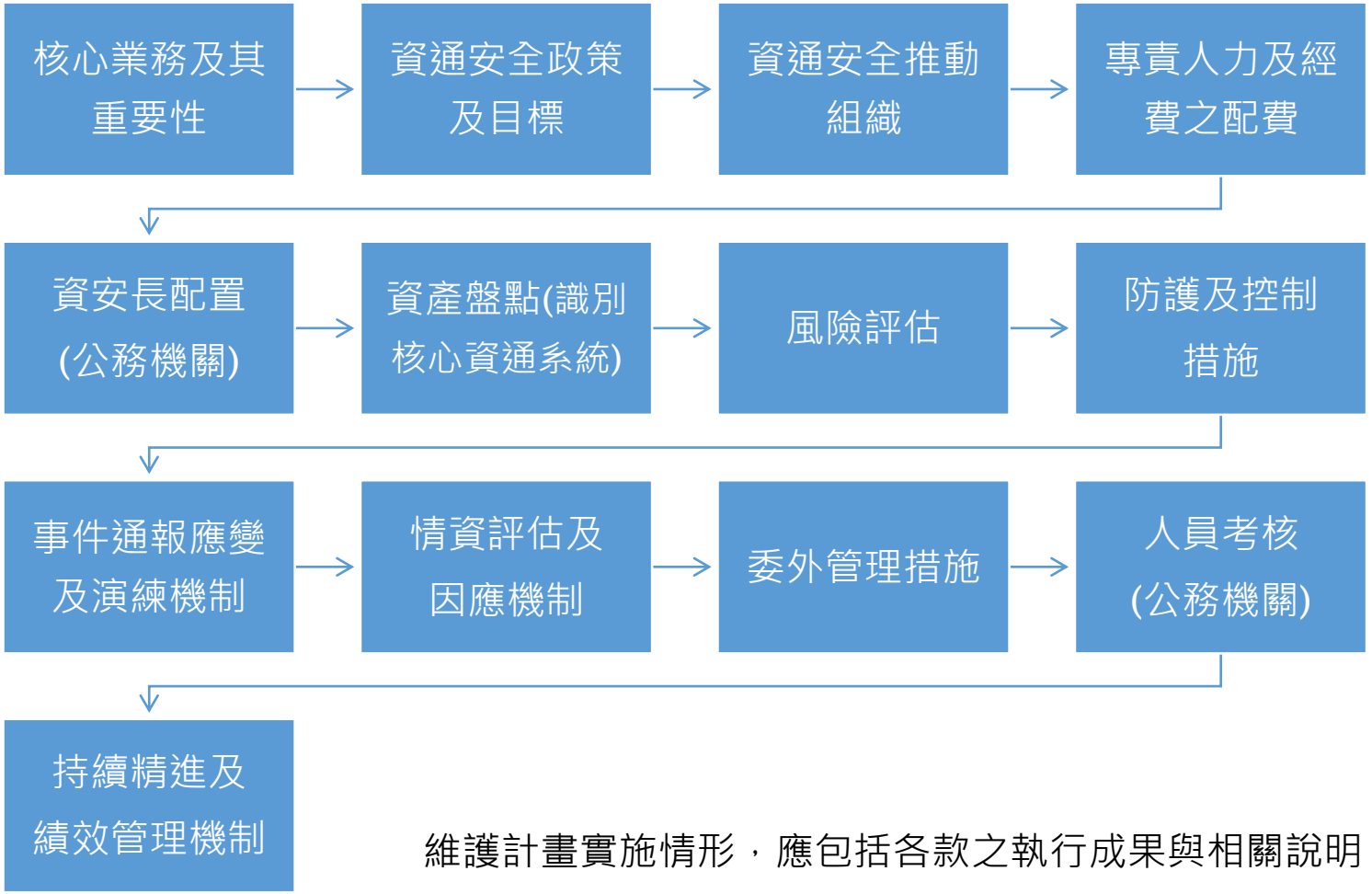
- 訂定資安事件通報應變機制
- 通報資安事件
- 提出事件調查改善報告

資通安全事件通報及應變辦法

資通安全管理法施行細則

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

資通系統建置、服務委外辦理注意事項

- 考量委外項目之性質、資通安全需求，選任適當之受託者，並監督其資通安全維護。

委外之前

- 受託者應具備完善之資通安全管理措施或通過第三方驗證
- 受託者應配置之資安專業人員(數量、資格、證照、經驗)
- 受託者得否複委託，及進行複委託應注之事項
- 受託業務涉及國家機密者，相關執行人員應接受適任性查核

委外之後

- 客製化開發者，應提供該資通系統之安全性檢測證明
- 非自行開發者，並應標示內容與其來源及提供授權證明。
- 受託者知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
- 委託結束後，應確認受託者持有之資料之返還或刪除
- 受託者應採取之其他資通安全相關維護措施
- 委託機關應以稽核或適當方式確認受託者之執行情形

本次調修重點

適任性查核

增列適任性查核進行方式說明(第4條第2項)

資安維護計畫項目

調修僅公務機關需人員考核機制(第6條第1項第12款)

新增得由他機關代為提出之情形(第6條第3項)

重大資安事件公告

調修重大資安事件公告及公告之例外規定(第11條)

CI 指定程序

新增中央目的事業主管機關依本法第16條第1項指定CI提供者前，應予其陳述意見之機會(第9條)

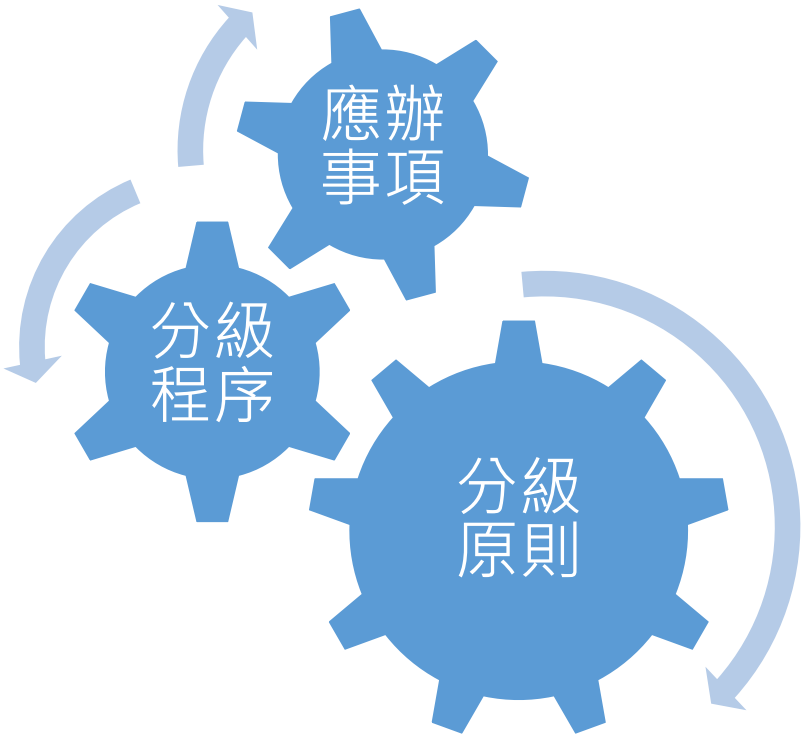
名詞定義

新增書面之定義(第5條)

核心系統之定義(第7條)

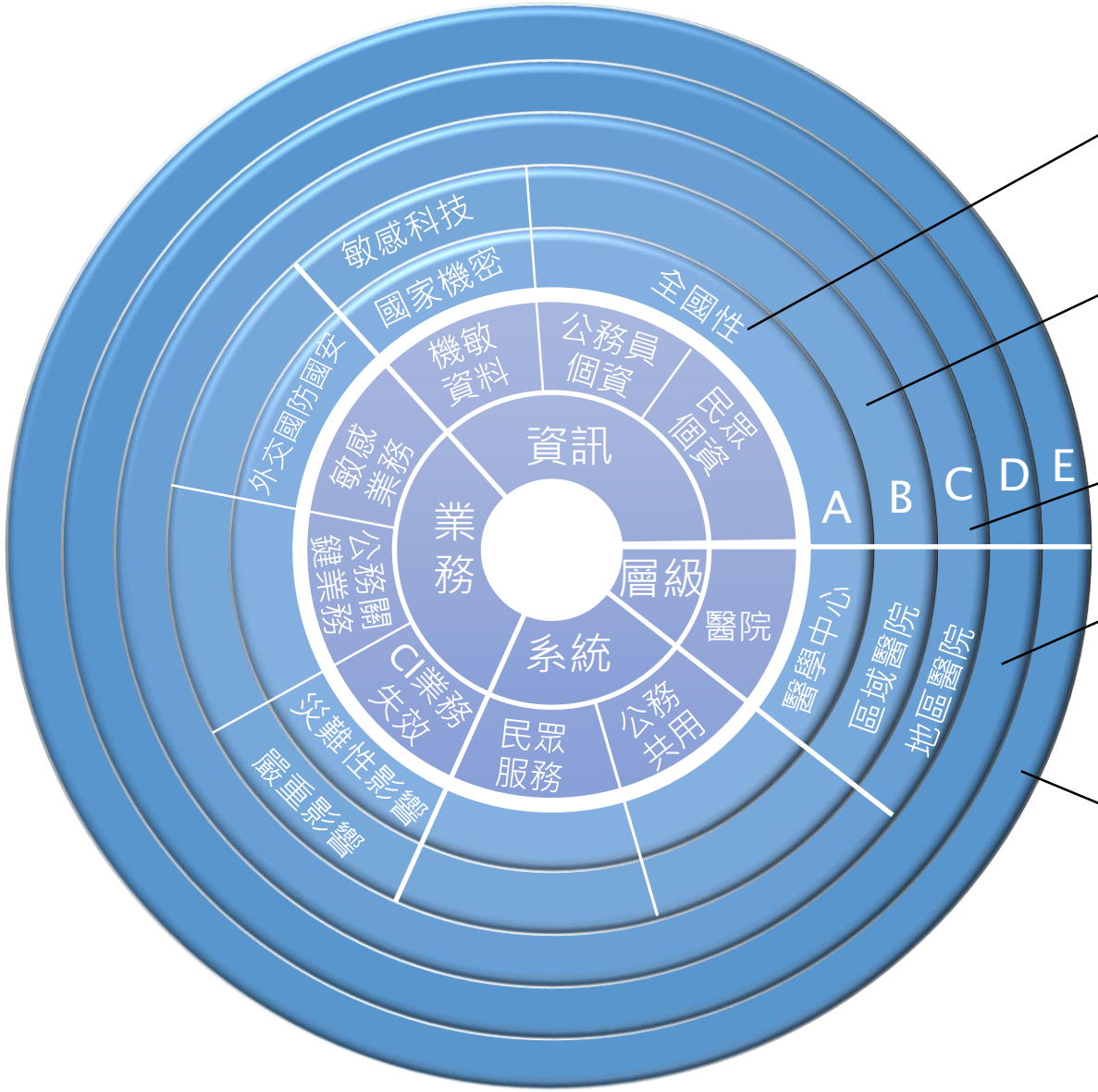
資通安全責任等級分級辦法

- 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



考量因素

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

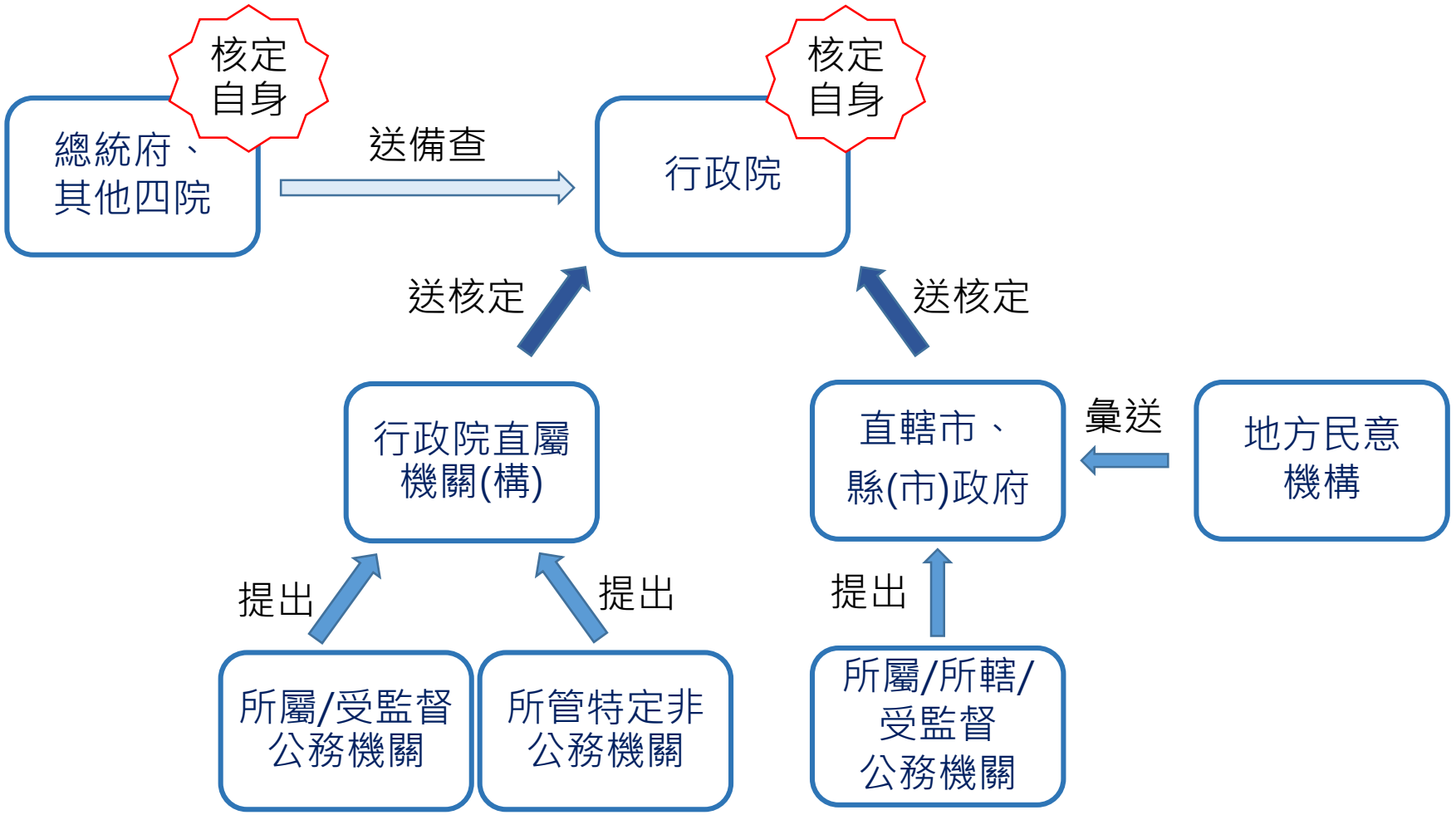
C級：有自行或委外發資訊系統，並設置伺服器者

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

本次調修重點

責任等級
新增E級

不具資通系統且不提供資通服務，或全部資訊業務由其他機關兼辦或代管者
(第8條)

責任等級
分級原則

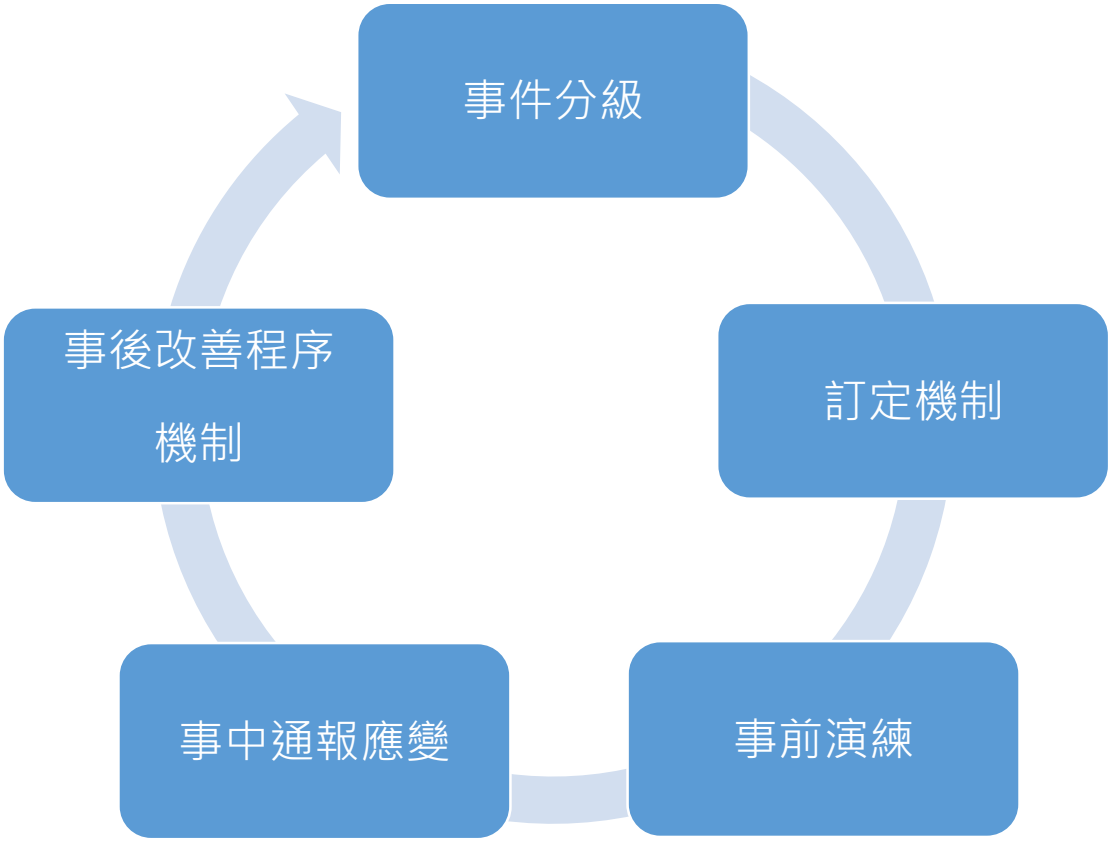
調修責任等級A,B,C,D 級判斷標準
(第4~7條，第10條)

應辦事項
調修

詳附表一至附表九

資通安全事件通報及應變辦法

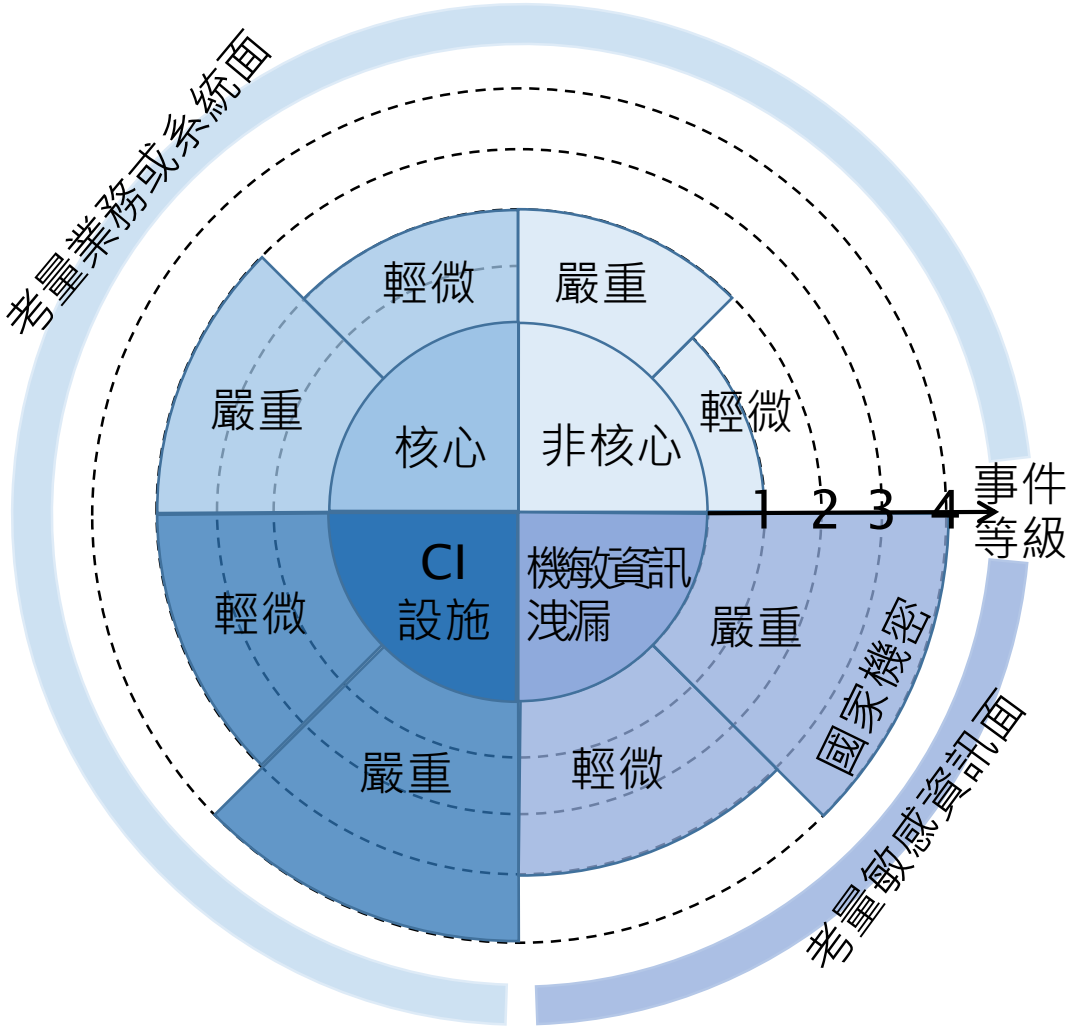
- 為強化各機關之資安事件之因應。
- 規範事件之分級、事前演練、事中通報及應變，以及事後改善之程序、機制。



資安事件定義

- 資通安全管理法第3條第4款：
  - 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

資通安全事件分級

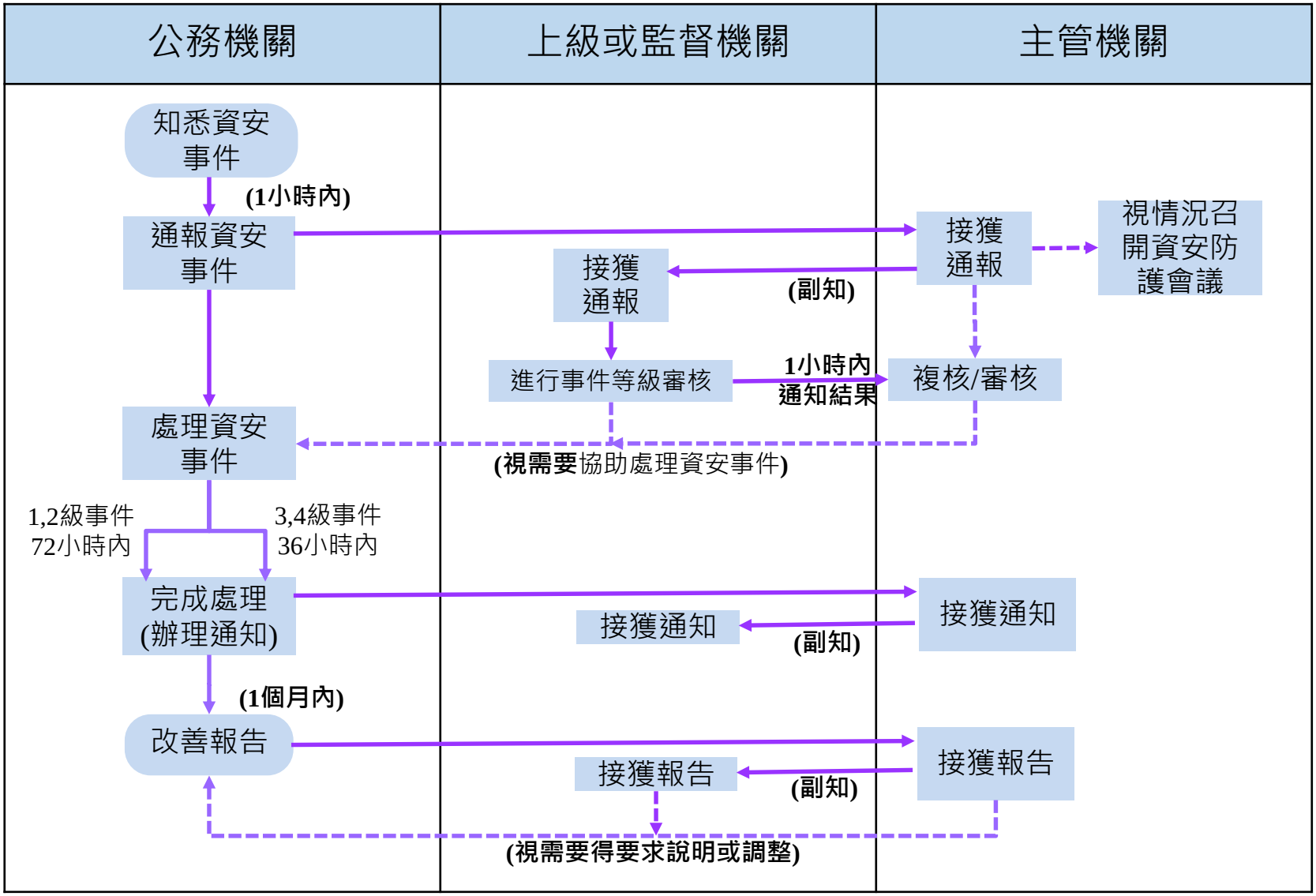


事件輕微或嚴重–考慮C,I,A三面向

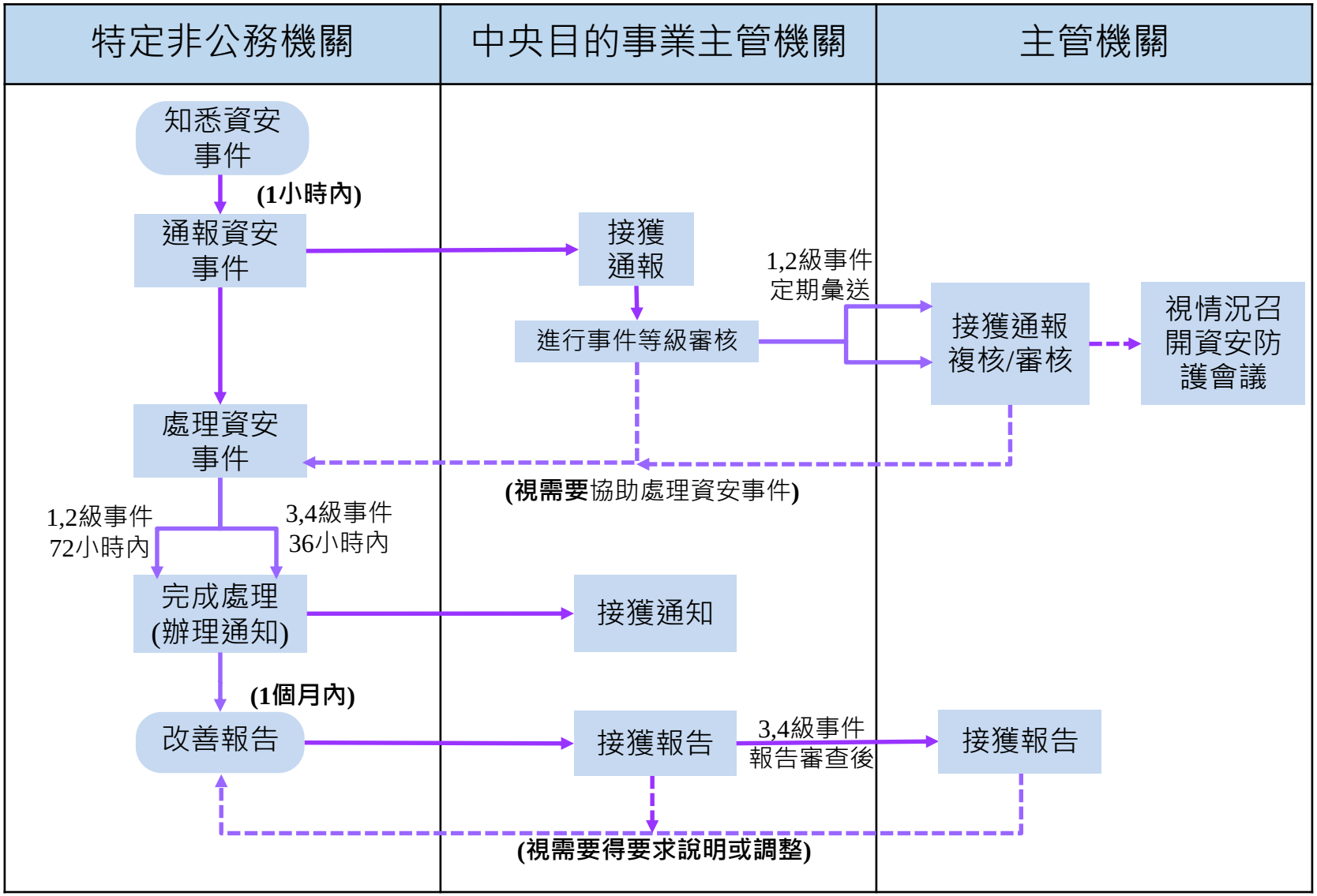
- 機密性
  - 業務資訊遭洩漏
- 完整性
  - 業務資訊遭竄改
  - 資通系統遭竄改
- 可用性
  - 資訊系統受影響或停頓，是否於可接受時間內回復

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



本次調修重點

事件等級判斷標準

調整1到4級事件判斷標準(第2條)

公務機關事件等級審核機制

調整直轄市、縣(市)政府應協助鄉(鎮、市、區)公所及民代表會，進行事件等級審核(第5條第2項)

公務機關資安演練

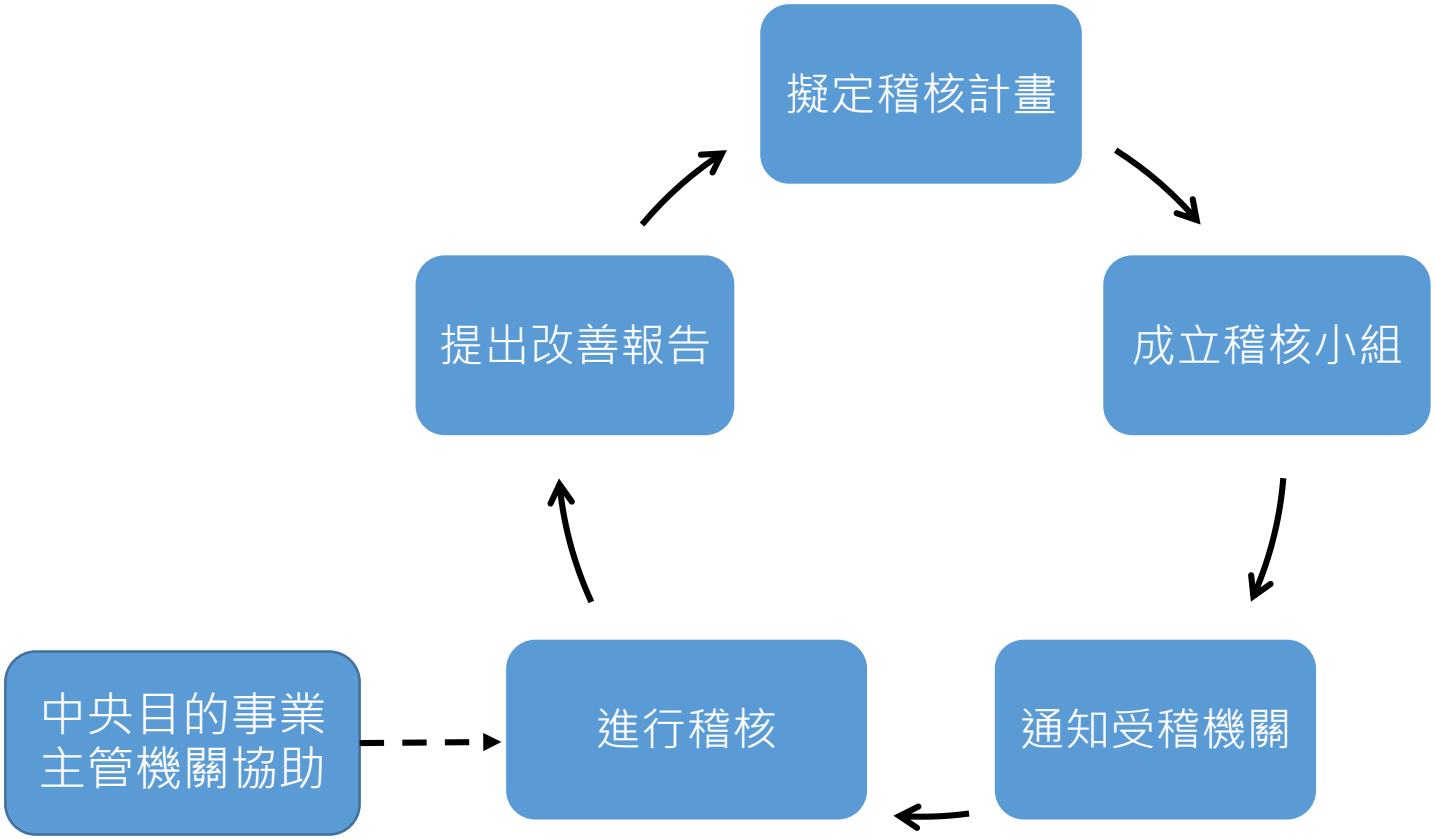
調整直轄市、縣(市)政府應協助鄉(鎮、市、區)公所及民代表會，進行資安演練(第8條)

主管機關辦理資安演練

區分公務機關及特定非公務機關，演練項目不同(第18、19條)

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

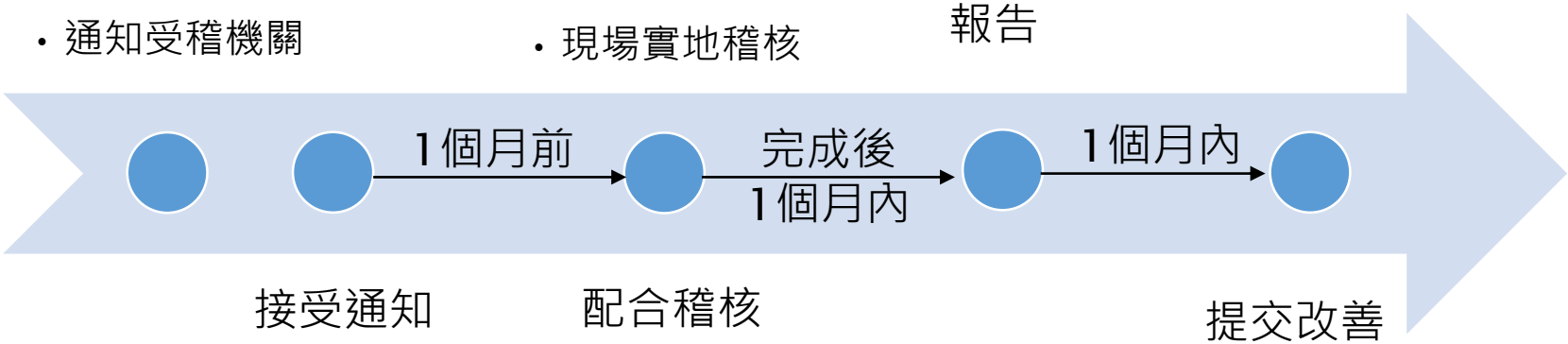
擬定稽核計畫

- 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



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

本次調修重點

稽核計畫通知

受稽機關如因業務或其他正當理由，得於收受通知後5日內，以書面敘明理由申請調整稽核日期(第4條第2項)

稽核進行方式

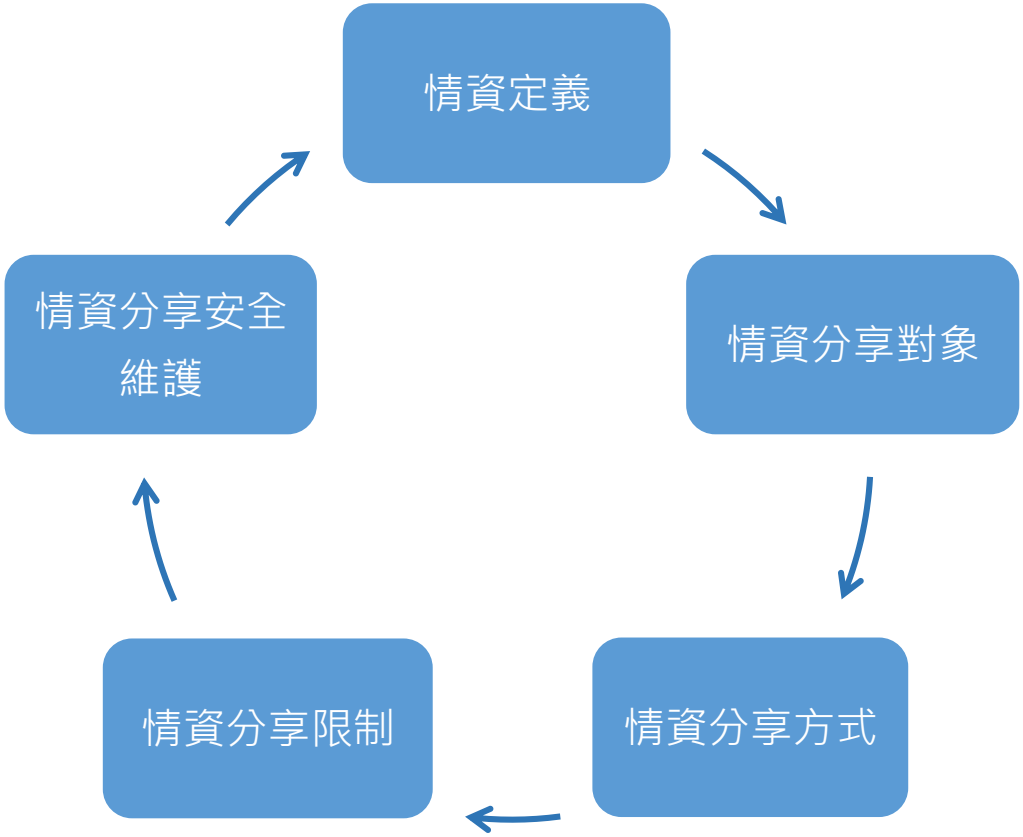
調整為兩階段進行，相關文件或證明資料改由現場提供(第5條)

稽核報告

主管機關於每季所定稽核作業完成後，交付稽核報告 (第7條)

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

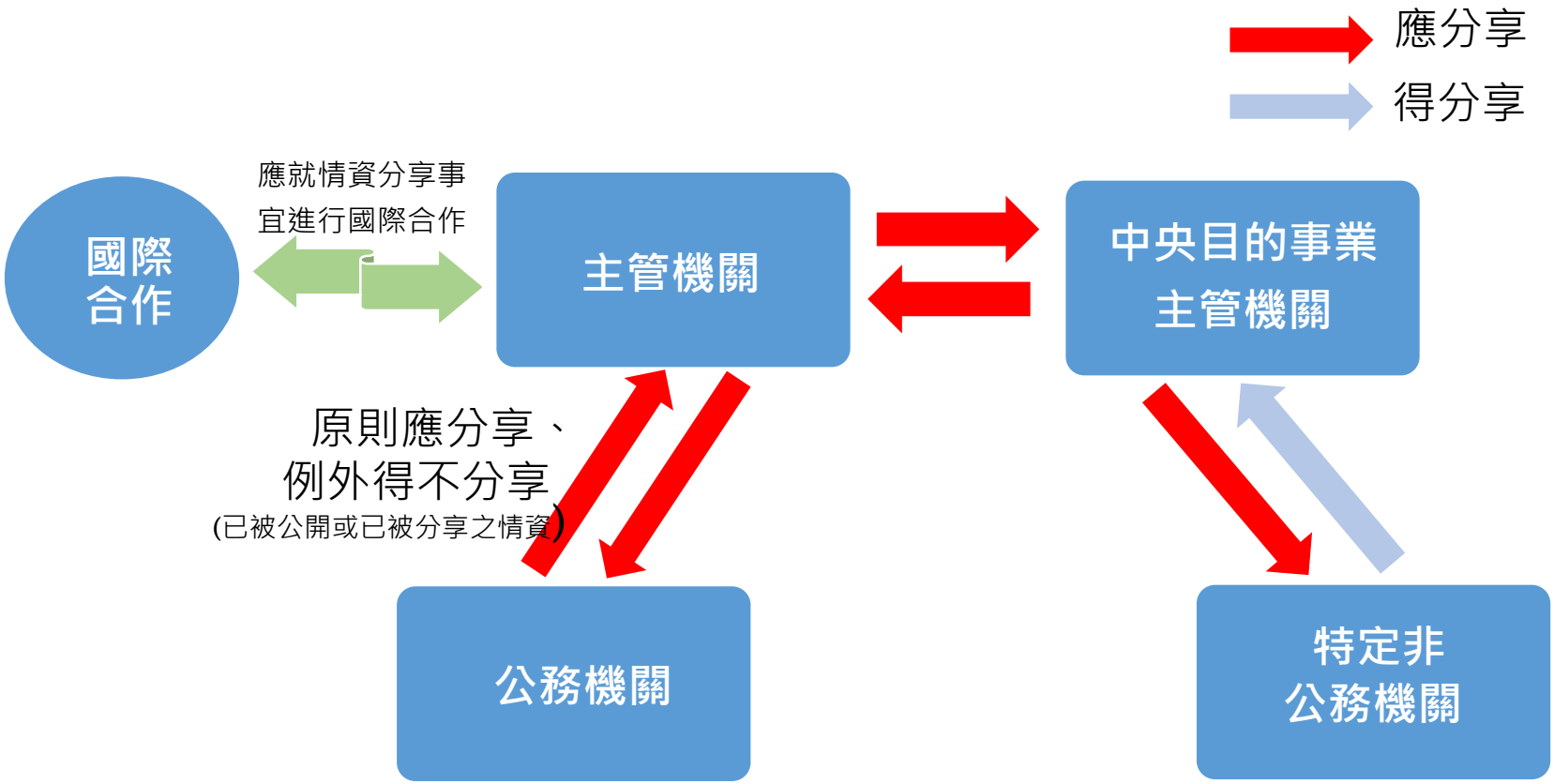
情資定義

情資分享例外

- 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

本次調修重點

情資分享之例外

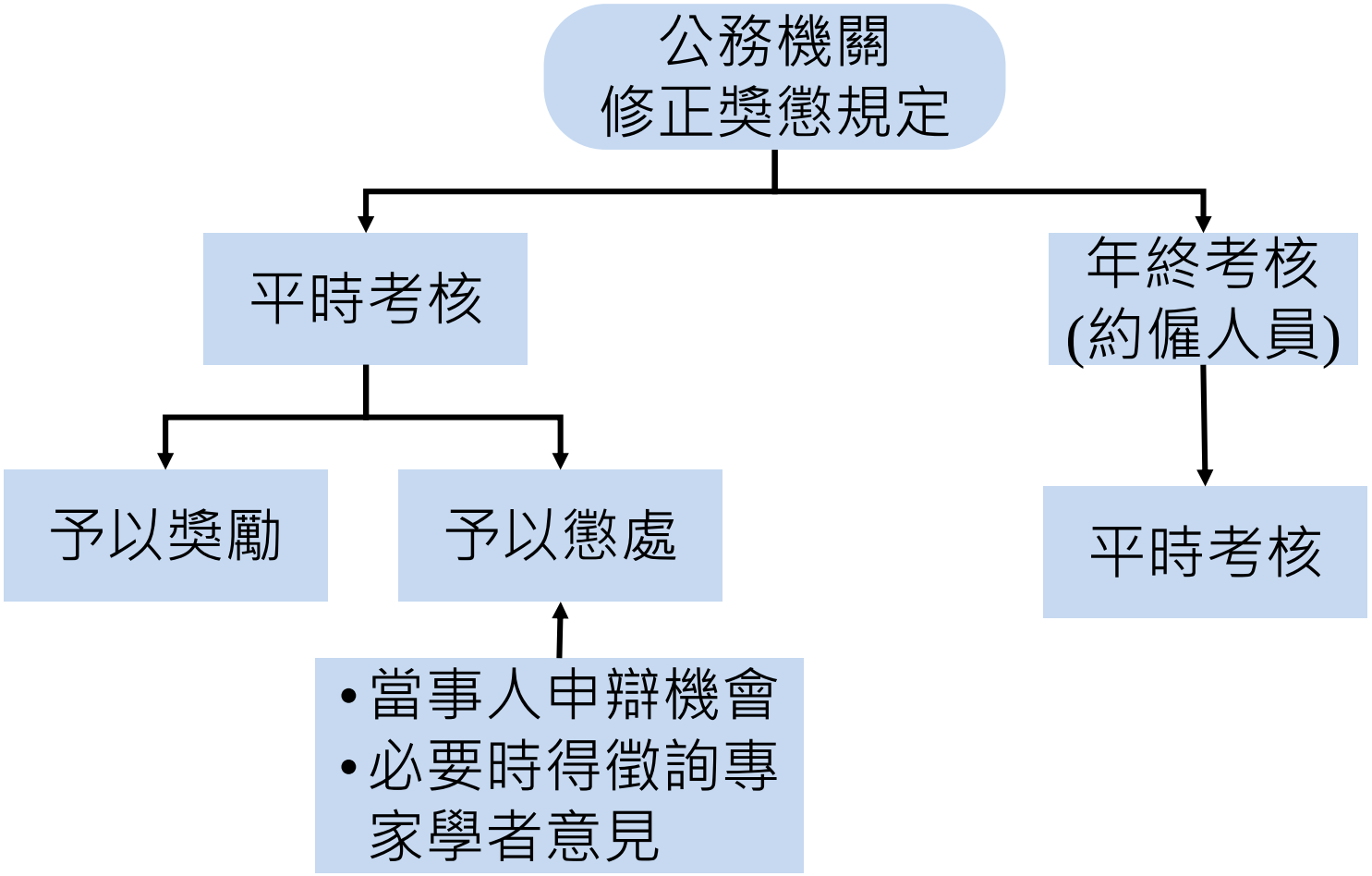
調修情資分享之例外規定
(第4條)

情資之保護機制

調整情資分享及收受情資應進行之保護機制
(第5、6條)

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



本次調修重點

機關自定獎懲基準	獎勵項目	懲處項目	申辯及意見徵詢	約聘僱人員適用
機關應依本辦法規定自行訂定獎懲基準(額度)，並報請上級機關備查或報請銓述部核備(第2條)	調整獎勵項目(第3條)	調整懲處項目(第4條)	機關作成懲處前，應給予當事人申辯之機會，必要時得就所涉資安事項，徵詢專家學者意見(第7條)	約聘僱人員之考核亦應審酌獎勵及懲處情形，並納入續聘之參考(第6條)

大綱

一、資通安全管理法架構

二、子法草案規範內容

三、整備作業

整備重點

納管機關

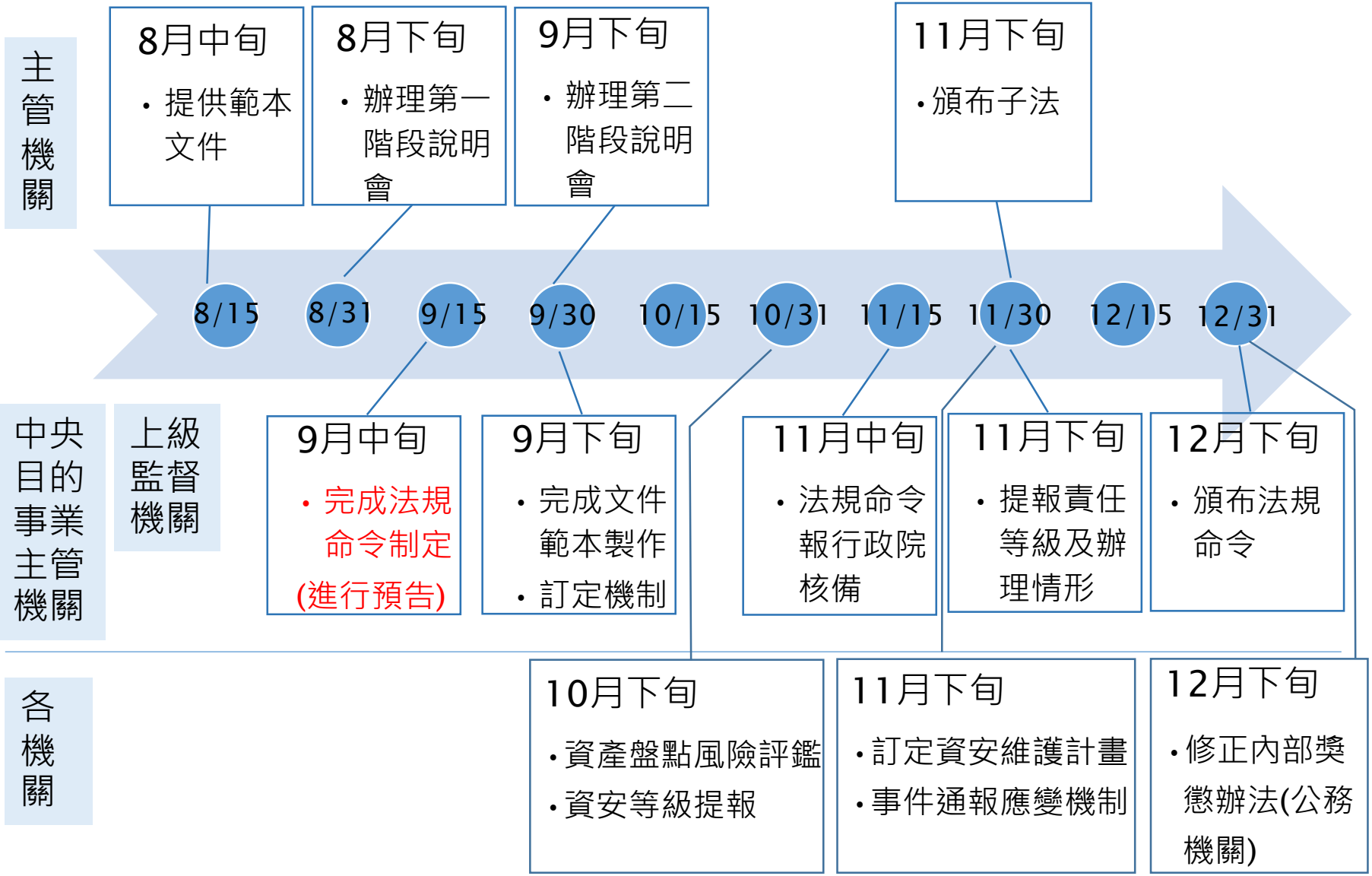
- 資產盤點
- 風險評鑑
- 機關資安責任等級
- 資安維護計畫、通報應變機制文件擬具
- 資安防護基準遵循

上級、監督機關或中央目的事業主管機關

- 行政規則註1或法規命令訂定註2
- 自身及所屬機關構資安責任等級核定
- 資安維護計畫、通報應變機制文件範本提供註3
- 所轄管機關協助

註1：指上級、監督機關須針對所轄公務機關，就稽核作業訂定相關行政規則(依據母法第13條說明)
註2：指中央目的事業主管機關須針對所轄特定非公務機關，就資通安全維護計畫等應遵循事項訂定辦法(法規命令)(依據母法第16條第6項及第17條第4項)
註3：行政院會提供風險評鑑、資安維護計畫、通報應變機制等文件範本供參。

辦理時程(107年)


主管機關
8月中旬
• 提供範本文件
8月下旬
• 辦理第一階段說明會
9月下旬
• 辦理第二階段說明會
11月下旬
• 頒布子法
8/15
8/31
9/15
9/30
10/15
10/31
11/15
11/30
12/15
12/31
中央目的事業主管機關
上級監督機關
9月中旬
• 完成法規命令制定
(進行預告)
9月下旬
• 完成文件範本製作
• 訂定機制
11月中旬
• 法規命令報行政院核備
11月下旬
• 提報責任等級及辦理情形
12月下旬
• 頒布法規命令
各機關
10月下旬
• 資產盤點風險評鑑
• 資安等級提報
11月下旬
• 訂定資安維護計畫
• 事件通報應變機制
12月下旬
• 修正內部獎懲辦法(公務機關)

資安是持續精進的風險管理