資通安全管理法及子法簡介

行政院資通安全處

107年11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

國家資通安全發展方案(106-109年)

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

資通安全法(資安法)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

107.11.21 進行施行前整備

D day 正式施行 子法發布

資安法法案結構

- 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 (如台電)
- 公營事業 (如台糖)
- 政府捐助之財團法人(如工研院)

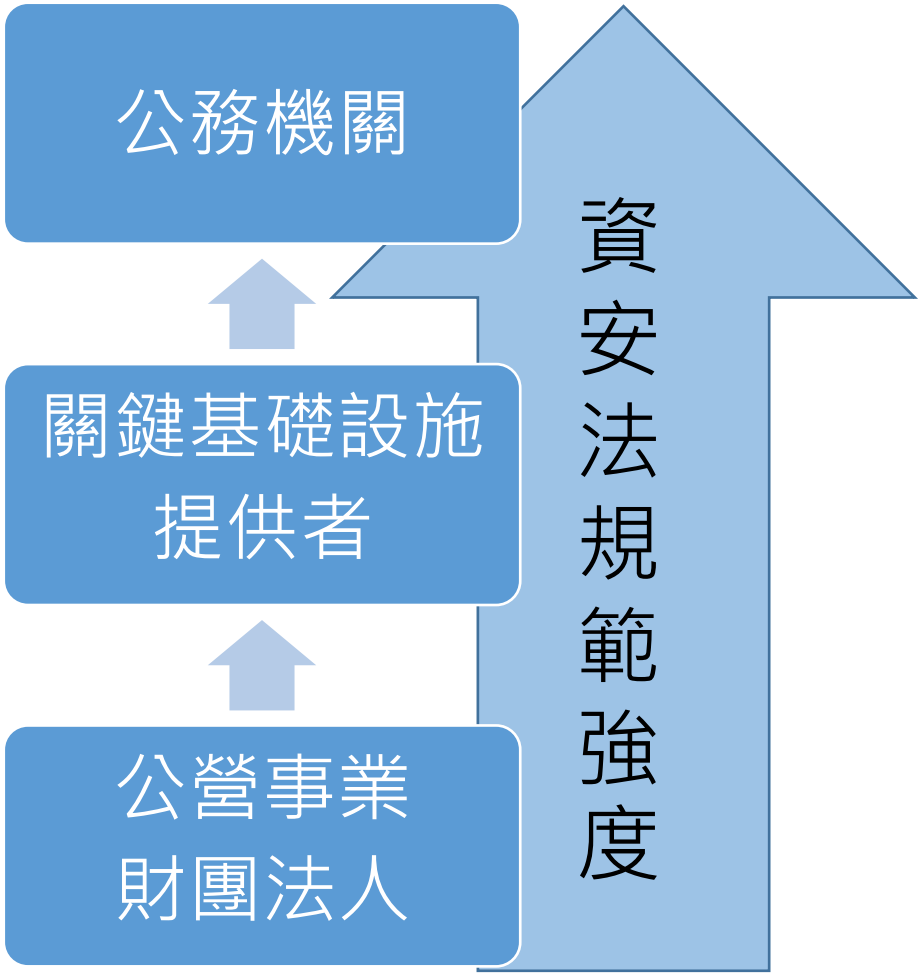
*資安管理法第3條第5款
公務機關：指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。

*資安管理法施行細則第2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、第二項規定之機關。

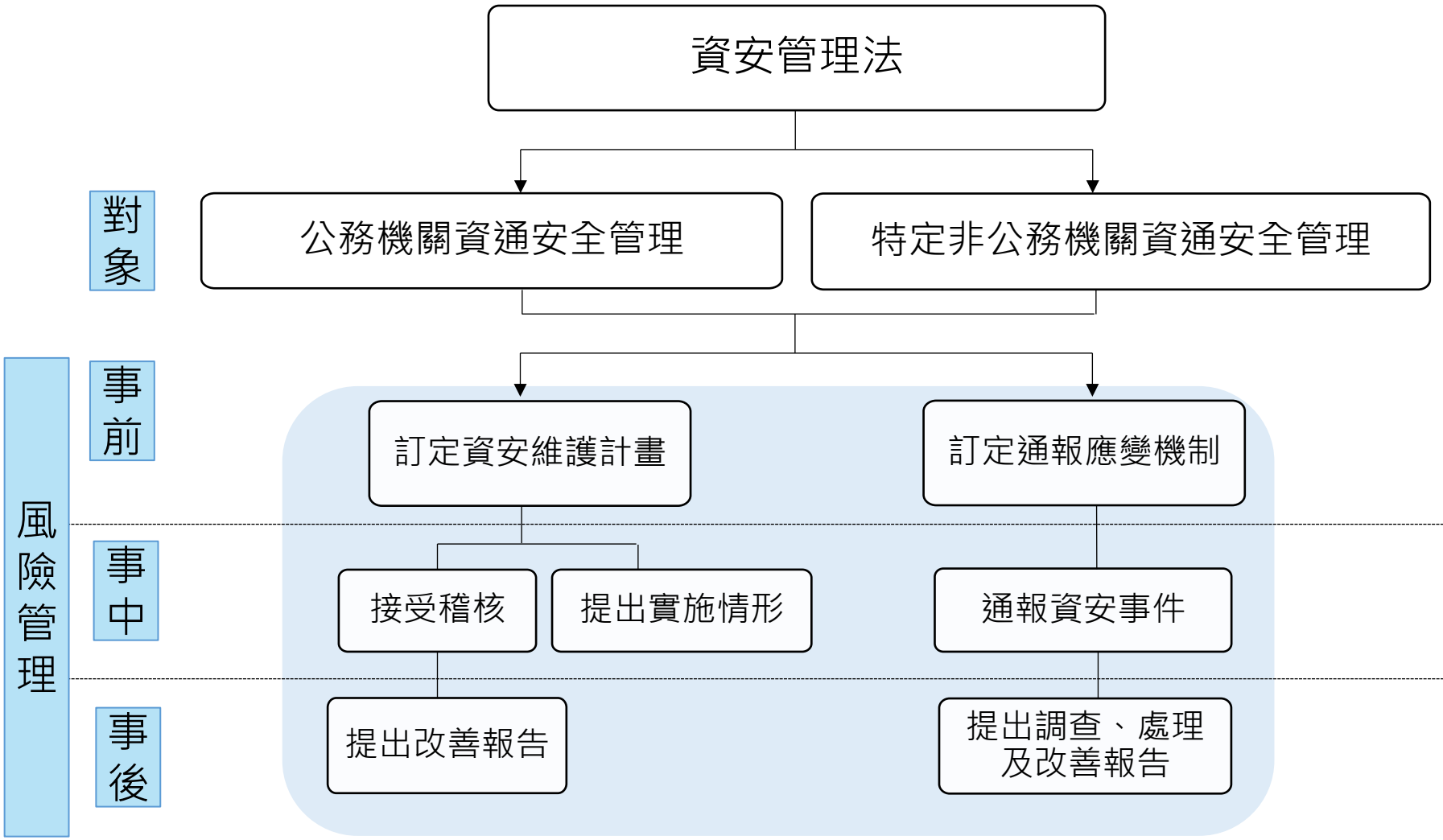
關鍵基礎設施(CI)

本法規範適用先後

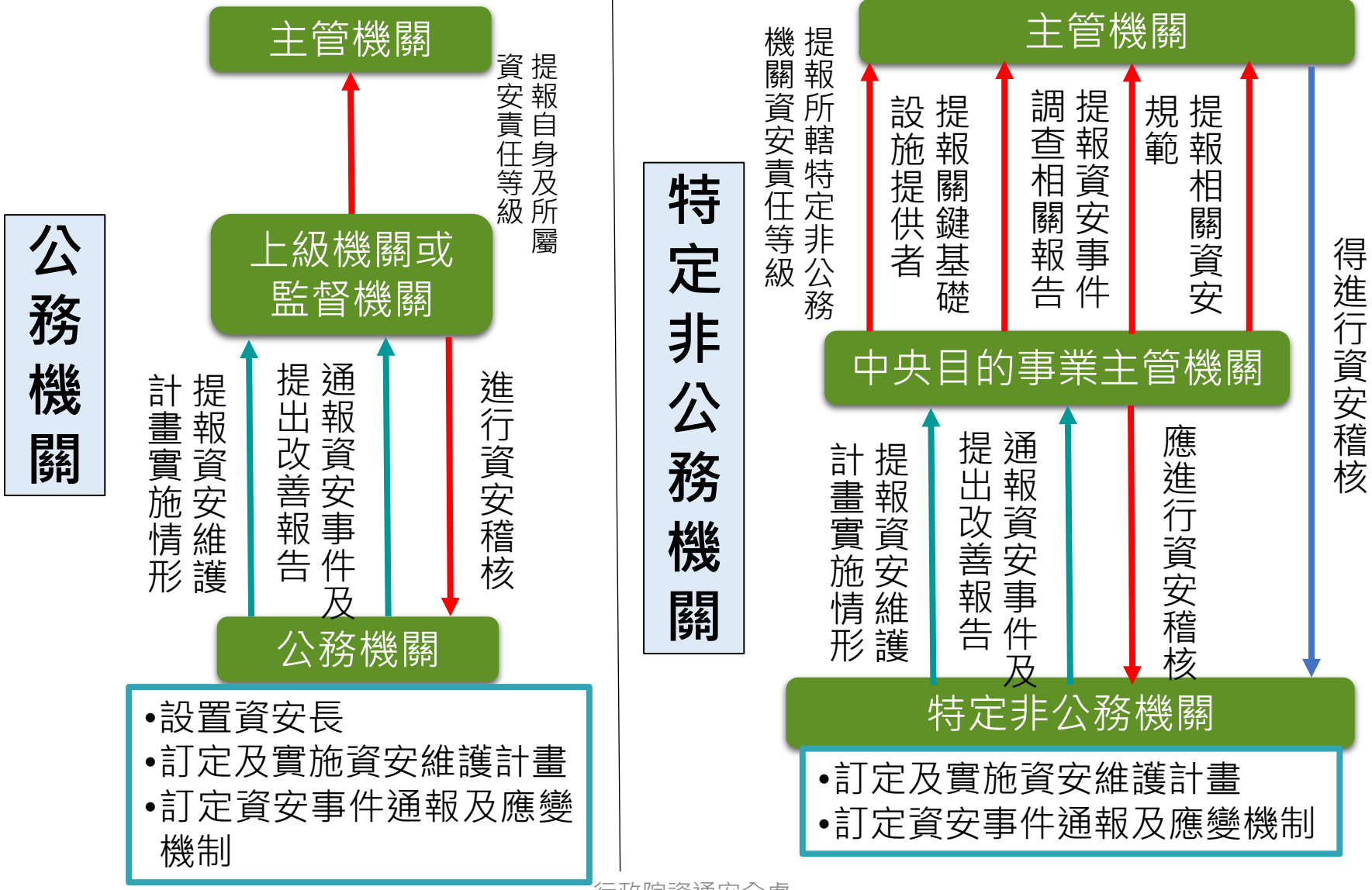
- 兼具公務機關及CI提供者
  - 優先適用公務機關之規定
  - 如：飛航服務總台
- 兼具公營事業/財團法人及CI提供者
  - 優先適用CI提供者之規定
  - 如：台電、中油



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
風險管理
事前
事中
事後
訂定資安維護計畫
訂定通報應變機制
接受稽核
提出實施情形
通報資安事件
提出改善報告
提出調查、處理及改善報告

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

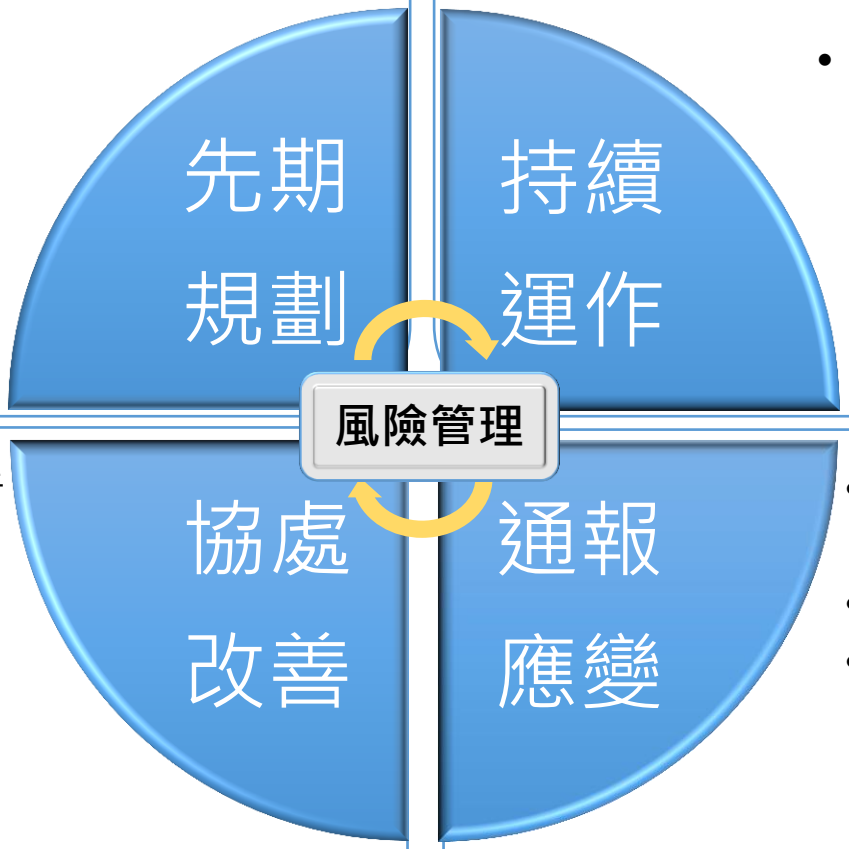
大綱

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

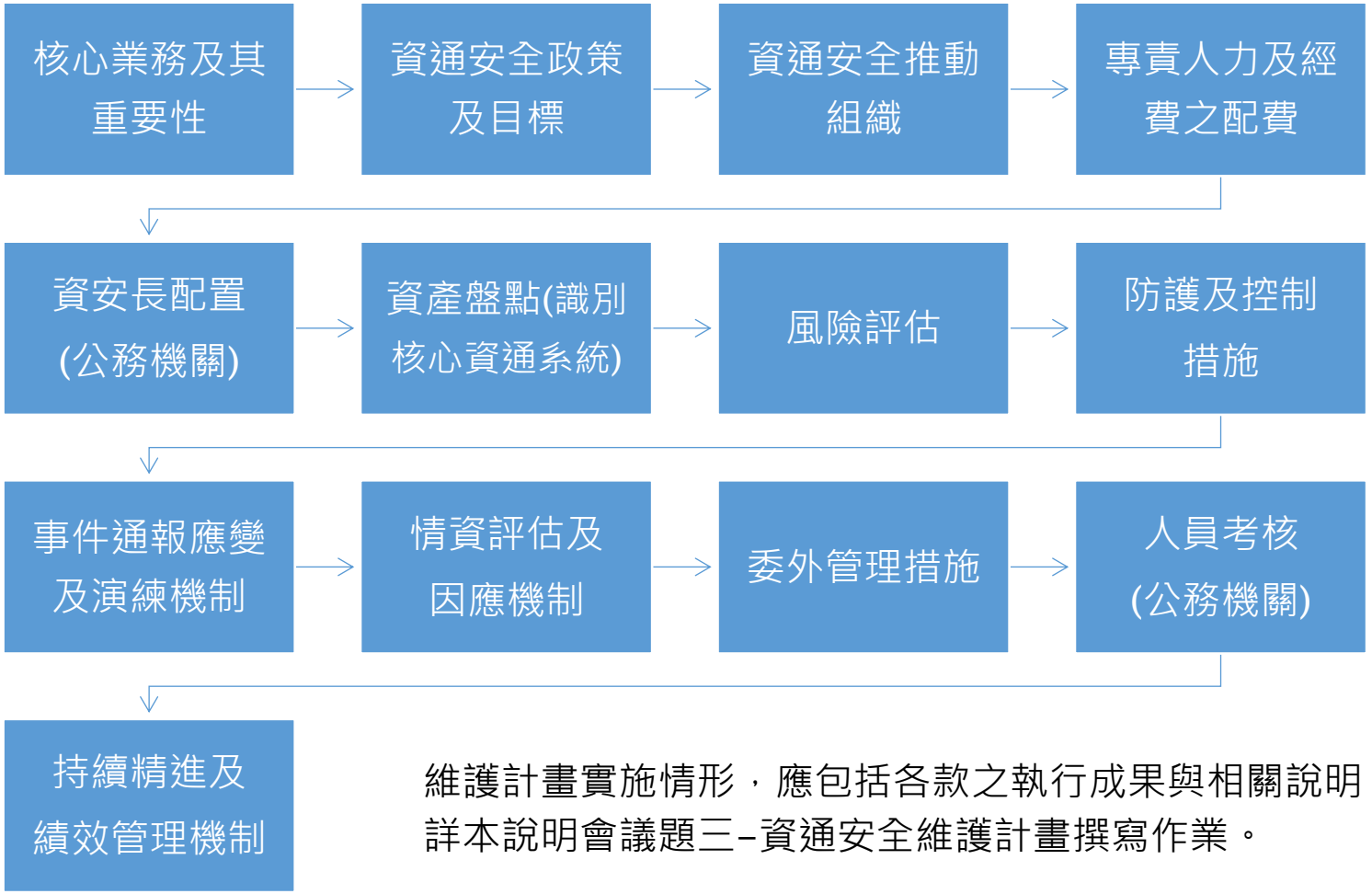
- 訂定資安事件通報應變機制
- 通報資安事件
- 提出事件調查改善報告

  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(13款)



維護計畫實施情形，應包括各款之執行成果與相關說明。
詳本說明會議題三–資通安全維護計畫撰寫作業。

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

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
	事件影響之範圍及損害評估
	損害控制及復原作業之歷程、事件調查及處理作業之歷程
	事件根因分析
	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

常見問題

委外注意事項何時要納入?是否只有增修適用

1. 第4條之規定包括委外之前受託者之選任，以及委外之後受託者之監督，委外開始之前即應開始注意。
2. 資安法施行後, 不論是新開發或是增修，只要有委外就要適用。

客製資通系統開發，是否需第三方安全性檢測

考量個案不同，受託者可自行使用第三方軟體進行安全性檢測。惟如該資通系統屬委託機關之核心資通系統，或委託案件金額在1,000萬元以上，委託機關應自行或另行委託第三方進行安全性檢測。

常見問題

受託者是否必須通過第三方驗證，第三方驗證之範圍

1. 過去資安事件發生的過程當中，有非常多的事件都是來自於委外廠商的管理問題
2. 希望透過規定子法的要求，要求資訊廠商”具備完善的資通安全管理措施”，原則上不一定要通過第三方驗證，但其是一個證明。
3. 第三方驗證的範圍為受託者辦理業務之相關程序和環境。

何謂完善的資通安全管理措施

依委託之項目個案判斷
如應用系統的委外：要考慮廠商的開發環境是否安全，程式的測試資料是否合宜等等
如SOC的監控：考量蒐集的資料是否有做好的管理、好的保護
機關在開規格標時，即可將要求的事項列入，或評選標時納入評分項目中

常見問題

資通安全維護計畫是否可由上級或監督機關訂定

1. 細則第6條末項，針對資通安全維護計畫之訂定、修正、實施和提出，可由上級或監督機關，或中央目的事業主管機關辦理，惟其維護計畫需包含所屬或所管之特定非公務機關。(詳§6III)
2. 亦可以提供範本方式協助所屬或所管特定非公務機關適用。

核心資通系統定義

1. 公務機關–依其組織法規，足認其核心權責所在
2. 特定非公務機關–主要服務各功能
3. 各機關–維運、提供CI設施所必要之業務
4. 各機關依資通安全責任等級分級辦法涉及A、B級機關之業務。

資通安全責任等級分級辦法

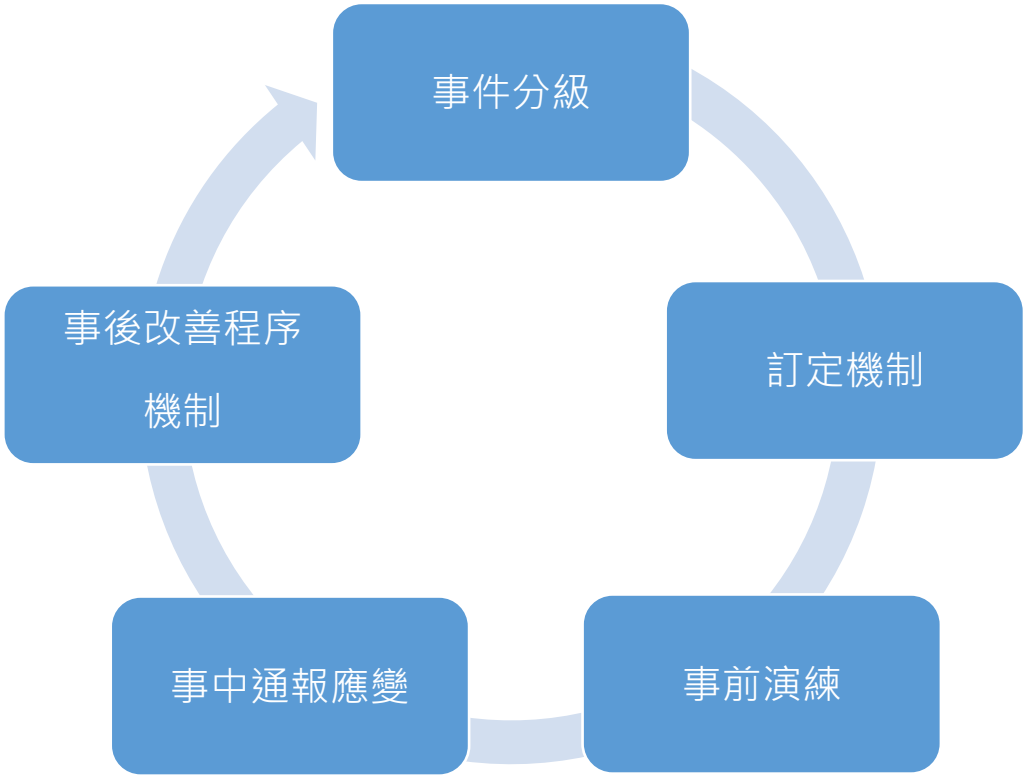
- 機關應考量其業務、資訊、系統、機關層級等因素訂定機關資安責任等級。
- 後續依該責任等級辦理相對應之應辦事項

考量因素

詳本說明會議題二–資安全責任等級分級及應辦事項說明。

資通安全事件通報及應變辦法

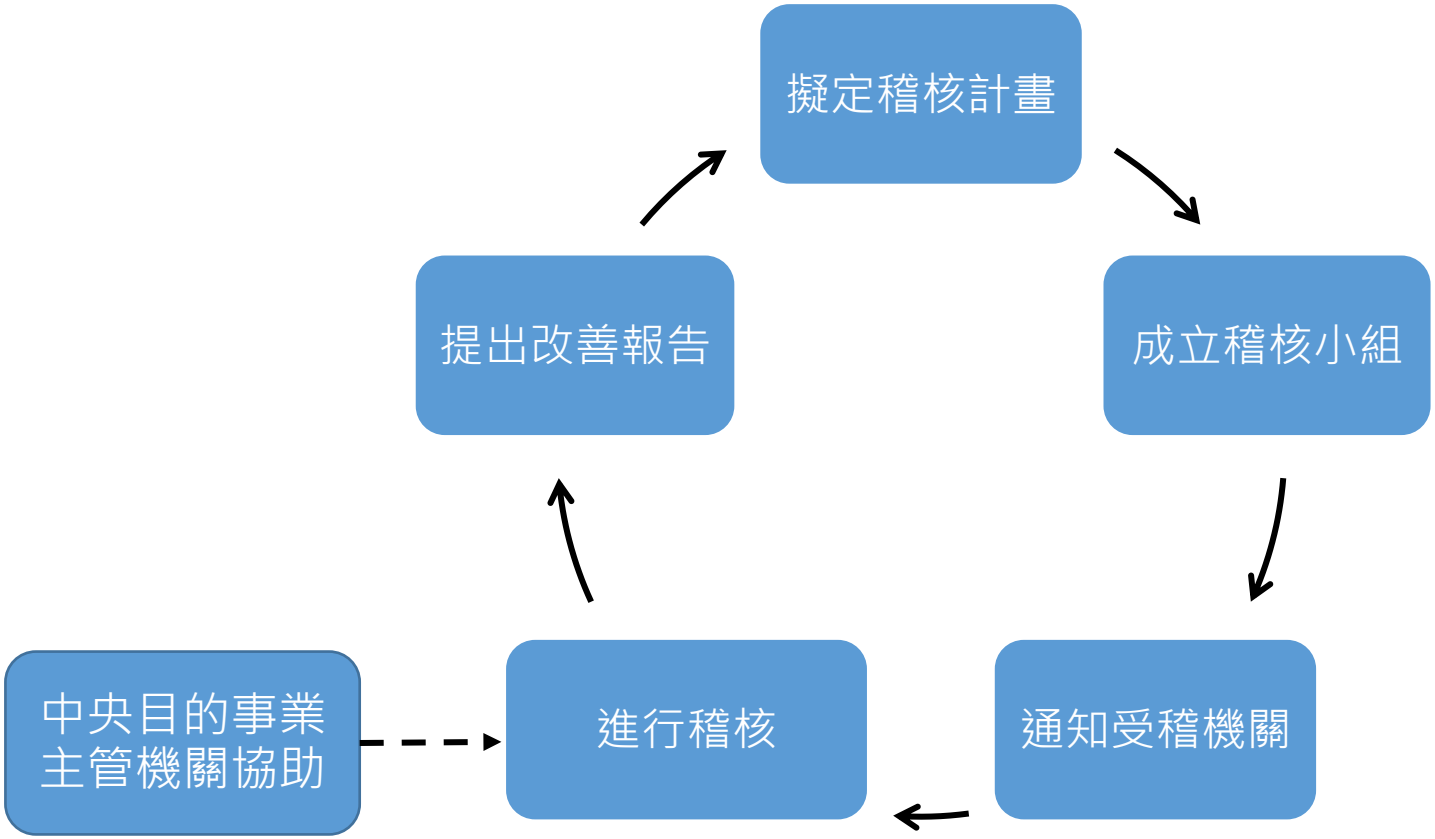
- 為強化各機關之資安事件之因應。
- 規範事件之分級、事前演練、事中通報及應變，以及事後改善之程序、機制。



詳本說明會議題四–資通安全事件通報、應變與演練實務。

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。



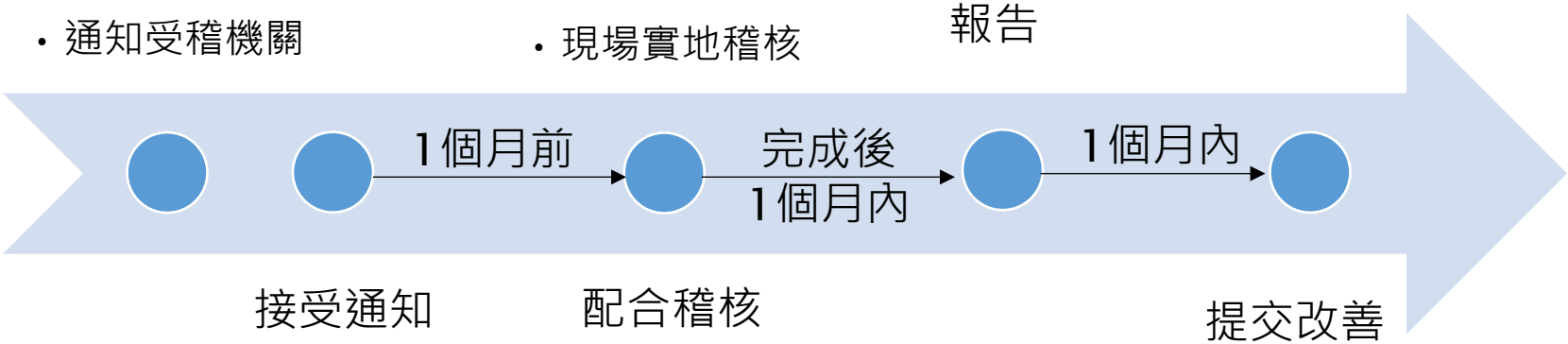
稽核程序

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
- 稽核前訪談
- 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

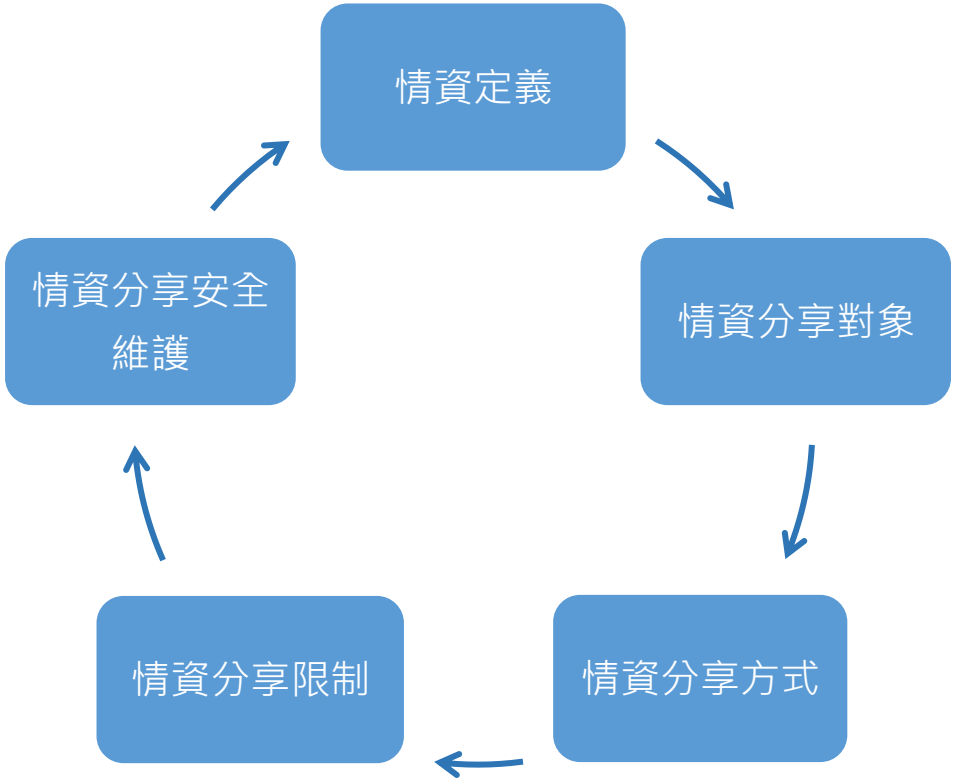
提交改善報告

中央目的事業主管機關

視主管機關需求派員為必要協助

資通安全情資分享辦法

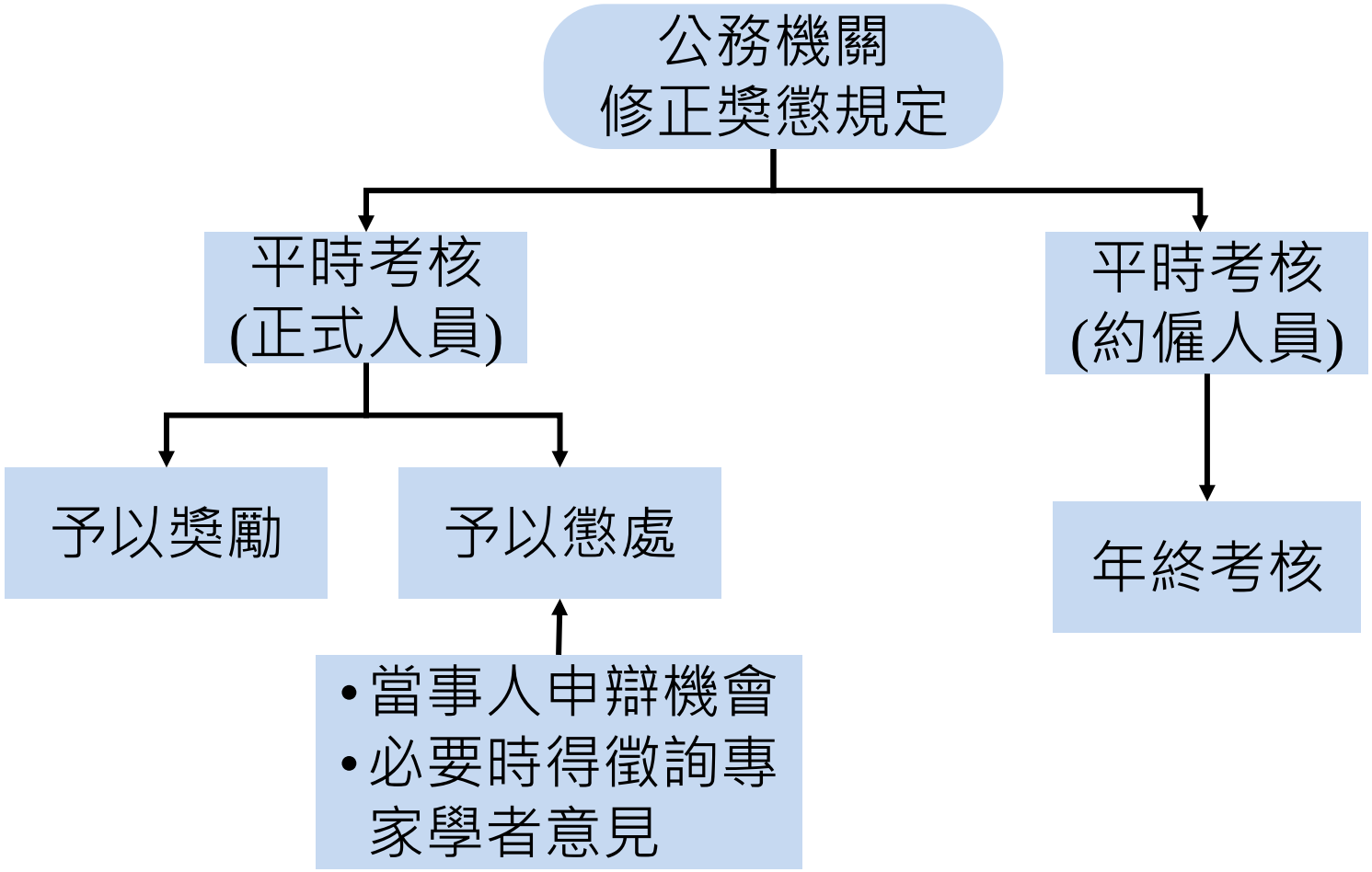
- 提升各機關對於資安之預警能力，強化資安相關資訊之交流。



詳本說明會議題五–資通安全情資分享實務。

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



公務機關所屬人員資通安全事項獎懲辦法

➢ 獎勵項目

- 訂定、修正及實施資通安全維護計畫，績效優良
- 稽核所屬或辦理資通安全演練作業，績效優良。
- 配合主管機關、上級或監督機關辦理稽核或資通安全演練作業，經評定績效優良。
- 積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。
- 辦理其他資通安全業務有具體功績。

(其餘可參考獎懲辦法第3條，共有12款事宜)

➢ 懲處項目

- 未依本法、本法授權訂定之法規或機關內部規範辦理資通安全管理事項(維護計畫、事件通報應變、稽核、情資分享)，情節重大。
- 辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。
- 其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

常見問題

機關是否需定訂定獎懲辦法

獎懲辦法裡面只有規定獎勵的項目跟懲處的項目，機關必須要修正既有的人事規定，訂定各項獎懲的額度，與辦法接軌

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

各機關作業建議

落實資安宣導
- 機關內資安意識宣導
- 資安相關獎懲規定

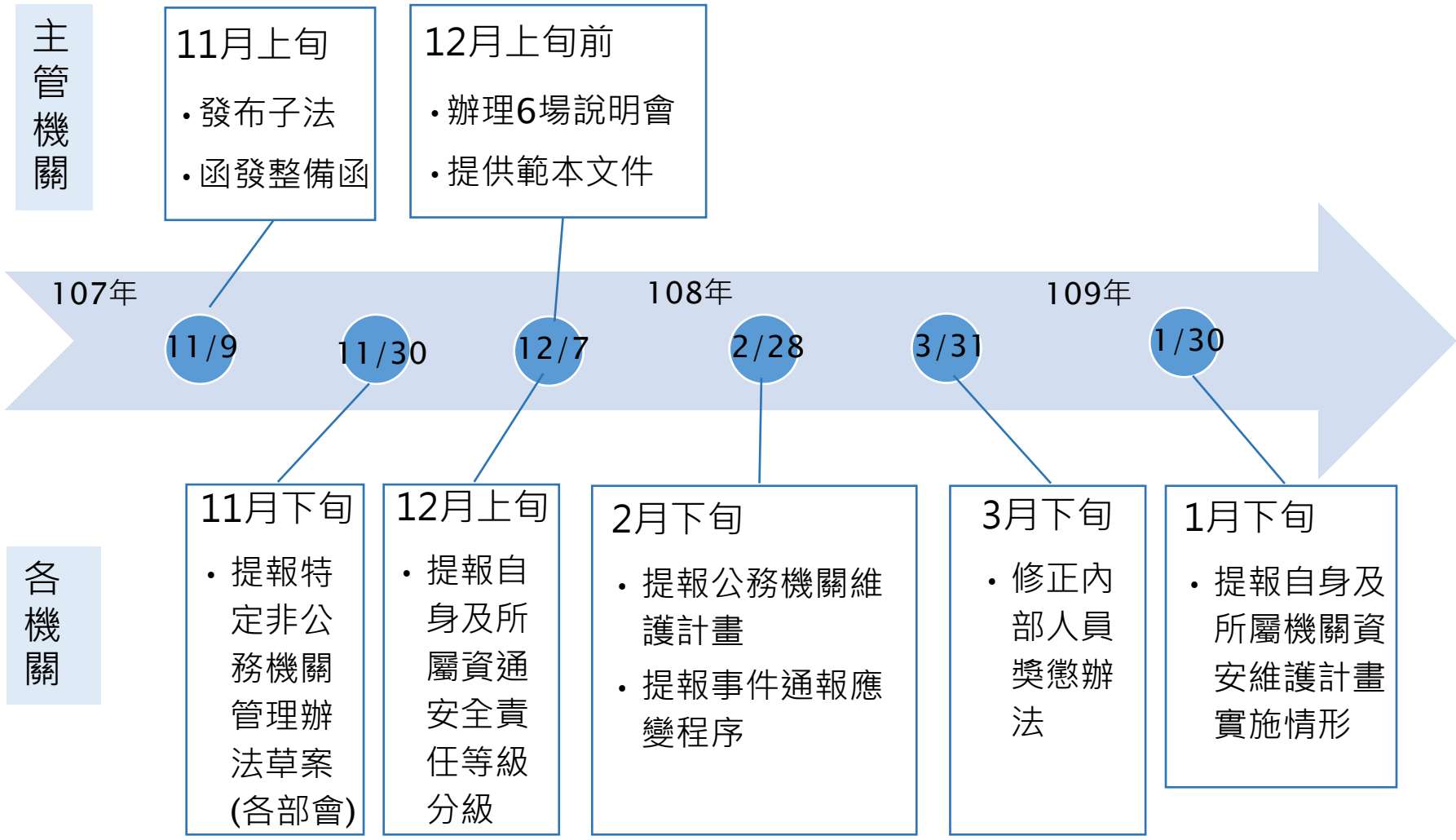
內部資安規範與本法之接軌
- 機關內資安作業流程與規定之銜接
- 人員獎懲規定之銜接

提升資安人員質與量
- 重新檢視資安人力適足性
- 指定資安專職、專責人力
- 提升資安人員之職能

檢視資安推動組織之組成
- 組成跨機關內部單位及所屬機關
- 形成與特定非公務機關之公私治理與參與模式

檢視資安預算之適足性

後續施行時程規劃


主管機關
11月上旬
• 發布子法
• 函發整備函
12月上旬前
• 辦理6場說明會
• 提供範本文件
107年
108年
109年
11/9
11/30
12/7
2/28
3/31
1/30
各機關
11月下旬
• 提報特定非公務機關管理辦法草案(各部會)
12月上旬
• 提報自身及所屬資通安全責任等級分級
2月下旬
• 提報公務機關維護計畫
• 提報事件通報應變程序
3月下旬
• 修正內部人員獎懲辦法
1月下旬
• 提報自身及所屬機關資安維護計畫實施情形

資安是持續精進的風險管理