教育體系因應
資通安全管理法之規劃說明

教育部資訊及科技教育司

108年1月21日

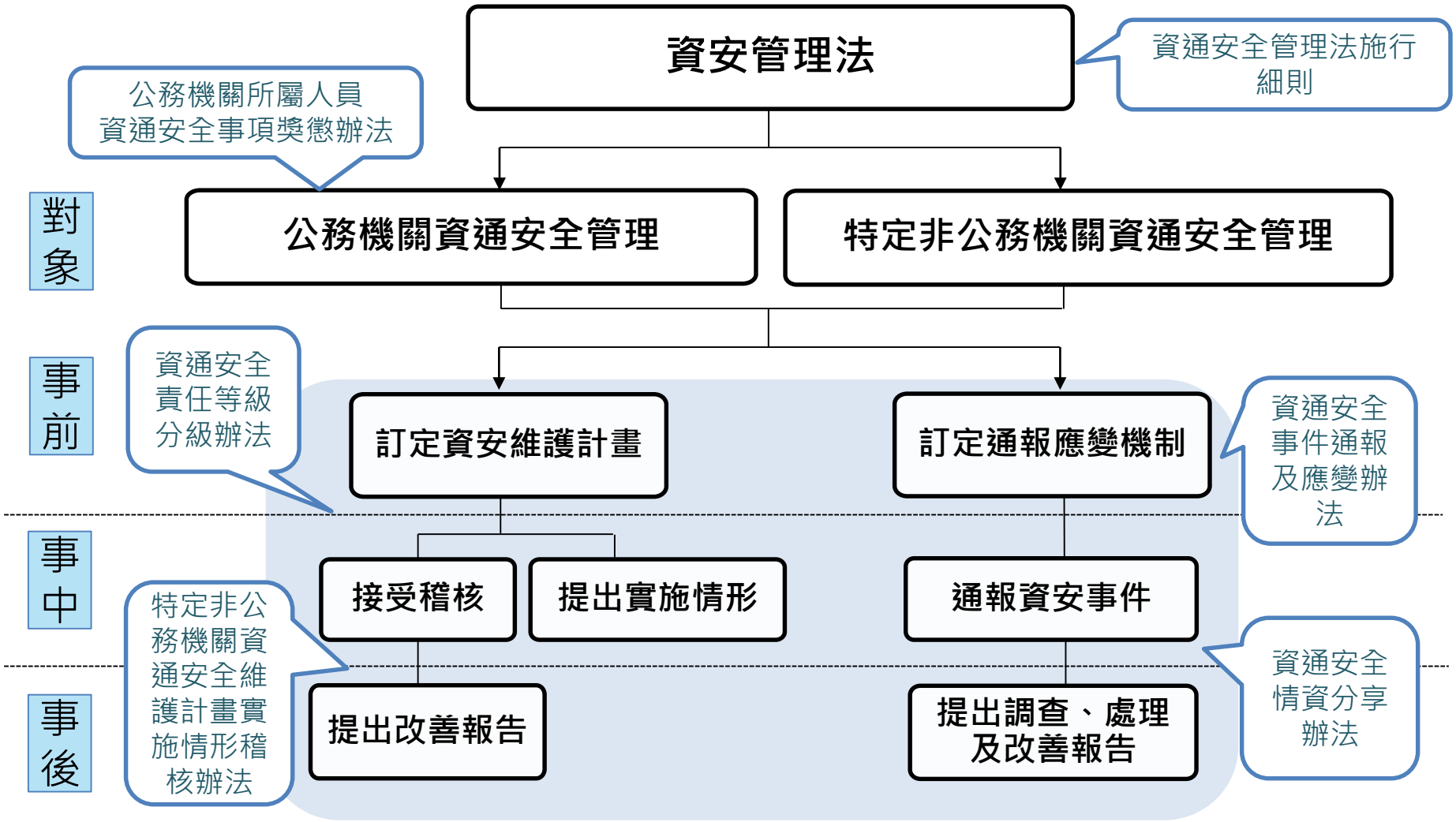
簡報大綱

- 資通安全管理法
- 資通安全責任等級
- 資通安全維護計畫
- 資通安全通報及應變

資通安全管理法

- 總統107年6月6日公布**資通安全管理法**。
- 行政院107年11月21日發布相關子法：
  - 資通安全管理法施行細則
  - **資通安全責任等級分級辦法**
  - **資通安全事件通報及應變辦法**
  - 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
- 行政院107年12月05日函定自**108年1月1日施行**。

資通安全管理法架構


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

資通安全管理法規範對象

公務機關

- 依法行使公權力之中央、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

教育體系規範對象

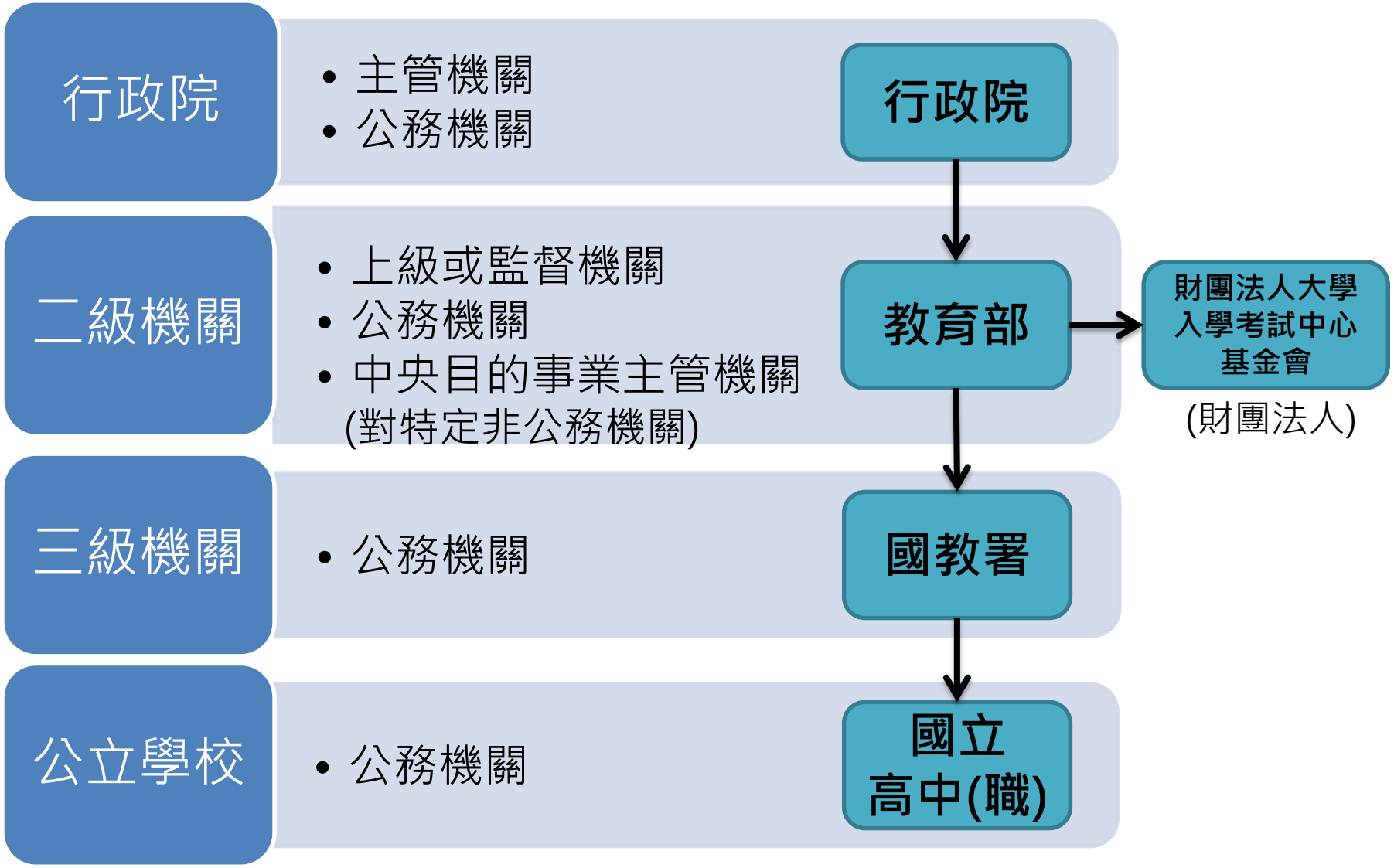
公務機關

- 教育部及所屬機關構
- 各級公立學校
- 試務機構
- 國家運動訓練中心

特定非公務機關

- 關鍵基礎設施提供者
- 政府捐助之財團法人

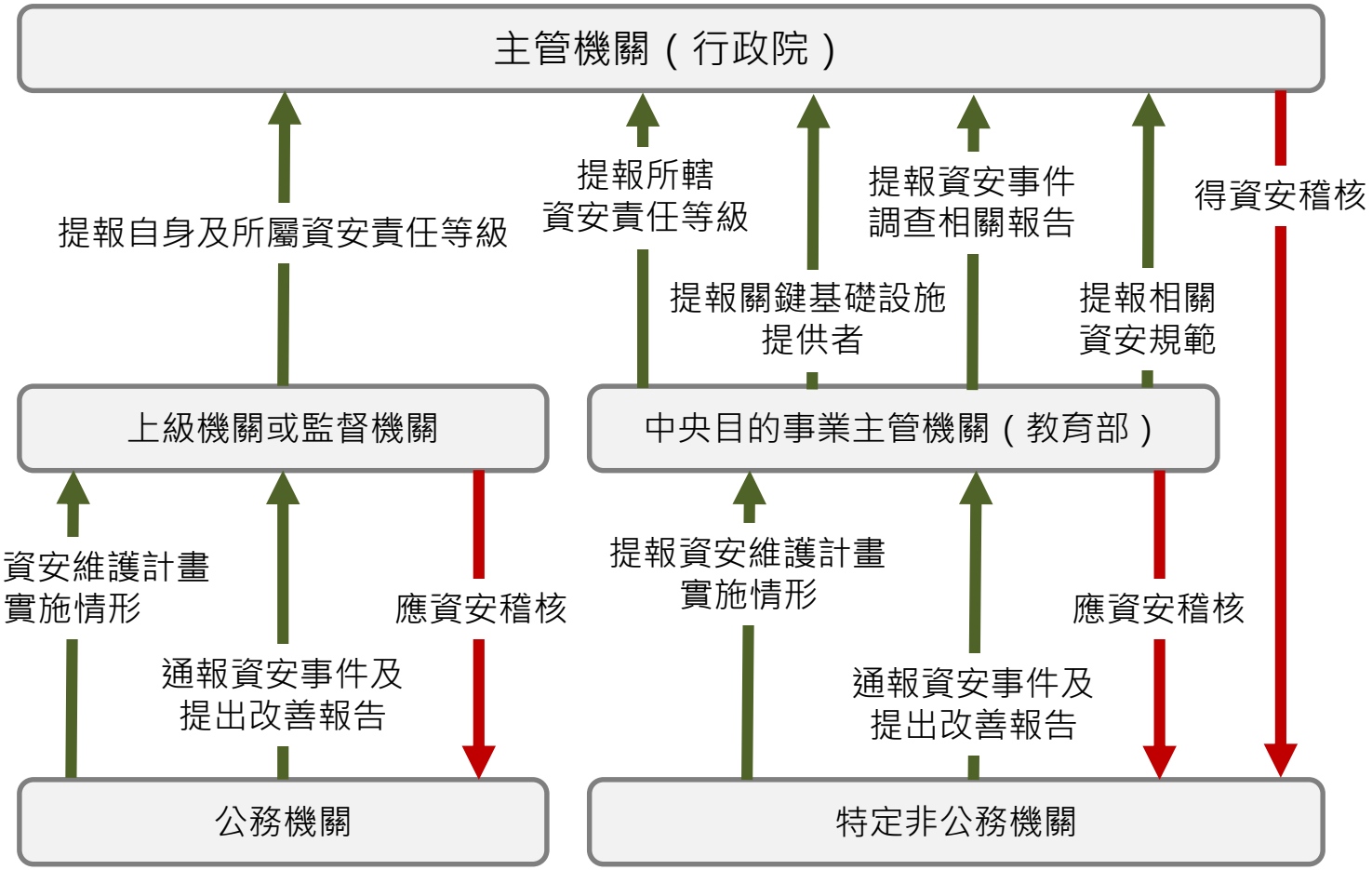
中央政府機關於本法之角色



地方政府機關於本法之角色

行政院	• 主管機關 • 公務機關	行政院
地方政府	• 上級或監督機關 • 公務機關	新北市政府
一級機關	• 公務機關	教育局
公立學校	• 公務機關	市立國中小

角色與權責



- 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

- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

資通安全責任等級

教育體系等級提交機關

- **提交機關**應每2年提交所屬責任等級，報行政院核定。
  - 教育部(行政院直屬機關)
    - 部屬機關、機構
    - 國立大專校院
    - 國立高級中等以下學校(由國教署負責)
    - 教育部主管政府捐助之財團法人
  - 各直轄市、縣（市）政府
    - 縣(市)立各級學校

- 資通安全責任等級分級辦法第3條

教育體系資安責任等級分級原則

	A級	B級	C級	D級
業務個資	■教育部 ■承接敏感業務、研究學校	■公立大專校院		
資通系統		■國家教育研究院 ■國家圖書館	■部屬機構(電台、博物館、圖書館) ■國家運動訓練中心 ■公立高級中等以下學校(有核心資通系統)	■公立高級中等以下學校(已向上集中無維運核心資通系統，無機房或僅設置通訊機房)
機關層級	■大學附設醫院(醫學中心)	■大學附設醫院(區域、地區醫院)		

*__核心資通系統__指依「資通安全管理法施行細則」第7條第2項：

- 支持各校「__核心業務__」持續運作必要之系統。
- 依分級辦法附表九「資通系統防護需求分級原則」，資通系統判定其防護需求等級為高者。

分級作業辦法應辦事項-管理面

辦理事項	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內		2年內
ISMS之導入及通過公正第三方之驗證	2年內全部核心資通系統導入資訊安全管理系統。	3年內完成第三方驗證；並持續維持期驗證有效性。		O*
業務持續運作演練	全部核心資通系統	每年1次	每2年1次	
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專職(責)人員（1年內）		4人	2人	1人*
資安治理成熟度評估（公務機關）		每年1次		X

***C級單位因應措施**

- ISMS導入
  - 短期：資科司後續將與國教署協調規劃**輔導團隊**，輔導C級學校導入教版管理規範。
  - 長期：高級中等以下學校全部**核心系統向上集中**為共通系統，將責任等級降至D級。
- 專職(責)人員
  - 短期：本部同意高級中等以下學校得以專責人員配置，兼任資訊行政教師減授教學節數。
  - 長期：國教署配合修正「高級中等學校組織設置及員額編制標準」，資安人力法制化。

分級作業辦法應辦事項-技術面

辦理項目	辦理內容	A	B	C
安全性檢測 全部核心資通系統*	網站安全弱點檢測	每年2次	每年1次	每2年1次
	系統滲透測試	每年1次	每2年1次	
資通安全健診*	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視	每年1次	每2年1次	
資通安全威脅偵測管理機制*	完成威脅偵測機制建置，並持續維運	1年內		X
	依行政院指定方式提交監控管理資料	O	O	X
資通安全防護 （啟用，並持續使用及適時進行軟、硬體之必要更新或升級）	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內		
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆（WAF）	1年內		X
	APT攻擊防禦	1年內	X	
政府組態基準 （GCB）	依主管機關公告之項目，完成GCB導入作業，並持續維運（公務機關）	1年內		X

應辦事項配套措施-技術面

應辦單位	辦理項目	因應措施
A、B、C級	網站安全弱點檢測	由**成功大學網站防護團隊**協助辦理。
	ABC級系統滲透測試	資科司將規劃**教育體系技術團隊**協助辦理。
	資通安全健診	請**北、南區學術資訊安全維運中心**協助辦理相關教育訓練課程。
A、B級	資通安全威脅偵測管理機制	臺灣學術網路連線單位可結合**臺灣學術網路資安監控系統(南、北SOC, Mini-SOC)**進行威脅偵測機制。

分級作業辦法應辦事項-認知與訓練

辦理事項	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每人每年各接受12小時之資通安全專業課程訓練或資通安全職能訓練*	至少4人	至少2人	至少1人
	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	每人3小時		
資通安全專業證照及職能訓練證書	初次受核定或等及變更後之一年內，資通安全專職（責）人員總計應持有之資通安全專業證照，並持續維持證照之有效性	4張以上	2張以上	1張以上
	資通安全專職人員總計應持有之資通安全職能評量證書，並持續維持證照之有效性（公務機關）	4張以上	2張以上	1張以上

***資通安全專業課程訓練或資通安全職能訓練**：
本部將請**教育體系資安團隊**協助辦理資安相關教育訓練課程，後續將公告於TACERT及A-ISAC網站。

分級作業辦法應辦事項-D、E級

面向	辦理項目	辦理細項	D	E
技術面	資通安全防護	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	X
認知與訓練	資通安全教育訓練	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	每人3小時	

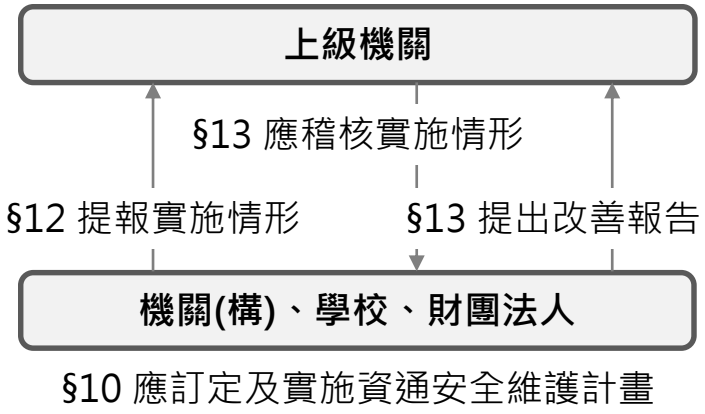
責任等級應辦事項調整

- **資通安全責任等級分級辦法第11條**
  - 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經**等級提交機關**同意，並報請主管機關備查後，免執行該事項或控制措施。
- 教育體系各單位因應措施
  - 教育部後續會規劃各單位應辦事項執行狀況調查，辦理審查事宜。
  - 因公私立學校應有一致性規範，後續教育體系各任務編組(區域網路中心、縣市教育網路中心)及私立學校，本司依「資通安全分級作業辦法」修訂「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」一併規範。

資通安全維護計畫

資通安全維護計畫

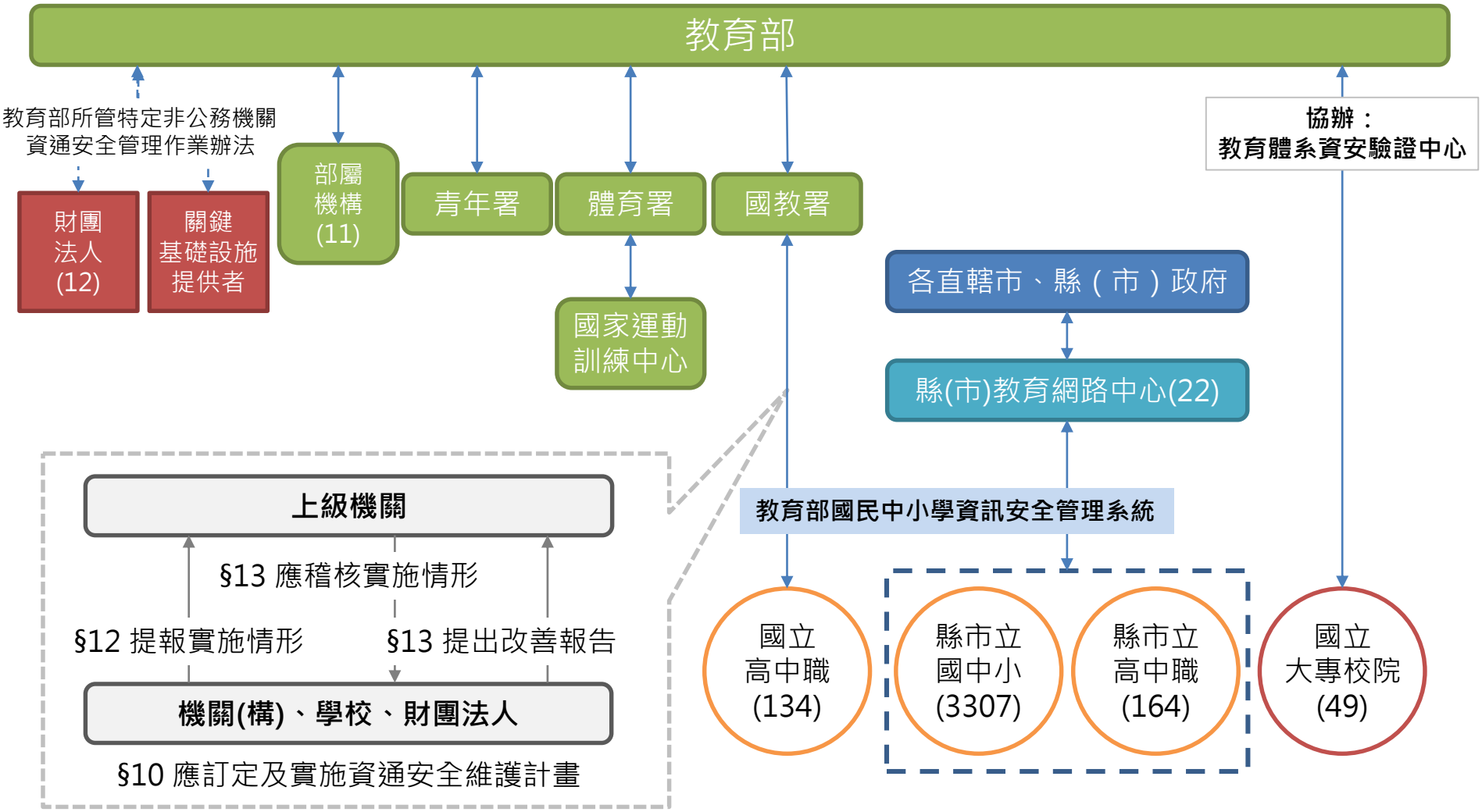
- 本法第10條，公務機關應訂定及實施資通安全維護計畫。
- 本法第12條，公務機關應每年向上級提出資通安全維護計畫實施情形。
- 本法第13條，公務機關應稽核其所屬機關之資通安全維護計畫實施情形。



訂定資通安全維護計畫

- 撰寫注意事項
  - 核心資通系統請依本法施行細則第7條規定盤點，如學校校務行政系統。
  - 各機關依其**資通安全責任等級**應辦事項。
  - 適用範圍為**全機關**，得包含**所屬機關**(如附屬學校)，惟內容應載明各自應遵循項目。
    - 如**國立大學維護計畫**，適用範圍包含**區域網路中心**。
  - 盤點機關各單位自行或委外開發之資通系統，**全部核心資通系統**皆須導入。
  - 已有資安規定與程序書者(**ISO四階文件**)，維護計畫內之項目，得直接引述內部文件編號及名稱。

教育體系稽核作業


教育部
教育部所管特定非公務機關
資通安全管理作業辦法
財團法人 (12)
關鍵基礎設施提供者
部屬機構 (11)
青年署
體育署
國教署
國家運動訓練中心
協辦：
教育體系資安驗證中心
各直轄市、縣（市）政府
縣(市)教育網路中心(22)
教育部國民中小學資訊安全管理系統
國立高中職 (134)
縣市立國中小 (3307)
縣市立高中職 (164)
國立大專校院 (49)
上級機關
§13 應稽核實施情形
§12 提報實施情形
§13 提出改善報告
機關(構)、學校、財團法人
§10 應訂定及實施資通安全維護計畫

教育體系稽核作業

- **教育部將委託「教育機構資安驗證中心」協助辦理公立大學相關稽核作業。**
- 高級中等以下學校，建議加入教育部補助新北市政府教育局開發「**國民中小學資訊安全管理系統**」。
  - **訂定維護計畫**：
    學校填報上傳「資通安全維護計畫」。
  - **學校提報實施情形**：
    學校填報實施情形題目。
  - **上級機關稽核實施情形**：
    評量人員線上評量審查，到校輔導訪視。

資通安全事件通報及應變

教育體系資通安全通報應變

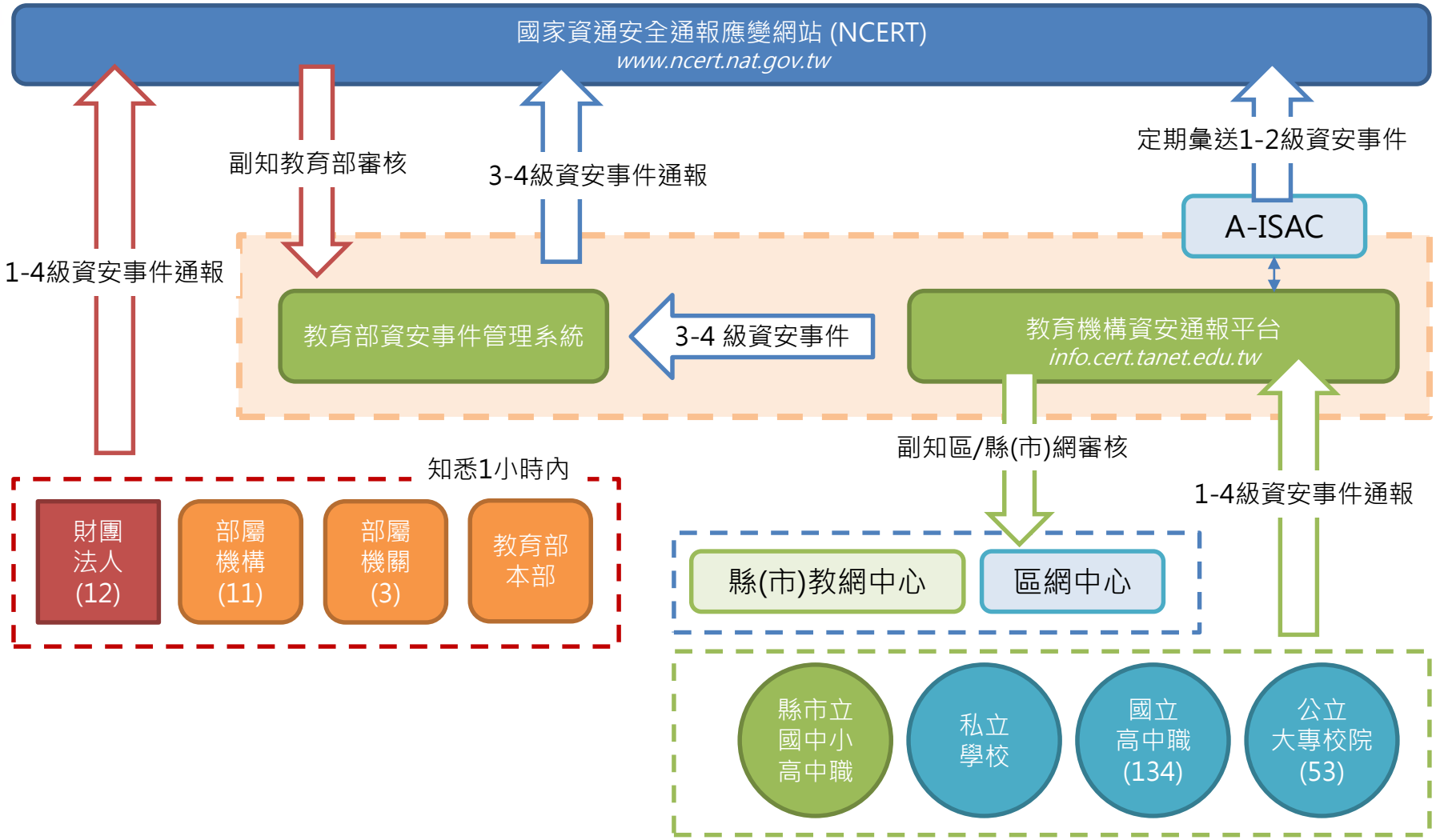
- **公務機關於本辦法施行前**，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關**繼續依該機制辦理資通安全事件之通報及應變**。

- 資通安全事件通報及應變辦法第20條

教育體系資通安全通報應變

- 本部與所屬機關構、財團法人
  - 依行政院規定至「國家資通安全通報應變網站」通報。
- 教育機構
  - 後續本司會訂定「教育機構資通安全通報應變綱要」送主管機關(行政院)核定。
  - 教育機構依上開規定至「教育機構資安通報平台」通報。

教育部通報應變機制


國家資通安全通報應變網站 (NCERT)
www.ncert.nat.gov.tw
副知教育部審核
3-4級資安事件通報
定期彙送1-2級資安事件
A-ISAC
1-4級資安事件通報
教育部資安事件管理系統
3-4 級資安事件
教育機構資安通報平台
info.cert.tanet.edu.tw
副知區/縣(市)網審核
1-4級資安事件通報
知悉1小時內
財團法人 (12)
部屬機構 (11)
部屬機關 (3)
教育部本部
縣(市)教網中心
區網中心
縣市立國中小高中職
私立學校
國立高中職 (134)
公立大專校院 (53)

感謝指導