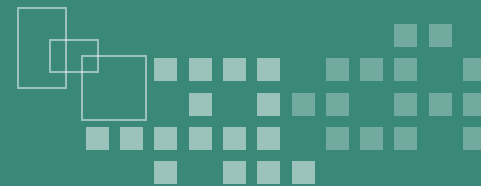




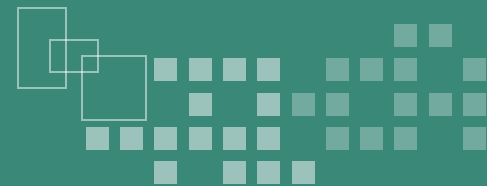
# 資通安全管理法(草案)

行政院資通安全處

105年11月10日



- ◆ 進程與規範要點
- ◆ 草案內容
- ◆ 後續推動事項
- ◆ 各界意見彙整



# 立法目的 (1/3)

## 我國現況：

- 現有資安相關法規目的各異
- 適用對象有限(僅限於特定部門或事項)
- 資安日受重視，但仍無以風險管理為核心之資通安全專法

### 資安法規

## • 未來：資通安全管理法及相關子法

## • 現況：

### 資安特別法(或條文)：

- 刑法36章、電信法、電子簽章法
- 國家機密保護法、個人資料保護法、
- 金融控股公司法、銀行法、
- 醫療法、人體生物資料庫管理條例 等

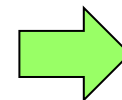
### 資安與相關政策規定

- 國家資通訊安全發展方案(102-105年)
- 國家資通安全通報應變作業綱要
- 行政院及所屬各機關資訊安全管理要點
- 行政院及所屬各機關資訊安全管理規範
- 政府機關(構)資安責任等級分級作業施行計畫
- 資訊系統分級與防護基準作業規定

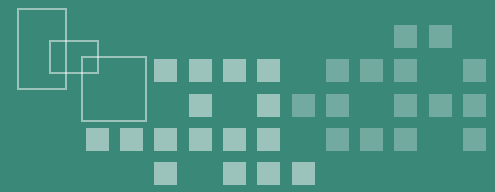
### 參考指引

- 安全控制措施參考指引
- 無線網路安全參考指引
- 資訊系統風險評鑑參考指引
- 資訊作業委外安全參考指引……等18份文件

行政院資通安全處



- 除規範公務機關外，亦包括關鍵基礎設施提供者等非公務機關
- 公務機關及非公務機關均應以風險管理為核心，訂定資通安全維護計畫及通報應變辦法，並接受相關查核



# 立法目的 (2/3)

規範對象



## 公務機關



- 中央與地方機關
- 行政法人

## 非公務機關



- 關鍵基礎設施提供者



- 適用資安責任等級分級之非公務機關

義務



- 非關鍵基礎設施提供者
- 中小企業或業務所涉資料或內容在我國市場之相對重要性較低者
- 未在我國立案且未受左列規範對象委託之外國公司

自願

方法

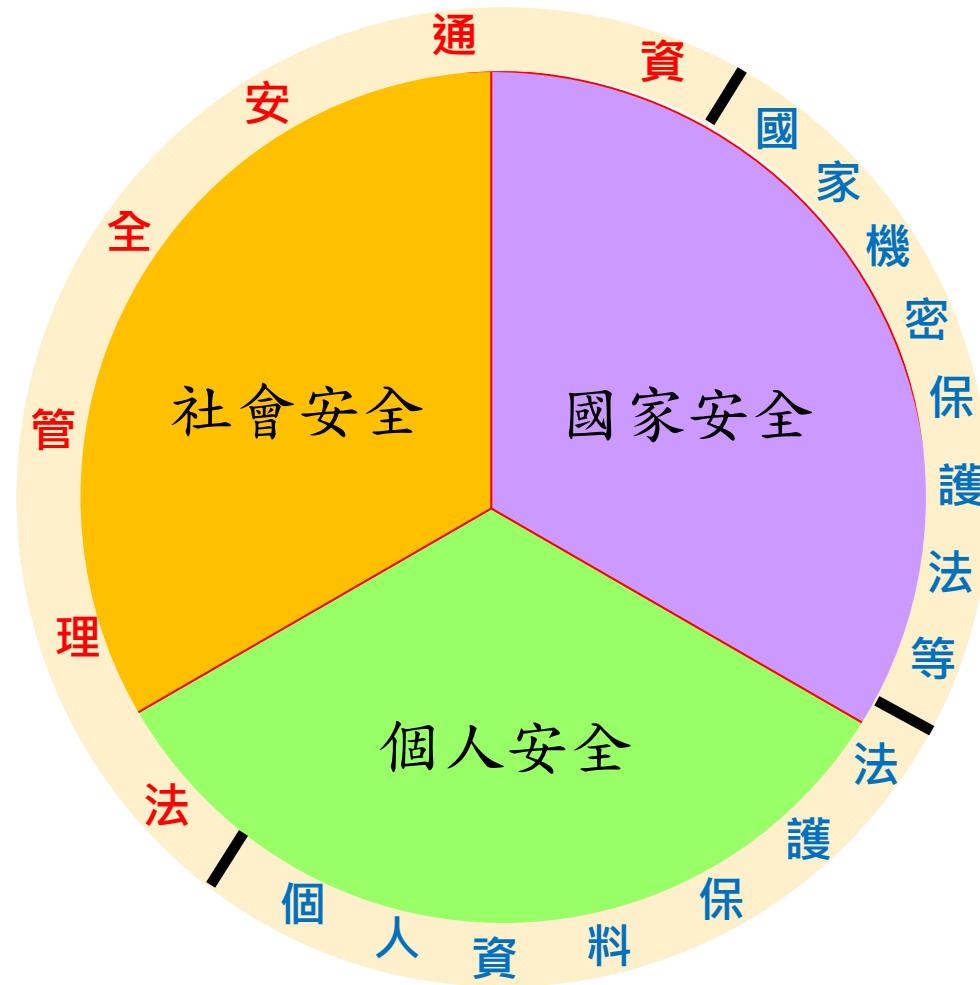
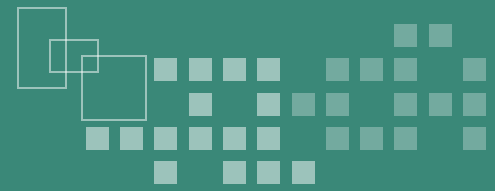
- 以風險管理為核心，從組織面、技術面、物理面、作業面，訂定並持續修訂及實施資通安全維護計畫，以及訂定相關通報應變機制
- 接受上級機關/監督機關或中央目的事業主管機關之查核或委託人之監督
- 非公務機關經發現有重大缺失或重大資通安全事件時，接受行政檢查；未履行義務時之罰鍰

目標

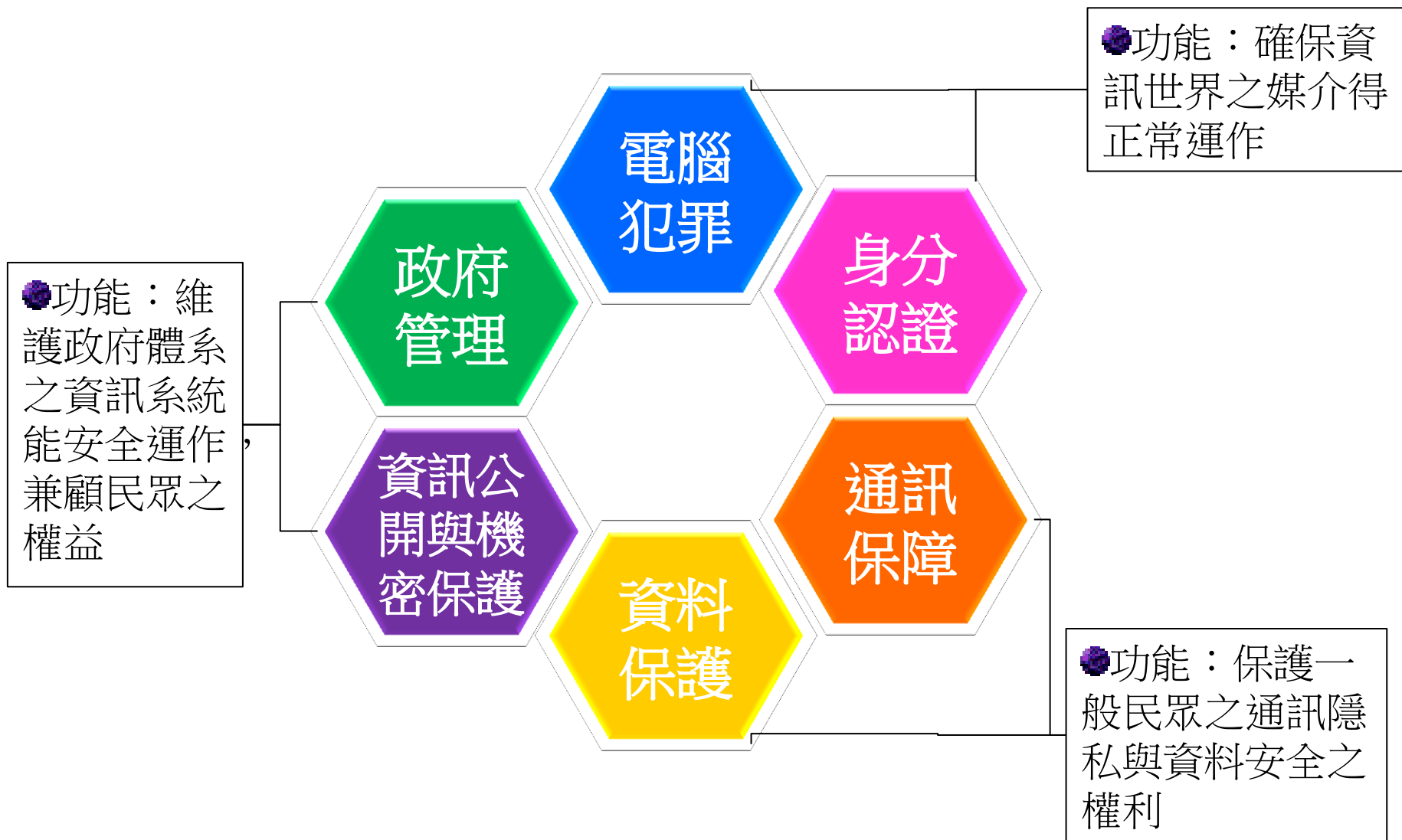
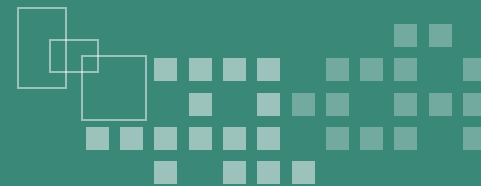
降低資通安全風險，減少資通安全事件並降低其損害及影響  
提升資通安全、促進國家、民眾福祉與產業競爭力

行政院資通安全處

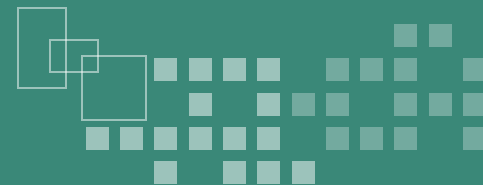
# 立法目的 (3/3)



# 資通安全所涉法規(1/2)

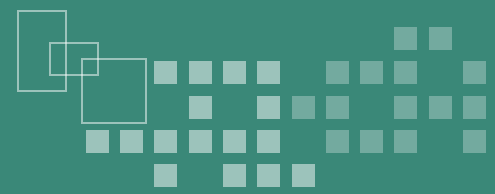


# 資通安全所涉法規(2/2)



類別	法規名稱
電腦犯罪	刑法第36章妨害電腦使用罪
身分認證	電子簽章法
	電子簽章法施行細則
	外國憑證機構許可辦法
通訊保障	通訊保障及監察法
	通訊保障及監察法施行細則
	電信法
資料保護	個人資料保護法
	個人資料保護法施行細則
	金融控股公司法
	銀行法
	醫療法

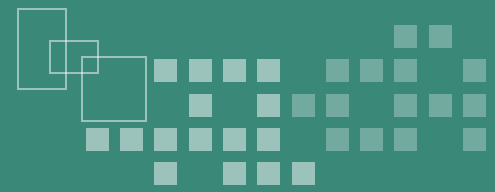
類別	法規名稱
資料保護	醫療機構電子病歷製作及管理辦法
	人體生物資料庫管理條例
	人體生物資料庫資訊安全規範
資訊公開與機密保護	國家機密保護法
	國家機密保護法施行細則
	檔案法
	檔案法施行細則
	政府資訊公開法
政府管理	行政院及所屬機關資訊安全管理要點



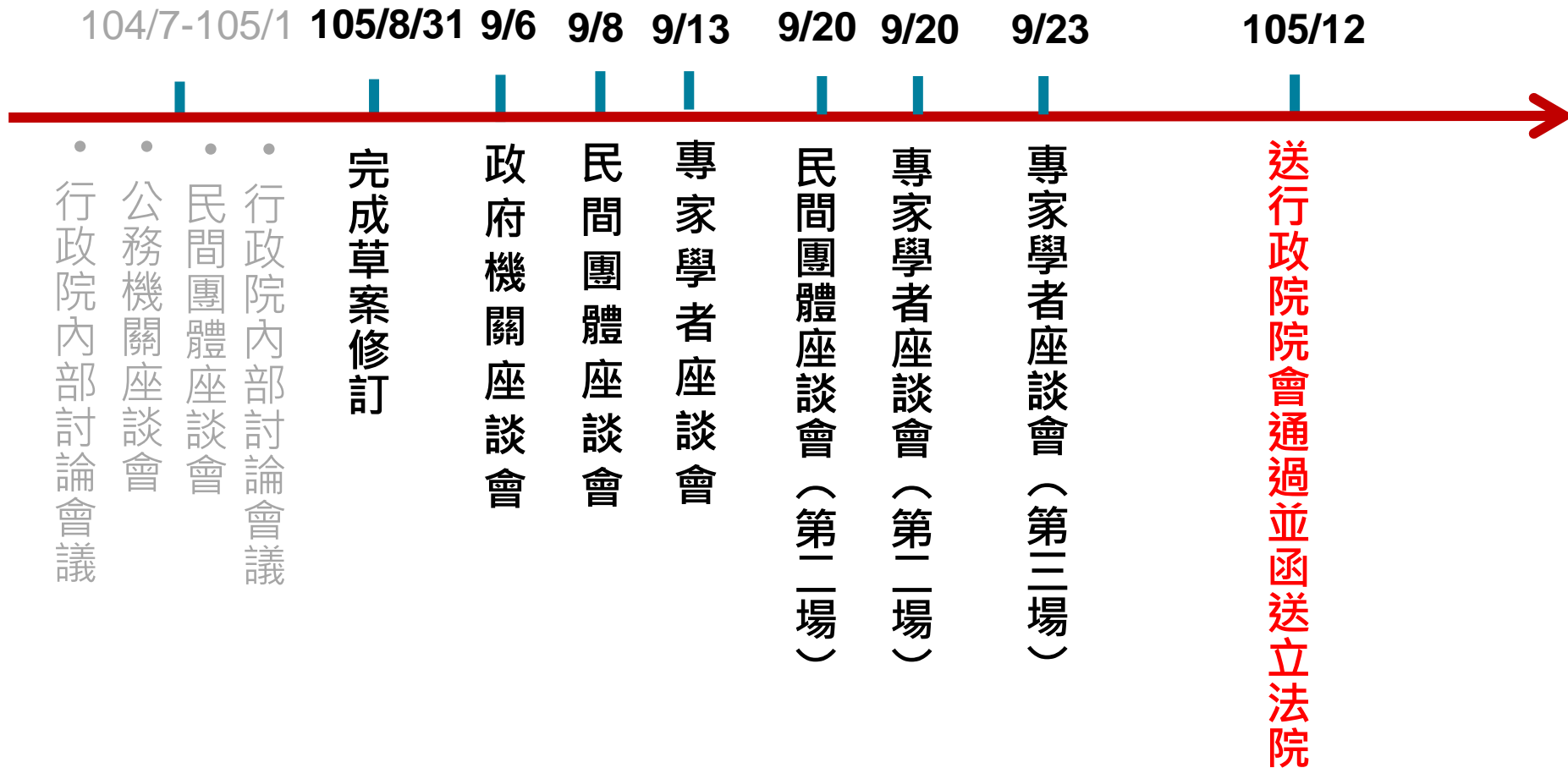
# 國際資安相關立法

	規範名稱	規範對象	規範內容重點
歐盟	<ul style="list-style-type: none"><li>• 網絡暨資訊系統安全指令(簡稱NIS指令)</li></ul>	<p>要求會員國應依指令要求規範下列對象：</p> <ul style="list-style-type: none"><li>• 公務機關</li><li>• 關鍵基礎設施提供者</li><li>• 數位服務提供者</li></ul>	<ul style="list-style-type: none"><li>• 應採行適當安全維護措施</li><li>• 應有適當機制進行稽查</li><li>• 應有有效之罰則</li></ul> <p>(註：NIS指令採最低要求立法，各會員國可自行依該指令訂立更嚴格的要求)</p>
美國	<ul style="list-style-type: none"><li>• 聯邦資訊安全現代化法(FISMA)</li></ul>	<ul style="list-style-type: none"><li>• 聯邦機關</li></ul>	<ul style="list-style-type: none"><li>• 應採行適當安全維護措施</li></ul>
	<ul style="list-style-type: none"><li>• 其他(如金融、醫療等領域法或聯邦貿易委員會法等)</li></ul>	<ul style="list-style-type: none"><li>• 各領域之服務提供者或企業</li></ul>	<ul style="list-style-type: none"><li>• 應採行適當安全措施</li><li>• 各主管機關會依規定進行稽查及處罰</li></ul>

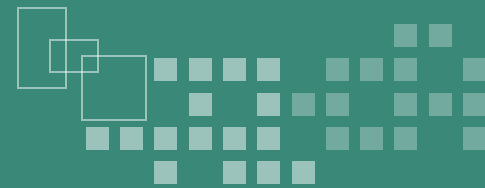




# 推動時程與規劃 (1/2)

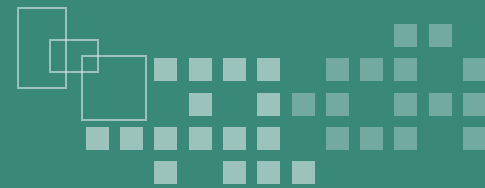


已提送至國發會公共政策網路參與平台(join)公開徵詢意見



## 後續訂定子法

- 行政院
  - 1、施行細則
  - 2、資安責任等級分級辦法
  - 3、資通安全事件通報應變辦法
  - 4、公務機關人員資安相關事項獎懲辦法
  - 5、情資分享辦法
- 中央目的事業主管機關
  - 1、非公務機關安全維護計畫訂定相關作業辦法
  - 2、資通安全查核相關辦法



# 新舊版草案差異

## 提升統籌機關之層級

- 舊版條文規定由科技部統籌資通安全相關事務，惟考量資通安全影響範圍涉及較廣，新版草案已於相關條文明定行政院於資通安全管理統籌之權責。

## 刪除資通安全管理及發展基金之設置

- 考量國家整體財政分配之適當性並保有彈性，因此刪除基金相關條文。

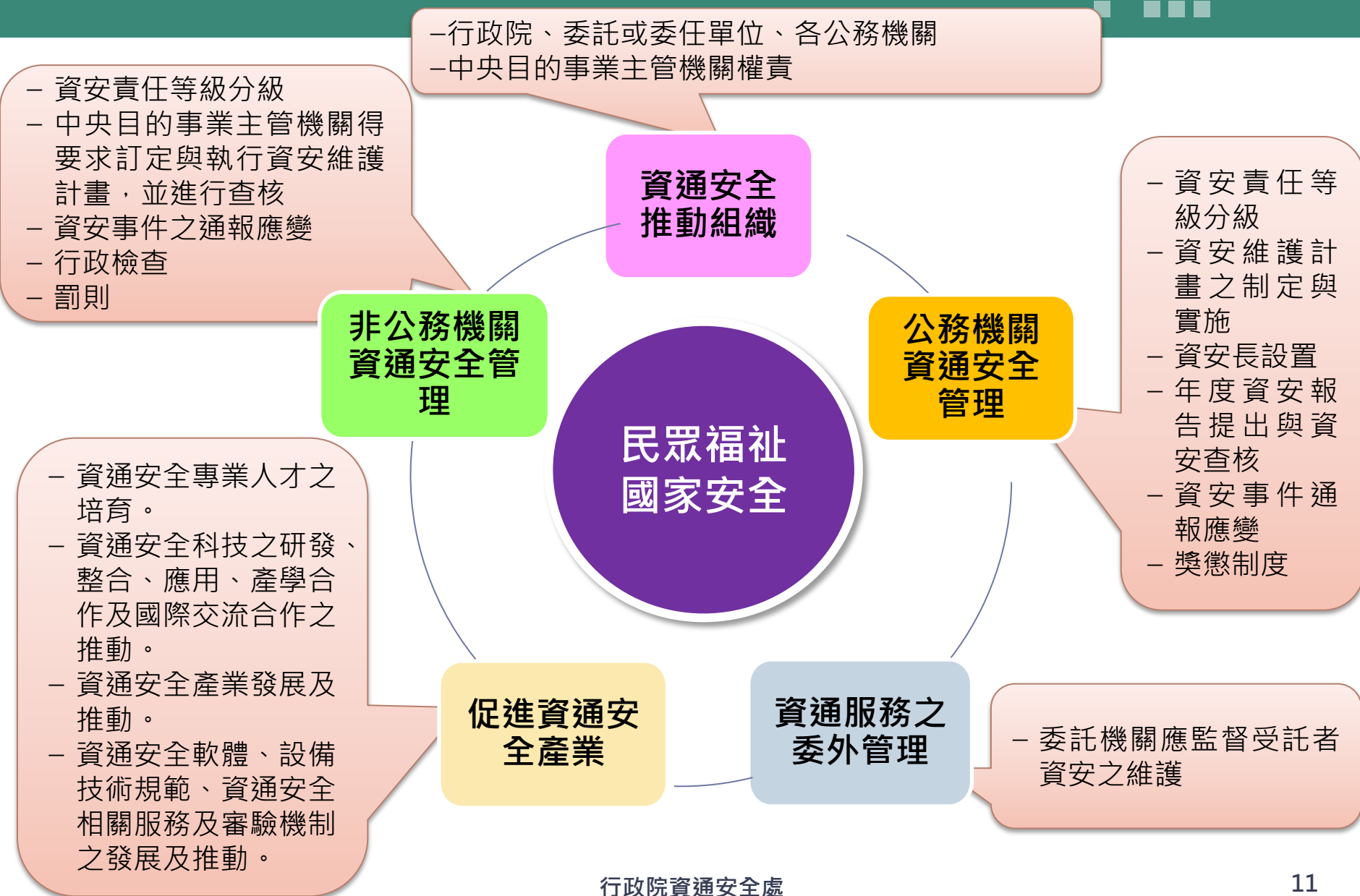
## 刪除國家資通安全會報相關規定

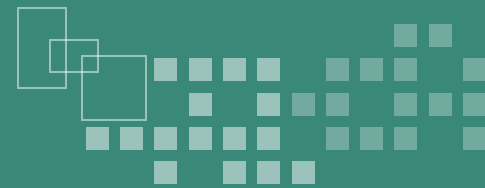
- 考量資通安全會報之組織及相關事項，已於「行政院國家資通安全會報設置要點」明定，因此刪除關於會報之條文。

## 刪除由中央目的事業主管機關指定非公務機關之規定

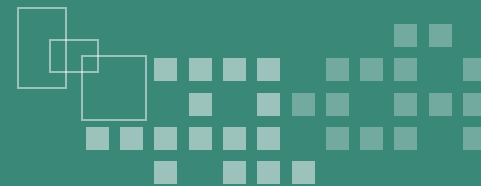
- 考量公務機關及關鍵基礎設施提供者對於國家安全與民眾福祉之影響較鉅，現階段宜以其為主要規範對象，以完備資通安全管理機制，爰刪除中央目的事業主管機關指定非公務機關之條文。

# 規範要點 (1/2)

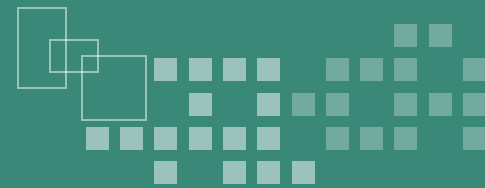




1. 明確資通安全政策制定與推動組織、行政院及中央目的事業主管機關之權責，以強化資安政策之制定、推動與執行之能量。
2. 規範公務機關應建立資通安全維護之機制。
3. 規範關鍵基礎設施提供者及受分級辦法納管之非公務機關應建立資通安全維護之機制。
4. 資通安全事件通報、應變及改善機制之規範。
5. 行政檢查與罰則及其他推動資通安全相關事項。



- ◆ 進程與規範要點
- ◆ 草案內容
- ◆ 後續推動事項
- ◆ 各界意見彙整



# 整體架構

## ❖ 本法以資通安全管理為核心，分為5個章節，計24條

### 資通安全管理法草案

#### 第1章 總則(§1~§8)

立法目的、名詞定義、資通安全產業之推動、行政院職責、幕僚任務委任或委託、資安責任等級分級、情資分享機制、資通委外監督

#### 第2章 公務機關資通安全管理(§9~§14)

資通安全管理與維護計畫、資通安全長之設置、年度資通安全報告之提出、資通安全查核、通報應變措施、獎懲措施

#### 第3章 非公務機關資通安全管理(§15~§18)

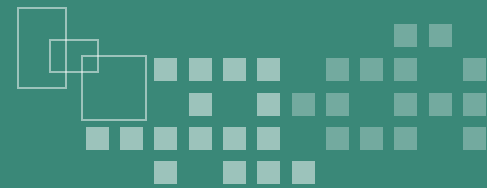
關鍵基礎設施提供者、資安責任等級分級納管之非公務機關資通安全維護之管理與監督、資通安全事件通報應變、行政檢查

#### 第4章 罰則(§19~§22)

行政處分

#### 第5章 附則(§23~§24)

施行細則授權、施行日期



# 保護客體與規範對象

## 保護客體

### 資通安全

指防止資通系統及透過其運作之資訊免於遭受未經授權之存取、使用、控制、洩漏、破壞、修改、銷毀或其他作為，以確保其機密性、完整性及可用性。

## 規範對象

### 公務機關

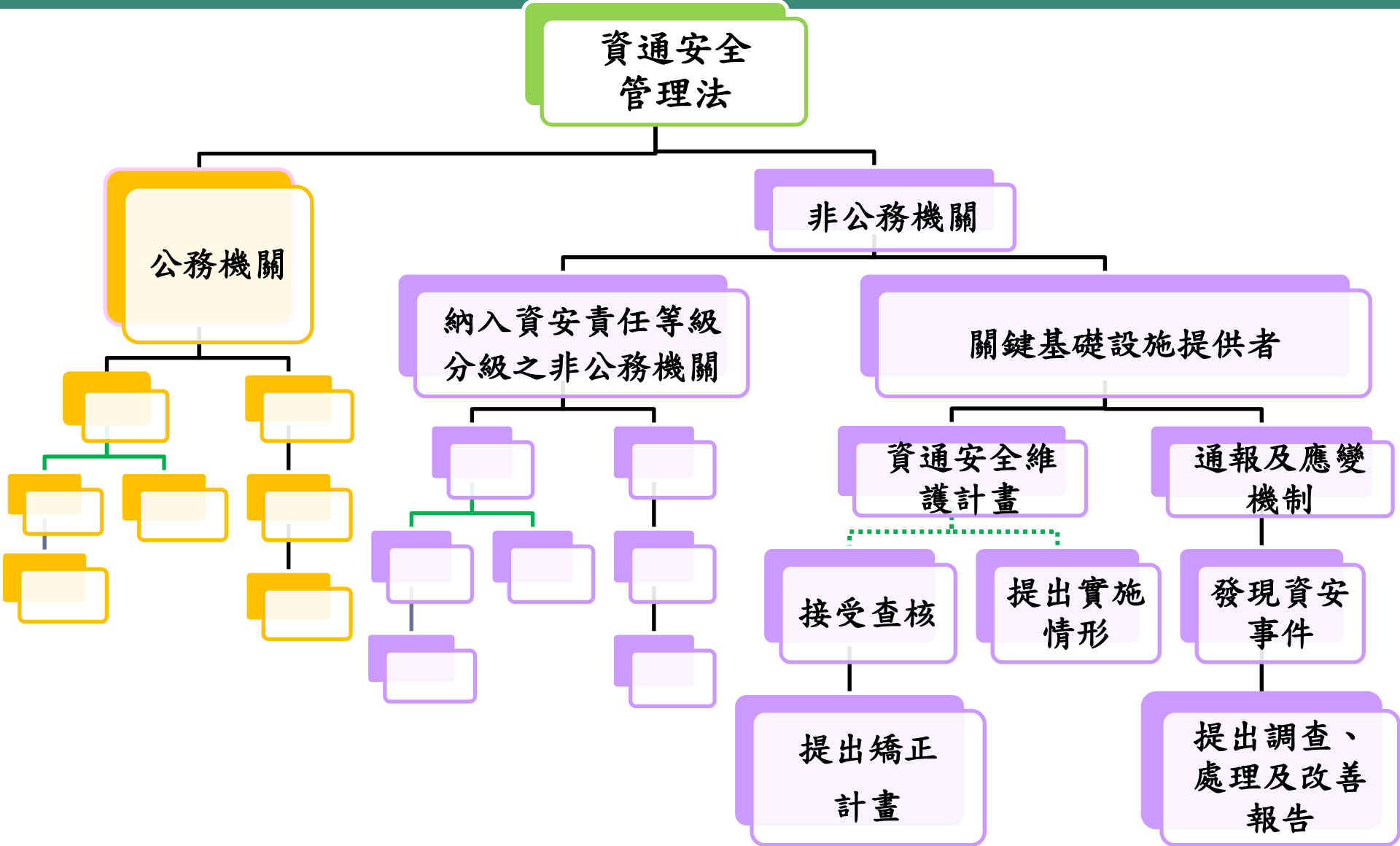
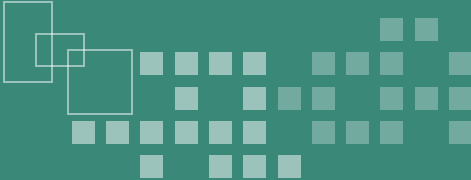
指依法行使公權力之中央、地方機關（構）或行政法人。

### 非公務機關

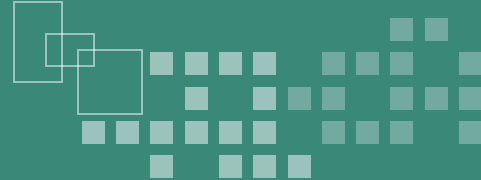
- 指公務機關以外之國（公）營事業、其他法人或團體。
- 區分為兩類：
  - ◎關鍵基礎設施提供者。
  - ◎適用資安責任分級之非公務機關。



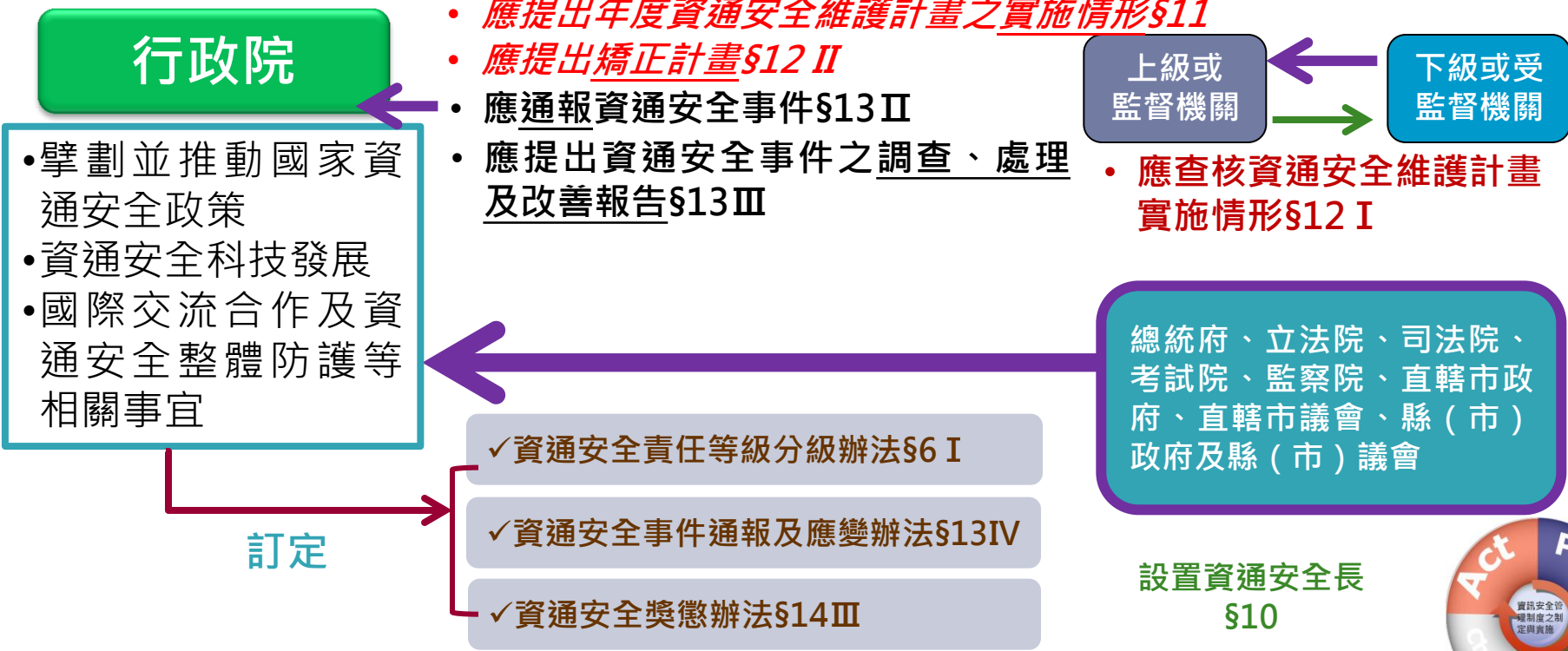
# 義務類型

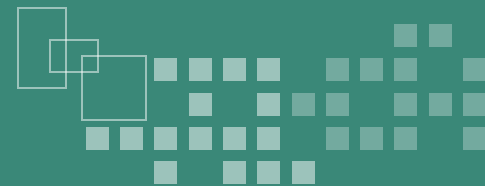


# 公務機關之資通安全管理



- ✓ 應訂定、修正及實施資通安全維護計畫 §9
- ✓ 應訂定通報及應變機制 §13 I





# 非公務機關之資通安全管理

關鍵基礎  
設施提供  
者

適用責任  
分級之非  
公務機關

資通安全維護計畫

- ①訂定、修正及實施資通安全維護計畫§15Ⅱ。
- ②提出資通安全維護計畫之實施情形§15Ⅲ。
- ③提出資通安全維護計畫之矯正計畫§15Ⅴ。

- ①訂定、修正及實施資通安全維護計畫§16Ⅰ。

- ②提出資通安全維護計畫之實施情形§16Ⅱ。
- ③提出資通安全維護計畫之矯正計畫§16Ⅲ。

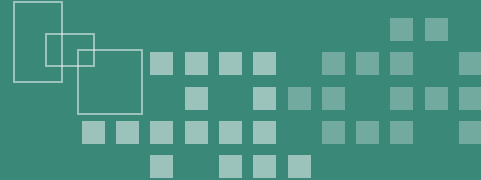
通報應變

- ④訂定通報及應變機制§17Ⅰ。
- ⑤通報資安事件，並提出調查、處理及改善報告§17Ⅱ、Ⅲ。

資通安全行政檢查 (§18)

罰則 (§19~§22)

# 關鍵基礎設施提供者



- ✓ 應訂定、修正及實施資通安全維護計畫§15 II
- ✓ 應訂定通報及應變機制§17 I

中央目的事業主管機關

- 應提出年度資通安全維護計畫之實施情形§15 III
- 應提出矯正計畫§15 V
- 應通報資通安全事件§17 II
- 應提出資通安全事件之調查、處理及改善報告§17 III

訂定



- 應查核資通安全維護計畫實施情形§15 IV

✓ 資通安全維護計畫辦法§15 VI

關鍵基礎設施提供者

關鍵基礎設施：指其功能一旦停止運作或效能降低，對國民生活、經濟活動、公眾安全或國家安全有重大影響之虞，並經行政院公告者§2

關鍵基礎設施提供者：  
□ 指維運或提供關鍵基礎設施之全部或一部，並經中央目的事業主管機關指定之非公務機關§2  
□ 由中央目的事業主管機關指定，並報請行政院核定之§15 I



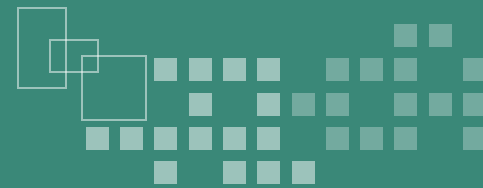
## 訂定

- 

- ## ✓資通安全維護計畫辦法§16IV

✓應訂定通報及應變機制  
§17 I





## ❖ 發動原因：

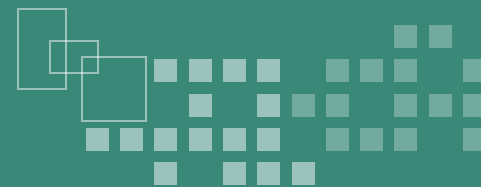
- 中央目的事業主管機關查核非公務機關之資通安全維護計畫發現重大缺失
- 非公務機關發生重大資通安全事件

## ❖ 執行方式：

- 得進入非公務機關之處所執行
- 非公務機關或其人員不得規避、妨礙或拒絕，違反者依本法或其他法律處罰或辦理之

## ❖ 參與檢查之人員就應秘密之資訊，負保密義務

# 罰則



未確實訂定、修正  
或實施資通安全維  
護計畫

令限期改正；屆期未改正者，按次處新臺幣十萬元以上二百萬元以下罰鍰

未通報資通安全事件

處新臺幣十萬元以上一百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之

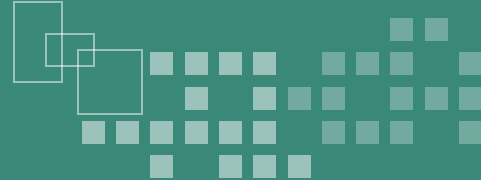
未提出資通安全維  
護計畫實施情形及  
矯正計畫

令限期改正；屆期未改正者，按次處新臺幣五萬元以上五十萬元以下罰鍰

規避、妨礙或拒絕  
行政檢查

處新臺幣二萬元以上二十萬元以下罰鍰

# 資通安全事件情資分享機制



情資分享

資通安全事件通報機制

其他情資



行政院建立資通安全情資分享機制

行政院、上級機關

中央目的事業主管機關

經濟部、金管會、交通部、NCC...等

公務機關資通安全事件通報(\$13)(強制通報)



公務機關

非公務機關資通安全事件通報(\$17)(強制通報)



關鍵基礎設施提供者



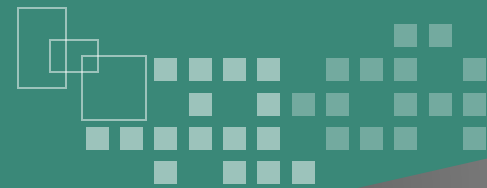
+ 適用資安責任等級分級之非公務機關

非公務機關資通安全事件通報(自願通報)



所有非公務機關





# 公私協力發展資通安全環境

整合民間力量  
+  
提供充份資源

1

資通安全專業人才之培育

2

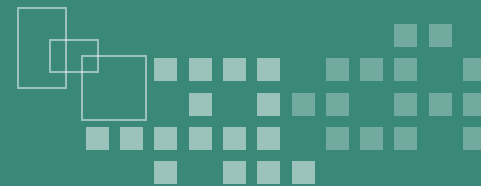
資通安全科技之研發、整合、應用、產學合作  
及國際交流合作之推動

3

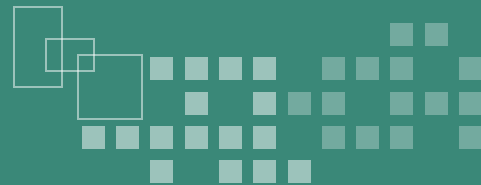
資通安全產業發展及推動

4

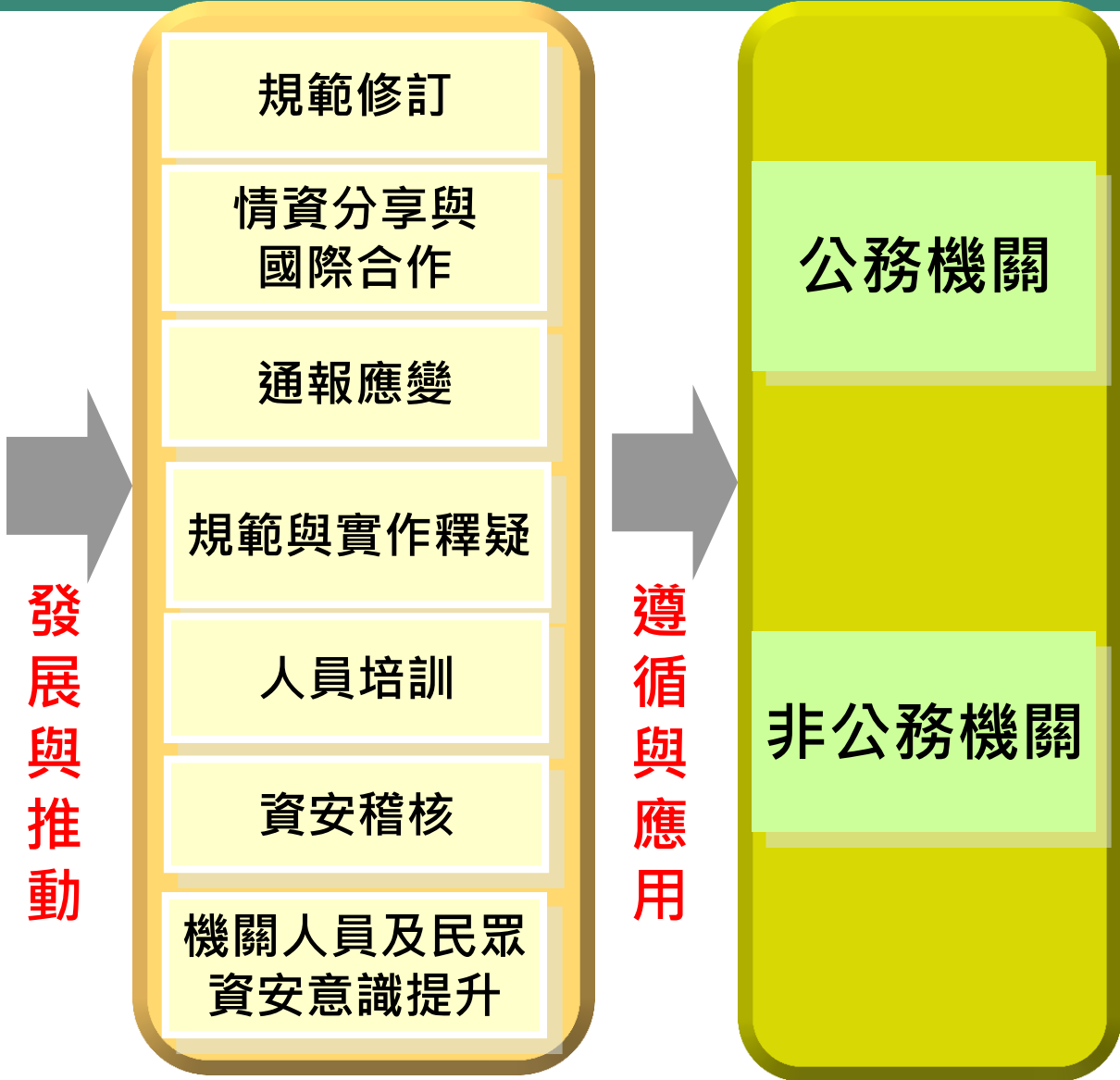
資通安全軟體、設備技術規範、資  
通安全相關服務及審驗機制之發展  
及推動。

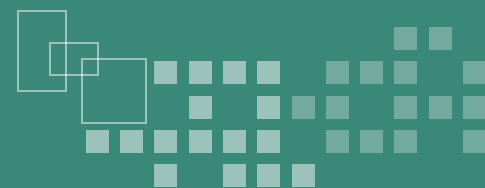


- ◆ 進程與規範要點
- ◆ 草案內容
- ◆ 後續推動事項
- ◆ 各界意見彙整



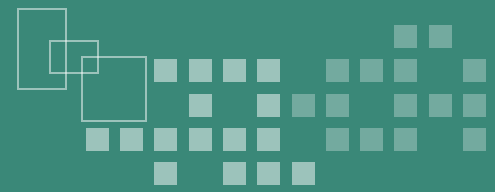
# 資通安全管理法推動措施 (1/3)





# 資通安全管理法推動措施 (2/3)

			現況	未來
1	規範修訂	法律	<ul style="list-style-type: none"><li>檢視既有法規之資安要求</li></ul>	<ul style="list-style-type: none"><li>其他<b>相關法規調整</b></li></ul>
		命令	<ul style="list-style-type: none"><li>無專法故無配套之命令</li></ul>	<ul style="list-style-type: none"><li><b>資安管理法子法</b>(施行細則、資安分級、通報應變、情資分享 etc.)</li></ul>
		其他	<ul style="list-style-type: none"><li>資安分級、通報應變綱要、系統分級與防護基準 etc.</li></ul>	<ul style="list-style-type: none"><li>資訊系統分級與防護基準</li><li><b>建立關鍵基礎設施相關資安防護基準</b></li><li>其他</li></ul>
2	情資分享與國際合作		<ul style="list-style-type: none"><li>ISAC情資分享機制</li><li>國際CERT資料交換</li><li>國際政策、機制與成效交流</li></ul>	<ul style="list-style-type: none"><li>建置公務機關情資分享平臺，擴大並完善公務機關間之情資分享</li><li><b>建立非公務機關自主情資提供之合作機制</b></li><li>持續進行情資分享交流及國際合作</li></ul>
3	通報應變		<ul style="list-style-type: none"><li>日常演練要求</li><li>透過相關通報應變平臺，進行通報</li></ul>	<ul style="list-style-type: none"><li><b>機關依稽核結果與安全維護評估，執行適當演練項目</b></li><li>強化機關通報應變平臺之功能與內容整合機制</li></ul>



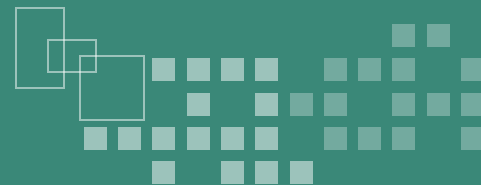
# 資通安全管理法推動措施 (3/3)

## 現況

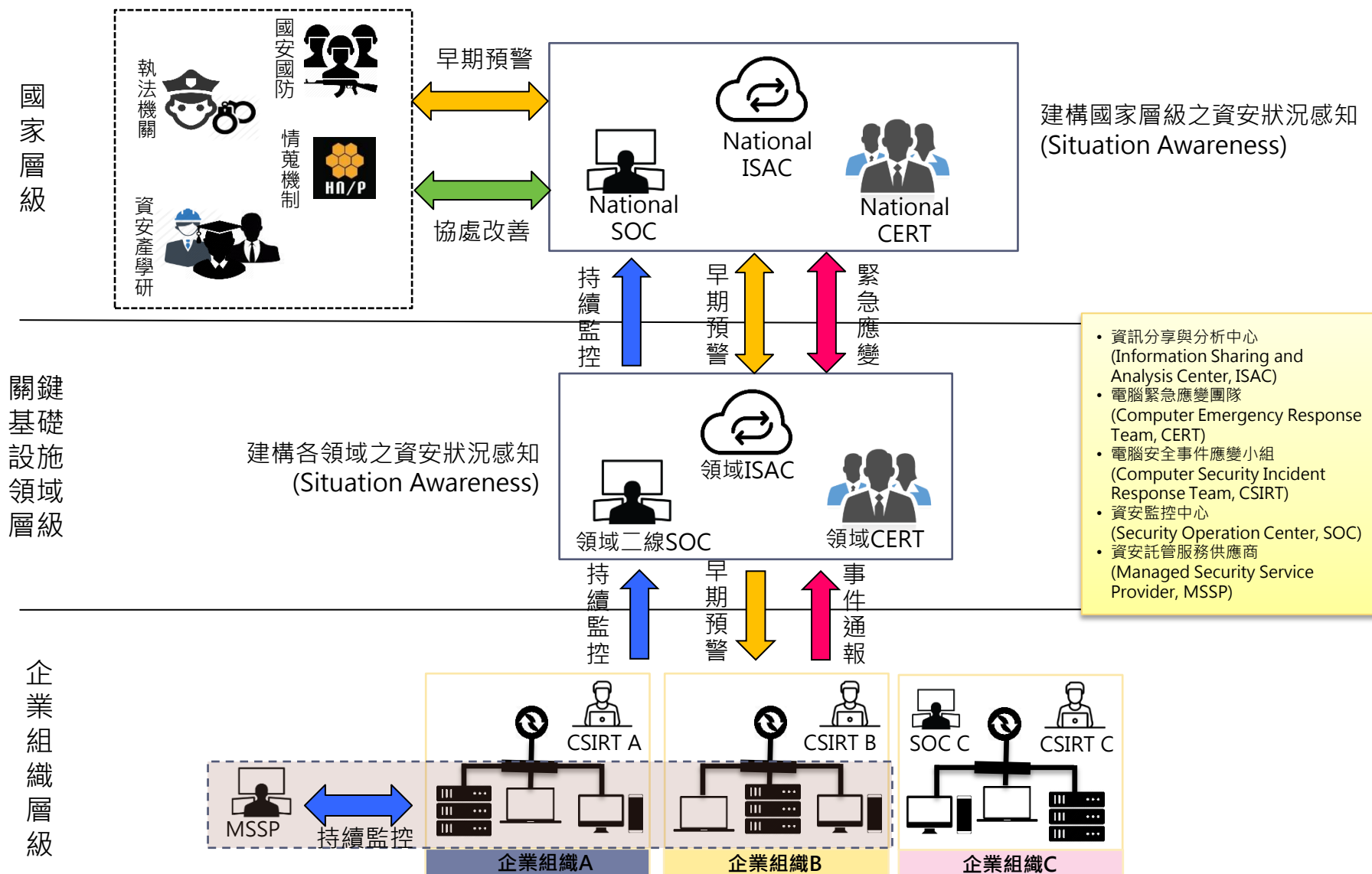
## 未來

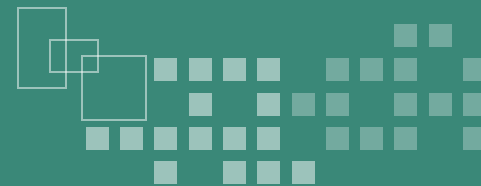
4	規範與實作釋疑	<ul style="list-style-type: none"><li>• SPMO諮詢專線</li><li>• 巡迴研討會</li><li>• 網站提供資安資訊</li></ul>	<ul style="list-style-type: none"><li>• 新增管理法相關諮詢服務</li><li>• 辦理巡迴研討會與說明會</li><li>• 更新網站提供資訊</li></ul>
5	人員培訓	<ul style="list-style-type: none"><li>• 依職能需求設計課程</li><li>• 教材編撰</li><li>• 考核機制</li></ul>	<ul style="list-style-type: none"><li>• 新增管理法訓練課程，並<b>規劃建立訓練認證機制</b></li><li>• 辦理訓練與評量</li><li>• 精進考核機制</li></ul>
6	資安稽核	<ul style="list-style-type: none"><li>• 行政院資安稽核</li></ul>	<ul style="list-style-type: none"><li>• 行政院資安稽核</li><li>• <b>上級機關稽核下級機關</b></li><li>• <b>中央目的事業主管機關稽核關鍵基礎設施提供者</b></li></ul>
7	機關人員及民眾資安意識提升	<ul style="list-style-type: none"><li>• 資安案例彙編</li><li>• 推廣活動</li></ul>	<ul style="list-style-type: none"><li>• 編撰資安案例彙編(含管理要訣)</li><li>• 辦理相關推廣活動</li></ul>

# 推動國家資安聯防

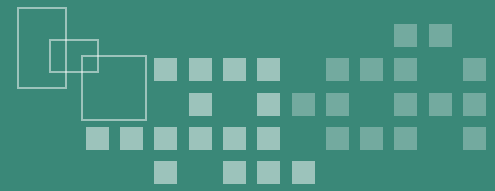


## 角色與關係





- ◆ 進程與規範要點
- ◆ 草案內容
- ◆ 後續推動事項
- ◆ 各界意見彙整



## ❖ 政府機關意見

- 應避免增加行政流程及文書作業
- 人力及預算不足

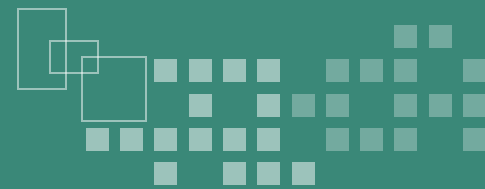
## ❖ 民間團體意見

- 應避免機關重複稽核
- 應明定納入本法的產業, 不宜逕由中央目的事業主管機關指定
- 建議提供投資抵稅優惠
- 罰則過重

## ❖ 專家學者意見

- 法條架構應更明確
- 罰則過輕





## 規範面

- 應避免增加行政流程及文書作業→將整併應提交之文件，以減輕機關行政作業
- 建議提供投資抵稅優惠→涉及稅基，經評估後暫不宜納入
- 罰則過輕/過重→部分罰則增列限期改正措施，如未改正將按次處以罰鍰

## 執行面

- 人力及預算不足→避免重覆作業，減低所需資源
- 應避免機關重複稽核→執行時將透過協調機制避免
- 應確認關鍵基礎設施提供者之主管機關→擬參照「國家關鍵基礎設施安全防護指導綱要」訂定
- 應訂定資通安全維護計畫參考範本→已進行規劃



報告完畢

敬請指導