



數位發展部資通安全署
Administration for Cyber Security, moda

112年9月22日預告版

資通安全管理法 修法草案重點

數位發展部資通安全署



修法期程


全面檢視
現行法規

專家研議

專家共同
討論及法
律意見書

部會協力

3~5月
機關意見
回饋



凝聚共識

8~9月
6場修法
工作坊



公共參與

9/22~11/20
「公共政策網
路參與平臺」
徵詢民眾意見

10/17~11/15
16場修法說明會
廣徵各界意見

數位部

法案審查

行政院

院會審查

立法院
審議



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署、公務機關及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第二方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)

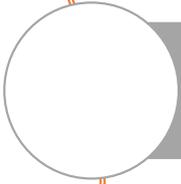


報告大綱

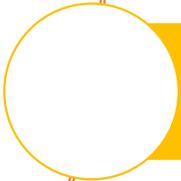
修法重點



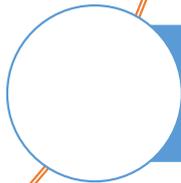
一.明確劃分權責機關



二.明確法源

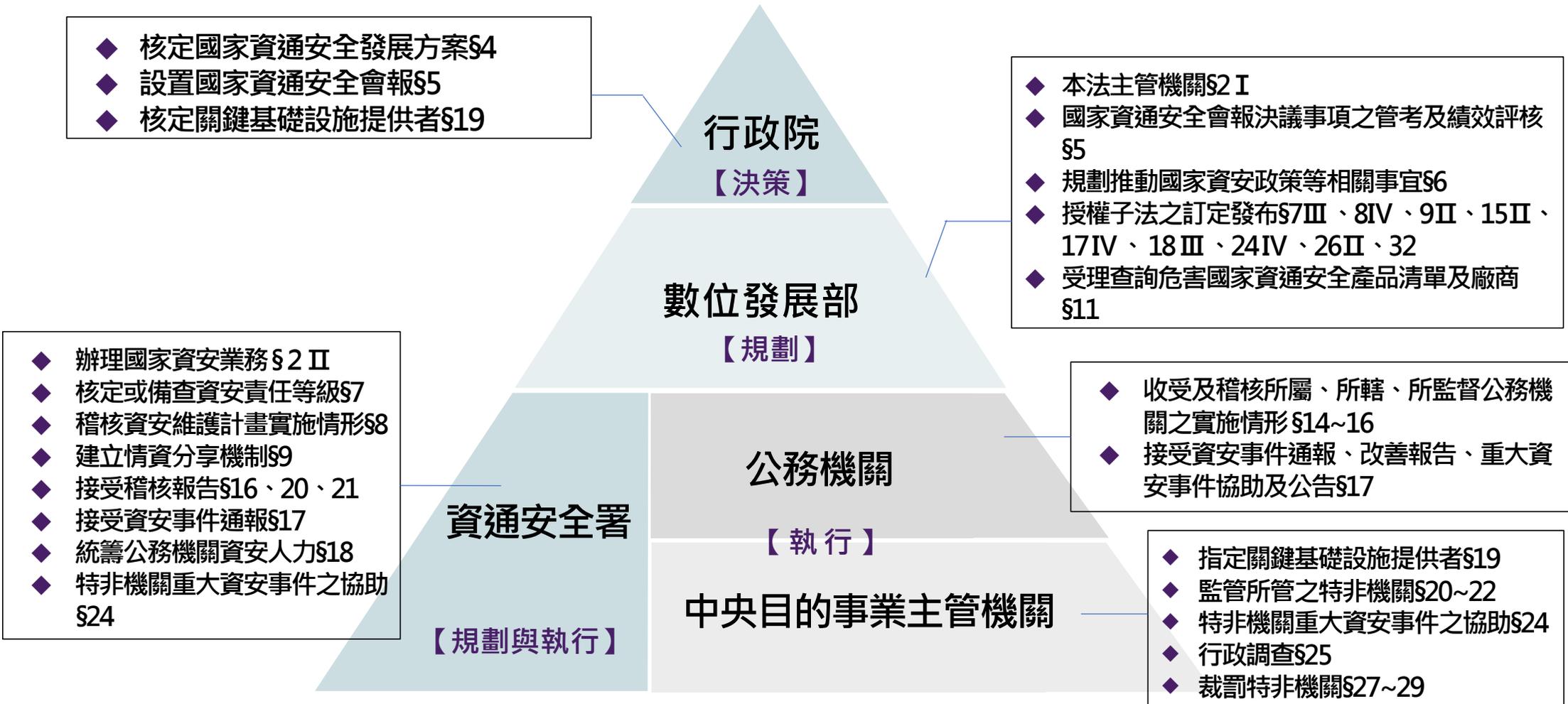


三.強化公務機關資安管理



四.修正特非機關範圍及強化資安管理

1-1 行政院、主管機關、資安署、公務機關及中央目的事業主管機關各別權責事項





1-2 國家資通安全會報

草案條文	現行條文	說明
<p>第5條</p> <p>為落實國家資通安全政策，各政府機關、中央及地方間，應致力配合推動執行國家資通安全措施，共同建構國家資通安全環境。</p> <p>為辦理國家資通安全政策、應變機制與重大計畫之諮詢審議，協調各政府機關、中央及地方間之資通安全相關事務，行政院應召開國家資通安全會報，其幕僚作業由主管機關辦理。</p> <p>前項國家資通安全會報決議事項，相關政府部門應予執行，由主管機關定期追蹤管考，並得辦理績效評核。</p> <p>第二項國家資通安全會報之組成、任務、議事程序及其他相關事項，由行政院定之。</p>		<ol style="list-style-type: none">1. 本條新增。2. 因應越趨增強之全球資通安全威脅及突發資通安全事件，各政府機關應建立中央地方聯防體系，以完備國家資通安全，爰規定第一項及第二項，以強化跨機關資通安全事件應處及協調能力。3. 另為確保落實國家資通安全會報決議事項，爰規定第三項。4. 第二項國家資通安全會報之組成、任務、議事程序及其他相關事項，於第四項授權由行政院定之。



報告大綱

修法重點

一.明確劃分權責機關



二.明確法源

三.強化公務機關資安管理

四.修正特非機關範圍及強化資安管理



2-1 本法用詞定義修正

草案條文	現行條文	說明
<p>第3條第3~5、7、8款</p> <p>三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀，或其他情形影響其機密性、完整性或可用性。</p> <p>四、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或保護措施失效之狀態發生，影響資通系統機能運作。</p>	<p>第3條第3~5、7、8款</p> <p>三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。</p> <p>四、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。</p>	<p>酌作文字修正，以符實際。</p>
<p>五、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。但不包括軍事機關及情報機關。</p>	<p>五、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。</p>	<p>因農田水利會已改制納入原行政院農業委員會農田水利署，本法納管之公法人目前僅存行政法人，爰修正第五款。</p>
<p>七、關鍵基礎設施：指行政院公告之關鍵領域中，該領域服務所依賴之系統或網路之實體或虛擬資產，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞者。</p> <p>八、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，經依第十九條規定通知者。</p>	<p>七、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。</p> <p>八、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，經中央目的事業主管機關指定，並報主管機關核定者。</p>	<p>配合機關權責劃分及現行實務作法酌修文字。</p>



2-2委外辦理之管理及監督機制

草案條文	現行條文	說明
<p>第10條</p> <p>公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應<u>選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。</u></p> <p>公務機關或特定非公務機關辦理前項委外業務，<u>應與受託者簽訂書面契約，載明雙方之權利義務及違約責任。</u></p>	<p>第9條</p> <p>公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。</p>	<ol style="list-style-type: none">1. 條次變更。2. 第一項酌作文字修正。3. 為強化各機關落實委外監督管理明定各機關應與受託者簽訂書面契約，並載明雙方之權利義務及違約責任，爰增訂第二項。

2-3 明定公務機關對危害國家資通安全產品之使用原則

現況
沿革



草案

公務機關及自行或委外營運供公眾使用之場地，不得採購、使用此類產品、公務用資通訊設備亦不得下載、安裝、使用，並開放公務機關查詢。



對照表：危害國家資通安全產品

草案條文	現行條文	說明
<p>第11條</p> <p>公務機關不得採購及使用危害國家資通安全產品；其自行或委外營運，提供公眾活動或使用之場地，亦同。但因業務需求且無其他替代方案者，經該機關資通安全長及其上級機關資通安全長核可，函報主管機關核定後，得以專案方式購置，並列冊管理</p> <p>公務人員獲配之公務用資通訊設備，不得下載、安裝或使用危害國家資通安全產品，並應遵守相關法令規範。</p> <p>公務機關得向主管機關查詢第一項產品及其廠商。</p>		<ol style="list-style-type: none">1. <u>本條新增</u>。2. 將各機關對危害國家資通安全產品限制使用原則提升至法律位階以符合法律保留原則。



2-4 明定關鍵基礎設施提供者之指定程序

草案條文	現行條文	說明
<p>第19條 中央目的事業主管機關應徵詢相關公務機關、民間團體、專家學者意見後，擬訂<u>關鍵基礎設施提供者之指定清單</u>，報請行政院核定，以書面通知之；<u>其指定基準、廢止條件及程序，由中央目的事業主管機關公告之。</u></p>	<p>第16條第1項 中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定<u>關鍵基礎設施提供者</u>，報請主管機關核定，並以書面通知受核定者。</p>	<ol style="list-style-type: none">1. 條次變更。2. 現行條文第一項移列本條前段，並依行政院一百十一年八月二十四日院臺規字第一一一〇一八四三〇七號公告，所列事項自一百十一年八月二十七日起仍由行政院管轄，爰予修正。3. 另考量關鍵基礎設施提供者之指定基準及程序，影響人民權益重大，有法律保留原則之適用，爰於本條後段增訂<u>關鍵基礎設施提供者之指定基準、廢止條件及程序</u>，授權由中央目的事業主管機關公告之。

2-5 機關委託、委任權限移轉之法規依據

草案條文	現行條文	說明
<p>第30條 <u>主管機關為辦理資通安全整體防護、國際交流合作及其他資通安全相關事務，得委託所監督行政法人、其他公務機關、法人或團體為之。</u> <u>資安署為辦理國家資通安全防護、演練、稽核及其他資通安全相關事務，得委託其他公務機關、法人或團體為之。</u> <u>公務機關為辦理第十五條第一項、第二十條第三項之稽核事項，得委任所屬機關或委託其他公務機關、法人或團體為之。</u> 前三項受委任、委託或複委託之公務機關、法人或團體，不得洩露辦理相關事務過程中所知悉之秘密。</p>	<p>第6條 主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。 前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉<u>關鍵基礎設施提供者</u>之秘密。</p>	<ol style="list-style-type: none"> 1. 條次變更。 2. 第一項酌作文字修正。 3. 配合修正條文第二條第二項規定，爰增訂第二項定明資安署得委託辦理國家資通安全防護、演練、稽核及其他資通安全相關事務之依據。 4. 增訂第三項，定明公務機關為辦理第十五條第一項、第二十條第三項公務機關稽核作業，得委任或委託辦理之依據。 5. 第二項規定移列為修正條文第四項，並考量受委任、委託或複委託者就執行或辦理相關事務過程中所獲悉之秘密，除有正當理由外，均有保密之義務，不限於關鍵基礎設施提供者之秘密，爰刪除「關鍵基礎設施提供者」等字，並酌作文字修正。



2-6 資安事件涉個資外洩時另依個資法辦理

草案條文	現行條文	說明
<p>第31條 本法所定資通安全事件，涉及個人資料檔案外洩時，公務機關及特定非公務機關應另依個人資料保護法及其相關法令規定辦理。</p>		<ol style="list-style-type: none">1. 本條新增。2. 資通安全管理法係要求納管之公務機關及特定非公務機關訂定「資通安全維護」計畫並依計畫實施相關資通安全管理事項、訂定資通安全事件之通報及應變機制、通報資通安全事件等，均係屬資通安全維護義務，與個人資料保護法係要求保有個人資料檔案者應採行適當之安全措施、訂定「個人資料檔案安全維護」計畫或業務終止後個人資料處理方法等，兩者之構成要件不同，並無普通法及特別法之關係，有予以明辨之必要，爰增訂本條。



報告大綱

修法重點

一.明確劃分權責機關

二.明確法源

三.強化公務機關資安管理

四.修正特非機關範圍及強化資安管理



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第三方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

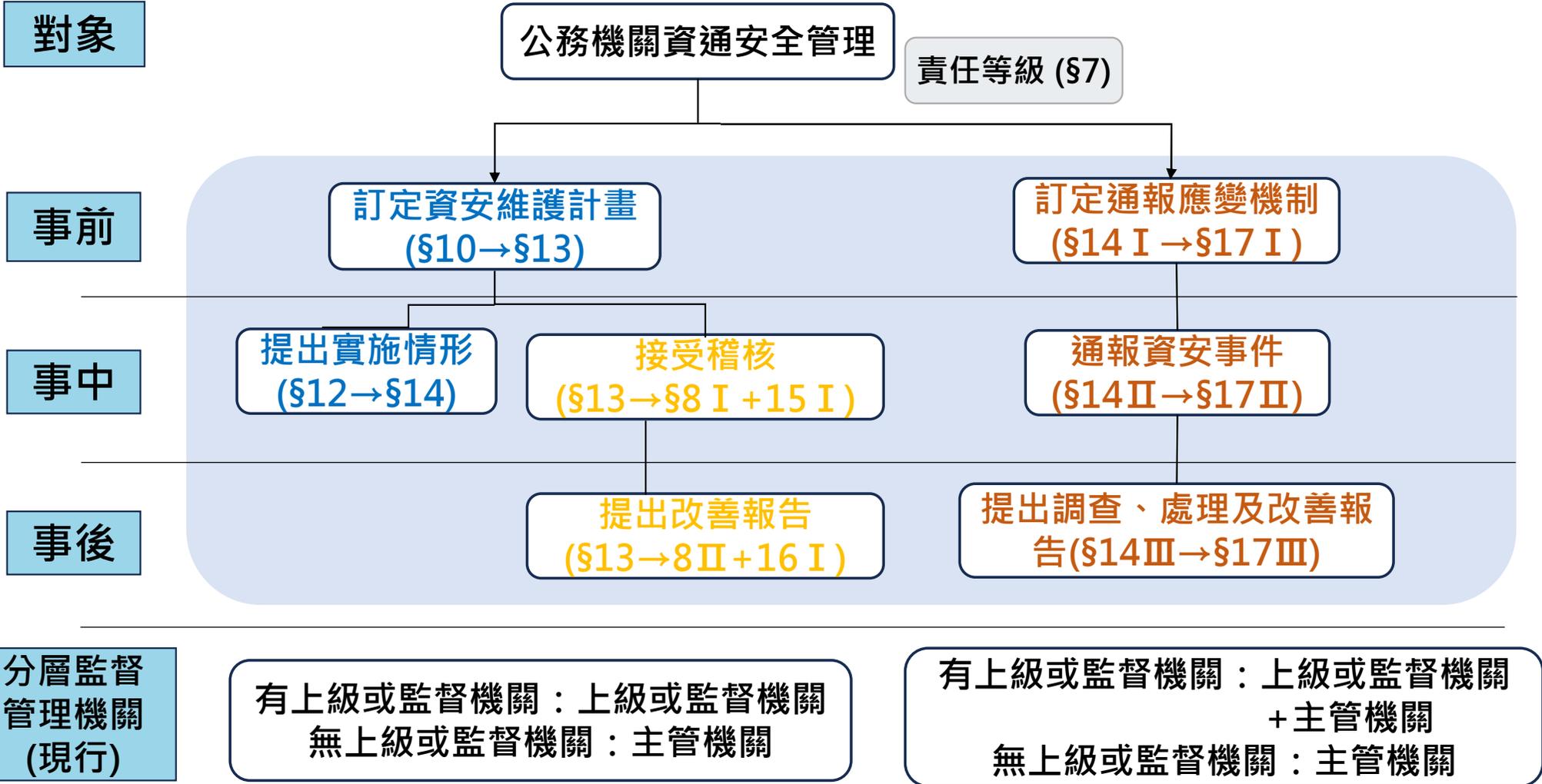
特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)



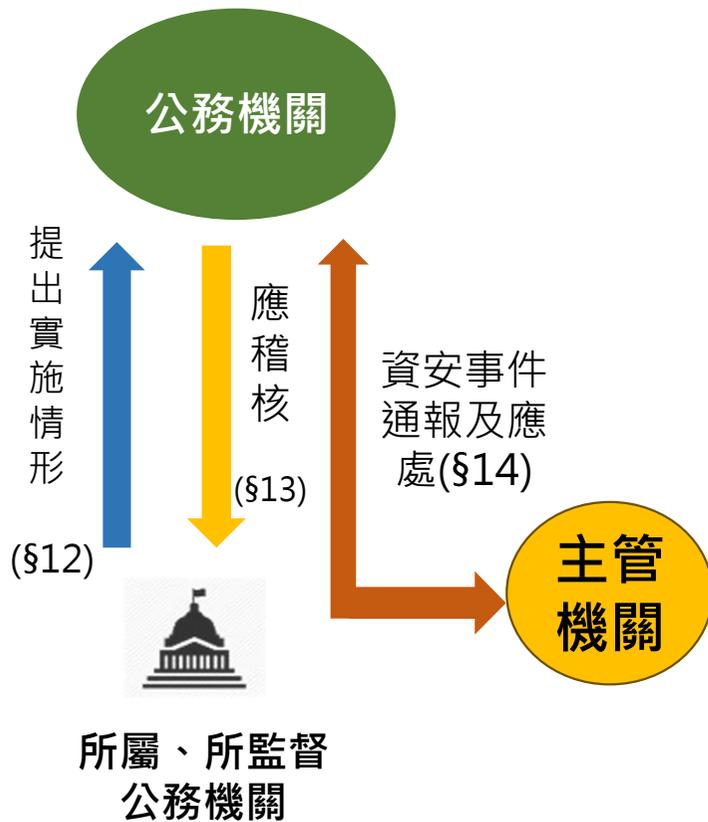
3-1分層監督管理模式調適



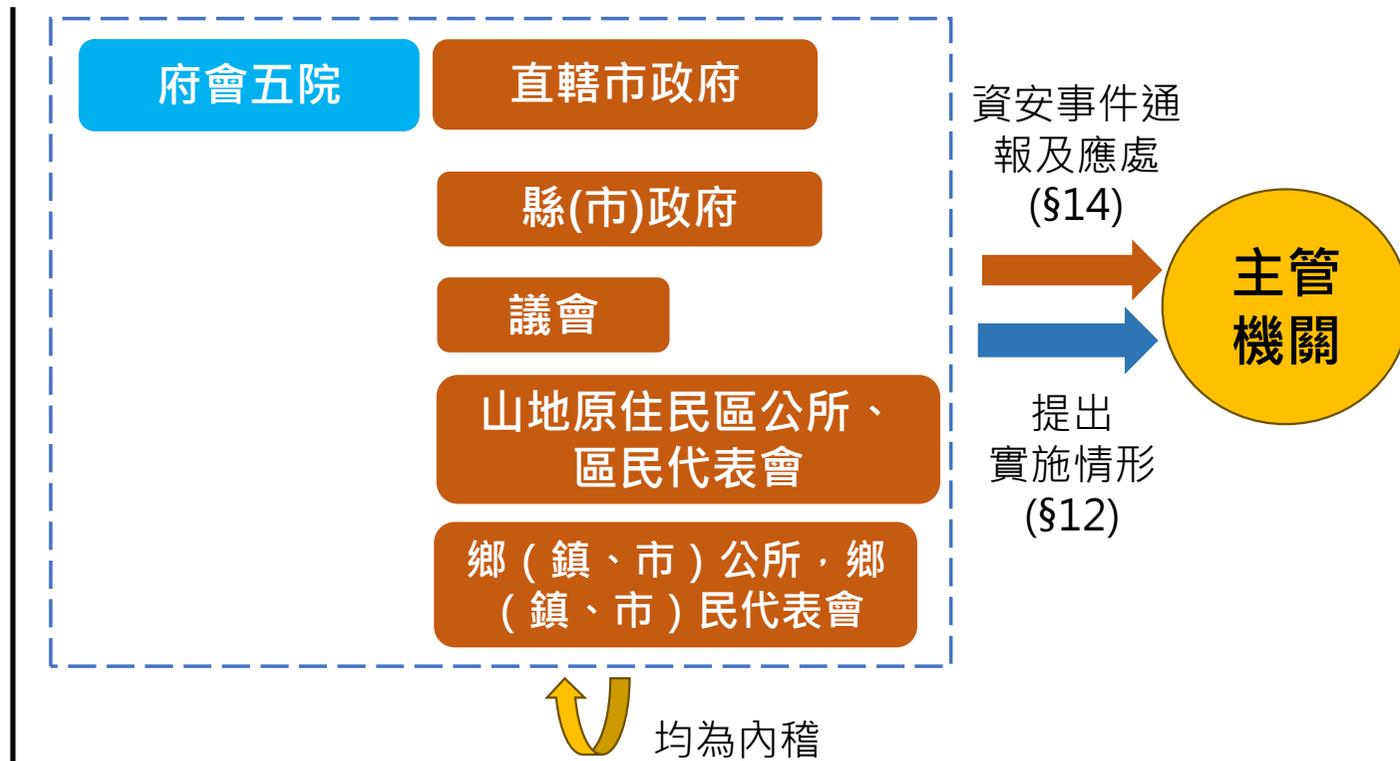


現行分層監督管理模式

有上級或監督機關



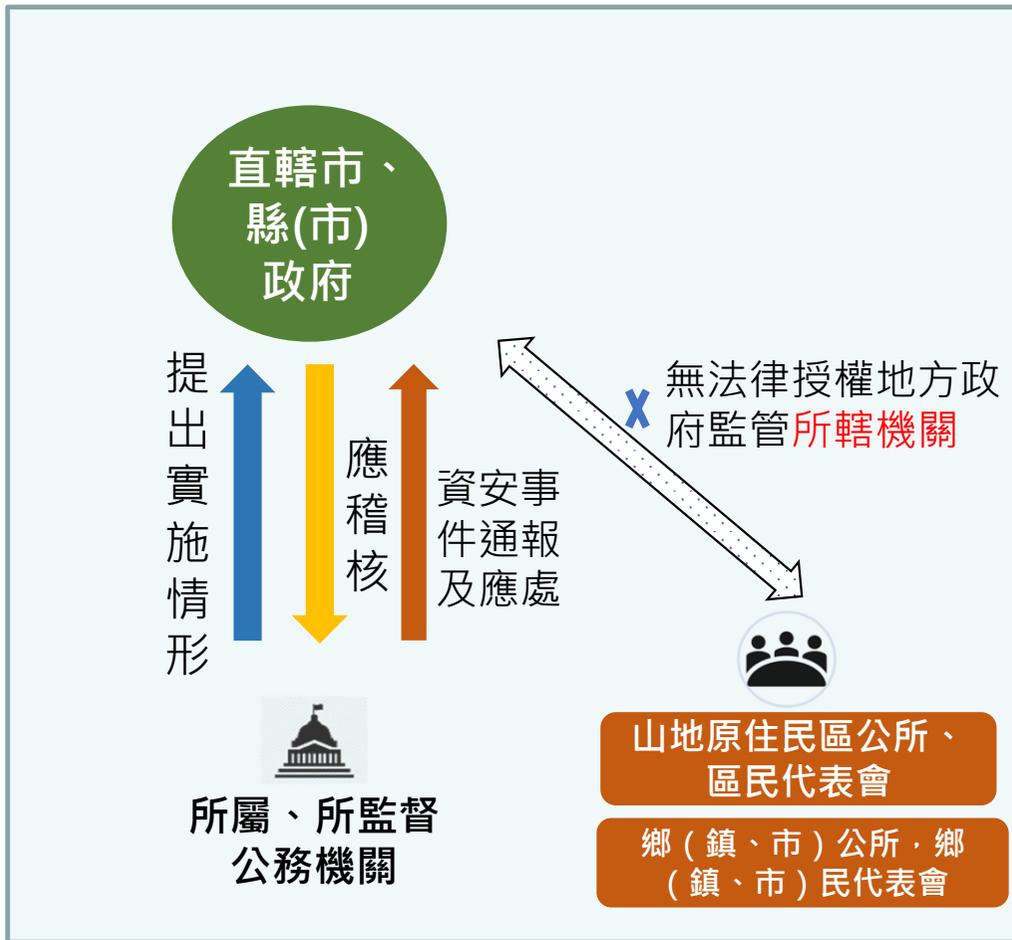
無上級或監督機關



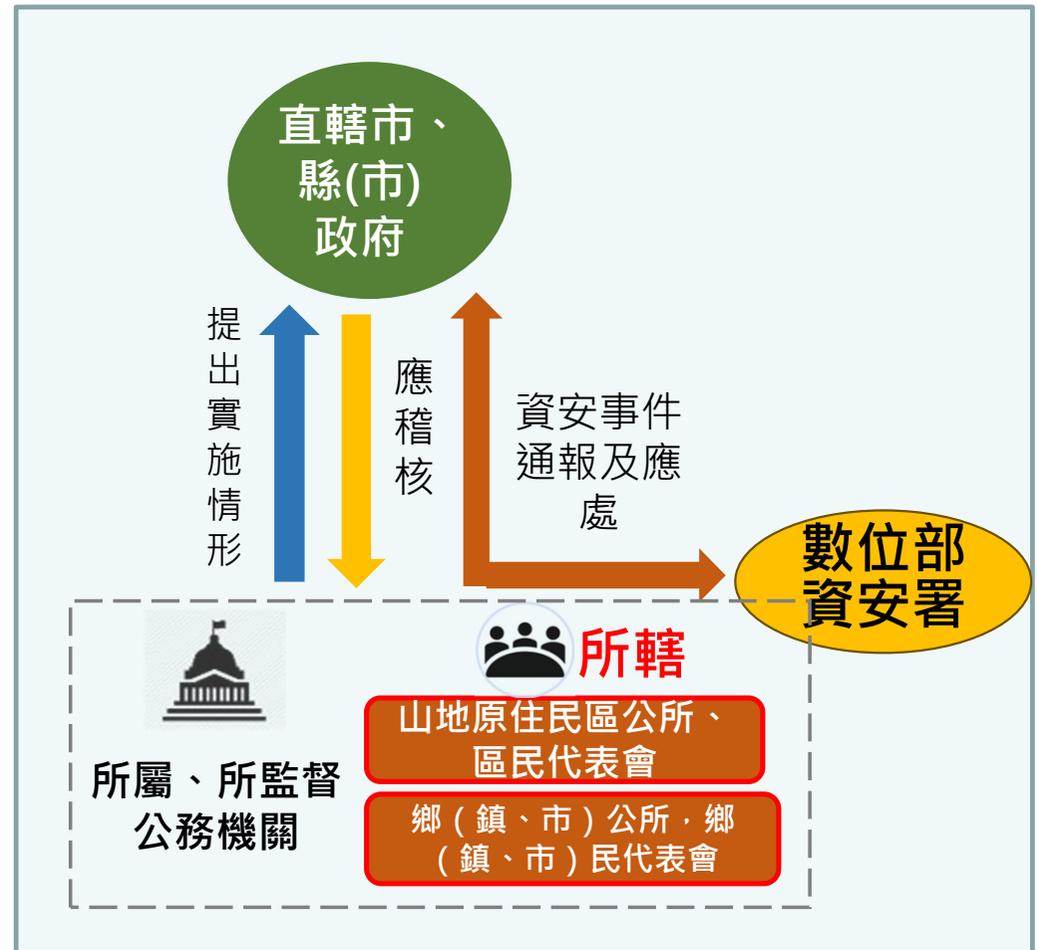


調修地方機關分層監督管理模式

現行



修正後





對照表：資通安全維護計畫實施情形提交

草案條文	現行條文	說明
<p>第14條 公務機關應每年向<u>上級機關或監督機關</u>提出資通安全維護計畫實施情形；無上級機關或監督機關者，其資通安全維護計畫實施情形應向下列機關提出： 一、<u>總統府、國家安全會議及五院</u>，向資安署提出。 二、<u>直轄市政府、直轄市議會、縣（市）政府及縣（市）議會</u>，向資安署提出。 三、<u>直轄市政府所轄山地原住民區公所、山地原住民區民代表會</u>向直轄市政府提出；<u>縣（市）政府所轄鄉（鎮、市）公所、鄉（鎮、市）民代表會</u>，向縣（市）政府提出。</p>	<p>第12條 公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。</p>	<ol style="list-style-type: none">1. 條次變更。2. 為明確規範公務機關資通安全維護計畫實施情形提出之管道，爰修正本條，按現行條文規定之運作模式定明公務機關資通安全維護計畫實施情形提出之對象。3. 為強化地區聯防，將直轄市山地原住民區公所、區民代表會、鄉（鎮市）公所以及鄉（鎮、市）民代表會之提出對象修正定明為直轄市政府及縣（市）政府，爰規定第三款



對照表：公務機關稽核範圍

草案條文	現行條文	說明
<p>第15條 公務機關應稽核其所屬、所監督之公務機關、<u>所轄鄉(鎮、市)公所、直轄市山地原住民區公所及鄉(鎮、市)民代表會、直轄市山地原住民區民代表會</u>之資通安全維護計畫實施情形。</p> <p><u>第十三條與前條資通安全維護計畫必要事項、實施情形之提出、前項稽核之頻率、內容、方法及其他相關事項之辦法，由主管機關定之。</u></p>	<p>第13條 公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。</p>	<ol style="list-style-type: none">1. 條次變更。2. 為落實資通安全聯防政策，公務機關資通安全維護計畫實施情形之稽核，採分層監督管理模式，依現行條文第一項規定，由上級機關或監督機關稽核之。惟無上級機關者，現行僅有內部稽核規定，爰於第一項增訂直轄市政府應稽核所轄直轄市山地原住民區公所、直轄市山地原住民區民代表會以及縣(市)政府應稽核所轄鄉(鎮、市)公所、鄉(鎮、市)民代表會。3. 修正條文第十三條與前條資通安全維護計畫必要事項、實施情形之提出、第一項稽核之頻率、內容、方法及其他相關事項，增訂第二項授權由主管機關以辦法定之。4. 現行條文第二項規定移列修正條文第十六條第一項，爰予刪除。



對照表：稽核改善報告

草案條文	現行條文	說明
<p>第16條 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應向稽核機關提出改善報告，並連同稽核結果依資安署指定之方式送交資安署。</p> <p>稽核機關或資安署，認有必要時，得要求受稽核機關進行說明或調整。</p>	<p>第13條第2項 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。</p>	<ol style="list-style-type: none">1. 除修正定明改善報告之提出對象外，並為利資安署掌握全國資通安全現況修正定明稽核結果及改善報告亦應送交該署。2. 為使稽核機關、資安署就受稽核機關之改善報告得進行監督及指導，爰增訂第二項，俾使其得就缺失或待改善事項妥為處理。



對照表：資安事件通報及應處

草案條文	現行條文	說明
<p>第17條第1~4項</p> <p>公務機關為因應資通安全事件，應訂定通報及應變機制。</p> <p>公務機關知悉資通安全事件時，<u>應向第十四條規定收受其實施情形之機關及資安署通報</u>。</p> <p>公務機關應向前項接獲通報機關提出資通安全事件調查、處理及改善報告前三項通報與應變機制之必要事項通報內容、報告之提出、演練作業及其他相關事項之辦法，由主管機關定之。</p>	<p>第14條</p> <p>公務機關為因應資通安全事件，應訂定通報及應變機制。</p> <p>公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。</p> <p>公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。</p> <p>前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。</p>	<ol style="list-style-type: none">1. 條次變更。2. 第一項未修正。3. 配合修正條文第十四條已定明公務機關資通安全維護計畫實施情形之提出對象，及實務運作現況，爰修正第二項及第三項。4. 為增進公務機關因應資通安全事件之處理能力，爰於第四項授權項目增訂演練作業俾利透過實施模擬演練以熟悉應變作為、



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第二方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

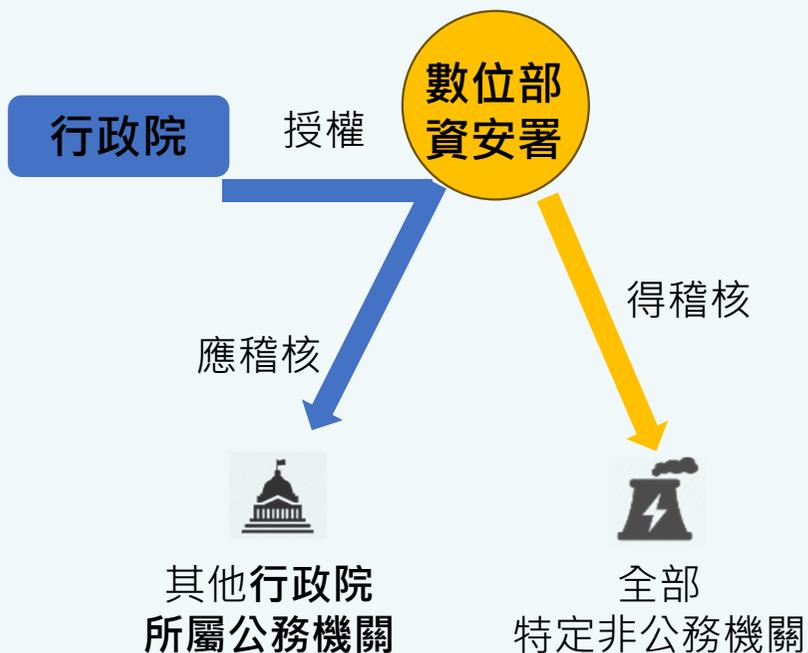
重大資安事件之行政調查程序及裁罰(\$25、29)



增訂資安署得稽核公務機關

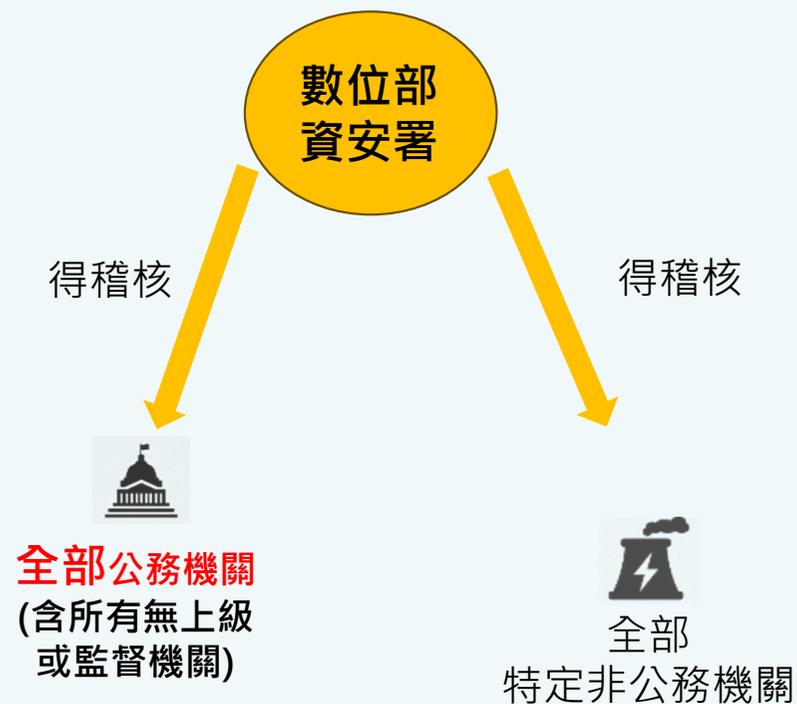
現行

- 主管機關(數位發展部)得稽核特定非公務機關
- 稽核其他公務機關需要其上級機關授權



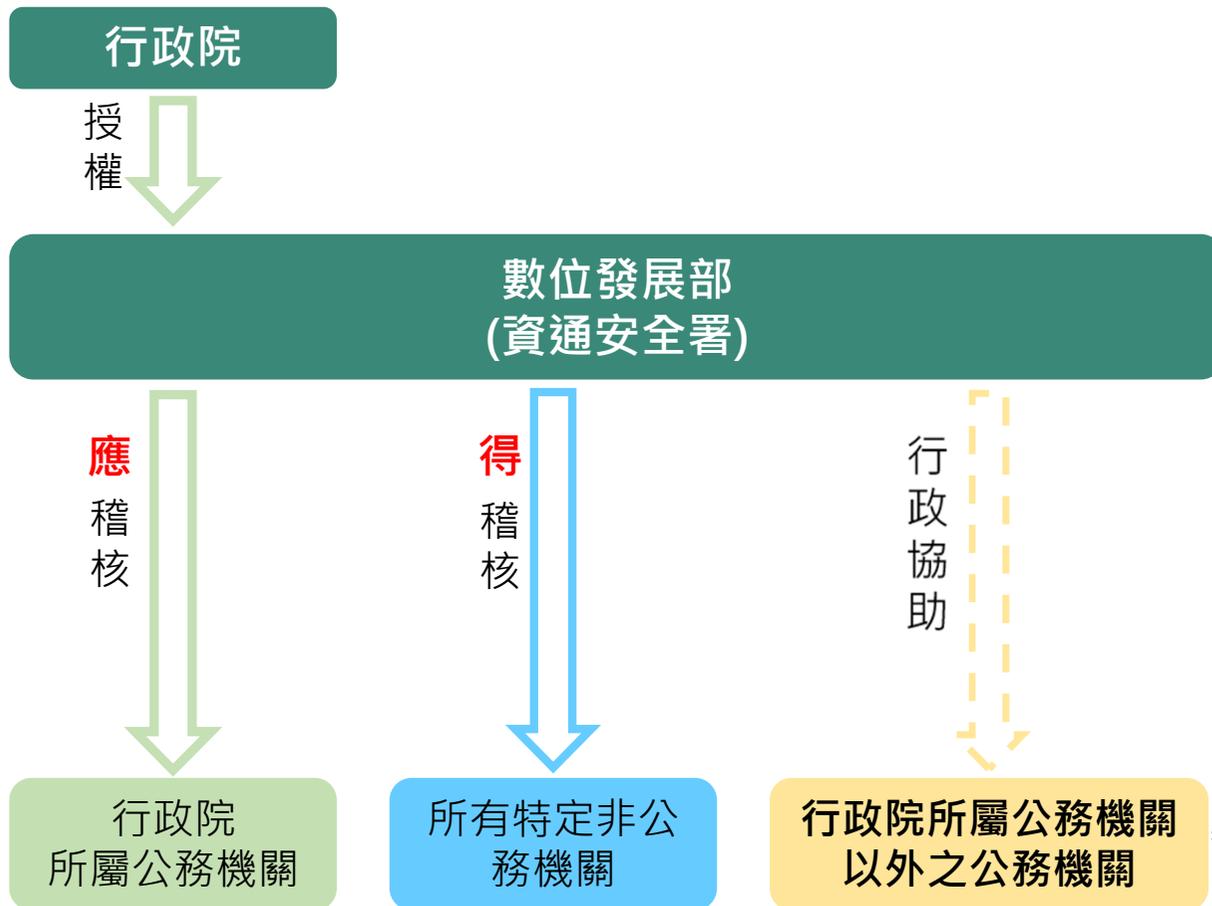
修正後

- 資安署得定期或不定期稽核公務機關及特定非公務機關，改善報告應送交上級機關、上級政府、監督機關或中央目的事業主管機關審查後，並送交資安署





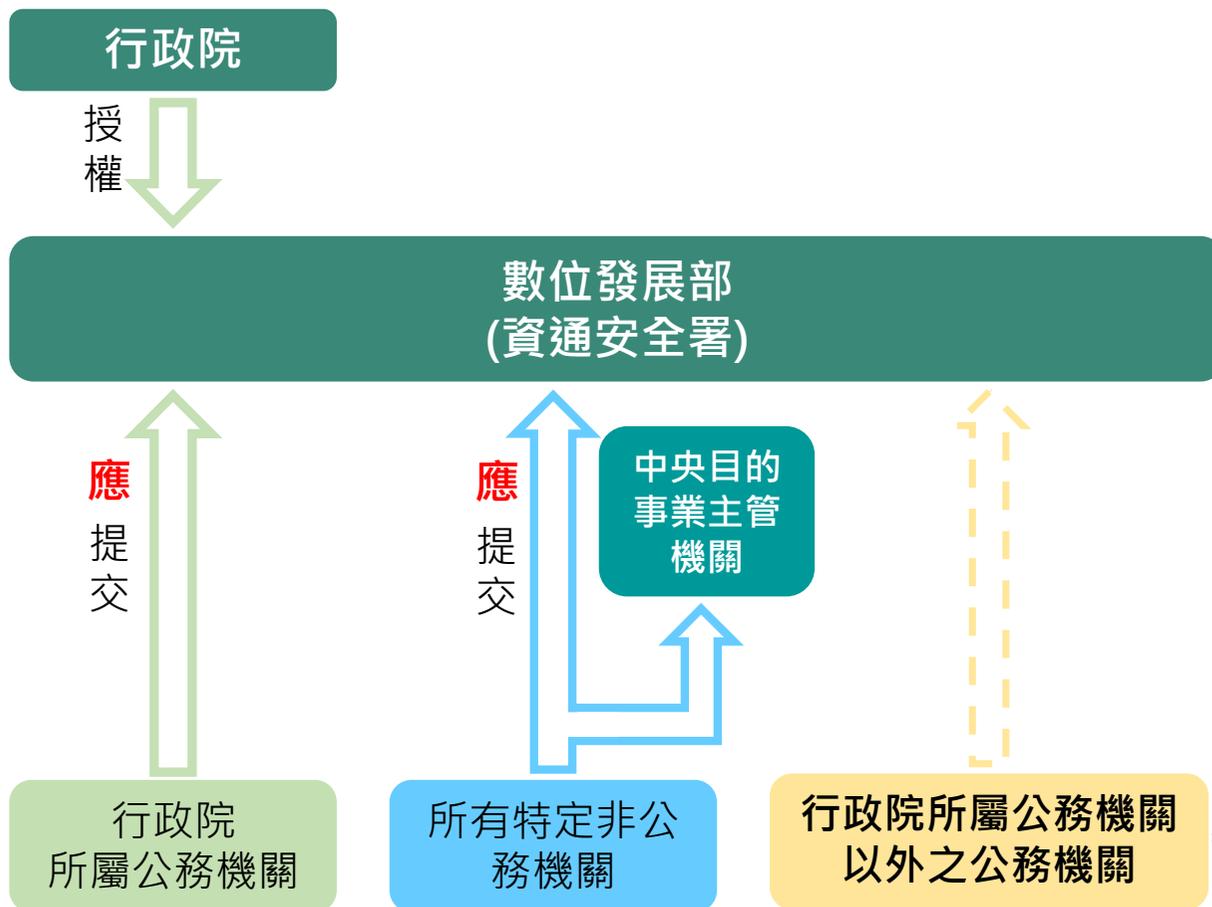
現行-實施稽核



*府會四院、直轄市縣市政府、直轄市
縣市議會、直轄市山地原住民區公所、
區民代表會、鄉(鎮)市公所、市民代
表會，及其所屬機關

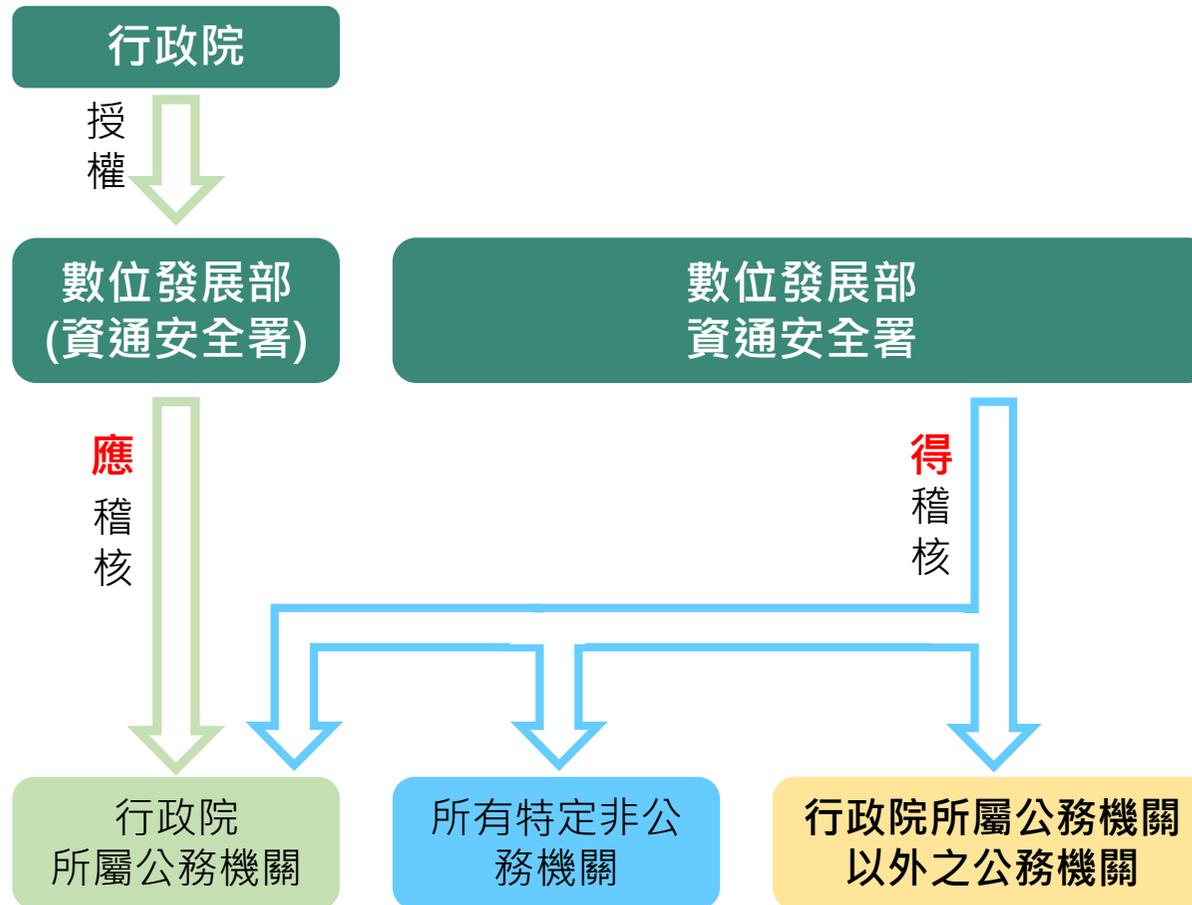


現行-提交稽核改善報告



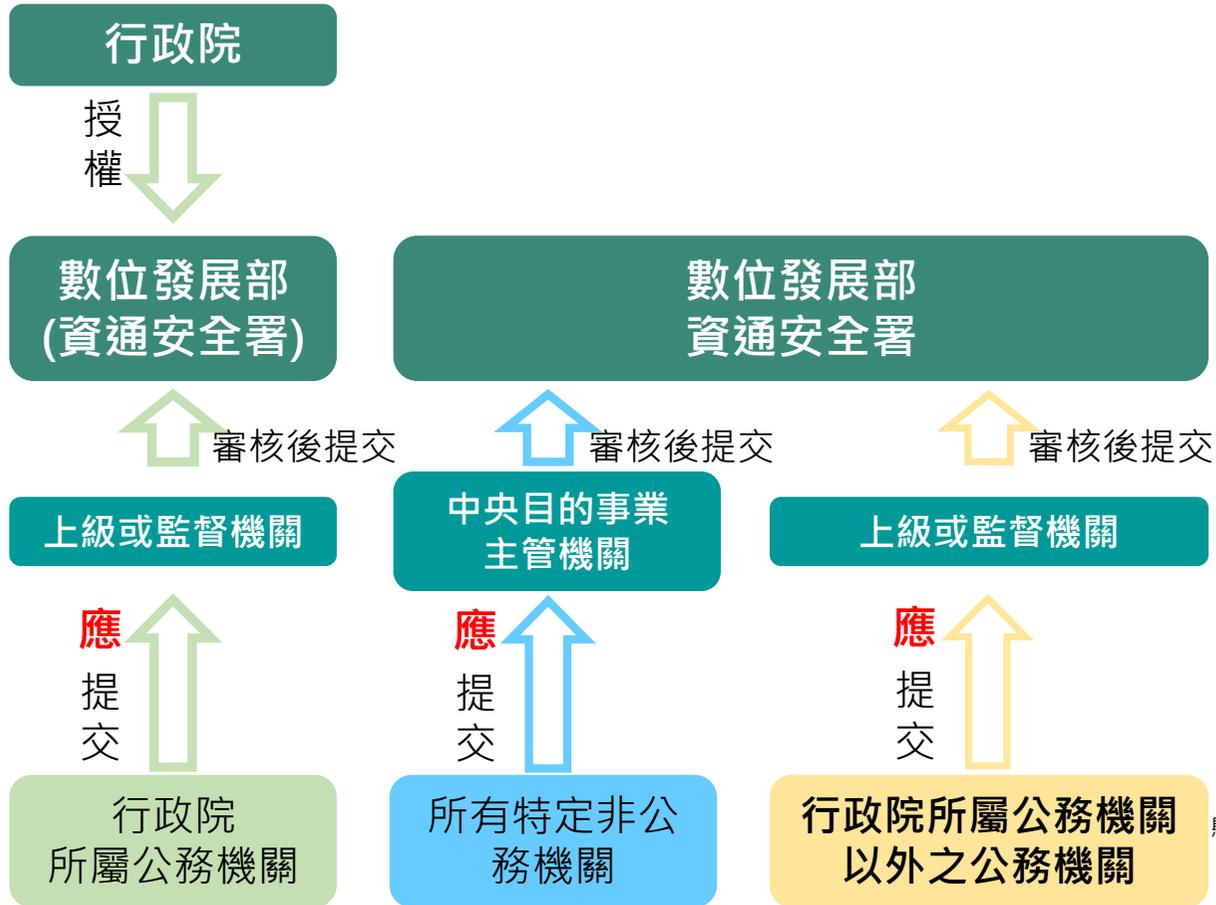


修正草案-實施稽核





修正草案-提交稽核改善報告

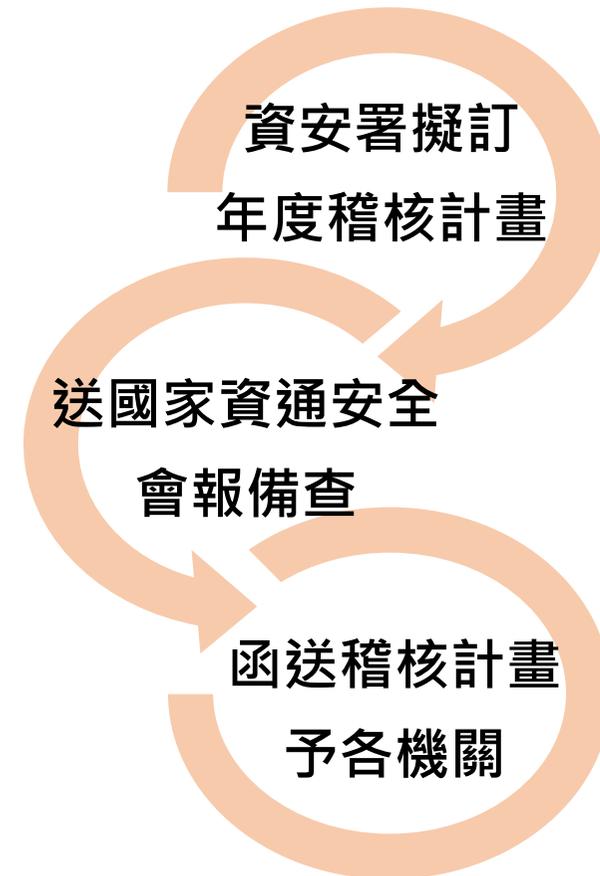


*府會四院、直轄市縣市政府、直轄市縣市議會、直轄市山地原住民區公所、區民代表會、鄉(鎮)市公所、市民代表會，及其所屬機關



預計辦理方式

- 由**資安署每年擬訂稽核計畫**，送各**上級機關**(府會四院、各部會行總處署及地方政府)。
- 由**資安署依計畫執行**，執行成果送交**國家資通安全會報備查**。
- 雖然資安署於修法後得稽核所有資安法納管對象，**各機關仍須依資安法規**定，**稽核其所屬、所監督、所轄機關之資通安全維護計畫實施情形**，以符合資安法分層監督管理精神。





對照表

草案條文	現行條文	說明
<p>第8條 資安署得定期或不定期稽核<u>公務機關</u>及特定非公務機關之資通安全維護計畫實施情形。</p> <p>前項稽核後，發現受稽核機關資通安全維護計畫實施情形有缺失或待改善者，改善報告應送交<u>上級機關、上級政府、監督機關或中央目的事業主管機關</u>審查後，並送交資安署。</p> <p>前項收受改善報告之機關認有必要時，得要求受稽核機關進行說明或調整。</p> <p>前三項資通安全維護計畫實施情形之稽核頻率、內容與方法及其他相關事項之辦法，由主管機關定之。</p> <p>第一項稽核由資安署擬訂年度計畫後辦理，年度計畫及年度成果報告應送交<u>國家資通安全會</u>報備查。</p>	<p>第7條 (第1項略)</p> <p>主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。</p> <p>特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。</p>	<ol style="list-style-type: none">1. 第一項由現行條文第七條第二項前段規定移列，並為協助公務機關檢視自身資通安全維護計畫實施情形增訂資安署得稽核公務機關。2. 第二項由現行條文第七條第三項規定移列，並配合實務執行需求修正就現行受稽核機關之改善報告送交及審查流程細緻化規範。3. 為使收受改善報告之機關得對受稽核機關進行監督及指導，爰增訂第三項，俾使其得就缺失或待改善事項妥為處理。4. 第四項由現行條文第七條第二項後段規定移列，並酌作修正。5. 為使第一項稽核辦理有據，並考量事涉公務機關及特定非公務機關，有賴各政府機關間配合推動執行，爰增訂第五項。



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第二方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)



3-2增訂重大資安事件之協助及公告

草案條文	現行條文	說明
<p>第17條第5項 第二項接獲通報機關知悉重大資通安全事件時，得提供公務機關相關協助，並於適當時機得公告與事件相關之必要內容及因應措施。</p>		<p>考量重大資通安全事件可能影響多數人民之生命、身體或財產安全，爰比照特定非公務機關之規定，增訂第五項，由接獲通報機關於知悉後，分別或共同公告必要之內容(例如發生原因、影響程度及目前控制之情形等)及因應措施，並提供相關協助，以利防範、避免損害之擴大。</p>



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第二方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)



3-3 資安人力類一條鞭



- 升遷、遷調受限
- 歷練不足，能力受限
- 資安人員流動率高

資安人力無統籌機制，
不利於國家整體資安防禦

資安人員統籌機制

3-3 資安人力類一條鞭

➢ 持續推動資安職能訓練、評量及核發資安職能證書，逐步建立資安人才資料庫，以協助用人機關檢視資安專業能力

➢ **調度支援**：遇有重大資通安全事件，得調度各級機關資通安全人員支援，並視為在職訓練的一環

➢ 推動專職人員之在職訓練

➢ **機關與機關人員績效評核及獎勵**

➢ 評量重點：法適應辦事項及資安管理作業執行情形、其他資安業務創新作為。





對照表

草案條文	現行條文	說明
<p>第18條 公務機關應符合其資通安全責任等級之要求，設置專職資通安全人員，辦理資通安全業務及應變處理；資通安全業務績效評核優良者，應予獎勵。</p> <p>資安署應妥善規劃推動專職人員之職能訓練，增進其資通安全專業知能；遇有重大資通安全事件，資安署得逕予調度各級機關資通安全人員支援之。</p> <p>前二項人員調度支援、績效評核、獎勵及職能訓練相關事項之辦法，由主管機關定之。</p>	<p>第15條 公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。</p> <p>前項獎勵事項之辦法，由主管機關定之。</p>	<ol style="list-style-type: none">1. 公務機關依資通安全責任等級分級辦法附表一、三、五之規定，應設置一定人數之專職人員辦理資通安全業務，為強化公務機關之資通安全防護能量，爰將其意旨修正納入第一項。2. 因資通安全人員之專業知能，與公務機關資通安全防護能量有密切關係，為強化並提升公務機關專職人員之職能，爰增訂第二項並明定重大資安事件，資安署得調度人員支援之規定，可同時加強訓練人員之應處能力。3. 現行條文第二項配合修正條文第一項及第二項，新增授權項目，並移列為第三項。



報告大綱

修法重點

一.明確劃分權責機關

二.明確法源

三.強化公務機關資安管理

四.修正特非機關範圍及強化資安管理



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第二方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

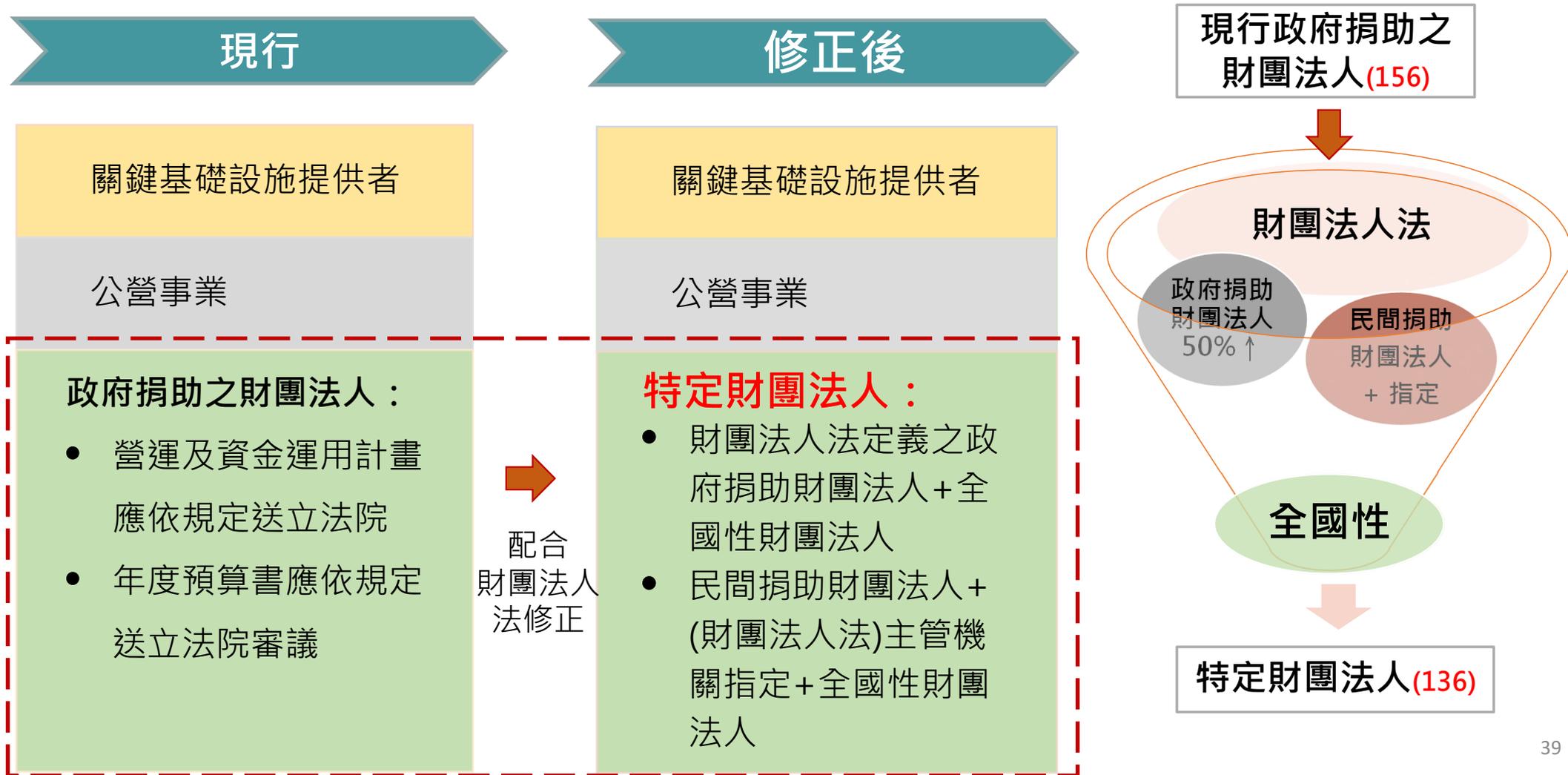
特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)



4-1修正特定非公務機關納管範圍(1/2)





4-1修正特定非公務機關納管範圍(2/2)

● 差異分析

減少納管 26 個 財團法人	增加納管 6 個 財團法人
<ul style="list-style-type: none">■ C級：6個■ D級：9個■ E級：10個■ 裁撤：1個	<ul style="list-style-type: none">■ 財團法人金融聯合徵信中心■ 財團法人證券投資人及期貨交易人保護中心■ 財團法人保險事業發展中心■ 財團法人汽車交通事故特別補償基金■ 財團法人住宅地震保險基金■ 財團法人保險安定基金



對照表

草案條文	現行條文	說明
<p>第3條 六、特定非公務機關：指關鍵基礎設施提供者、公營事業或特定財團法人。</p> <p>九、特定財團法人：指符合財團法人法第二條第二項、第三項或第六十三條第一項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者。</p>	<p>第3條 六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。</p> <p>九、政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。</p>	<ol style="list-style-type: none">1. 第六款配合第九款用詞修正為特定財團法人。2. 現行條文第九款制定公布時財團法人法尚未完成立法，考量該法已制定公布施行，爰定明符合財團法人法第二條第二項、第三項或第六十三條第一項規定，且屬該法第二條第八項所定全國性財團法人者，為本法所稱特定財團法人，爰修正第九款。



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第二方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

特定財團法人定義(\$3⑨)

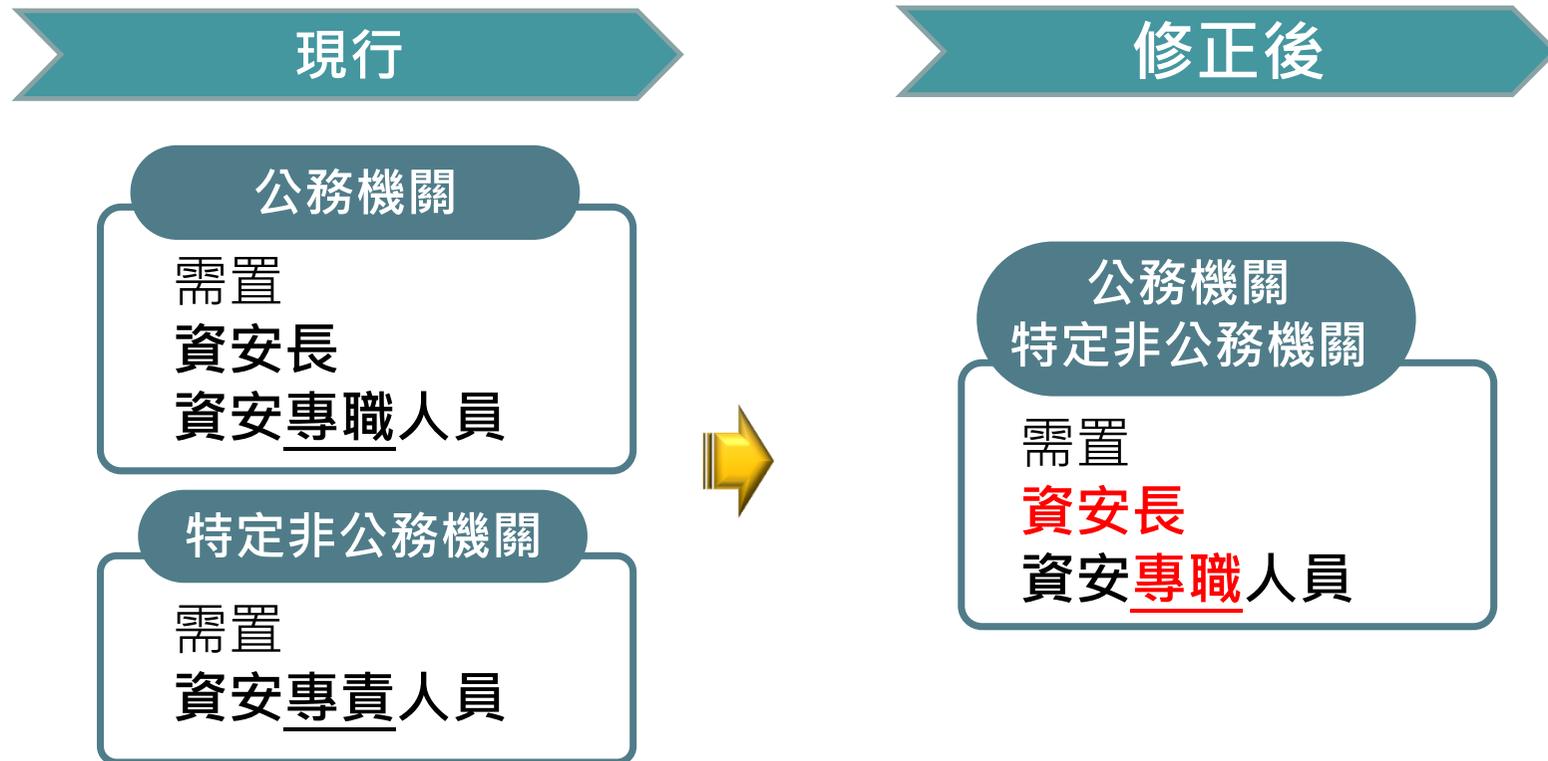
專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)



4-2 應設置專職人員及資安長

- 強化特定非公務機關資通安全能量，規劃比照公務機關應設置資安長及資安專職人員。





對照表：專職人員

草案條文	現行條文	說明
<p>第20條 第1項 <u>關鍵基礎設施提供者</u>應符合其所屬資通安全責任等級之要求，<u>設置資通安全專職人員</u>，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p>	<p>第16條第2項 關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p>	<p>符合特定資通安全責任等級之機關，應設置專人專職辦理資通安全業務之要求，宜由現行法規命令提昇至法律位階，爰予修正。</p>
<p>第21條第1項 <u>關鍵基礎設施提供者以外</u>之特定非公務機關，應符合其所屬資通安全責任等級之要求，<u>設置資通安全專職人員</u>，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p>	<p>第17條第1項 關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p>	



對照表：資安長

草案條文	現行條文	說明
<p>第23條 特定非公務機關應置資通安全長，由特定非公務機關之代表人、管理人、其他有代表權人或其指派之適當人員擔任，負責推動及監督機關內資通安全相關事務。</p>		<ol style="list-style-type: none">1. 本條新增。2. 為確保有效推動資通安全維護事項，比照公務機關規定特定非公務機關應置資通安全長，由其成立相關推動組織及督導推動相關工作。



修正重點鳥瞰圖

修法目標

明確劃分權責機關

明定行政院、主管機關、資安署及中央目的事業主管機關各別權責事項

設置國家資通安全會報、決議事項之執行及合作協力義務(\$5)

修法重點

明確法源

用詞定義修正(\$3)

委外辦理之管理及監督機制(\$10)

明定危害國家資安產品之管制(\$11)

明定關鍵基礎設施提供者之指定程序(\$19)

委任權限移轉之法規依據(\$30)

資安事件涉個資外洩時另依個資法辦理(\$31)

強化公務機關資安管理

分層監督管理模式調適：第三方稽核、資安計畫實施情形之提出對象、資安事件通報對象(\$8、14、15、16、17II)

重大資安事件之協助及公告(\$17V)

資安人員統籌機制：資安人力類一條鞭(\$18)

修正特非機關範圍及強化資安管理

特定財團法人定義(\$3⑨)

專職人員及資安長之設置(\$20、21、23)

重大資安事件之行政調查程序及裁罰(\$25、29)



4-3 重大資安事件之行政調查程序及裁罰

事中-無法主動確認應處情形

- **現行規定**：發生重大資安事件，主管機關或中央目的事業主管機關僅得提供**協助(不具強制力)**。
- **問題**：在改善報告送交前，縱使再次發生資安事件，政府無法主動、即時且有效的確認應變處置是否確實有效。

即時、主動確認



事後-難以掌握改善情形

- **現行規定**：由中央目的事業主管進行改善報告之審查；如為重大資安事件另送數位部資安署，且原則皆採**書面審查**模式。
- **問題**：書面審查，較難掌握機關是否確實完成改善及機關防護措施是否失效。

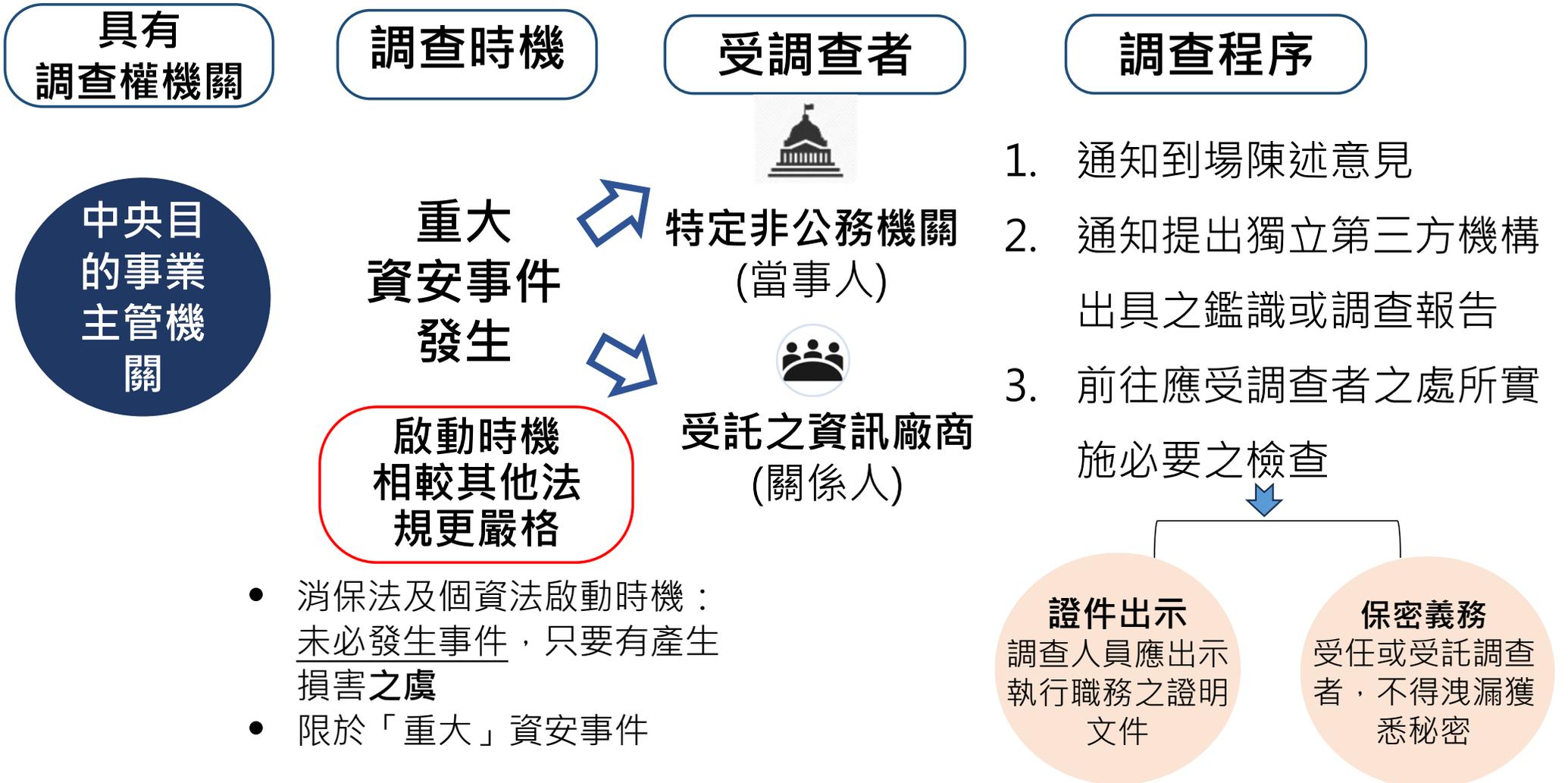
確實掌握改善情形



增加**行政調查**權限



修正草案





對照表

草案條文	現行條文	說明
<p>第25條</p> <p>中央目的事業主管機關為辦理特定非公務機關發生重大資通安全事件之調查，得依下列程序辦理：</p> <ol style="list-style-type: none">一. 通知當事人或關係人到場陳述意見。二. 通知當事人及關係人提出獨立第三方機構出具之鑑識或調查報告。三. 派員、委任或委託其他機關(構)前往當事人及關係人之處所實施必要之檢查。 <p>前項所定關係人，以第一項特定非公務機關委託辦理資通系統之建置、維運或資通服務之提供之受託者，且與重大資通安全事件相關者為限。</p> <p>受調查者對於中央目的事業主管機關依第一項所為之調查，不得規避、妨礙或拒絕。</p> <p>執行調查之人員應出示有關執行職務之證明文件；其未出示者，受調查者得拒絕之。</p> <p>第一項第三款受委任或委託之機關(構)對於辦理受任或受託事務所獲悉特定非公務機關之秘密，不得洩漏。</p>		<ol style="list-style-type: none">1. 本條新增。2. 為落實特定非公務機關資通安全之維護，強化中央目的事業主管機關之監督權責，爰規定第一項賦予中央目的事業主管機關對於重大資通安全事件之調查權。3. 為符合法律明確性原則，定明應受調查之關係人範圍，爰增訂第二項。4. 配合第一項規定中央目的事業主管機關對特定非公務機關重大資通安全事件之調查權責，爰於第三項增訂受調查者對主管機關所為調查措施，無正當理由不得規避、妨礙或拒絕，並於第四項增訂中央目的事業主管機關執行調查時應出示證明文件之程序。5. 為避免特定非公務機關之秘密，因重大資通安全事件之調查而洩漏，爰增訂第五項受委任或委託機關(構)之保密義務。



對照表：規避行政調查之罰則

草案條文	現行條文	說明
<p>第29條 違反第二十五條第三項規定，規避、妨礙或拒絕調查者，由中央目的事業主管機關處新臺幣十萬元以上一百萬元以下罰鍰。</p>		<ol style="list-style-type: none">1. 本條新增。2. 配合修正條文第二十五條第三項，增訂違反者之處罰規定。



數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理