國家資通安全通報應變

作業綱要

中 華 民 國 102 年 9 月 9 日

目　錄

第 1 章 前言

行政院國家資通安全會報(以下簡稱本會報)為有效掌握我國政府機關及公民營事業機構之資通訊及網路系統遭受破壞、不當使用等資通安全事件(以下簡稱資安事件)，能迅速雙向通報及緊急應變處置，並在最短時間內回復，以確保國家利益與政府之正常運作，特訂定國家資通安全通報應變作業綱要(以下簡稱本綱要)。

本綱要分為 6 章，除前言外依整體作業、通報作業、應變作業、資安演練作業、獎懲及減責標準等逐項規範或說明。其中整體作業含本會報組織架構、主管機關職掌、資安事件影響等級定義及作業流程等，明確律定於資安事件發生時通報應變作業程序；通報作業含各級政府機關(構)、主管機關及本會報通報作業方式及要求；應變作業含各級政府機關(構)事前安全防護、事中緊急應變、事後復原作業及主管機關應變作業檢討等；資安演練含本會報所辦理及資通安全處理小組應辦理之相關資通安全演練作業，據以檢測各級政府機關(構)資通安全防護及應變管控能力；獎懲及減責標準含提報獎勵標準、懲處規定及減責規定等。

本綱要務請各級政府機關(構)落實執行，俾配合推動提升通報應變時效、健全資安防護能力、深化資安認知及教育等措施，以全面強化政府資安防護機制，確認政府擁有安全、可信賴的資通訊環境。

第 2 章 整體作業

2.1 行政院國家資通安全會報組織架構

本會報負責國家資通訊安全相關事項之政策諮詢審議、協調及推動，其幕僚作業由行政院資通安全辦公室(以下簡稱資安辦)辦理，本會報下設網際防護及網際犯罪偵防等二體系，下設相關組，組織架構如圖 1。

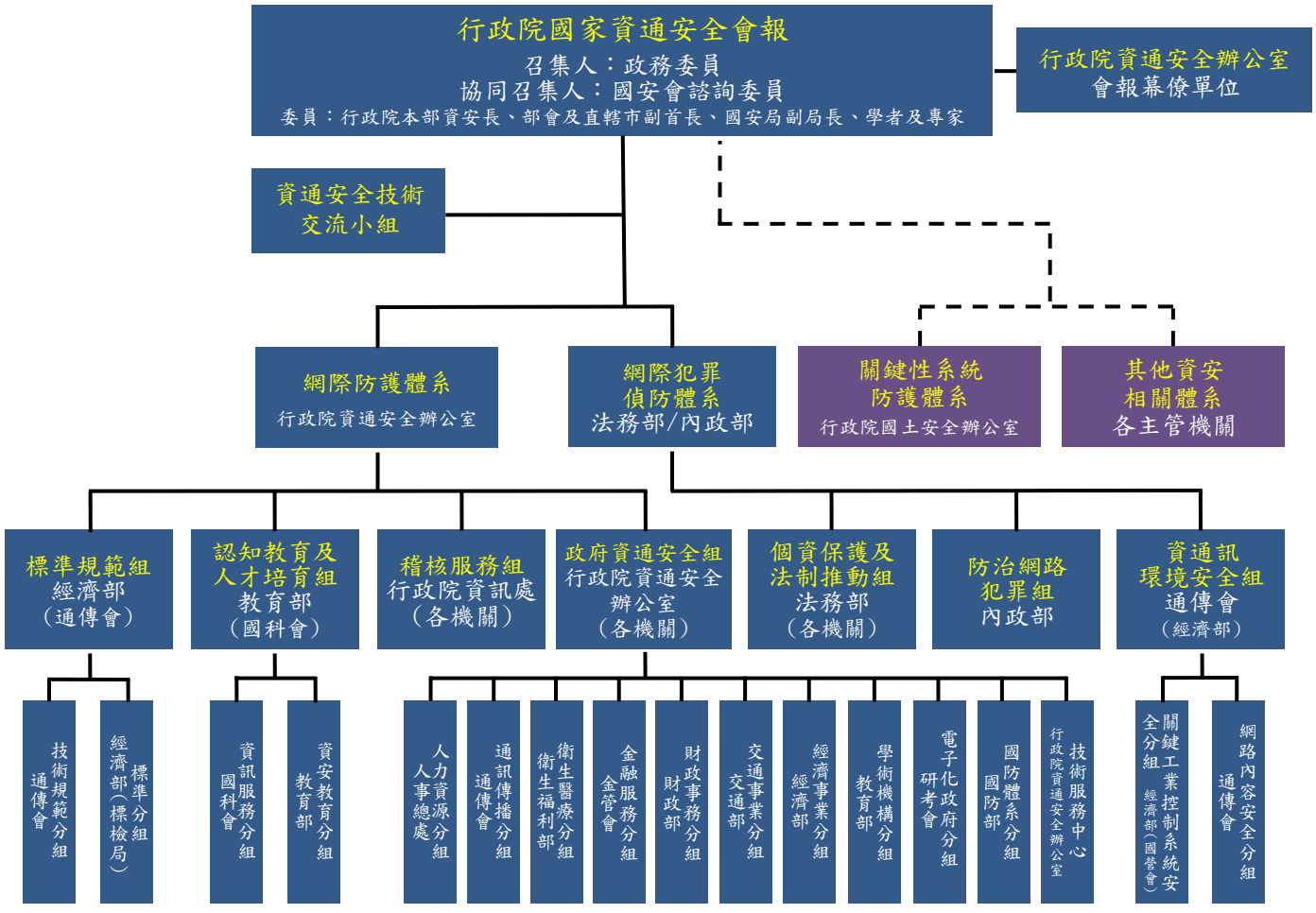

圖 1 行政院國家資通安全會報組織架構圖

網際防護體系由資安辦主辦，負責整合資安防護資源，推動資安相關政策；網際犯罪偵防體系由法務部及內政部共同主辦，負責防範網路犯罪、維護民眾隱私及建立資通訊基

礎建設安全等工作。

網際防護體系之政府資通安全組由資安辦主責，負責規劃、推動政府各項便民資通訊應用服務之安全機制，輔導政府機關資安技術服務、資安防護及應變，統合政府機關資安人力充實及運用,其下包括國防體系分組、電子化政府分組、學術機構分組、經濟事業分組、交通事業分組、財政事務分組、金融服務分組、衛生醫療分組、通訊傳播分組及人力資源分組等 10 個分組，並成立行政院國家資通安全會報技術服務中心(以下簡稱技術服務中心)，為執行國家資通安全通報應變作業之技術幕僚單位。各分組之主責機關及轄管範圍如下表：

表 1 政府資通安全組各分組主責機關及轄管範圍表

分組別	主責機關	轄管範圍
國防體系	國防部	國防體系
電子化政府	行政院研究發展考核委員會	電子化政府
學術機構	教育部	學校及研究機構
經濟事業	經濟部	電力、石油、自來水及瓦斯等事業機構
交通事業	交通部	郵政及交通運輸等事業機構
財政事務	財政部	財稅及關貿等事務機構
金融服務	金融監督管理委員會	金融服務業
衛生醫療	衛生福利部	衛生醫療機構
通訊傳播	國家通訊傳播委員會	電信及通訊傳播業
人力資源	行政院人事行政總處	人力資源相關

2.2 主管機關

應由機關之副首長兼任資安長(無副首長者由首長指派)，並設置「資通安全處理小組」，由資安長擔任召集人，

負責制定資安事件通報應變作業計畫，執行資通安全預防、危機通報及緊急應變處理相關措施，並納入機關(構)業務永續運作計畫之一部分；同時亦須協助所屬機關(構)之資安事件通報及應變處理作業，主管機關列表詳如附件。

2.3 資安事件影響等級

資安事件影響等級分為 4 個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」。

（一）4級事件

符合下列任一情形者，屬 4 級事件：

1. 國家機密資料遭洩漏。
2. 國家重要資訊基礎建設系統或資料遭竄改。
3. 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

（二）3級事件

符合下列任一情形者，屬 3 級事件：

1. 密級或敏感公務資料遭洩漏。
2. 核心業務系統或資料遭嚴重竄改。
3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

（三）2級事件

符合下列任一情形者，屬 2 級事件：

1. 非屬密級或敏感之核心業務資料遭洩漏。
2. 核心業務系統或資料遭輕微竄改。
3. 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

（四）1級事件

符合下列任一情形者，屬 1 級事件：

1. 非核心業務資料遭洩漏。
2. 非核心業務系統或資料遭竄改。
3. 非核心業務運作遭影響或短暫停頓。

2.4 通報及應變作業流程

資安事件通報及應變作業流程如圖 2 所示，相關作業程序請參見「第 3 章 通報作業」及「第 4 章 應變作業」。

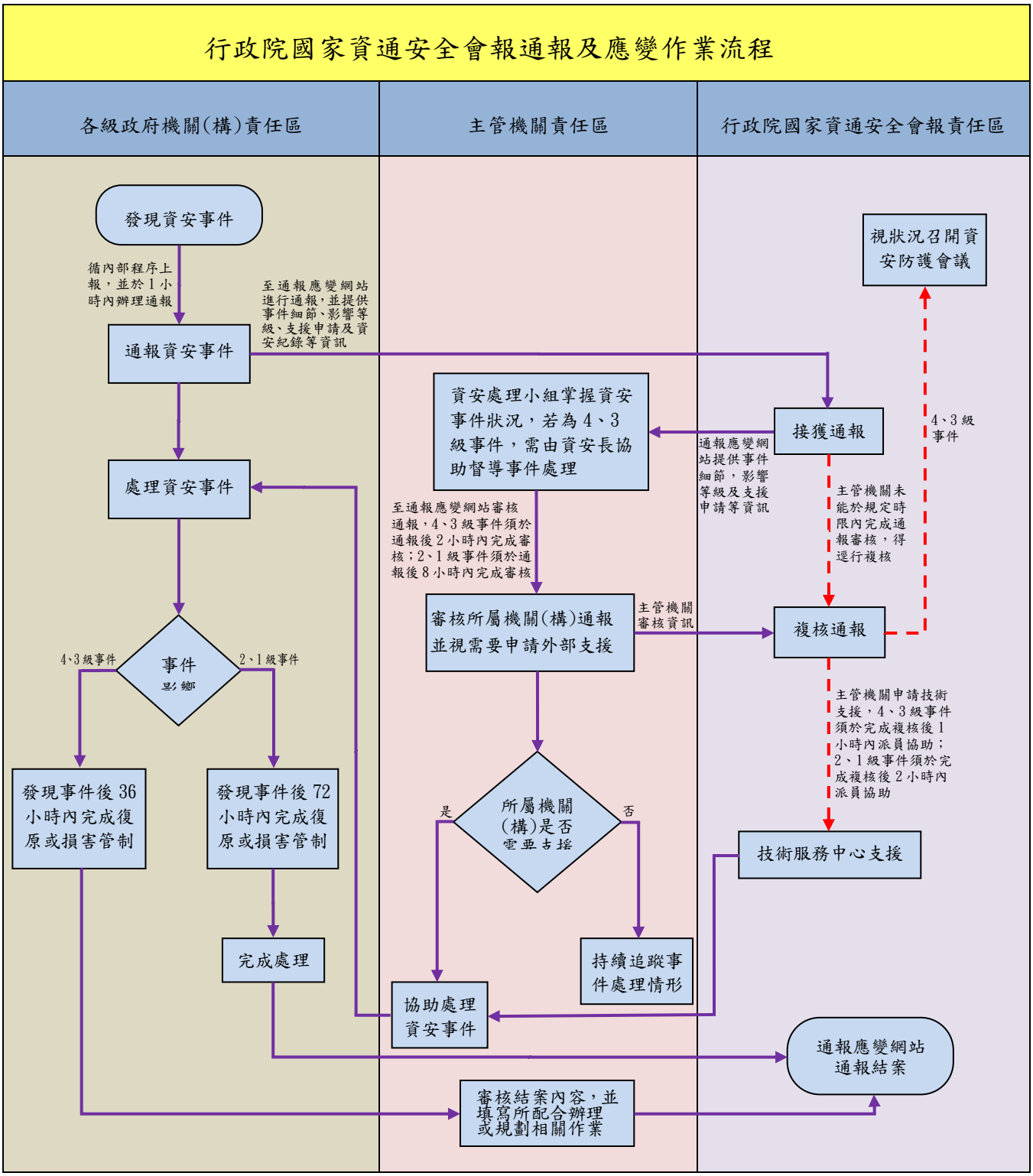

圖 2 資安事件通報及應變作業流程

各級政府機關(構)通報資安事件或進行結案，以及主管機關審核所屬機關(構)資安事件通報或結案時，均須至國家資通安全通報應變網站(以下簡稱通報應變網站)登錄作業，該網站營運維護、資安事件通報管理、技術諮詢及支援等服務，由本會報委託技術服務中心負責，聯繫資訊如下：

（一）網址：https://www.ncert.nat.gov.tw

（二）聯絡電話：(02)2733-9922（24小時專線電話）

（三）傳真：(02)2733-1655

（四）電子郵件：service@icst.org.tw

依本綱要進行資安事件通報、處理及聯繫等相關作業，各級政府機關(構)須至通報應變網站登錄並定期更新資訊主管及資安聯絡人(至少2位，並以資安專責人員為優先)等相關資訊；倘屬主管機關，則另須登錄並定期更新資安長及資安審核人等相關資訊，以確保資安通報流程之順利運作。

第 3 章 通報作業

3.1 各級政府機關(構)

（一）各級政府機關(構)發現資安事件後除應循內部程序上報外，並須於 1 小時內，至通報應變網站通報登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關(構)或重要民生設施運作，需橫向通知本會報政府資通安全組相關分組。

（二）如因網路或電力中斷等事由，致使無法上網填報資安事件，須於發現資安事件後 1 小時內，與技術服務中心聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。

（三）進行資安事件處理，「4」、「3」級事件須於 36 小時內完成復原或損害管制；「2」、「1」級事件須於 72 小時內完成復原或損害管制。

（四）完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理辦法及完成時間。

3.2 主管機關

（一）主管機關(資通安全處理小組)在接獲所屬機關(構)通報後，應主動掌握事件狀況、協助所屬機關(構)進行資安事件應變處理，並督導事件處理過程。如資安事件屬「4」、「3」級事件，技術服務中心將主動通知主管機關之資安長及資訊主管。

（二）主管機關須至通報應變網站審核所屬機關(構)資安事件通報，並評估該事件是否影響其他政府機關(構)或重要民生設施運作以及事件影響等級之合理性，視需要申請技術支援。如資安事件屬「4」、「3」級事件，

須於通報後 2 小時內完成審核；「2」、「1」級事件，須於通報後 8 小時內完成審核。

（三）各級政府機關(構)完成資安事件處理後，至通報應變網站通報結案，如資安事件屬「4」、「3」級事件，主管機關將接獲所屬機關(構)結案申請後，須至通報應變網站審核所屬機關(構)資安事件結案內容，並針對該資安事件填寫所配合辦理或規劃相關作業。

3.3 行政院國家資通安全會報

（一）技術服務中心依據通報機關(構)及其主管機關提供之資訊，評估通報內容及事件等級合理性，並得視需要變更事件等級；如主管機關未能於規定時限內完成通報審核，得逕行複核之。

（二）主管機關申請技術支援，如資安事件屬「4」、「3」級事件，技術服務中心須於完成複核後 1 小時內，派員協助主管機關處理資安事件；「2」、「1」級事件，技術服務中心須於完成複核後 2 小時內，派員協助主管機關處理資安事件。

（三）本會報政府資通安全組應彙整各級資安事件，並定期提供國家安全會議國家資通安全辦公室，俾供研析相關因應作為。

（四）如接獲「4」、「3」級資安事件通報，得視狀況邀集國家安全會議國家資通安全辦公室及相關機關(單位)召開緊急應變會議，並逐級陳報至本會報召集人決定是否召開資安防護會議。

第 4 章 應變作業

4.1 各級政府機關(構)

各級政府機關(構)應自行建立資安事件之事前安全防護、事中緊急應變及事後復原作業之具體機制，至少須包含下列各項：

（一）事前安全防護

1. 應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。
2. 應規劃建置資通安全整體防護環境，作好機關內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。
3. 應依資通安全防護需要，執行入侵偵測、安全掃描及弱點檢測等安全檢測工作，並制定系統與資料備份管理辦法，以做好事前防禦準備。
4. 應實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。
5. 應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，定期實施內部稽核，以儘早發現系統安全弱點並完成修復補強。
6. 委外管理機關(構)須於合約內，訂定承商提供相關資安紀錄，並制定資安紀錄備份管理辦法。
7. 應依資訊系統分類分級與鑑別機制，識別資訊系統安全等級，訂定資訊系統相關防護與復原措施。
8. 應每年定期規劃辦理資安認知教育訓練。
9. 各級政府機關(構)無論自建或委外資安監控(Security Operation Center, SOC)服務，應配合建立監控情蒐回傳機制，定期回傳予技術服務中心。

10. 各級政府機關(構)應建置並保存相關設備之系統日誌。

（二）事中緊急應變

1. 應就資安事件發生原因、影響等級、可能影響範圍、可能損失、是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。
2. 查詢國家資通安全通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，尋求解決方案。如無法解決，應迅速向主管機關或技術服務中心反應，請求提供相關技術支援。
3. 依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。
4. 視資安事件損壞程度，遵循機關內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。
5. 評估資安事件對業務運作造成之衝擊，並進行損害管制。
6. 資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以聯繫檢警調單位協助偵查。
7. 各級政府機關(構)如發生重大(「4」、「3」級)資安事件，應主動提供相關設備系統日誌予技術服務中心，俾提供相關協助。

（三）事後復原作業

1. 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後即進行安全備份、資料復原等相關事宜。
2. 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。

3. 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。
4. 資安事件結束後，應彙整事件之歷程概述、損害情形、後續可能影響、應變措施及強化作為等資訊，並提送「資通安全處理小組」及本會報政府資通安全組檢討，以強化資通安全防護機制。

4.2 主管機關

主管機關(資通安全處理小組)應於資安事件處理完成後，針對以下項目進行應變作業檢討。

（一）人力資源：檢討執行人員是否充足與適當。
（二）作業程序：檢討人員辦理通報作業的熟悉程度與程序是否適當。
（三）事件處理：檢討人員事件應變處理措施是否適當。
（四）其他：其他須檢討事項。

4.3 行政院國家資通安全會報

（一）當資安事件涉及網路犯罪相關議題時，資安辦應立即協調本會報網際犯罪偵防體系，邀集相關機關(單位)組成專案小組協助處理，並於事件結束後，由專案小組簽報處理情形，副知本會報網際防護體系(政府資通安全組)，並要求受害機關(單位)改善。
（二）當資安事件對資通訊以外之關鍵基礎設施(Critical Infrastructure, CI)造成威脅時，資安辦應立即通報行政院國土安全辦公室啟動相關應辦機制，以控管損害。
（三）當資安事件對國家安全造成威脅時，資安辦應立即通報國家安全會議國家資通安全辦公室啟動相關應辦機制，以控管損害。

第 5 章 資安演練作業

5.1 資通安全會報演練作業

5.1.1 資安攻防演練

（一）演練目的：

1. 檢測政府機關(構)之資安防護能力。
2. 強化政府機關(構)在資安事件發生時之緊急應變、系統復原、協調管控等能力。
3. 檢討我國整體資安防護措施，並研討資安防護精進作為。

（二）一般說明：演練範圍、時間、重點、編組、整備作業、防護作業、攻擊作業、評審監控、獎懲及注意事項，依本會報所訂定政府機關(構)資安演練計畫執行。

5.1.2 資通安全通報演練

（一）演練目的：

1. 測試機關資安審核人及聯絡人聯絡管道是否暢通。
2. 檢驗「國家資通安全通報應變網站」所登錄機關資安審核人及聯絡人資料之正確性。
3. 測試各機關於發現資安事件時，是否可正確、快速執行通報作業。

（二）一般說明：演練範圍、方式、時間、獎懲及注意事項，將由本會報不定期辦理。

5.1.3 防範惡意電子郵件社交工程演練

（一）演練目的：

1. 為提高人員警覺性以降低社交工程攻擊風險。

2. 規範機關自訂社交工程防制目標、舉辦相關資安教育訓練與宣導，以強化公務人員資安意識並檢驗機關宣導社交工程防制成效。

（二）一般說明：演練範圍、總體目標、宣導要點、演練時間、對象、前置作業、結果陳報、作業要點及獎懲事項，將由本會報不定期辦理。

5.1.4 其他演練

配合本會報規劃，不定期辦理資安相關演練。

5.2 資通安全處理小組演練作業

5.2.1 資通安全通報演練

（一）演練目的：檢驗「資通安全處理小組」及所屬機關(構)之資安通報機制及應變能力。

（二）演練時間：每年辦理 1 次，確實執行日期由各資通安全處理小組自行決定，惟須於每年 9 月底前完成。

（三）一般說明：

1. 各資通安全處理小組在本項演練作業中，應分組分工執行各項任務。如規劃組(危機處理分組)負責規劃演練之各種模擬狀況及選出演練單位；管控組(安全預防分組)負責通知參演單位及支援處理作業；督察組(稽核分組)負責保管模擬狀況題庫及登錄各階段演練時間，組織架構如圖 3：

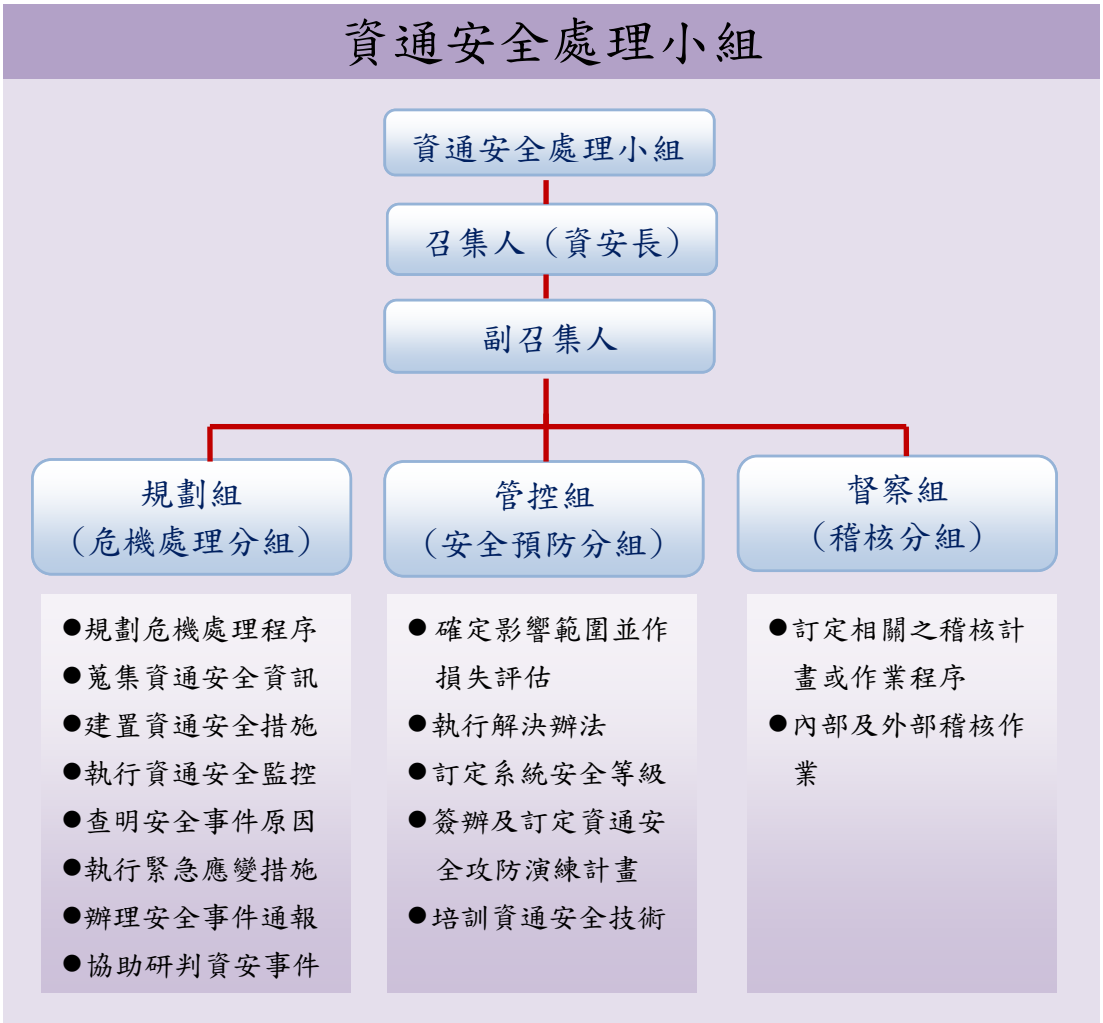

圖 3 資通安全小組組織架構

2. 演練計畫應簽奉資通安全處理小組之召集人資安長核定後實施。
3. 演練實施前，除應邀集所屬各單位實施作業講習外，亦請與本會報政府資通安全組聯繫。
4. 遴選演練對象方式，由各資通安全處理小組之規劃組以無預警隨機方式選取所屬 1/3(含以上)之單位為演練對象。
5. 演練前，資通安全處理小組之規劃組需先規劃資安影響等級分別為 1、2、3、4 級演練之各種模擬狀況(至少 10 種以上)，用隨機選取方式，分配予所選出之參與演練單位，密封交督察組保管。

6. 各種模擬狀況中，可明定該狀況是可由資通安全處理小組支援解決或須由技術服務中心支援解決，以檢驗不同流程之處理方式。
7. 演練完成後將「演練成果報告」併「演練時間紀錄表」，於 1 個月內主動送本會報政府資通安全組備查，並由該組彙整各資通安全處理小組所報成果，視情況邀集相關單位研商辦理獎勵及改善事宜。
8. 「演練成果報告」、「演練時間紀錄表」及「支援處理及回覆單」等相關表單請至通報應變網站下載。

5.2.2 防範惡意電子郵件社交工程演練

（一）演練目的：提高「資通安全處理小組」及其所屬機關(構)對社交工程攻擊防制認知。

（二）演練時間：每年不定期至少辦理 2 次，由資通安全處理小組自行規劃及執行，惟須於每年 4 月底前辦理第 1 次演練，並於 9 月底前辦理第 2 次演練。

（三）一般說明：

1. 演練對象由資通安全處理小組自行決定，惟主管機關及所屬機關須 1/4(含)以上具有公務電子郵件人員參與演練。
2. 演練實施前須訂定演練計畫，簽奉機關資安長核定。
3. 完成演練作業後，須由機關資安長召開「檢討會議」，檢討辦理情形及演練結果，演練報告須經機關資安長核定，並於每次演練完成後 1 個月內主動送本會報政府資通安全組備查。

第 6 章 獎懲及減責標準

6.1 獎勵標準

具以下事蹟之一者，由本會報政府資通安全組主責機關(單位)建議相關機關(構)對所屬人員予以適度之獎勵：

（一）所通報之資安事件資料完整且具時效性，足以警示其他機關(構)及早防範，防止資安事件擴大。

（二）完成資安事件處理後，通報結案時所提供解決辦法，可供其他機關(構)及時採用，防止資安事件擴大。

（三）於資安事件通報後，積極辦理相關回復工作，降低對機關(構)影響程度，績效卓著。

（四）提供技術服務中心分析之紀錄，有效預防機關(構)內發生資安事件，並可供其他機關(構)事前應對及預防之用。

（五）積極推動資通安全防護及通報至所屬機關(單位)，績效卓著。

6.2 懲處標準

具以下情事之一者，由本會報政府資通安全組主責機關(單位)建議相關機關(構)視情節輕重對所屬人員予以適度之懲處：

（一）通報之資安事件資料，經查明不實。

（二）未遵循本綱要規定落實資安事件通報應變作業及提供資安紀錄等，致國家或社會受有重大損害時，依法追訴行為人涉及湮滅證據等相關刑事責任；此外，另追究行為人、其主責機關資安長及相關人員之行政責任。

另，各受委託資安業者倘未依程序通報，將建議解除合約。

6.3 減責標準

遵循本綱要規定確實辦理資安事件通報及應變作業並提供資安紀錄，仍致政府或民眾權益受損時，本會報政府資通安全組主責機關(單位)應協助提供資料予相關機關(構)，並建議減輕其責。

附件　主管機關列表

編號	機關名稱	編號	機關名稱
1	行政院	17	行政院環境保護署
2	內政部	18	行政院海岸巡防署
3	外交部	19	國立故宮博物院
4	國防部	20	行政院大陸委員會
5	財政部	21	行政院經濟建設委員會
6	教育部	22	金融監督管理委員會
7	法務部	23	行政院國軍退除役官兵輔導委員會
8	經濟部	24	行政院原子能委員會
9	交通部	25	行政院國家科學委員會
10	文化部	26	行政院研究發展考核委員會
11	衛生福利部	27	行政院農業委員會
12	蒙藏委員會	28	行政院勞工委員會
13	僑務委員會	29	公平交易委員會
14	中央銀行	30	行政院公共工程委員會
15	行政院主計總處	31	行政院原住民族委員會
16	行政院人事行政總處	32	客家委員會

編號	機關名稱	編號	機關名稱
33	中央選舉委員會	47	彰化縣政府
34	飛航安全調查委員會	48	雲林縣政府
35	國家通訊傳播委員會	49	嘉義縣政府
36	臺灣省政府	50	屏東縣政府
37	福建省政府	51	宜蘭縣政府
38	臺北市政府	52	花蓮縣政府
39	新北市政府	53	臺東縣政府
40	臺中市政府	54	澎湖縣政府
41	臺南市政府	55	金門縣政府
42	高雄市政府	56	連江縣政府
43	桃園縣政府	57	基隆市政府
44	新竹縣政府	58	新竹市政府
45	苗栗縣政府	59	嘉義市政府
46	南投縣政府		