資通安全管理採購指引懶人包介紹

財團法人電信技術中心
黃嘉章經理

2019/06/13

大綱

1. 資通安全管理採購指引懶人包介紹

2. 資通安全管理採購指引懶人包專家審查建議討論

3. 資通安全管理採購指引懶人包交流討論

1.資通安全管理採購指引懶人包介紹

1.計畫緣起

總統府107/06/06正式公布
《資通安全管理法》
以維護國家安全和公共利益

工研院107/07/27宣佈啟動
「資安整合服務平台」

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

建立合規實務
激發資安需求

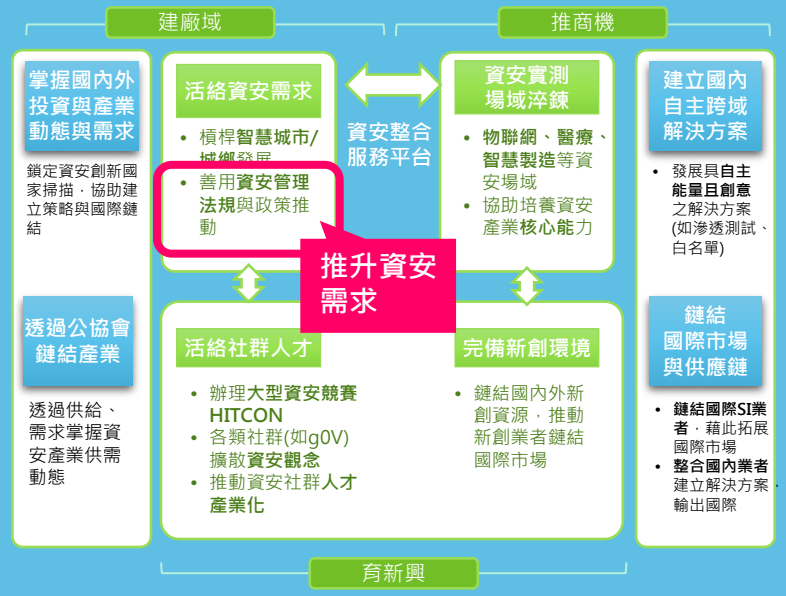
產品安全開發檢測工具
套裝企業資訊安全風險評估
客製化的專業滲透測試
新興資訊安全解決方案導入

維護國家安全。資安即國安

打造資訊安全防護金鐘罩

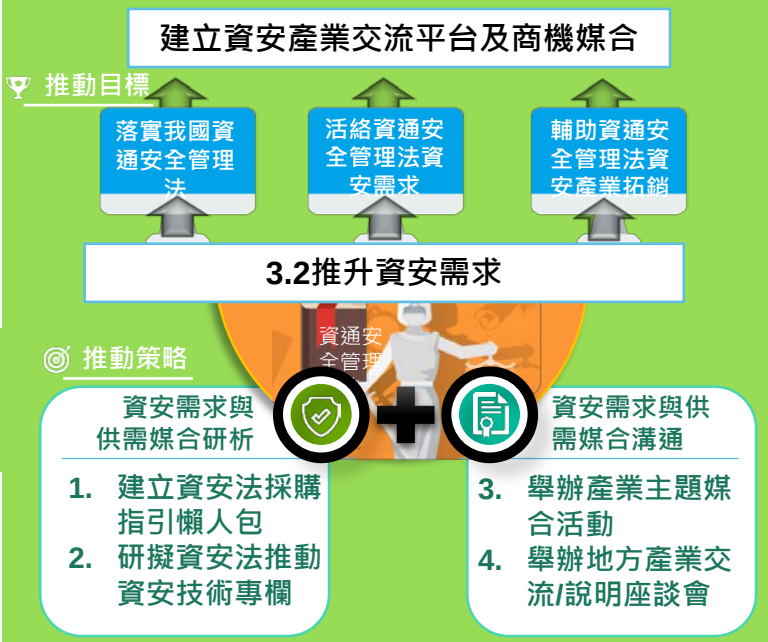
1.計畫緣起
- 推升資安需求計畫

新興資安產業生態系推動計畫
計畫執行策略



協助適用法規機關落實我國資通安全管理法、活絡資通安全管理法資安需求與輔助資通安全管理法資安產業拓銷

推升資安需求
計畫



2.懶人包介紹

1. 導讀

透過流程圖及Step-by-Step大富翁方式快速協助各機關所屬資通安全責任等級與查閱懶人包內容

2. 《資通安全管理法》入門

從資通安全管理法架構、角色與權責、資安維護計畫介紹、資安事件注意事項等議題快當讓各機關掌掃該法主要注意事項

3. 《資通安全管理法》採購指引懶人包綜整

在閱讀懶人包之前提供綜整各級機關適用主題及包各主題建議投標廠商或設備資格供參

4. 《資通安全管理法》採購指引懶人包

採用管理、技術與認知訓練三構面方式呈現各應辦事項之要求、重要性、推行重點、建議實作及相關建議資安服務/產品及廠商

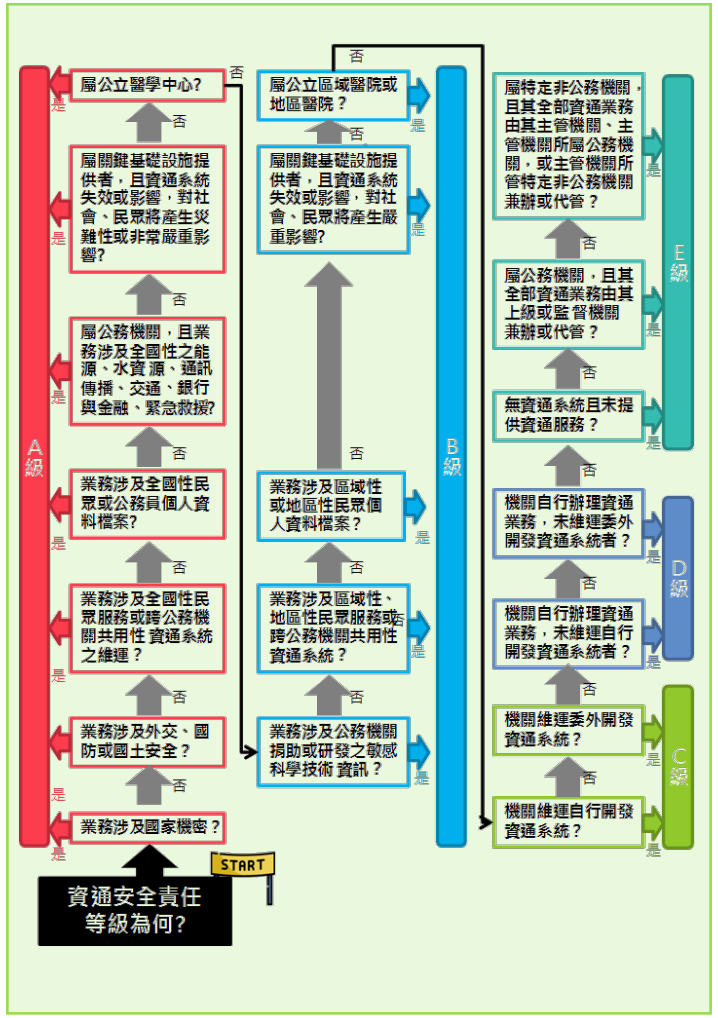
5. 《資通安全管理法》推動資安專欄

共有主法與子法5個主題分別請資安專家針對各主題提供資安法在推行重點講解及看法

6. 《資通安全管理法》採購指引懶人包附錄

彙整《資通安全管理法》採購指引懶人包所有議題及相對廠商名錄供各機關參閱

2.懶人包介紹 - 第1章導讀

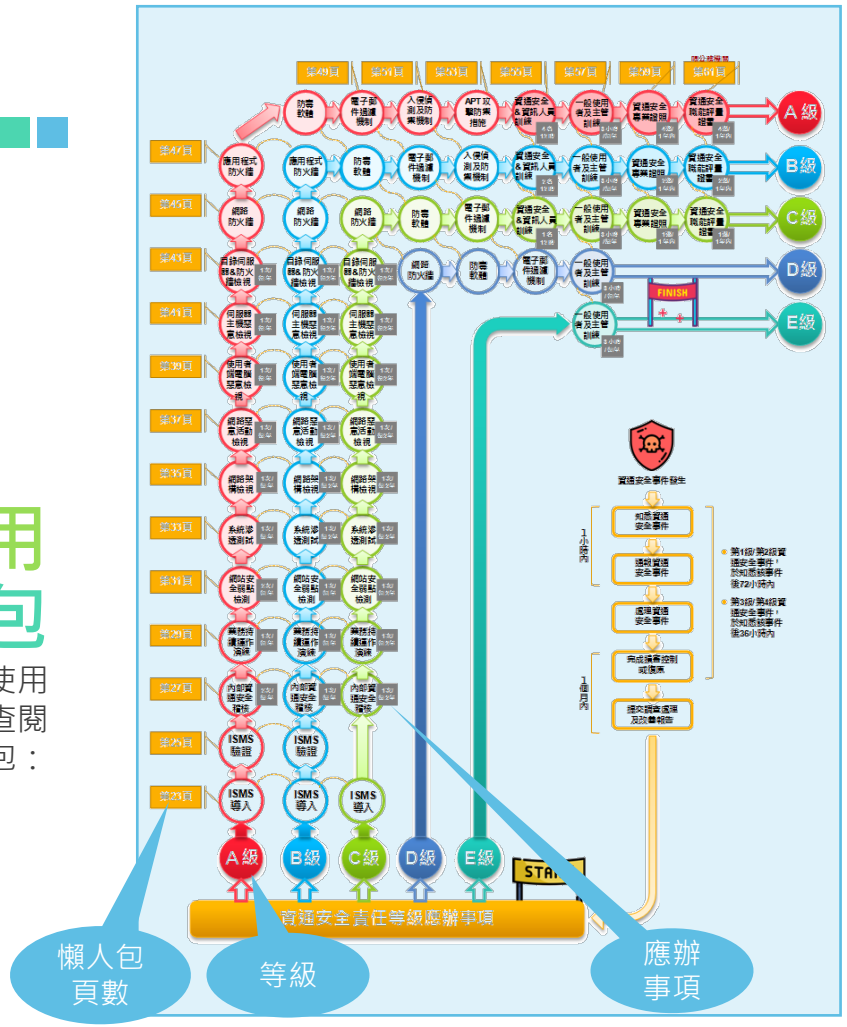


協助各機關判定資通安全責任等級

各資通安全責任等級機關可利用流程圖方式逐步協助判定資通安全責任等級

協助各機關使用懶人包

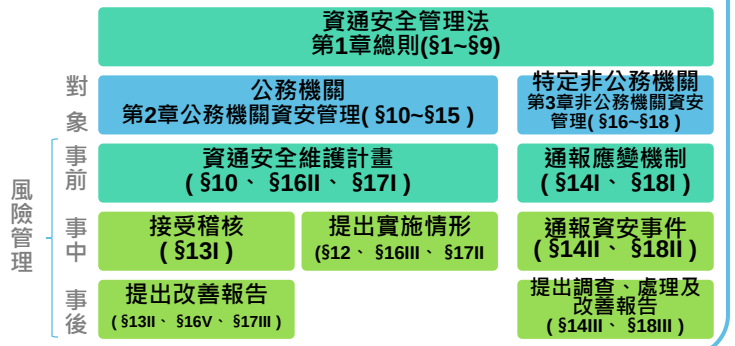
各資通安全責任等級機關可使用 step-by-step 大富翁遊戲查閱《資通安全管理法》採購指引懶人包：



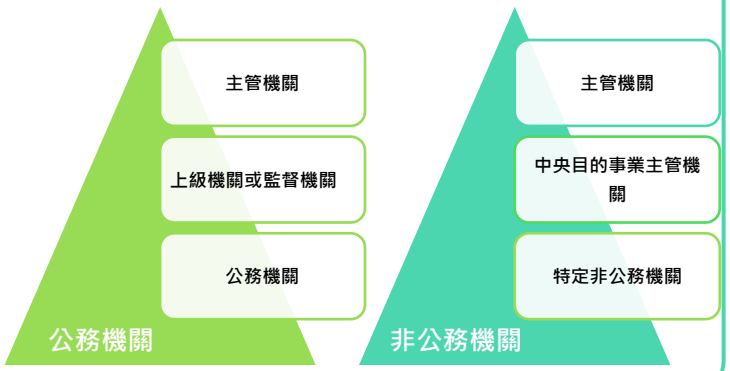
2.懶人包介紹 - 第2章《資通安全管理法》入門

1 資通安全管理法架構

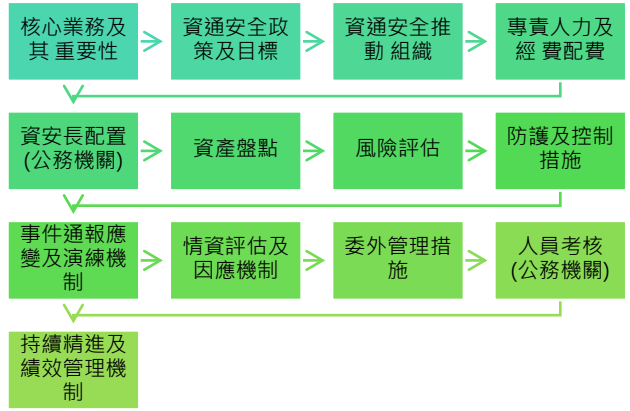
主法共包含23條且主法架構如下：



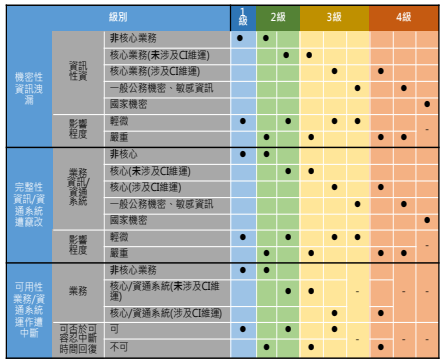
2 資通安全管理法角色與權責



3 資通安全維護計畫介紹



4 資安事件注意事項



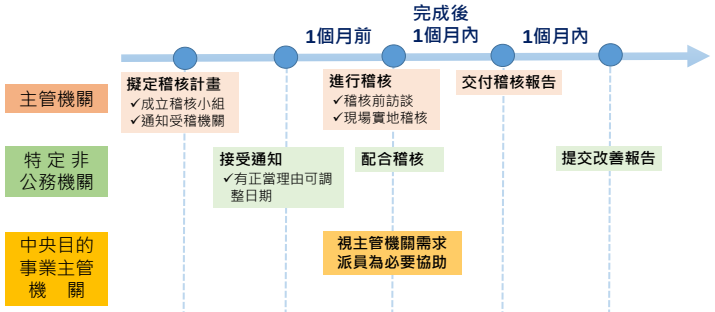
公告事項

- ✓發生之時間
- ✓原因
- ✓影響程度
- ✓控制情形
- ✓後續改善措施

不予以公告之情形

- 涉及個人、法人或團體營業上祕密或經營事業有關資訊
- 公開有侵害公務機關、個人、法人或團體之權利或其他正當利益
- 其他依法規規定應祕密、限制或禁止公開之情形

5 特定非公務機關資通安全維護計畫實施情形稽核



6 資通安全責任等級分級辦法

2.懶人包介紹 - 第3章《資通安全管理法》採購指引懶人包綜整

《資通安全管理法》採購指引懶人包與各級機關適用綜整

面向	辦理項目	辦理項目細項	A級	B級	C級	D級	E級
管理面	資訊安全管理系統導入		✓	✓	✓	無	無
	資訊安全管理系統驗證		✓	✓	無	無	無
	內部資通安全稽核		✓	✓	✓	無	無
	業務持續運作演練		✓	✓	✓	無	無
技術面	安全性檢測	網站安全弱點檢測	✓	✓	✓	無	無
		系統滲透測試	✓	✓	✓	無	無
	資通安全健診	網路架構檢視	✓	✓	✓	無	無
		網路惡意活動檢視	✓	✓	✓	無	無
		使用者端電腦惡意活動檢視	✓	✓	✓	無	無
		伺服器主機惡意活動檢視	✓	✓	✓	無	無
		安全設定檢視	✓	✓	✓	無	無
	資通安全防護	防毒軟體	✓	✓	✓	✓	無
		網路防火牆	✓	✓	✓	✓	無
		電子郵件過濾機制	✓	✓	✓	✓	無
		入侵偵測及防禦機制	✓	✓	無	無	無
		應用程式防火牆	✓	✓	無	無	無
		進階持續性威脅攻擊	✓	無	無	無	無
認知訓練面	資通安全教育訓練	資通安全及資訊人員	✓	✓	✓	無	無
		一般使用者與主管	✓	✓	✓	✓	✓
	資通安全專業證照及職能訓練證書	資通安全專業證照	✓	✓	✓	無	無
		資通安全職能評量證書(限公務機關適用)	✓	✓	✓	無	無

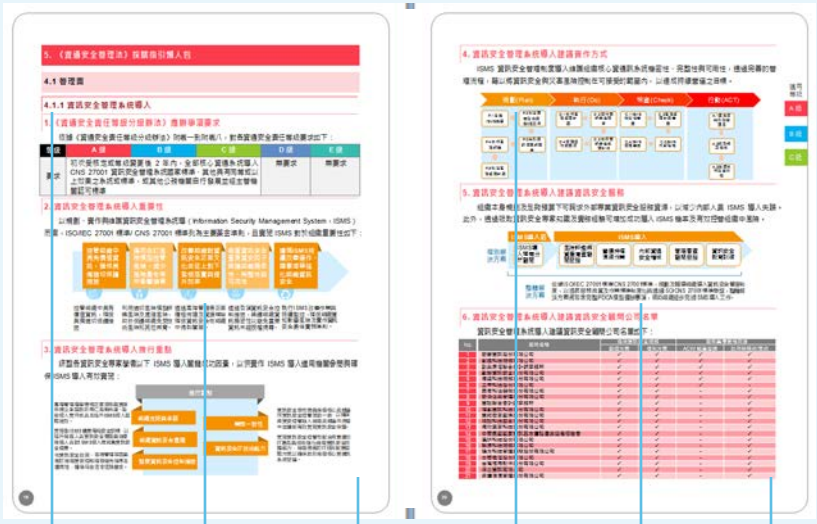
《資通安全管理法》採購指引懶人包各主題建議投標廠商或設備資格綜整

面向	辦理項目	辦理項目細項	建議投標廠商或設備資格
管理面	資訊安全管理系統導入		1. 已通過公正第三方認可/具政府採購網決標經歷。 2. 建議專案小組具備ISO 27001 LA、CISSP相關資安專業證照。 3. 建議具有相當年份ISO 27001輔導顧問年資。
技術面	安全性檢測	網站安全弱點檢測	1. 已通過公正第三方認可。 2. 執行3件以上之經驗。 3. 檢測項目須符合OWASP TOP 10 之項目。 4. 執行人員需接受過CEH或其他類似相關課程訓練。 5. 掃描工具需取得授權使用的商用軟體。
		系統滲透測試	1. 已通過公正第三方認可。 2. 執行3件以上之經驗。 3. 測試項目包含作業系統、...
認知訓練面	資通安全教育訓練	資通安全及資訊人員 一般使用者與主管	1. 訓練機構為登記有案之社、財團法人；公私立大專以上院校；依公司法設立之公司。 2. 講師具備資安專業證照。 3. 講師擁有從事資安相關工作或資安授課經驗2年以上，具資安實務能力。
	資通安全專業證照及職能訓練證書	資通安全專業證照 資通安全職能評量證書(限公務機關適用)	1. 訓練機構為國際組織或原廠授權教育訓練中心。 2. 講師具國際組織或原廠認證資格。

2.懶人包介紹 - 第4章《資通安全管理法》採購指引懶人包

21項研析主題

- 管理面
  - 資訊安全管理系統導入
  - 資訊安全管理系統驗證
  - 內部資通安全稽核
  - 業務持續運作演練
- 技術面
  - 安全性檢測
    - 網站安全弱點檢測
    - 系統滲透測試
  - 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
    - 安全設定檢視
  - 資通安全防護
    - 網路防火牆
    - 應用程式防火牆
    - 防毒軟體
    - 電子郵件過濾機
    - 入侵偵測及防禦機制
    - 進階持續性威脅攻擊
- 認知訓練面
  - 教育訓練
    - 資通安全及資訊人員
    - 一般使用者與主管
  - 專業證照&職能證書
    - 資通安全專業證照
    - 資通安全職能評量證書



每研析主題皆包含6個項目：

1. 應辦事項要求
   - 提供應辦事項要求讓適用機關了解必須符合要求內容
2. 重要性
   - 應辦事項要求對適用機關重要性及產生效果
3. 推行重點
   - 實施應辦事項要求關鍵成功因子，有助於對適用機關掌握重點
4. 建議實作方式
   - 建議實作方式，作為資安法實施參考與整備基礎
5. 建議資安服務/產品
   - 各別研析對應解決方案之資安服務
6. 建議資安服務/產品名單

2.懶人包介紹 - 第4章《資通安全管理法》採購指引懶人包(續)

21項研析主題　**295+**家建議資安服務/產品廠商名單

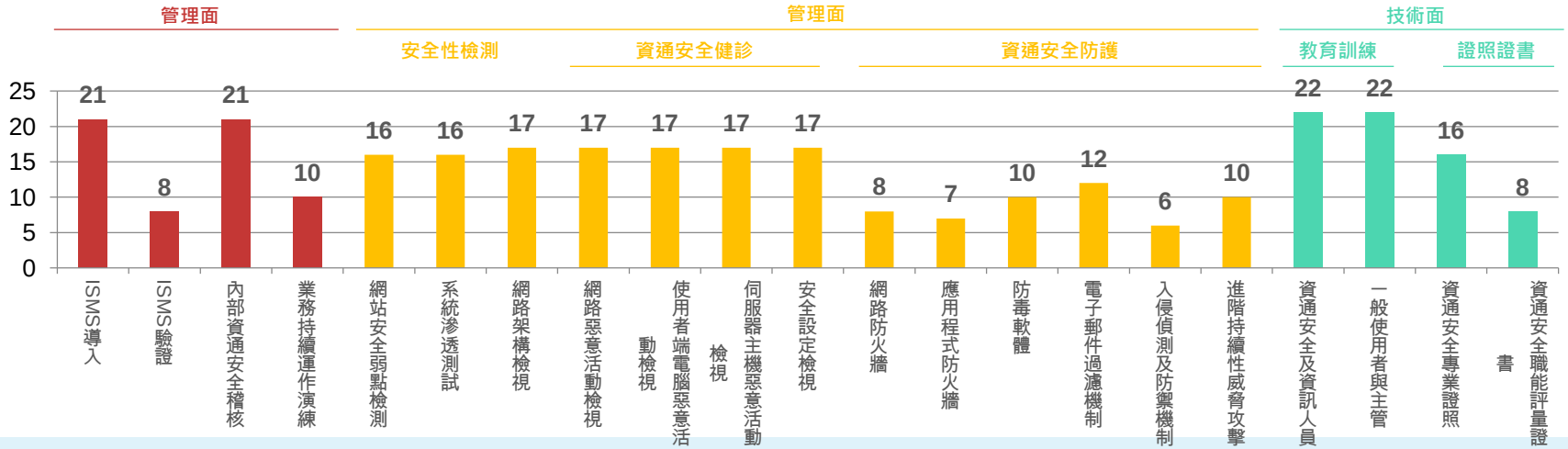
管理面

技術面

認知訓練面

建議廠商名單來源：

- ACW網站能量登錄通過名單
- 資安整合服務平台廠商
- 政府共同供應契約合格廠商
- 政府採購網決標經歷廠商
- 國內資通安全服務/產品廠商
- 國外資通安全服務/產品廠商



ISMS導入	ISMS驗證	內部資通安全稽核	業務持續運作演練	網站安全弱點檢測	系統滲透測試	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	安全設定檢視	網路防火牆	應用程式防火牆	防毒軟體	電子郵件過濾機制	入侵偵測及防禦機制	進階持續性威脅攻擊	資通安全及資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能評量證書
安碁資訊 *	台灣檢驗	安碁資訊 *	安碁資訊	安碁資訊 #	安碁資訊 #	果核數位 #	果核數位 #	果核數位 #	果核數位 #	果核數位 #	豪勉科技	豪勉科技	趨勢科技	趨勢科技	中華資安	中華資安	鑒真數位	鑒真數位	(ISC)2	文化大學
創逸科技 *	英國標準協會	創逸科技 *	勤業眾信	勤業眾信 #	勤業眾信 #	漢昕科技 #	漢昕科技 #	漢昕科技 #	漢昕科技 #	漢昕科技 #	眾至資訊	趨勢科技	中華數位	中華數位	數聯資安	數聯資安	關貿網路	關貿網路	CompTIA	健行技大
勤業眾信 *	艾法諾	勤業眾信 *	青年創業協會總會安全衛生技術中心	創逸科技	創逸科技	關貿網路 #	關貿網路 #	關貿網路 #	關貿網路 #	關貿網路 #	勤崧科技	數聯資安	中華資安	眾至資訊	安碁資訊	安資捷	三甲科技	三甲科技	CREST	逢甲大學
三甲科技	環奧國際	三甲科技	德諾科技	安華聯網	安華聯網	聯準科技	聯準科技	聯準科技	聯準科技	聯準科技	桓基科技	台灣思科	資通電腦	碩琦科技	豪勉科技	安碁資訊	精誠資訊	精誠資訊	EC-Council	崑山科大
數聯資安 *	香港漢德	數聯資安 *	德諾科技	華電聯網	華電聯網	華電聯網	華電聯網	華電聯網	華電聯網	華電聯網	大同世界	Forcepoint	數聯資安 #	數聯資安	趨勢科技	關貿網路	中華軟協	中華軟協	Elearning Security	元智大學
德諾科技 *	環亞貝爾	德諾科技 *	創逸科技	三甲科技	三甲科技	安華聯網	安華聯網	安華聯網	安華聯網	安華聯網	台灣思科	Fortinet	凌群電腦	安資捷股	安資捷股	豪勉科技	中華電信學院	中華電信學院	GIAC	中興大學
美思科法	優麗國際	美思科法	安侯企業	凌群電腦	凌群電腦	德欣寰宇	德欣寰宇	德欣寰宇	德欣寰宇	德欣寰宇	Forcepoint	桓基科技	神通資訊	安碁資訊	安華聯網	精誠軟體	台灣數位安全聯盟	台灣數位安全聯盟	ISACA	朝陽科技
安侯企業	立恩威國際	安侯企業	博創資訊	策略數位	策略數位	美思科法	美思科法	美思科法	美思科法	美思科法	Fortinet		精誠軟體	創逸科技	勤業眾信	趨勢科技	巨匠電腦	巨匠電腦	ISFCE	靜宜大學
資誠聯合		資誠聯合	精誠科技	果核數位	果核數位	凌群電腦	凌群電腦	凌群電腦	凌群電腦	凌群電腦			安源電腦	網擎資訊	眾至資訊	中華數位	安華聯網	安華聯網	Offensive Security	
博創資訊		博創資訊	德欣寰宇	漢昕科技	漢昕科技	策略數位	策略數位	策略數位	策略數位	策略數位			曜揚科技	桓基科技	三甲科技	勤業眾信	協志聯合	協志聯合	BSI	
資拓宏宇		資拓宏宇		數聯資安	數聯資安	數聯資安	數聯資安	數聯資安	數聯資安	數聯資安				安源電腦			南部科學園區產學協會	南部科學園區產學協會	SGS	
精誠科技		精誠科技		光盾資訊	光盾資訊	光盾資訊	光盾資訊	光盾資訊	光盾資訊	光盾資訊				曜揚科技			勤業眾信	勤業眾信	電腦技能基金會	
德欣寰宇		德欣寰宇		中芯數據	中芯數據	中芯數據	中芯數據	中芯數據	中芯數據	中芯數據							TGIIDA	TGIIDA	資策會	
NII		NII		中華資安	中華資安	中華資安	中華資安	中華資安	中華資安	中華資安							緯育股份	緯育股份	恆逸中心	
漢昕科技		漢昕科技		優易資訊	優易資訊	安碁資訊	安碁資訊	安碁資訊	安碁資訊	安碁資訊							文化大學	文化大學	巨匠電腦	
聯準科技		聯準科技		中華電信數據分公司	中華電信數據分公司	優易資訊	優易資訊	優易資訊	優易資訊	優易資訊							健行科大	健行科大	電腦稽核協會	
璞方科技		璞方科技				中華電信數據分公司	中華電信數據分公司	中華電信數據分公司	中華電信數據分公司	中華電信數據分公司							逢甲大學	逢甲大學		
中華電信		中華電信															崑山科大	崑山科大		
台灣應用		台灣應用															元智大學	元智大學		
偉立資訊		偉立資訊															中興大學	中興大學		
昇達價值		昇達價值															朝陽科大	朝陽科大		
																	靜宜大學	靜宜大學		

■ACW能量登錄 ■政府採購網決標紀錄 ■官網 ■政府共同供應契約 ■技術服務中心 ■原廠授權 ■AB認可

*表示兼具ACW能量登錄與政府採購網決標紀錄　#表示兼具ACW能量登錄與政府共同供應契約資格

2.懶人包介紹 - 第5章與第6章

《資通安全管理法》採購指引懶人包附錄

依據《資通安全管理法》子法「資通安全責任等級分級辦法」制定各等級應辦事項，針對以下研析議題彙整建議資訊安全服務/產品廠商，以供各不同適用等級機關構予以參閱。

《資通安全管理法》推動資安專欄

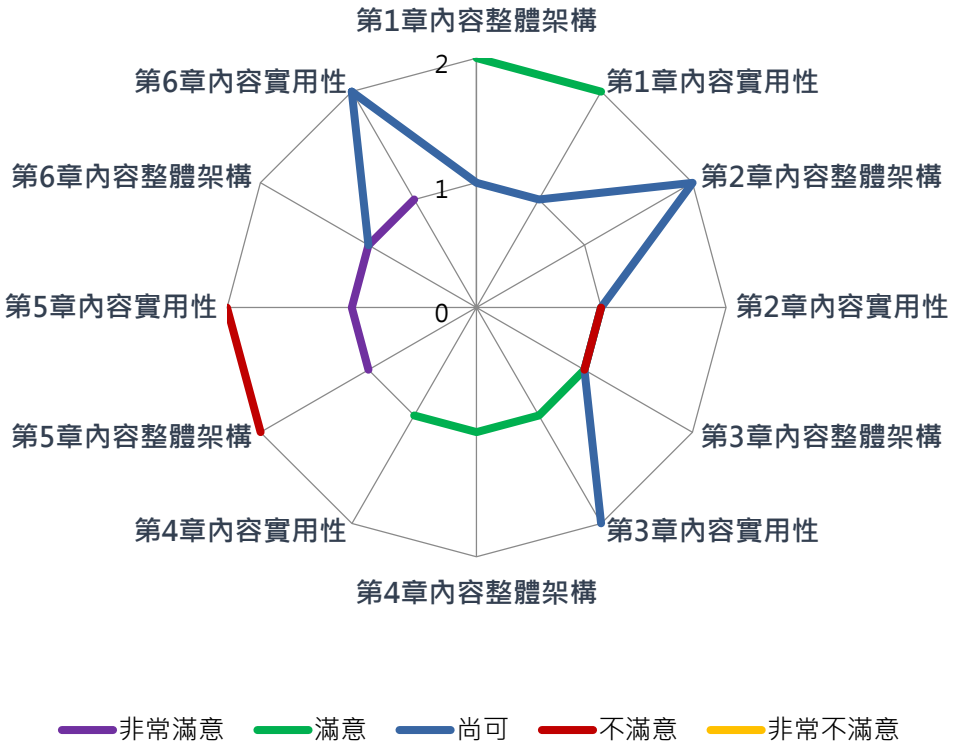
依《資通安全管理法》一主法及六子法精選五項資安議題，並結合國內資安服務廠商知識提供《資通安全管理法》推動資安專欄，供《資通安全管理法》適用單位快速掌握推行及建置重點。

2. 資通安全管理採購指引懶人包專家審查建議討論

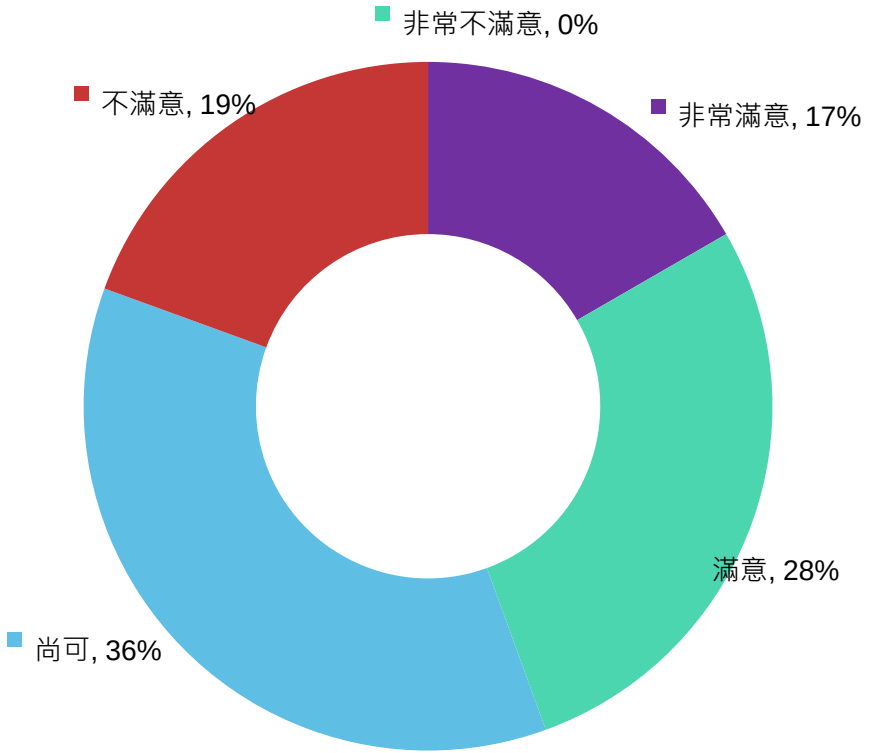
2. 資通安全管理採購指引懶人包專家審查建議討論

依據三位委員回覆書面審查滿意度與回饋綜整如下：

專家書面審查回覆滿意度各章節綜整



專家書面審查回覆滿意度綜整圓餅圖



2. 資通安全管理採購指引懶人包專家審查建議討論(續)

章節	委員	建議	回覆
1	馬委員正維	「第1章導讀」建議由上往下(倒置)較順暢。	謝謝委員指導，將在06/13專家交流會議與所有專家討論後決議導讀順序。
	陳委員泉錫	「第1章導讀」(p.4)建議起始點應從左上角開始。	
	潘委員城武	「第1章導讀」分級需能清楚辨別，可舉例。	謝謝委員指導，謹遵辦理，懶人包將增加舉例以供各級機關參考之用。
	陳委員泉錫	「第1章導讀」(p.5)右下側圖示所指時間(如72小時等)未說明是系統回復時間。	謝謝委員指導，謹遵辦理，將會在時間上多增加說明以免閱讀者誤解。
2.2	潘委員城武	「第2.2章資通安全管理法角色與權責」角色與權責可更表達讓人易懂。	感謝委員指導，會在6/13進一步了解委員想法，以了解修正要點作調整。
2.3	潘委員城武	「第2.3章資通安全維護計畫介紹」要淺顯易懂。	感謝委員指導，會在6/13進一步了解委員想法，以了解修正要點作調整。
2.4	潘委員城武	「第2.4章資安事件注意事項」簡捷些。	感謝委員指導，會在6/13進一步了解委員想法，以了解修正要點作調整。
	陳委員泉錫	「第2.4章資安事件注意事項」須修正，資安事件分級表不易瞭解。	感謝委員指導，資安事件分級表是依據「資通安全事件通報及應變辦法」文字內容進行簡化，為讓各機關了解資安事件分級表，未來會在推廣說明會作說明。
2.5	潘委員城武	「第2.5章特定非公務機關資通安全維護計畫實施情形稽核」更意象化些。	感謝委員指導，會在6/13進一步了解委員想法，以了解修正要點作調整。
	馬委員正維	「第2.5章特定非公務機關資通安全維護計畫實施情形稽核」建議刪減，非必要性。	感謝委員指導，有鑑於該本懶人包亦可供為特定非公務機關使用，懇請保留該章節供特定非公務機關參閱。
2.6	馬委員正維	「第2.6章資通安全責任等級分級辦法」建議刪減，與導讀重覆。	感謝委員指導，謹遵辦理。
	潘委員城武	「第2.6章資通安全責任等級分級辦法」簡捷些。	感謝委員指導，本章節將依馬委員建議作刪除。

2. 資通安全管理採購指引懶人包專家審查建議討論(續)

章節	委員	建議	回覆
3	馬委員正維	「第3章《資通安全管理法》採購指引懶人包綜整」建議刪減，本節用途較不明確？	感謝委員指導，該章節主要是作為懶人包導讀作全面性了解之用，並且主要有2個綜整項目包含各級機關適用總表及建議投標廠商或設備資格綜整，懇請保留供各級機關參閱之用。
	潘委員城武	「第3章《資通安全管理法》採購指引懶人包綜整」簡捷些,要分流。	感謝委員指導，會在6/13進一步了解委員想法，以了解修正要點作調整。
4	馬委員正維	「第4章《資通安全管理法》採購指引懶人包」建議增述一般採購案之辦理模式，可將管理面、技術面及認知訓練面系合併於同一專案中辦理。	感謝委員指導，會在6/13進一步了解委員想法，以了解修正要點作調整。
	馬委員正維	「第4章《資通安全管理法》採購指引懶人包」建議增述應強調未列入建議廠商名單中，並不表示其未具提供該項服務之能力。	感謝委員指導，謹遵辦理。
	馬委員正維	「第4章《資通安全管理法》採購指引懶人包」建議內容建議再精簡，本懶人包內容太多(不夠懶)，使用者在閱讀及使用時之便利性較不足。	感謝委員指導，第4章懶人包各研析主題將簡化為1頁，以供各級機關參閱。
	潘委員城武	「第4章《資通安全管理法》採購指引懶人包」簡捷些,要分流。	感謝委員指導，回覆同上。
	陳委員泉錫	P46「防毒軟體」未提供可信賴之防毒軟體(廠商)，而是提供資安顧問公司名單，似與標題未合。	謝謝委員指導，謹遵辦理，懶人包將會調整為提供防毒軟體產品廠商，而非病毒檢測服務廠商。
	陳委員泉錫	P52「APT」實作建議似過於抽象，缺少具體而可用於要求機關人員遵循之作法。	謝謝委員指導，謹遵辦理，懶人包將會調整APT實作建議，以供各機關參閱。
5	馬委員正維	「第5章《資通安全管理法》推動資安專欄」本節目的不具體？	謝謝委員指導，本節將主要會有5項精選文章，用來提供給各級機關作為推動資安法參考之用，在草稿版次目前僅提供1個精選文章，謹遵辦理將此章節刪除。
	潘委員城武	「第5章《資通安全管理法》推動資安專欄」簡捷些,要分流。	感謝委員指導，謹遵辦理將此章節刪除。

3. 資通安全管理採購指引懶人包交流討論

3.資通安全管理採購指引懶人包交流討論

推廣對象

為發揮懶人包推廣效益，有鑑需求使用端之業務及採購部門及其標案面向（如採購標、專案標）不同，應以何部門為主進行推廣較為合宜？

懶人包分冊

針對資安法分級，本懶人包目前以完整版進行推廣，是否需分冊進行設計？

廠商名單

為鼓勵機關使用國產品，懶人包中廠商名單：

- 是否全數羅列亦或僅列重點廠商或羅列參考網址，何者較為合宜？
- 另目前建議之採購名單是否妥適，是否需增減？
- 廠商名單是否增列聯絡資訊（如網址、聯絡電話等）？

感謝聆聽
敬請指教