國家資通安全研究院
National Institute of Cyber Security

112年資安服務廠商評鑑機制

指導單位：數位發展部
主辦單位：數位發展部資通安全署
執行單位：國家資通安全研究院

【公開資訊】

大綱

1. 目的
2. 廠商評鑑機制
3. 112年廠商評鑑精進
4. 廠商評鑑作業說明
5. 附件
   1) 5類資安服務評鑑架構
   2) SOC監控有效性客觀評分計算公式
   3) 機關評鑑表

1. 目的

國家資通安全研究院
National Institute of Cyber Security

- 目的

  為協助政府機關(構)導入優質民間資安服務，強化資安防護能力，針對資安服務廠商之服務能量及專業技術進行評鑑，評鑑結果將提供政府機關(構)選擇委外廠商之參考

- 預期效益

  –強化與業界交流互動，提升廠商專業與服務能量，助益政府提升資安防護能力

  –擴散廠商評鑑結果之應用，協助拓展廠商商機與服務範疇

- 評鑑原則

  依據共契資安服務採購規範要求訂定

廠商評鑑歷程

國家資通安全研究院
National Institute of Cyber Security

102年	**廠商評鑑試辦，以書面評鑑方式** ➢ 2項評鑑：SOC監控/資安健診服務
103年	**首次以實地與展示評鑑方式進行** ➢ 5項評鑑：SOC監控、資安健診、弱點掃描、滲透測試、社交郵件測試服務
104年 | 106年	受評廠商： 7 家-10家
107年	**共契資安服務由台銀轉至工業局執行** ➢ 受評廠商：14家
108年	**參與共契資安服務廠商數大幅增加**(21家廠商參與投標/17家合格) ➢ 受評廠商：14家，SOC資安監控服務廠商增加
109年	**SOC監控有效性驗證試行(6家SOC廠商)** ➢ 受評廠商：13家
110年	**SOC監控有效性納入正式評鑑(客觀評分)** ➢ 受評廠商：13家
111年	**共契資安服務採購改採最有利標(得標數計28家)** ➢ 受評廠商：16家
112年	**放寬受評廠商資格，不限共契廠商**

2.廠商評鑑機制

國家資通安全研究院
National Institute of Cyber Security

註：紅字表示異動

指導單位：數位部　主辦單位：數位部資安署　執行單位：國家資通安全研究院

受評廠商資格

資安服務廠商

- 依公司法設立之公司、登記有案之法人、依法設立之營利機構
- 應通過ISO 27001或CNS27001 驗證
- 具服務實績

※服務實績定義

- SOC服務：近1年至少服務1個公務機關6個月以上，且具112年監控有效性成績
- 資安健診、弱點掃描、滲透測試及社交工程演練服務：近1年至少完成1個公務機關之服務

資安服務類別

1. SOC服務
2. 資安健診
3. 弱點掃描
4. 滲透測試
5. 社交工程演練

評鑑方式(註1)

委員評鑑 (70%)

- 實地評鑑 (適用 SOC服務)
- 展示評鑑

機關評鑑 (30%)

由採購機關進行評鑑

評鑑構面

1. 學習成長
2. 服務流程
3. 專業技術
4. 服務品質

評鑑結果

A級	90分(含)以上者
B級	80分(含)以上且未滿90分者
C級	70分(含)以上且，未滿80分者
D級	60分(含)以上，且未滿70分者
E級	未滿60分者

於資安院網站公布評鑑結果

註1：同1家受評廠商且同1類資安服務，每年實施機關評鑑，每2年執行1次委員評鑑

3.112年廠商評鑑精進

國家資通安全研究院
National Institute of Cyber Security

1)放寬受評廠商資格

註：紅字表示異動

國家資通安全研究院
National Institute of Cyber Security

- 凡符合以下資格之資安服務廠商皆可參加，不限共契廠商
- 受評廠商資格調整為(3項皆要符合)

1. 依公司法設立之公司、登記有案之法人、依法設立之營利機構
2. 通過ISO 27001或CNS 27001 驗證
3. 具服務實績：履約期間於廠商評鑑廠商說明會日期往前 1 年內**(111/6/1-112/6/1)** ，且符合以下要求

資安服務類別	服務實績要求
1.SOC服務	至少服務1個公務機關(註1)6個月以上，且具112年監控有效性成績
2.資安健診服務 3.弱點掃描服務 4.滲透測試服務 5.社交工程演練服務	至少完成1個公務機關之服務

註1：公務機關指依法行使公權力之中央或地方機關或行政法人

2) 擴大機關評鑑範圍

註：紅字表示異動

國家資通安全研究院
National Institute of Cyber Security

- 機關評鑑範圍
  - 履約期間於廠商評鑑廠商說明會日期往前 1 年內**(111/6/1-112/6/1)**
  - 評鑑機關須符合採購機關條件(註2)
    - 共契資安服務之採購機關(產業署提供)(以111年共契採構機關為主)
    - 其他採購方式之採購機關 (非共契採購由廠商提供名單)

註2：採購機關
- 包括總統府、國家安全會議、行政院、監察院、司法院、立法院、考試院以及前開機關所屬之各級部會、機關與公營事業；
- 與各級地方政府及其所屬機關(構)、學校、議會以及公營事業。

5類資安服務之評鑑方式

國家資通安全研究院
National Institute of Cyber Security

- 5類資安服務類別之評鑑方式

項次	資安服務類別	機關評鑑	委員評鑑	
			展示評鑑	實地評鑑
1	SOC服務	V		V
2	資安健診服務	V	V	
3	弱點掃描服務	V	V	
4	滲透測試服務	V	V	
5	社交工程演練服務	V	V	

評鑑方式_委員評鑑說明

委員評鑑配分

國家資通安全研究院
National Institute of Cyber Security

- 資安服務類別之4構面配分
  - 1.、2.、4.為共通構面，各資安服務類別之評鑑內容一致，主要差異為**3.專業技術構面**
  - 專業技術構面，新增評鑑選項彈性，後續說明

項次	資安服務類別/評鑑構面	1.學習成長構面	2.服務流程構面	3.專業技術構面	4.服務品質構面	加分	總分
1	SOC服務	10%	10%	60%	20%	5	105 (註)
2	資安健診服務	10%	10%	60%	20%	-	100
3	弱點掃描服務	10%	10%	60%	20%	-	100
4	滲透測試服務	10%	10%	60%	20%	-	100
5	社交工程演練服務	10%	10%	60%	20%	-	100

註：委員評分80分、客觀評分25分

1.、2.、4.共通構面之評鑑內容

國家資通安全研究院
National Institute of Cyber Security

評鑑構面	評鑑項目	評鑑細項
1. 學習成長 10%	1.1 資安國際驗證(5%)	1.1.1廠商國際驗證
	1.2 專業證照(5%)	1.2.1專業技術證照表現
		1.2.2技術人力年資經歷
2. 服務流程 10%	2.1支援人力(5%)	2.1.1專案技術支援人力配置
	2.2資安服務作業流程(5%)	2.2.1資安服務作業流程SOP
		2.2.2資安服務風險管理作業
4. 服務品質 20%	4.1 交付內容品質(10%)	4.1.1服務報告內容品質表現
	4.2 專業技術服務能力(10%)	4.2.1技術服務整體表現

3)專業技術構面_新增評鑑選項彈性

國家資通安全研究院
National Institute of Cyber Security

- 考量廠商可能未提供全部服務內容，故將各類資安服務之**專業技術構面**區分為必評項目與選評項目
- 各類資安服務之核心服務設為必評，受評廠商除必評項目外，得選評其他評鑑項目

資安服務類別	3.專業技術構面	
	必評項目	選評項目
1.SOC服務	3.1 SOC監控維運 3.2 資安事件處理 3.3 情資回傳	-
2.資安健診服務	3.1 網路架構檢視 3.2 有線網路惡意活動檢視 3.3 使用者電腦惡意活動檢視 3.4 伺服器主機惡意活動檢視 3.5 防火牆連線設定檢視 3.6 目錄伺服器(AD)設定檢視	3.7 政府組態基準(GCB)設定檢視 3.8 資料庫安全檢視
3.弱點掃描服務	3.1 主機系統弱點掃描 3.2 Web網頁弱點掃描	3.3 網頁個資掃描
4.滲透測試服務	3.1 作業系統測試 3.2 網站服務測試 3.3 應用程式測試 3.4 密碼破解與無線服務測試	-
5.社交工程演練服務	3.1 電子郵件演練樣板設計 3.2 電子郵件演練發信系統 3.3 電子郵件演練統計分析	3.4 簡訊演練

註：紅字表示異動

SOC服務-專業技術構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- SOC服務包含SOC監控維運、資安事件處理、情資回傳等項目，全為必評項目，評鑑內容與客觀評分之來源說明(同111年)
- 112年監控有效性客觀評分，以112年1月~112年 6 月之SOC監控有效性分析指標(GSOC 2.0)之平均結果計之

評鑑構面	必/選評	評鑑項目	評鑑細項
3. 專業技術 60%+ 5分	必評	3.1SOC監控維運 (10%)	3.1.1 監控偵測機制
	必評	3.2資安事件處理 (20%)	3.2.1 資安事件處理能力
			3.2.2 根因調查與改善建議能力
	必評	3.3 情資回傳 (30%)	3.3.1 回傳能力(10%) (客觀評分)
			3.3.2 情資品質分析(10%) (客觀評分)
			3.3.3 資安威脅預警(10%)
	必評	3.4 監控有效性加分(5分)	3.4.1 偵測能力(2分) (客觀評分)
			3.4.2 情資回饋能量(3分) (客觀評分)

SOC監控有效性分析指標

1.回傳能力	1.1資安監控情資格式正確率
	1.2資安防護項目回傳率
3.情資品質	3.1資安監控情資品質分析

2.偵測能力	2.1網路攻防演練驗證
	2.2資安院資安警訊驗證
	2.3機關通報資安事件驗證
3.情資品質	3.2資安監控情資回饋能量

註：紅字表示異動

資安健診-專業技術構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- 調修評鑑項目目錄伺服器(AD)設定檢視
- 資安健診服務，包含資安法要求之3.1-3.6項目，為必評項目，其餘2項GCB設定檢視與資料庫安全檢視為選評項目
- 調修配分，GCB設定檢視原10%，調修成AD 設定檢視5%、GCB設定檢視5%

評鑑構面	必/選評	評鑑項目	評鑑細項
3. 專業技術 60%	必評	3.1網路架構檢視(10%)	3.1.1 主機位置配置檢視 3.1.2 網路區域配置檢視 3.1.3 網路架構設計邏輯檢視
	必評	3.2 有線網路惡意活動檢視(10%)	3.2.1 封包監聽與分析 3.2.2 網路設備紀錄檔分析
	必評	3.3 使用者電腦惡意活動檢視(10%)	3.3.1 使用者電腦惡意程式或檔案檢視 3.3.2 使用者電腦更新檢視
	必評	3.4 伺服器主機惡意活動檢視(10%)	3.4.1 伺服器主機惡意程式或檔案檢視 3.4.2 伺服器主機更新檢視
	必評	3.5 防火牆連線設定檢視(5%)	3.5.1 防火牆連線設定檢視
	必評	3.6.目錄伺服器(AD)設定檢視(5%)	3.6.1 AD GCB 設定檢視
	選評	3.7 政府組態基準(GCB)設定檢視(5%)	3.7.1 作業系統GCB設定檢視 3.7.2 瀏覽器GCB設定檢視 3.7.3 網通設備GCB設定檢視 3.7.4 應用程式GCB設定檢視
	選評	3.8 資料庫安全檢視(5%)	3.8.1~3.8.7 特權帳號管理、資料加密、存取授權、稽核紀錄、委外管理、備份保護、弱點管理

註：紅字表示異動

弱點掃描服務-專業技術構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- 新增評鑑項目網頁個資掃描(10%)
- 弱點掃描服務，包含主機系統弱點掃描、Web網頁弱點掃描2項必評項目，其餘網頁個資掃描為選評項目
- 調修配分，主機系統弱點掃描、Web網頁弱點掃描，原各30%調修為各25%

評鑑構面	必/選評	評鑑項目	評鑑細項
3. 專業技術 60%	必評	3.1 主機系統弱點掃描 (25%)	3.1.1 作業系統未修正漏洞檢測 3.1.2 常用應用程式漏洞檢測 3.1.3 網路服務程式檢測 3.1.4 木馬程式檢測 3.1.5 後門程式檢測 3.1.6 帳號密碼破解測試 3.1.7 系統之不安全與錯誤設定檢測 3.1.8 網路通訊埠檢測
	必評	3.2 Web網頁弱點掃描 (25%)	3.2.1 Broken Access Control 3.2.2 Cryptographic Failures 3.2.3 Injection 3.2.4 Insecure Design 3.2.5 Security Misconfiguration 3.2.6 Vulnerable and Outdated Components 3.2.7 Identification and Authentication Failures 3.2.8 Software and Data Integrity Failures 3.2.9 Security Logging and Monitoring Failures 3.2.10 Server-Side Request Forgery (SSRF)
	選評	3.3 網頁個資掃描 (10%)	3.3.1 對外網頁之個資檔案掃描 3.3.2 掃描之個資特徵

註：紅字表示異動

滲透測試服務-專業技術構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- 滲透測試服務包含作業系統測試、網站服務測試、應用程式測、密碼破解與無線服務測試，全為必評項目，評鑑內容同111年

評鑑構面	必/選評	評鑑項目	評鑑細項
3. 專業技術 60%	必評	3.1 作業系統測試(10%)	3.1.1 遠端服務 3.1.2 本機服務
	必評	3.2 網站服務測試(20%)	3.2.1 設定管理 3.2.2 使用者認證 3.2.3 連線管理 3.2.4 使用者授權 3.2.5 邏輯漏洞 3.2.6 輸入驗證 3.2.7 Web Service 3.2.8 Ajax
	必評	3.3 應用程式測試(25%)	3.3.1 電子郵件服務 3.3.2 網站服務 3.3.3 檔案傳檔服務 3.3.4 遠端連線服務 3.3.5 網路服務
	必評	3.4 密碼破解與無線服務測試(5%)	3.4.1 密碼強度測試 3.4.2 無線服務測試

社交工程演練-專業技術構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- 新增評鑑項目簡訊演練(10%)
- 社交工程演練包含電子郵件演練3.1-3.3為必評項目、簡訊演練為選評項目
- 電子郵件演練新增評鑑細項觸發行為判斷(人為或非人為觸發)
- 調修配分，電子郵件演練統計分析原20%調至10%

評鑑構面	必/選評	評鑑項目	評鑑細項
3. 專業技術 60%	必評	3.1電子郵件演練樣板設計(20%)	3.1.1 演練郵件內容設計 3.1.2 演練郵件附件支援樣態 3.1.3 自行撰寫設定介面
	必評	3.2電子郵件演練發信系統(20%)	3.2.1 發信系統客製化管理 3.2.2 錯誤訊息管理 3.2.3 系統備援機制 3.2.4 觸發行為判斷(人為或非人為觸發)
	必評	3.3電子郵件演練統計分析 (10%)	3.3.1 開啟郵件統計分析 3.3.2 點閱郵件連結/附件統計分析 3.3.3 郵件類型測試結果統計分析
	選評	3.4 簡訊演練(10%)	3.4.1 演練簡訊內容設計 3.4.2 發簡訊系統管理 3.4.3 演練統計分析(點閱簡訊內容之連結)

註：紅字表示異動

3)專業技術構面_新增評鑑選項彈性
委員評鑑成績計算方式

國家資通安全研究院
National Institute of Cyber Security

- 全部評鑑：單一資安服務類別評鑑所有項目
  - 專業技術構面成績計算：依所有評鑑項目之得分合計
- 部分評鑑：單一資安服務類別僅評鑑部分項目
  - 專業技術構面成績計算：(受評項目得分合計 / 受評項目配分合計) X 專業技術構面配分

範例：以弱點掃描服務為例，共計 3 項評鑑項目，廠商僅參加 2 項服務

專業技術成績：((20+23)/(25+25))X60=51.6

評鑑構面	評鑑項目	得分
3. 專業技術構面(60%)	3.1. 主機系統弱點掃描(25%)(必評)	20
	3.2. Web網頁弱點掃描(25%)(必評)	23
	3.3. 網頁個資掃描(10%)(選評)	未評
原始得分		43
專業技術構面成績		51.6

廠商評鑑小組組成

國家資通安全研究院
National Institute of Cyber Security

- 資安服務廠商評鑑小組
  - 召集人1人，由資安院院長擔任
  - 副召集人2人，由資安院副院長擔任
  - 評鑑委員11-21人：由政府機關(構)、學術、研究領域及資安院等具資安實務經驗之學者或專家擔任
- 遴選條件
  - 擔任政府機關(構)之資訊單位正副主管或具資安實務經驗者
  - 任職於大專校院、國內法人或研究機構，具資安實務經驗者
- 112年評鑑小組委員
  - 當然委員10位、外部委員10位(政府機關委員5位、學/研委員5位)
  - 每類資安服務委員人數至少5位(當然委員2+外部委員3)

評鑑方式_機關評鑑說明

機關評鑑之4構面配分

國家資通安全研究院
National Institute of Cyber Security

- 資安服務類別之4構面配分
  - 1.、2.、4.為共通構面，各資安服務類別之評鑑內容一致，主要差異為 **3.專業技術構面**

序號	資安服務類別/評鑑構面	1.學習成長	2.服務流程	3.專業技術	4.服務品質	總分
1	SOC服務	10%	10%	60%	20%	100
2	資安健診服務	10%	10%	60%	20%	100
3	弱點掃描服務	10%	10%	60%	20%	100
4	滲透測試服務	10%	10%	60%	20%	100
5	社交工程演練服務	10%	10%	60%	20%	100

機關評鑑表-共通構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- 資安服務類別之1.、2.、4.共通構面問項

評鑑構面	評鑑項目
1. 學習 成長 10%	1.1 專案人員之專業證照表現
	1.2 專案人員之資安年資/經驗
2. 服務 流程 10%	2.1 專案技術人力配置
	2.2 資安服務作業流程SOP
	2.3 資安服務風險管理作業
4. 服務 品質 20%	4.1 交付文件內容品質
	4.2 整體技術服務表現
	4.3 整體服務品質表現

機關評鑑表-專業技術構面評鑑內容

國家資通安全研究院
National Institute of Cyber Security

- 資安服務類別之專業技術構面問項，以服務前、中、後之廠商表現，由採購機關角度進行評鑑

評鑑構面	階段	SOC服務	資安健診服務	弱點掃描服務	滲透測試服務	社交工程演練服務
3. 專業技術構面 60%	服務前	1.監控範圍規劃與溝通 2.監控設備部署維護	1.前置作業規劃與溝通 2.檢視工具之使用	1.前置作業規劃與溝通 2.掃描工具之使用	1.前置作業規劃與溝通 2.測試工具之使用	1.前置作業規劃與溝通 2.社交工程演練規劃
	服務中	3.情資分析與回傳 4.資安事件通知與內容 5.資安事件處理 6.資安威脅預警分享	3.檢視結果之分析能力 4.檢視結果之驗證能力	3.掃描結果之分析能力 4.掃描結果之驗證能力	3.檢測結果之分析能力 4.檢測結果之驗證能力	3.社交工程演練內容設計 4 社交工程演練統計分析
	服務後	7.資安事件之改善建議 8.諮詢服務	5.檢視結果之改善建議 6.諮詢服務	5.掃描結果之改善建議 6.諮詢服務	5.檢測結果之改善建議 6.諮詢服務	5.社交工程演練結果之改善建議 6.諮詢服務

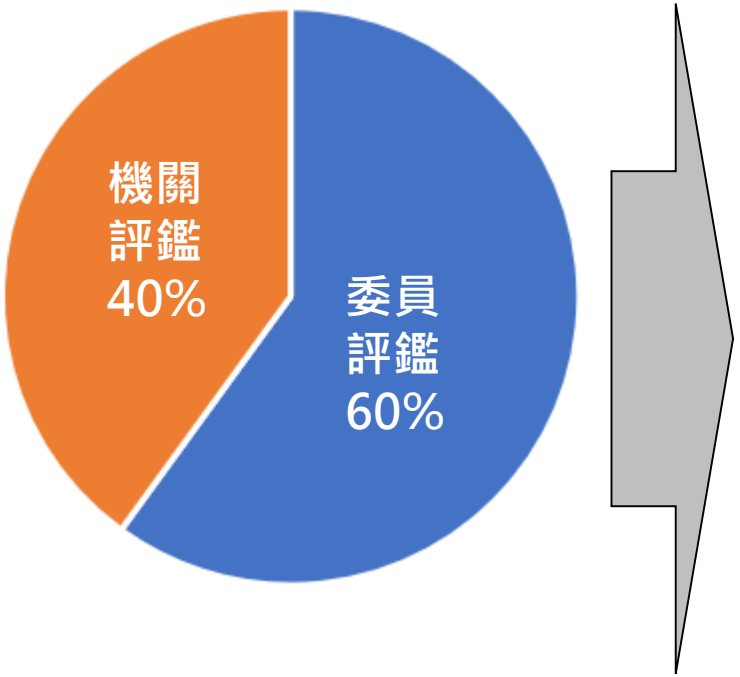
詳見附件3：機關評鑑表

4)調修評鑑方式之配分

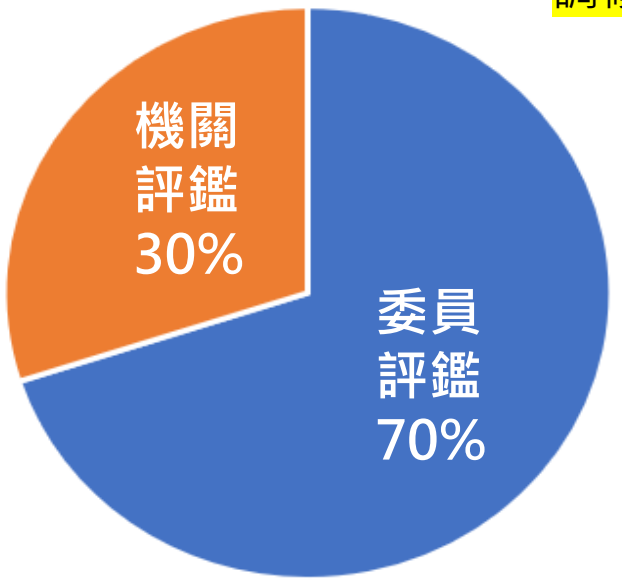
國家資通安全研究院
National Institute of Cyber Security

- 提升專業評鑑之定位，提高委員評鑑比例
- 降低機關評鑑數量差異之影響

原規劃



調修後　註：紅字表示異動



- 廠商總評鑑成績以「委員評鑑」與「機關評鑑」2項成績合計之
- 成績分配為委員評鑑占70%、機關評鑑占30%(計算至小數點第2位，小數點第3位四捨五入)

5)調修評鑑結果公布資訊

國家資通安全研究院
National Institute of Cyber Security

- 考量評鑑機制調整與其他因素，評鑑結果公布資訊調修
  - 以資安服務類別之評鑑等第(A~E)為主
  - 因應新增評鑑選項彈性，新增揭露評鑑項目資訊
  - 原廠商資安服務特色說明，不易區別差異且無顯著幫助，故移除

受評廠商	SOC服務	資安健診服務	弱點掃描服務	滲透測試服務	社交工程演練服務
甲廠商	B ☑SOC監控維運 ☑資安事件處理 ☑情資回傳	B ☑網路架構檢視 ☑有線網路惡意活動檢視 ☑使用者電腦惡意活動檢視 ☑伺服器主機惡意活動檢視 ☑防火牆連線設定檢視 ☑目錄伺服器(AD)設定檢視 ☐政府組態基準(GCB)設定檢視 ☐資料庫安全檢視	B ☑主機系統弱點掃描 ☑Web網頁弱點掃描 ☐網頁個資掃描	B ☑作業系統測試 ☑網站服務測試 ☑應用程式測試 ☑密碼破解與無線服務測試	B ☑電子郵件演練樣板設計 ☑電子郵件演練發信系統 ☑電子郵件演練統計分析 ☐簡訊演練
乙廠商	A ☑SOC監控維運 ☑資安事件處理 ☑情資回傳	A ☑網路架構檢視 ☑有線網路惡意活動檢視 ☑使用者電腦惡意活動檢視 ☑伺服器主機惡意活動檢視 ☑防火牆連線設定檢視 ☑目錄伺服器(AD)設定檢視 ☑政府組態基準(GCB)設定檢視 ☑資料庫安全檢視	A ☑主機系統弱點掃描 ☑Web網頁弱點掃描 ☑網頁個資掃描	A ☑作業系統測試 ☑網站服務測試 ☑應用程式測試 ☑密碼破解與無線服務測試	A ☑電子郵件演練樣板設計 ☑電子郵件演練發信系統 ☑電子郵件演練統計分析 ☑簡訊演練

範例：
☑受評項目
☐未受評項目

評鑑作業與週期

國家資通安全研究院
National Institute of Cyber Security

評鑑方式	機關評鑑	委員評鑑	
		展示評鑑	實地評鑑 (適用 SOC服務)
實施說明	由資安署發函至採購機關， 由機關填復資安服務機關評鑑表	• 廠商簡報(含DEMO) • 書面資料查證 • 詢答(Q&A)	• 廠商簡報 • 書面資料查證 • 實地查證(含DEMO) • 詢答(Q&A)
評鑑地點	資安院彙整	執行機關指定 (資安院) (註1)	受評廠商
實施週期	每年1次	每2年1次(註2)	

註1：廠商同年受評多個資安服務(內含SOC服務)，評鑑地點以受評廠商為主

註2 ：

- 對於同1家受評廠商且同1類資安服務，每2年執行1次委員評鑑
- 第1年委員評鑑成績，以該年委員評鑑配分計算
- 第2年委員評鑑成績，以前1年之委員評鑑成績計算(SOC服務例外)

評鑑作業時間規劃

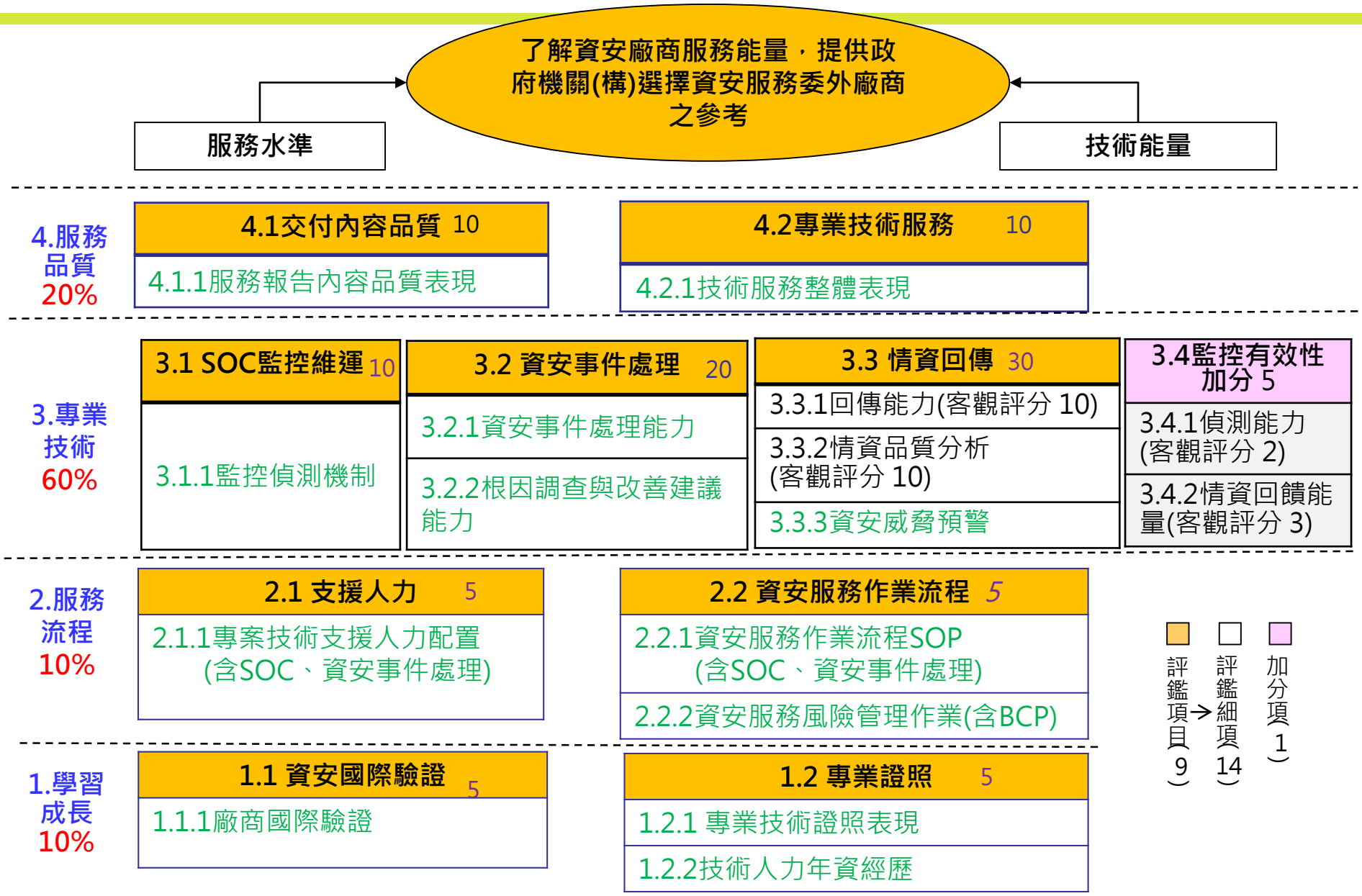
國家資通安全研究院
National Institute of Cyber Security

評鑑資安服務數量	簡報+Demo	委員提問與討論	評鑑討論會議 (評鑑小組內部會議)
原則	基本10分鐘； 每1項服務15分鐘	基本15分鐘； 每1項服務10分鐘	基本10分鐘； 每1項服務5分鐘
1類服務者	25	25	15
2類服務者	40	35	20
3類服務者	55	45	25
4類服務者	70	55	30
5類服務者	85	65	35
實地評鑑 SOC監控服務訪視 (適用 SOC服務評鑑)	+20 (含廠商摘要說明5分鐘)		

附件1. 5類資安服務評鑑架構

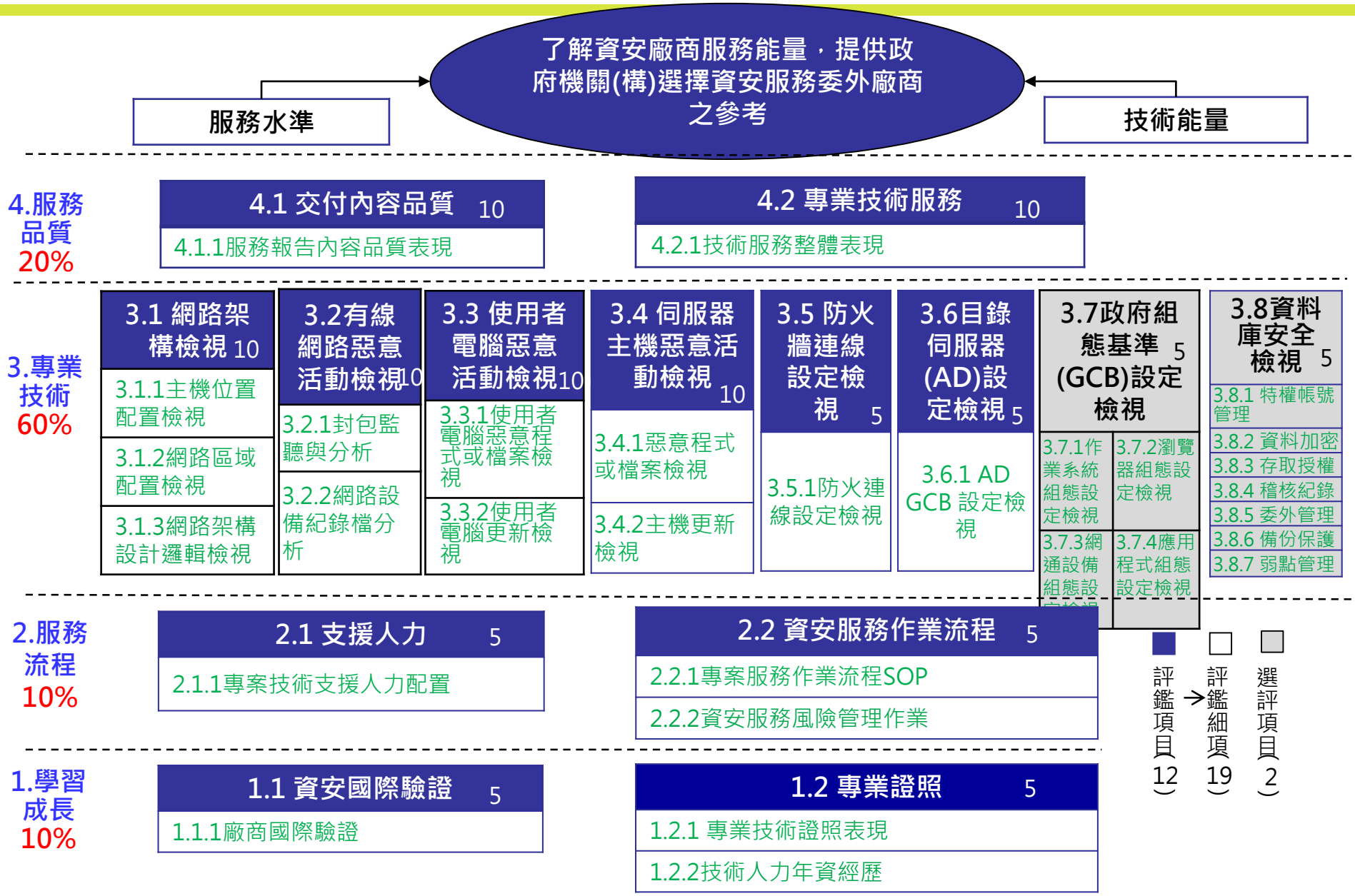
SOC服務評鑑架構

國家資通安全研究院
National Institute of Cyber Security



資安健診服務評鑑架構

國家資通安全研究院
National Institute of Cyber Security



弱點掃描服務評鑑架構

國家資通安全研究院
National Institute of Cyber Security

了解資安廠商服務能量，提供政府機關(構)選擇資安服務委外廠商之參考

服務水準

技術能量

4.服務品質 20%

4.1交付內容品質 10	4.2專業技術服務 10
4.1.1服務報告內容品質表現	4.2.1技術服務整體表現

3.專業技術 60%

3.1主機系統弱點掃描 25	3.2 Web網頁弱點掃描 (OWASP Top 10：2021) 25	3.3 網頁個資掃描 10
3.1.1作業系統未修正漏洞檢檢測 3.1.2常用應用程式漏洞檢測 3.1.3網路服務程式檢測 3.1.4木馬程式檢測 3.1.5後門程式檢測 3.1.6帳號密碼破解測試 3.1.7系統之不安全與錯誤設定檢測 3.1.8網路通訊埠檢測	3.2.1 Broken Access Control 3.2.2 Cryptographic Failures 3.2.3 Injection 3.2.4 Insecure Design 3.2.5 Security Misconfiguration 3.2.6 Vulnerable and Outdated Components 3.2.7 Identification and Authentication Failures 3.2.8 Software and Data Integrity Failures 3.2.9 Security Logging and Monitoring Failures 3.2.10 Server-Side Request Forgery (SSRF)	3.3.1 對外網頁之個資檔案掃描 3.3.2 掃描之個資特徵

2.服務流程 10%

2.1 支援人力 5	2.2資安服務作業流程 5
2.1.1專案技術支援人力配置	2.2.1資安服務作業流程SOP 2.2.2資安服務風險管理作業

1.學習成長 10%

1.1 資安國際驗證 5	1.2 專業證照 5
1.1.1廠商國際驗證	1.2.1 專業技術證照表現 1.2.2技術人力年資經歷

評鑑項目(8) → 評鑑細項(26)　選評項目(1)

滲透測試服務評鑑架構

國家資通安全研究院
National Institute of Cyber Security

了解資安廠商服務能量，提供政府機關(構)選擇資安服務委外廠商之參考

服務水準

技術能量

4.服務品質 20%

4.1 交付內容品質 10	4.2 專業技術服務 10
4.1.1 服務報告內容品質表現	4.2.1 技術服務整體表現

3.專業技術 60%

3.1 作業系統測試 10	3.2 網站服務測試 20			3.3 應用程式測試 25		3.4 密碼破解與無線服務測試 5
3.1.1 遠端服務	3.2.1 設定管理	3.2.2 使用者認證	3.2.3 連線管理	3.3.1 電子郵件服務	3.3.2 網站服務	3.4.1 密碼強度測試
3.1.2 本機服務	3.2.4 使用者授權	3.2.5 邏輯漏洞	3.2.6 輸入驗證	3.3.3 檔案傳檔服務	3.3.4 遠端連線服務	3.4.2 無線服務測試
	3.2.7 Web Service		3.2.8 Ajax	3.3.5網路服務		

2.服務流程 10%

2.1 支援人力 5	2.2 資安服務作業流程 5
2.1.1 專案技術支援人力配置	2.2.1 資安服務作業流程SOP
	2.2.2 資安服務風險管理作業

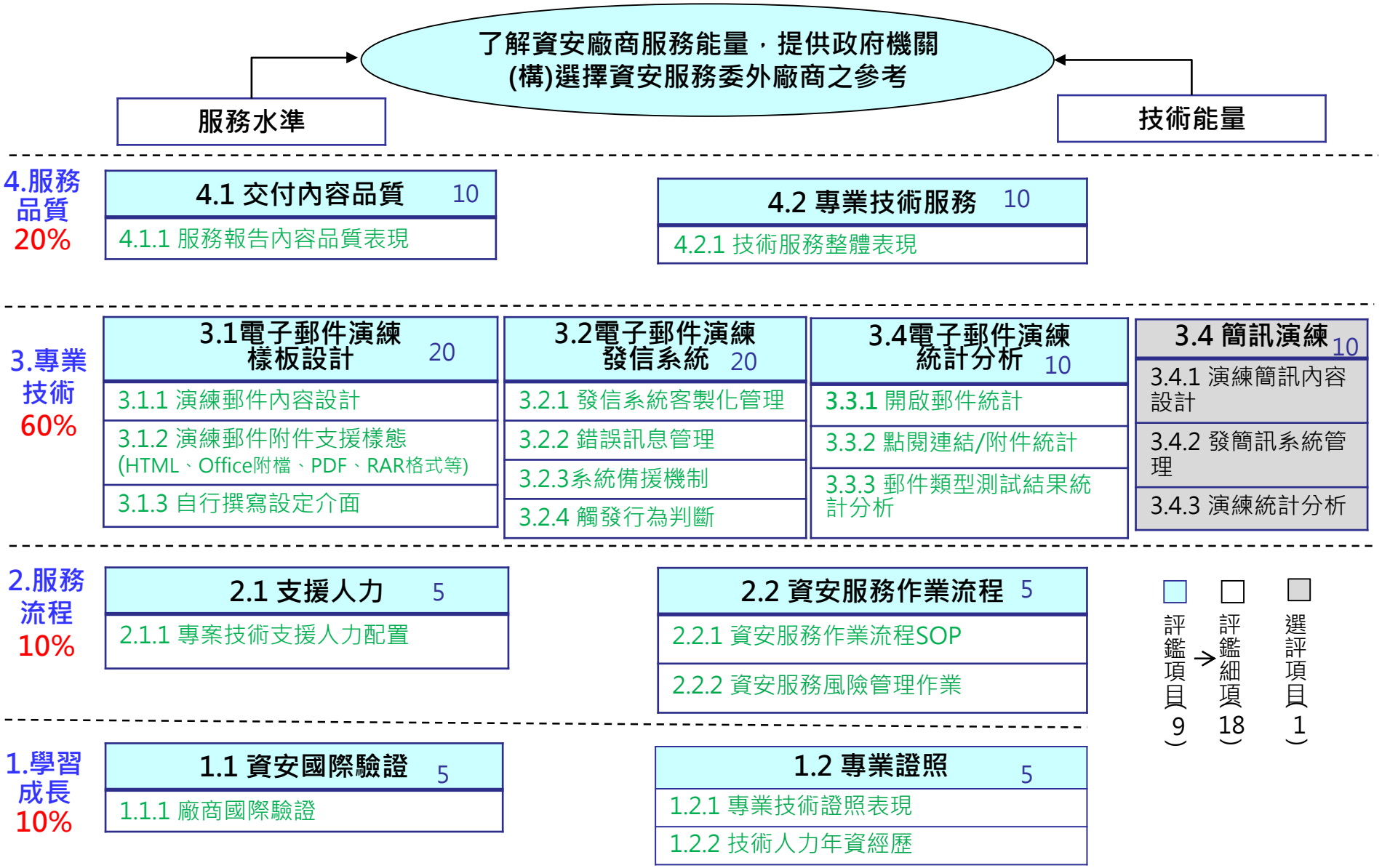
1.學習成長 10%

1.1 資安國際驗證 5	1.2 專業證照 5
1.1.1 廠商國際驗證	1.2.1 專業技術證照表現
	1.2.2 技術人力年資經歷

□ 評鑑項目 10) → □ 評鑑細項 25)

社交工程演練服務評鑑架構

國家資通安全研究院
National Institute of Cyber Security



附件2.
SOC監控有效性客觀評分計算公式

SOC服務_客觀評分總覽

國家資通安全研究院
National Institute of Cyber Security

- SOC監控有效性客觀評分計分原則與配分(112年1月至6月之表現)

廠商評鑑評鑑細項	對應聯防監控有效性			廠商評鑑配分
	項目	分析指標	驗證標的	
3.3.1 回傳能力	1. 回傳能力	1.1 資安監控情資格式正確率	1.1.1 依據「聯防監控資安監控情資回傳STIX格式規範」規定之「資安監控單」與「情資分析單」進行正確性驗證	5
		1.2 資安防護項目回傳率	1.2.1 依據SOC業者回傳「監控設備狀況單」之資安防護項目資訊，評估其監控偵測之回傳情形	5
3.3.2 情資品質分析	3. 情資品質	3.1 資安監控情資品質分析	3.1.1 依據SOC業者回傳之資安監控情資評估內容正確性	3
			3.1.2 依據SOC業者回傳之資安監控情資之有效情資回傳率	2
			3.1.3 依據SOC業者回傳之情資分析單，評估是否有萃取分析之指標情資，可包含具備受害偵測指標(IOC)、攻擊指標(IOA)	5
3.4.1 偵測能力	2. 偵測能力	2.1 網路攻防演練驗證	2.1.1 以機關網路攻防演練狀況，評估SOC業者偵測能力	2 (加分)
		2.2 資安院資安警訊驗證	2.2.1 以機關被通知之資安警訊，評估SOC業者偵測能力	
		2.3 機關通報資安事件驗證	2.3.1 以機關主動通報之資安事件，評估SOC業者偵測能力	
3.4.2 情資回饋能量	3. 情資品質	3.2 資安監控情資回饋能量	3.2.1 評估SOC業者回傳之資安監控情資有無額外回饋資訊，包含網際攻擊狙殺鍊分類資訊(Cyber Kill Chain, CKC)、MITRE ATT&CK、駭客工具、威脅手法分析情資、跨機關關聯性事件情資或重大資安弱點資訊等	1(加分)
			3.2.2 依據SOC業者回傳之資安監控情資之ATT&CK威脅樣態(Technique)資訊，評估其涵蓋率(ATT&CK官網最新公告之威脅樣態資訊為準)	1(加分)
			3.2.3 依據SOC業者回傳之資安監控情資之情資調查率	1(加分)

3.3.1 回傳能力計算公式(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 資安監控情資格式正確率計分標準
  - –總分5分，以比率 * 總分
    - ➢例如：格式正確率98%，0.98 * 5 = 4.9分

廠商評鑑評鑑細項	對應聯防監控有效性			廠商評鑑配分
	項目	分析指標	驗證標的	
3.3.1 回傳能力	1. 回傳能力	1.1 資安監控情資格式正確率	1.1.1依據「聯防監控資安監控情資回傳STIX格式規範」規定之「資安監控單」與「情資分析單」進行正確性驗證	5
		1.2 資安防護項目回傳率	1.2.1 依據SOC業者回傳「監控設備狀況單」之資安防護項目資訊，評估其監控偵測之回傳情形	5

3.3.1 回傳能力計算公式(2/2)

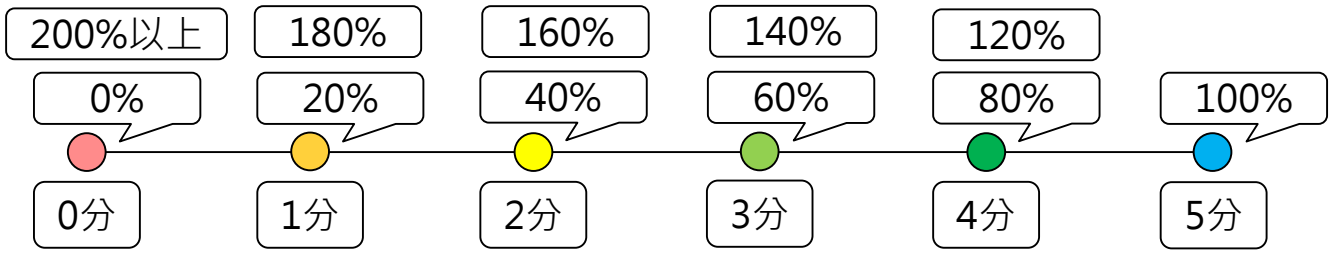
國家資通安全研究院
National Institute of Cyber Security

- 資安防護項目回傳率
  - 回傳率計算公式

$$\frac{\text{實際回傳之機關數量}}{\text{監控設備狀況單資安防護項目機關數量}}$$

    - 若監控設備狀況單資安防護項目機關數量如實呈報，回傳率100%
    - 若監控設備狀況單資安防護項目機關數量多報，回傳率低於100%
    - 若監控設備狀況單資安防護項目機關數量少報，回傳率高於100%
  - 計分標準
    - 以回傳率對應分數門檻級距

    例如：回傳率190%，5 – 4.5 = 0.5分



3.3.2 情資品質分析計算公式

國家資通安全研究院
National Institute of Cyber Security

- 內容正確性計分標準
  - 總分3分， 完全正確3分，1欄位錯誤2分， 2欄位錯誤1分，3欄位(含)以上錯誤0分
- 有效情資回傳率計分標準
  - 總分2分，有效情資回傳率80%(含)以上即2分
    - ➢有效情資回傳率達80%即滿分
  - 不足80%，以比率 * 總分
- 萃取分析之指標情資計分標準
  - 總分5分，萃取分析之指標情資比率達50%(含)以上即5分
    - ➢萃取分析之指標情資比率達50%即滿分
  - 不足50%，以比率 * 總分

廠商評鑑評鑑細項	對應聯防監控有效性			廠商評鑑配分
	項目	分析指標	驗證標的	
3.3.2 情資品質分析	3. 情資品質	3.1 資安監控情資品質分析	3.1.1 依據SOC業者回傳之資安監控情資評估內容正確性	3
			3.1.2 依據SOC業者回傳之資安監控情資之有效情資回傳率	2
			3.1.3 依據SOC業者回傳之情資分析單，評估是否有萃取分析之指標情資，包含受駭偵測指標(IOC)、攻擊指標(IOA)	5

3.4.1 偵測能力加分計算公式

國家資通安全研究院
National Institute of Cyber Security

- 網路攻防演練驗證、資安院資安警訊驗證及機關通報資安事件驗證，綜合開單率計分標準
  - 總加分2分，以比率 * 總加分
    - 例如：綜合開單率50%，0.5 * 2分 = 1分
    - 綜合開單率NA不予加分

廠商評鑑評鑑細項	對應聯防監控有效性			廠商評鑑配分
	項目	分析指標	驗證標的	
3.4.1 偵測能力	2. 偵測能力	2.1 網路攻防演練驗證	2.1.1 以機關網路攻防演練狀況，評估SOC業者偵測能力	加2分
		2.2 資安院資安警訊驗證	2.2.1 以機關被通知之資安警訊，評估SOC業者偵測能力	
		2.3 機關通報資安事件驗證	2.3.1 以機關主動通報之資安事件，評估SOC業者偵測能力	

3.4.2 情資回饋能量加分計算公式

國家資通安全研究院
National Institute of Cyber Security

- 額外回饋資訊計分標準
  - –總分1分，以比率 * 總加分
- 攻擊手法涵蓋率計分標準
  - –總分1分，以比率 * 總加分
- 情資調查率計分標準
  - –總分1分，以比率 * 總加分

廠商評鑑評鑑細項	對應聯防監控有驗證			廠商評鑑配分
	項目	分析指標	驗證標的	
3.4.2 情資回饋能量	3. 情資品質	3.2 資安監控情資回饋能量	3.2.1 評估SOC業者回傳之資安監控情資有無額外回饋資訊，包含網際攻擊狙殺鍊分類資訊(Cyber Kill Chain, CKC)、MITRE ATT&CK、駭客工具、威脅手法分析情資、跨機關關聯性事件情資或重大資安弱點資訊等	加1分
			3.2.2 依據SOC業者回傳之資安監控情資之ATT&CK威脅樣態(Technique)資訊，評估其涵蓋率(ATT&CK官網最新公告之威脅樣態資訊為準)	加1分
			3.2.3 依據SOC業者回傳之資安監控情資之情資調查率	加1分

分數試算-SOC_A

國家資通安全研究院
National Institute of Cyber Security

- SOC監控有效性(客觀評分)分數試算範例
  - –含加分共獲得21.47分

廠商評鑑評鑑細項	對應聯防監控有效性				廠商評鑑配分試算
	項目	分析指標	驗證標的		
3.3.1 回傳能力	1.回傳能力	1.1資安監控情資格式正確率	100%		5
		1.2資安防護項目回傳率	100%		5
3.3.2 情資品質分析	3.情資品質	3.1資安監控情資品質分析	3.1.1內容正確性	完全正確	3
			3.1.2有效情資回傳率	80%	2
			3.1.3萃取分析之指標情資	50%	5
3.4.1 偵測能力	2.偵測能力	2.1網路攻防演練驗證	NA		(0+1)/(4+3)=0.14 0.14*2分=0.28 +0.28(加分)
		2.2資安院資安警訊驗證	開單0則，共4則		
		2.3機關通報資安事件驗證	開單1則，共3則		
3.4.2 情資回饋能量	3.情資品質	3.2資安監控情資回饋能量	3.2.1額外回饋資訊比率	99.66%	0.99(加分)
			3.2.2攻擊手法涵蓋率	20%	0.2(加分)
			3.2.3情資調查率	0%	0(加分)
合計					21.47

分數試算-SOC_B

國家資通安全研究院
National Institute of Cyber Security

- SOC監控有效性(客觀評分)分數試算範例
  - –含加分共獲得21.19分，監控偵測能力為NA，不加分

廠商評鑑 評鑑細項	對應聯防監控有效性				廠商評鑑 配分試算
	項目	分析指標	驗證標的		
3.3.1 回傳能力	1.回傳能力	1.1資安監控情資格式正確率	100%		5
		1.2資安防護項目回傳率	100%		5
3.3.2 情資品質 分析	3.情資品質	3.1資安監控情資品質分析	3.1.1內容正確性	完全正確	3
			3.1.2有效情資回傳率	80%	2
			3.1.3萃取分析之指標情資	50%	5
3.4.1 偵測能力	2.偵測能力	2.1網路攻防演練驗證	NA		0(加分)
		2.2資安院資安警訊驗證	NA		
		2.3機關通報資安事件驗證	NA		
3.4.2 情資回饋 能量	3.情資品質	3.2資安監控情資回饋能量	3.2.1額外回饋資訊比率	99.66%	0.99(加分)
			3.2.2攻擊手法涵蓋率	20%	0.2(加分)
			3.2.3情資調查率	0%	0(加分)
合計					21.19

附件3. 機關評鑑表

機關評鑑表_共通構面

國家資通安全研究院
National Institute of Cyber Security

- 機關評鑑_共通構面(1、2、4)問項與說明

評鑑構面	評鑑項目	問項說明
1. 學習 成長 10%	1.1 專案人員之專業證照	評估專案人員之資安專業素質，專業證照表現
	1.2 專案人員之資安年資/經驗	評估專案人員之資安專業素質，專案人員之資安年資/經歷
2. 服務 流程 10%	2.1 專案技術人力配置	評估廠商之專案人力支援之合宜性
	2.2 資安服務作業流程SOP	評估廠商資安服務之SOP，包含服務前、服務中及服務後之相關作業流程，其準備度、掌控度及完整度
	2.3 資安服務風險管理作業	評估廠商於資安服務期間，是否事先告知資安服務時可能造成的風險，例如業務中斷等，並提醒機關確認備份事宜與其他相關配合作業；關於資安服務之資料保護，是否遵守資料在地化之規範
4. 服務 品質 20%	4.1 交付文件內容品質	廠商交付文件內容是否依採購規範要求，提供完整說明與相關需求改善建議；文件之可讀性、可用性、正確性、完整性及時效性之表現等
	4.2 整體技術服務表現	各項技術服務要求是否滿足共契採購規範之要求、技術服務效率及突發狀況處理等整體表現
	4.3 整體服務品質表現	評估廠商之配合度、主動性、溝通能力、服務態度、時程管理、遵守機關規定及售後服務等整體服務品質表現

機關評鑑表_SOC服務_專業技術構面

國家資通安全研究院
National Institute of Cyber Security

- 機關評鑑_SOC服務_專業技術構面

評鑑構面	評鑑項目	問項說明
3. 專業技術 60%	3.1 前置作業規劃與溝通	監控前對於資安服務之規劃與溝通，事先了解監控標的之用途、相關軟硬體及網路環境，並說明監控之風險與需要機關配合事項等
	3.2 監控設備部署維護	監控設備之部署符合機關需求，監控設備運作是否穩定及監控設備故障之維護作業
	3.3 情資分析與回傳	對於監控情資分析之能力，包含驗證正確性、時效性及配合政府聯防監控回傳監控情資等；且對於廠商每月提供機關「監控設備狀況單」之表現
	3.4 資安事件通知與內容	廠商判斷為資安事件時，是否即時並有效通知機關相關人員，提供相關資安事件內容，並協助機關內部溝通呈報與資安事件通報作業
	3.5 資安事件處理	廠商協助機關資安事件處理之表現，包含根因分析、資料蒐集、影響範圍評估及惡意程式分析等
	3.6 資安威脅預警分享	針對資安威脅預警服務，透過適當管道或平台，定期分享機關相關資安威脅資訊
	3.7 資安事件之改善建議	針對資安事件根因調查後，提出具體改善建議之情形，強化機關之資安防護
	3.8 諮詢服務	對於資安服務期間或後續是否提供諮詢服務並協助問題解決

機關評鑑表_資安健診服務_專業技術構面

國家資通安全研究院
National Institute of Cyber Security

- 機關評鑑_資安健診服務_專業技術構面

評鑑構面	評鑑項目	問項說明
3. 專業技術 60%	3.1 前置作業規劃與溝通	檢視前對於資安服務之規劃與溝通，是否事先了解檢視標的之用途、相關軟硬體及網路環境，並說明檢視之風險與需要機關配合事項等
	3.2 檢視工具之使用	檢視工具之合宜性、安全性、版本更新及限制使用大陸資通設備情形等
	3.3 檢視結果之分析能力	針對檢視結果進行分析，確認檢視之有效性與鑑別風險等級等
	3.4 檢視結果之驗證能力	針對檢視結果，進行再次確認，對於特殊需求或例外管理進行確認，確保檢視結果之準確性
	3.5 檢視結果之改善建議	針對檢視結果，是否清楚說明弱點原因，並提出具體改善建議，強化機關之資安防護
	3.6 諮詢服務	對於資安服務期間或後續是否提供諮詢服務並協助問題解決

機關評鑑表_弱點掃描服務_專業技術構面

國家資通安全研究院
National Institute of Cyber Security

- 機關評鑑_弱點掃描服務_專業技術構面

評鑑構面	評鑑項目	問項說明
3. 專業技術 60%	3.1 前置作業規劃與溝通	掃描前對於資安服務之規劃與溝通，是否事先了解掃描標的之用途、相關軟硬體及網路環境，並說明掃描流程與需要機關配合事項等
	3.2 掃描工具之使用	掃描工具之合宜性、安全性、版本更新、是否有使用限制大陸資通設備情形等
	3.3 掃描結果之分析能力	針對掃描結果是否進行分析，確認掃描之有效性及鑑別風險等級等
	3.4 掃描結果之驗證能力	針對掃描結果，是否進行再次確認，例如是否有特殊需求或例外管理，確保掃描結果之準確性
	3.5 掃描結果之改善建議	針對掃描結果，是否清楚說明弱點原因，並提出具體改善建議
	3.6 諮詢服務	對於資安服務期間或後續是否提供諮詢服務，協助問題解決

機關評鑑表_滲透測試服務_專業技術構面

國家資通安全研究院
National Institute of Cyber Security

- 機關評鑑_滲透測試服務_專業技術構面

評鑑構面	評鑑項目	問項說明
3. 專業技術 60%	3.1 前置作業規劃與溝通	檢測前對於資安服務之規劃與溝通，是否事先了解檢測標的之用途、相關軟硬體及網路環境，並說明檢測流程與需要機關配合事項等
	3.2 檢測工具之使用	檢測工具之合宜性、安全性、版本更新、是否有使用限制大陸資通設備情形等
	3.3 檢測結果之分析能力	針對檢測結果是否進行分析，確認檢測之有效性及鑑別風險等級等
	3.4 檢測結果之驗證能力	針對檢測結果，是否進行再次確認，例如是否有特殊需求或例外管理，確保檢測結果之準確性
	3.5 檢測結果之改善建議	針對檢測結果，是否清楚說明弱點原因，並提出具體改善建議
	3.6 諮詢服務	對於資安服務期間或後續是否提供諮詢服務，協助問題解決

機關評鑑表_社交工程演練服務_專業技術構面

- 機關評鑑_社交工程演練服務_專業技術構面

評鑑構面	評鑑項目	問項說明
3. 專業技術 60%	3.1 前置作業規劃與溝通	演練前對於資安服務之規劃與溝通，是否事先了解演練標的，並說明演練之風險與需要機關配合事項等
	3.2 社交工程演練規劃	社交演練規劃，考量機關使用者習慣、性別、年齡、家庭及興趣等因素，規劃派送時間與派送內容等
	3.3 社交工程演練內容設計	•社交演練內容設計，依機關族群特質設計內容，涵蓋3種以上不同類型的內容，例如八卦、休閒、保健、財經、情色、新奇或時事等資訊 •社交郵件設計包含本文、附檔及可連結資訊，提供附檔樣式多樣性。
	3.4 社交工程演練統計分析	針對社交郵件演練結果之「開啟郵件」、「點閱連結/開啟附件」或簡訊演練之點閱簡訊內容之連結等統計與受測者行為分析
	3.5 社交工程演練結果之改善建議	針對演練結果提出具體改善建議
	3.6 諮詢服務	對於資安服務期間或後續是否提供諮詢服務並協助問題解決

國家資通安全研究院
National Institute of Cyber Security

報告完畢