受託者資通安全聯合查核指引

行政院資通安全處

中華民國 110 年 12 月

目錄

一、 目的

受託者[1]資通安全聯合查核指引(以下簡稱本指引)旨在協助機關落實「資通安全管理法」第九條、「資通安全管理法施行細則」第四條有關選任及監督受託者之法遵要求及強化其監督管理機制，以聯合查核為原則，藉由集結政府機關之查核資源與能量，監督受託者之資通安全維護情形，並減少受託者受機關查核之頻率，進而兼顧落實政府機關供應鏈資通安全管理之效。

二、 適用對象

本指引適用對象為「資通安全管理法」納管之公務機關。

三、 查核類型

(一) 定期查核

機關依法遵要求對受託者辦理定期查核，以確認受託業務之執行情形時，機關可依當年度對受託者執行查核之規劃，尋找具共同受託者且亦規劃辦理查核作業之機關，辦理受託者資通安全聯合查核作業。

[1] 受託者係指依資通安全管理法第九條規定，公務機關委外辦理資通系統之建置、維運或資通服務之提供之受託者。

(二) 專案查核

機關於知悉受託者發生可能影響受託業務之資通安全事件時，應適當評估辦理受託者資通安全查核之必要。機關可尋找具共同受託者且其受託業務亦可能受事件影響之機關，辦理受託者資通安全聯合查核作業。

四、 查核形式

受託者資通安全聯合查核以實地查核為原則，機關並得視需要辦理技術檢測；惟查核範圍應以受託之專案範圍及可能影響機關受託業務之內部共用性資通系統(例如：防火牆、電子郵件系統)或資通安全管理政策等範圍為限。

(一) 技術檢測

機關得視需要辦理技術檢測，或從其契約規定，請受託者提供一年內由第三方檢測機構所出具之技術檢測報告。惟辦理專案查核時，機關應辦理技術檢測。

技術檢測之項目，建議至少包括但不限於下述內容：

1. 使用者電腦安全檢測：例如弱點掃描、防毒軟體、安全性修補程式更新、應用程式更新及惡意程式檢測等項目。
2. 網路惡意活動檢視：例如惡意中繼站連線阻擋檢測。

3. 核心資通系統安全檢測：針對核心資通系統進行滲透測試，包括檢測資通系統之權限存取、應用程式、系統弱點、系統通訊保護等項目，若資通系統使用單一簽入（Single Sign-On, SSO）進行權限控管，則亦納入檢測範圍。

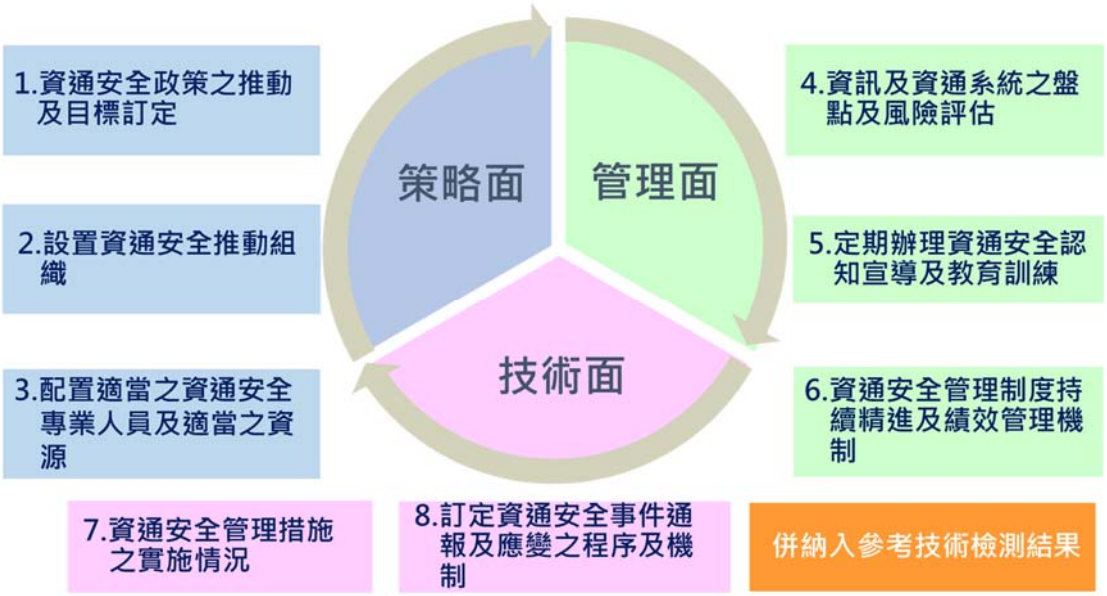
4. 網路架構檢測：透過訪談及實際檢視方式，驗證網路及系統之管理及安全控制措施、網路及系統架構之備援機制、防火牆規則及存取控制，並確認資通系統管理及防護情形。

5. 網域主機安全防護檢測：針對單位之網域主機進行防毒軟體、安全性修補程式更新、應用程式更新及惡意程式檢測等檢測。

6. 物聯網設備檢測：針對專案範圍內所使用之網路印表機、門禁設備、網路攝影機、無線網路基地台及路由器、環控系統等項目執行檢測作業，檢測設備存在之資安風險。

(二) 實地查核

實地查核作業建議依策略面、管理面及技術面等三大構面、八大查核項目(如圖一)，據以實施查核；倘有執行技術檢測，則檢測結果亦應併於實地查核加以驗證及查核。機關可依專案性質及契約內容等需求，調整查核項目。



圖一、實地查核項目[2]

五、 團隊組成及職責

(一) 甲方機關

即參與受託者資通安全聯合查核之機關，其須配合辦理事項如下：

1. 以正式公文書面授權甲方機關代表籌組聯合查核團隊，正本受文者包括甲方機關代表及受託者。
2. 推薦查核委員[3]予甲方機關代表，甲方機關代表得視實際情形審酌遴選查核委員。
3. 其他辦理受託者資通安全聯合查核之協作事項。

[2] 查核項目表範本如附件一，本表格須請受查核方於實地查核前填復，俾查核委員參考。
[3] 查核委員須推派機關內部具資安查核經驗、有資安稽核專業證照者擔任，且須熟悉資安相關法令或政策、專案契約規範等要求為佳。

(二) 甲方機關代表

由各參與受託者資通安全聯合查核之甲方機關共同推選之，建議分別以機關意願、機關層級及專案規模作為遴選條件；倘機關有意願擔任甲方機關代表者，經各甲方機關同意後出任之；無機關主動擔任甲方機關代表時，則以機關層級高者為優先進行遴選，當機關層級相同時，以專案規模(專案決標金額)大者為優先；倘經遴選後結果仍相同者，抽籤決定之。近二年曾擔任同一受託者資通安全聯合查核之甲方機關代表者，得免除參與甲方機關代表遴選。

甲方機關代表負責統籌辦理聯合查核事宜，職責包括(但不限)：

1. 與受託者洽談查核場域、查核範圍及時程等，並簽署受託者資通安全聯合查核專案規範授權書(範本如附件二)。
2. 籌組受託者資通安全聯合查核團隊，包括甲方機關領隊、查核委員及工作小組等，其中甲方機關領隊應由機關資安長或經資安長授權之人員擔任。
3. 執行實地查核作業，並完成查核報告。
4. 追蹤及管考查核發現事項。
5. 辦理聯合查核作業相關之行政協調、業務聯繫及公文書等程序事宜。

(三) 查核委員

策略面、管理面及技術面查核委員建議至少各遴選二、二、三名委員擔任，

倘機關推派之候選查核委員人數不足時，得請資通安全管理法主管機關推薦適當人選。

（四） 工作小組成員

由甲方機關代表籌組，得邀其他甲方機關派員參與，負責聯合查核作業期間之工作協助等事項。

（五） 技術檢測團隊

甲方機關經評估後，如需執行技術檢測，得籌組技術團隊執行技術檢測作業。

（六） 資通安全管理法主管機關

資通安全管理法主管機關得基於督導公務機關落實法遵要求之責，提供機關問題諮詢、查核計畫範本、實地查核觀察及相關查核諮詢等協助；倘機關經評估有執行技術檢測之必要且提請協助時，主管機關應提供適當協助，以落實供應鏈資通安全管理。

（七） 觀察員

實地查核可視需要安排觀察員(各構面以一名為原則)於現場觀摩[4]，累積查核實務經驗；技術檢測則不建議安排觀察員參與。

[4] 機關規劃或已建立觀察員遴選機制者始可選派觀察員參與實地查核。

六、 查核標的與範圍

(一) 查核標的

甲方機關委託辦理建置、維運資通系統或提供資通服務之受託者，倘有分包之情形，得視需要查核分包者。

(二) 查核範圍

包括受託者涉及甲方機關專案之所有場域(含專案辦公室及該公司所屬場域)，並得涵蓋租借之場所(例如：機房)及採多場域查核；惟場域及範圍應依甲、乙(受託者)雙方之合意劃定。

七、 查核頻率

(一) 定期查核

機關應依資通安全責任等級、受託者承作之資通系統防護需求等級、專案規模等評量指標，辦理受託者定期查核作業。其評量基準建議參考如下：

1. 資通安全責任等級A級或B級機關且承作機關核心資通系統之受託者，機關應每年辦理一次受託者資通安全查核。

2. 資通安全責任等級A級或B級機關且承作機關非核心資通系統者之受託者，其專案決標金額逾新臺幣一千萬元者，應至少每二年辦理一次受託者資通安全查核。

3. 其他非屬上述範疇者，應由機關依評量指標排定查核優先序，辦理受託者資通安全查核。

(二) 專案查核

知悉受託者發生可能影響受託業務之資通安全事件時，即可啟動專案查核，惟同一資通安全事件[5]以一年內查核一次為原則；機關辦理受託者資通安全查核後一年內，如再度因同一事件根因造成機關通報第三級或第四級資通安全事件時，則機關應評估是否再次對該受託者進行資通安全查核。

八、 查核結果

查核結果應於實地查核結束會議(Close meeting)經所有查核委員及乙方逐項確認後形成報告，並納入追蹤改善。倘甲、乙雙方就查核委員所開立缺失或改善建議無共識時，應由甲方機關領隊及乙方與會之最高主管(例如公司資安長)居中協調並達成共識；若仍無共識者，應作成紀錄並由所有甲方機關及乙方予以簽認。

[5] 同一資通安全事件係指受害標的(指系統、服務或網路狀態)及事件根因皆相同之事件。

甲方機關代表應於實地查核後一週內，將受託者資通安全聯核查核報告以密件函送予所有甲方機關及乙方參處並追蹤改善。甲方機關應要求乙方針對查核結果所列改善建議或缺失，就能立即改善者予以根本處理改善，未能立即改善者，則應依甲方機關要求、資安風險等級、投入資源等因素規劃全面改善之作法，排定改善優先序並限期改善，且於未完成改善前，應擬訂配套機制以降低風險。

九、 經費支應

執行受託者資通安全聯合查核所需相關經費(例如：差旅、誤餐費等)由各甲方機關公務預算項下自行支應。

十、 注意事項

(一) 受託者資通安全聯合查核專案規範授權書應一式二份，分別由甲方機關代表、乙方留存。

(二) 參與查核之團隊成員均須簽署保密同意書(範本如附件三)。

(三) 常見問題 Q&A 如附件四。

附件一--受託者查核項目表(範本)

○○○（公司名單）受託者查核項目表

編號：○○

填表日期：○○○年○○月○○日

查核人員：○○○

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	□	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	指派高階主管擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	公司內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	□	□	□	有訂定人員錄用之安全評估措施。
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	公司依規定配置資安人員。
	3.3 是否具備相關專業資安證照或認證？	□	□	□	專業人員具備ISO27001之證照。
	3.4 是否配置適當之資源？	□	□	□	公司已投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	資產依規定指定管理者及使用者。

	4.3 是否定有資訊、資通系統分級與處理之相關規範？	☐	☐	☐	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	☐	☐	☐	已進行風險評估及擬定相應之控制措施。
5.定期辦理資通安全認知宣導及教育訓練	5.1 是否定期辦理資通安全認知宣導？	☐	☐	☐	有定期辦理宣導。
	5.2 是否對同仁進行資安評量？	☐	☐	☐	按期進行資安評量。
	5.3 同仁是否依層級定期舉辦資通安全教育訓練？	☐	☐	☐	有定期辦理教育訓練。
	5.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	☐	☐	☐	同仁均瞭解單位之資通安全政策及目標。
6.資通安全管理制度持續精進及績效管理機制	6.1 是否設有稽核機制？	☐	☐	☐	訂有稽核機制。
	6.2 是否定有年度稽核計畫？	☐	☐	☐	有訂定年度稽核計畫。
	6.3 是否定期執行稽核？	☐	☐	☐	有按期執行稽核。
	6.4 是否改正稽核之缺失？	☐	☐	☐	訂有稽核後之缺失改正措施。
	6.5 是否訂定安全維護計畫持續改善機制？	☐	☐	☐	有訂定持續改善措施。
	6.6 是否追蹤過去缺失之改善情形？	☐	☐	☐	有追蹤缺失改善之情形。
	6.7 是否定期召開持續改善之管理審查會議？	☐	☐	☐	定期召開管理審查會議。
7.資通安全管理措施之實施情況	7.1 人員進入重要實體區域是否訂有安全控制措施？	☐	☐	☐	機房訂有門禁管制措施。
	7.2 重要實體區域之進出權利是否定期審查並更新？	☐	☐	☐	離職人員之權限已刪除。
	7.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	☐	☐	☐	對於進出人員監督其活動。
	7.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	☐	☐	☐	按時檢測機房物理面之情況。
	7.5 各項安全設備是否定期檢查？同仁有否施予適當之安全設備使用訓練？	☐	☐	☐	依規定定期檢查並按時提供同仁安全設備之使用訓練。
	7.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	☐	☐	☐	陪同或監視第三方支援人員。
	7.7 重要資訊處理設施是否有特別保護機制？	☐	☐	☐	對於核心系統主機設置特別保護機制。

	7.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	□	□	□	定期檢查物理面之風險。
	7.9 電源之供應及備援電源是否作安全上考量？	□	□	□	有設置備用電源。
	7.10通訊線路及電纜線是否作安全保護措施？	□	□	□	電纜線老舊，設有安全保護措施。
	7.11設備是否定期維護，以確保其可用性及完整性？	□	□	□	設備按期維護。
	7.12設備送場外維修，對於儲存資訊是否訂有安全保護措施？	□	□	□	訂有相關之保護措施。
	7.13可攜式之電腦設備是否訂有嚴謹之保護措施(如設通行碼、檔案加密、專人看管)？	□	□	□	攜帶式設備訂有保護措施。
	7.14設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	設備報廢前均有進行資料清除程序。
	7.15公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	人員下班後將機敏性公文妥善存放。
	7.16系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	系統開發測試與正式作業區隔。
	7.17是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	按時更新病毒碼。
	7.18是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	定期進行相關系統之病毒掃瞄。
	7.19是否定期執行各項系統漏洞修補程式？	□	□	□	定期進行漏洞修補。
	7.20是否要求電子郵件附件及下載檔案在使用前須檢查有無惡意軟體(含病毒、木馬或後門等程式)？	□	□	□	系統設有檢查之機制。
	7.21重要之資料及軟體是否定期作備份處理？	□	□	□	有定期做備份處理。
	7.22備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	備份資料均有測試。
	7.23對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	均有設加密之保護措施。
	7.24是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	□	□	□	訂有可攜式媒體之管理程序。
	7.25是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	訂有使用者存取權限註冊及註銷之作業程序。
	7.26使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	□	□	定期檢視使用者存取權限。
	7.27通行碼長度是否超過六個字元(建議以 8 位或以上為宜)？	□	□	□	通行碼符合規定。
	7.28通行碼是否規定須有大小寫字母、數字及符號組成？	□	□	□	通行碼符合規定。
	7.29是否依網路型態(Internet、Intranet、Extranet)訂定適當之存取權限管理方式？	□	□	□	依規定訂定適當之存取權限。

	7.30對於重要特定網路服務，是否作必要之控制措施，如身分鑑別、資料加密或網路連線控制？	□	□	□	對於特定網路有訂定相關之控制措施。
	7.31是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	□	□	□	有針對行動式電腦訂定管理政策。
	7.32重要系統是否使用憑證作為身分認證？	□	□	□	針對重要系統設有身分認證。
	7.33系統變更後其相關控管措施與程序是否檢查仍然有效？	□	□	□	系統更新後相關措施仍有效。
	7.34是否可及時取得系統弱點之資訊並作風險評估及採取必要措施？	□	□	□	可即時取得系統弱點並採取應變措施。
8.訂定資通安全事件通報及應變之程序及機制	8.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	有訂定通報應變程序。
	8.2 公司同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	□	□	□	同仁及受託者均知悉通報應變程序，並定期宣導。
	8.3 是否留有資通安全事件處理之紀錄文件，紀錄中並有改善措施？	□	□	□	有留存相關紀錄。

單位主管：○○○　　資通安全長：○○○

註：陳核層級請公司依需求調整。

附件二-受託者資通安全聯合查核專案規範授權書(範本)

受託者資通安全聯合查核專案
規範授權書

1、專案資訊

受查核對象：　○○公司(契約乙方以下稱本公司)
查核範疇：○○部及●●部契約甲方可查核之範疇，惟可視實需於協議後擴增，俾徹底檢視本公司資訊環境之安全防護能力及資安潛在風險。
查核期間：０年０月０日起至０年０月０日止，可視實需於協議後擴增；另執行時間為每週一至週五全天(二十四小時)，例假日(或國定假日)不執行。
執行單位：授權資安查核團隊(名冊如附件)執行

2、查核規範

1. 資安查核團隊遵守下列四原則：
   (1) 相關資料非經本公司同意不得攜出，若有必要須經本公司依程序簽核後辦理。
   (2) 不可造成永久性破壞致影響本公司運作。
   (3) 執行人員須遵守進入本公司有關處所相關規定，若有窒礙之處，由雙方協商。
   (4) 查核作業須在雙方監控機制下完成，俾釐清責任歸屬。
2. 為有效檢測整體資安強度，作業在不造成永久性破壞前提下，不限制任何手法、工具、參數、途徑或方式。如有檢測成功，得以畫面佐證。
3. 查核結果完成畫面佐證後，須對機敏資訊去識別化。
4. 查核過程中如有發生異常狀況(如受測系統停止運作等)，請立即向聯繫窗口反映。
5. 查核作業由資安查核團隊攜帶資訊設備，進入本公司執行查核，資訊設備攜出本公司務必完成儲存媒體格式化作業。
6. 本公司於查核作業期間提供資安查核團隊作業空間與網路環境，團隊得於該空間(包含但不限於)運用相關資源執行；另外網測試得於機關外部執行。
7. 本公司將派遣知悉機關內網路架構、系統拓樸與檔案屬性之專人配合

作業，該員亦須簽訂保密切結書，並不得將專案期間所獲悉資訊回報本公司。

8. 本公司配合查核範疇含括如下：

(1) ○○公司○○辦公室之對外網路及對外主機。
(2) 參與專案有關之資通系統開發、測試場域之主機及相關設備。
(3) 參與資通系統開發、測試、維運之專案成員及其個人電腦等作業用裝置（或設備）。
(4) 前述場域之作業環境與空間、人員等。
(5) 本公司核心資通訊系統，如 AD 目錄服務系統。

9. 本公司可代訂餐點(便當等)，並由資安查核團隊自費付款。

10. 本公司將先期完成新聞稿撰擬備用，如遇新聞事件，以本公司公關部門優先主動回應為原則，資安查核團隊與本公司其他部門成員均不可擅自對外發布訊息。

11. 資安查核團隊因任務所知悉或持有本公司之資訊與本專案輪廓、編組與細節，應負保密義務，不得以任何形式揭露於第三方，或對無關人員透漏，或為其本身或他人之利益而使用，本公司同仁亦比照辦理。

12. 本公司管理階層與○○部(資安查核團隊機關代表)建立高階即時聯繫窗口，如遇突發事件，由雙方共同協議後，管制所屬遂行各項決議。

3、簽署

本授權書正本一式二份，由本公司、資安查核團隊機關代表簽署後生效且具同等效力，各執一份為憑。本授權內時程與權利義務之免除、限制、增刪、修正或修改，應由合法授權代表人以書面簽署之文件為之。

簽署人：

本公司代表:_____

資安查核團隊機關代表:_____

中華民國_____年_____月_____日

附件三- 保密同意書(範本)

○○○○公司資通安全聯合查核參與人員保密同意書

本人_____（下稱簽署人）為參與○○、○○等機關(下稱機關)辦理○○○○公司(下稱受查核公司)資通安全聯合查核(以下簡稱本案)，於本案執行期間有知悉、可得知悉或持有受查核公司業務秘密，簽署人同意恪遵本同意書下列事項：

一、 簽署人對受查核公司或機關所揭露口頭及書面之相關機密資訊或文件(包括但不限於經註明為機密或其他同義文字之有形資訊，或以口頭方式揭露且於揭露時聲明其為機密等，以下簡稱「機密資訊」)，應嚴守保密義務。

二、 簽署人應遵守國家機密保護法、資通安全管理法、個人資料保護法、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、著作權法及其他相關法令之規定，並對因執行本案或因執行本案之機會所知悉之機密資訊負有保密義務；且上開各義務不因簽署人與受查核公司間，就本案擔任技術檢測或實地查核團隊成員相關事宜之法律關係解除、終止或完成而失其效力。

三、 簽署人就因參與本案或因參與本案之機會，所知悉或接觸之受查核公司、機關或其他第三人之機密資訊,除因執行本案所必須,且事先經受查核公司書面同意者,或法律另有明文規定外，不得有下列行為：

(一) 全部或一部重製或留存上開機密資訊；
(二) 以任何方式向任何第三人揭露上開機密資訊之全部或一部；
(三) 以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；
(四) 以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；
(五) 揭露、公開或使用上開機密資訊之全部或一部。

四、 簽署人因執行本案所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬機關所有。

五、 簽署人如違反第三條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致受查核公司或機關，遭受任何不利益，或受第三人法律上請求或訴追者，簽署人應賠償受查核公司或機關,因此所生之一切損失及費用(包括但不限於賠償金、和解金、律師費及訴訟費用等)。

六、 簽署人應避免使人誤認推薦特定對象、產品或服務；且參與本案相關事務或出席會議，應親自為之。

此　致

○○○○公司

立 同 意 書 人
姓　　名：　　（簽章）

中　　華　　民　　國　　年　　月　　日

附件四-常見問答 Q&A

Q1、資通安全聯合查核結果是否為他人或他機關所悉？

1. 聯合查核團隊成員均須簽署保密同意書，非經甲方書面同意，查核過程中所知悉事項不得以任何形式洩露或交付第三人，並嚴守保密義務。

2. 受託者資通安全聯核查核報告應由甲方機關代表以密件函送予所有甲方機關及乙方(受託者)參處並追蹤改善，非屬前述受文對象，不應獲悉查核結果。

Q2、機關查核具資安查核專業之人員尚不足，是否可委託第三方顧問公司協助受託者資安聯合查核作業？

考量受託者資安查核範圍涉及甲、乙雙方契約內容，為免衍生違約疑慮，團隊成員建議以甲方機關、資通安全管理法主管機關等適當人員參與為宜。

Q3、技術檢測作業是否會造成受查核方(受託者)系統環境或網路架構之作業異常？

1. 技術檢測係針對受託者公司場域(查核範圍所屬專案之使用者電腦、核心資通系統、網路架構及網域主機、物聯網(IoT)設備、網路惡意活動檢視等)進行弱點掃瞄、滲透測試或安全性檢視等非破壞性檢測作業，不會造成受託者系統環境、網路架構或作業場域之異常。

2. 另技術檢測範圍須於實際檢測前經甲、乙雙方及檢測團隊溝通合意後為之，且於技術檢測作業當下應有乙方人員於現場確認檢測步驟及檢測結果。

Q4、受託者資通安全聯合查核應於啟動後多久內完成？

1. 倘以甲方機關代表及乙方合意後為啟動日(以 D 為代稱)，則應於 D+30 日內完成實地查核作業，甲方機關代表並應於 D+37 日內(即實地查核完一週內)將受託者資通安全聯合查核報告以密件函送予所有甲方機關及乙方(受託者)參處並追蹤改善。

2. 倘有辦理技術檢測作業，則實地查核以技術檢測結束後二週內完成為原則。

Q5、經甲、乙雙方及查核委員完成簽署之實地查核報告，於正式行文前是否可再進行內容之調整與編修？

1. 一旦經由甲、乙方及所有查核委員逐項確認並簽署後之實地查核報告即已具備其效力，不宜再調修報告內容。

2. 惟倘經確認報告內容有重大瑕疵者，得取得所有查核委員同意後適當調修報告內容，並再進行重新簽署以完成實地查核報告。

Q6、何謂同一資通安全事件？機關是否可重複對受託者進行資通安全查核？

1. 同一資通安全事件係指受害標的(指系統、服務或網路狀態)及事件根因皆相同之事件，受害標的範圍包括委託機關或受託者。

2. 同一資通安全事件以一年查核一次為原則，機關於辦理受託者資通安全查核後一年內再度因同一事件根因造成機關通報第三級或第四級資通安全事件時，則機關應評估是否再次對該受託者進行資通安全查核。