電信事業資通安全管理手冊

國家通訊傳播委員會

中華民國 101 年 9 月 3 日

目　錄

電信事業資通安全管理手冊

中華民國 98 年 8 月 11 日 0984302058 號簽上網公告
中華民國 99 年 6 月 11 日 0994301464 號簽上網公告
中華民國 101 年 9 月 3 日 1014302984 號簽上網公告

一、依據

本手冊依電信事業[1]資通安全管理作業要點第二點規定訂定之，主要為提供產業規範，輔導目的事業逐漸落實資通安全管理機制。

二、目的

基於保障資通安全[2]及維護使用者權益原則，確保通訊系統設備、資料及網路安全，本手冊包含下列要項：

（一）資通安全管理標準。

（二）資通安全等級評估。

（三）資通安全管理機制及教育訓練。

（四）資通安全應變通報。

（五）資通安全實施評鑑。

（六）年度提報資料要求。

[1] 電信事業：指經營電信服務供公眾使用之事業。
[2] 資通安全簡稱資安。

三、要項說明

（一）資通安全管理標準

電信事業實施資通安全管理,建議參照下列CNS國家標準或ISO/IEC 27000系列國際標準，建立資通安全管理機制：

1、資訊安全管理系統要求事項：CNS/ISO/IEC 27001

2、資訊安全管理作業規範：CNS/ISO/IEC 27002

3、資訊安全管理系統實施指引：ISO/IEC 27003

4、資訊安全管理測量方法： ISO/IEC 27004

5、資訊安全管理風險管理：CNS/ISO/IEC 27005

6、電信事業資訊安全管理實作指引：ISO/IEC 27011

（二）資通安全等級評估

1、電信事業應依據下列步驟，實施高階風險評鑑作法（High-Level Risk Assessment)，評估資通安全等級，以定義資通安全範圍與邊界，確定資通安全需求水準，作為後續訂定風險處理優先順序之參考：

（1）依據執照核發之營業項目範圍內，調查電信事業營運所需之資產群組，若組織規模龐大者，得區分為不同之事業體或部門，區分為以下三大類，分別進行資產群組之調查：

- 關鍵業務類資產：

  指電信事業之核心網路設備(交換、傳輸、網管等)、接取網路設備、管線基礎設施等。

- 支援業務類資產：

  指第二類電信轉售服務業務及支援電信事業營運所需之資訊處理設施，但非屬關鍵業務者，例如：客服管理系統、帳務管理系統，或是涉及客戶個人資料蒐集、處理及利用者。

- 行政業務類資產：

  指電信事業內部輔助單位，例如：人事、行政、總務等之業務資產。

（2）依據每一資產群組失效後之「衝擊影響程度」，評估資通安全等級，決定資通安全管理機制改善之優先順序，並每年定期更新。

（3）填寫「電信事業資通系統安全等級自我評估彙整表」（詳見附件一）及「電信事業資通安全等級自我評估說明表」（詳見附件二）。

2、評估資通安全等級步驟如下：

（1）需將支援電信事業營運所需之「關鍵業務」、「支援業務」及「行政業務」等資產群組全部納入，決定資產安全等級，逐步建立資通安全管理機制。

（2）針對每個資產群組依「影響業務運作」、「資料保護受到損害」、及「法律規章之遵循」等之影響構面，分別評定各影響構面之資產安全等級，區分為 A、B、C 三級。

（3）資產群組失效之衝擊影響程度，依據各影響構面，採用最高原則方式處理，當有任一影響構面之衝擊影響程度為 A 者，則該資產群組之資產安全等級應評估為 A;如全部影響構面之衝擊影響程度均為 C 者，該資產群組之資產安全等級則評估為 C。

（4）最後將所有經評定資產群組之資產安全等級彙整，取其最高者，作為評定企業之資通安全等級之依據，如最高之資產群組資產安全等級為 A 者，其資通安全等級為 A 級；如最高之資產群組資產安全等級為 B 者，其企業之資通安全等級為 B 級；如最高之資產群組資產安全等級為 C 者，其企業之資通安全等級為 C 級。

（三）資通安全管理機制

1、電信事業之資產群組，其資產安全等級經評定為 A 級者，得視需要參考 CNS/ISO/IEC 27005 標準，進一步實施詳細風險評鑑（Detailed Risk Assessment），可參考附件三範例或是自行定義其風險管理作法，以決定風險處理策略。

2、電信事業應依自我評估之資通安全等級，訂定資通安全管理實施計畫，並每年定期進行內部稽核乙次（可參考電信事業資通安全管理實施計

畫範本)。

3、電信事業應依照「資通安全管理實施計畫執行工作事項表」(附件四)之資通安全等級，規劃資通安全管理實施計畫，每年應執行下列工作事項：

(1) 防護縱深

- 資通安全等級為 A 級者，防護縱深宜建置至少包括防毒閘道設備、網路型防火牆、入侵偵測防禦系統、網路型垃圾郵件過濾設備、路由交換器、乙太網路交換器、應用軟體控管設備、網頁應用防火牆等取得本會資通設備安全審驗證明之進階型設備。
- 資通安全等級為 B 級者，防護縱深宜建置至少包括防毒閘道設備、網路型防火牆、入侵偵測防禦系統、網路型垃圾郵件過濾設備等取得本會資通設備安全審驗證明之基礎型設備。
- 資通安全等級為 C 級者，防護縱深宜建置至少包括防火牆、入侵偵測防禦系統、防毒軟體、垃圾郵件過濾設備等設備。

(2) 推動方式

電信事業應成立資安推動小組，建立資通安全管理機制，將資通安全等級區分為 A、B、C 三級，以選擇適用之安全基準。

- 資通安全等級評定為 C 級者，應實施「資通安全管理內部稽核表」(詳見附件五)之最小限度安全需求項目。
- 資通安全等級評定為 B 級者，應實施「資通安全管理內部稽核表」之全部控制措施。
- 資通安全等級評定為 A 級者，除實施前述「資通安全管理內部稽核表」之全部控制措施外，另實施適用之「ISO/IEC 27011 增項稽核表」(詳見附件六)，並以通過資訊安全管理系統第三方驗證為目標，逐年改善最終及於全企業。

(3) 稽核方式

- 每年至少執行一次內部稽核。
- 已通過資訊安全管理系統驗證之資產群組，應定期維持更新及辦理

稽核工作。

（四）資通安全認知訓練

為建立電信事業員工正確資通安全認知、提升安全防護水準，應推動內部資通安全教育訓練，並依照附件五，規劃每年應辦理之資通安全教育訓練及宣導時數如下：

主管、資通訊人員、業務人員及一般人員，每年至少須分別達到 3、12、6、3 小時之資通安全認知訓練。

（五）資通安全應變通報

電信事業應建立資通安全事故應變作業機制，當發生資通安全事故時，應立即填具「國家通訊傳播委員會資通安全事故通報單」（附件七）向本會通報，並採取應變措施。

（六）資通安全實施評鑑

1、內部稽核

電信事業每年應自我評估資產群組之資通安全等級，選擇適用之安全控制措施，至少執行一次內部稽核，並將稽核結果依規定填寫於本手冊之相關附件：

電信事業依附件五、六執行內部稽核時，須填具附件如下：

（1）檢查項目勾選「符合」者，須備妥相關佐證資料以供查核。

（2）檢查項目勾選「不符合」者，須填具「資通安全管理矯正／預防措施一覽表」（附件八）及「資通安全管理矯正／預防措施單」（附件九）。

（3）檢查項目勾選「不適用」者，須填具「內部稽核表檢查項目勾選不適用之說明」（附件十）及「增項稽核表檢查項目勾選不適用之說明」（附件十一）

2、外部驗證

電信事業得向辦理資通安全管理系統驗證之機構申請外部驗證，

其申請驗證範圍應符合資通安全管理系統 CNS/ISO/IEC 27001 標準及本手冊附件六之規定。

前項驗證機構須經本會認可之本國認證體系認證，經驗證合格之電信事業，本會將於網站上公布。

3、行政檢查

電信事業如發生附件七之資通安全事故影響等級為 3 級或 4 級者，依其自我評估之資通安全等級，須於 1 週內備妥下列相關資料，以供本會行政檢查之用。

（1）重大資安事故應變措施之處理說明。

（2）資通安全管理實施計畫。

（3）資安管理手冊附件五至附件十一、各檢查項目之佐證資料、或經本會認可之資通安全管理機制驗證機構產出之稽核報告。

（七）年度提報資料要求

1、各電信事業應於每年 3 月底前，依其自我評估之資通安全等級，提報下列資料至本會：

（1）附件一、附件二、附件五，資通安全等級評定為 A 級者須提報附件六（B 級及 C 者不須提報）。

（2）依要項說明三（六）執行內部稽核，檢查項目勾選「不符合」者，須提報附件八及附件九。

（3）依要項說明三（六）執行內部稽核，檢查項目勾選「不適用」者，須提報附件十及附件十一。

2、電信事業經本會認可之資通安全管理機制驗證機構進行外部驗證，並取得 CNS/ISO/IEC 27001 證明者，僅須提報附件一、附件二、附件六、附件八（附件六檢查項目勾選「不符合」者須提報）、附件九（附件六檢查項目勾選「不符合」者須提報）及附件十一（附件六檢查項目勾選「不適用」者須提報），得免提報附件五及附件十，惟須檢附該驗證證書及驗證報告等相關資料影本。

3、電信事業經本會認可之資通安全管理機制驗證機構進行外部驗證，並取得 CNS/ISO/IEC 27001 標準及附件六 ISO/IEC 27011 增項稽核表驗證合格證明者，僅須提報附件一、附件二及附件十一（附件六驗證時檢查項目勾選「不適用」者須提報），得免提報附件五、附件六、附件八至附件十，惟須檢附該驗證證書及驗證報告等相關資料影本。

附件一 電信事業資通安全等級自我評估彙整表

公司名稱			
單位主管		評估日期：	
評估人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

資產群組	業務類別	影響構面／影響等級（註二）			資產安全等級
		影響業務運作	資料保護受到損害	法律規章之遵循	
	☐關鍵業務	☐A	☐A	☐A	☐A
	☐支援業務	☐B	☐B	☐B	☐B
	☐行政業務	☐C	☐C	☐C	☐C
	☐關鍵業務	☐A	☐A	☐A	☐A
	☐支援業務	☐B	☐B	☐B	☐B
	☐行政業務	☐C	☐C	☐C	☐C
	☐關鍵業務	☐A	☐A	☐A	☐A
	☐支援業務	☐B	☐B	☐B	☐B
	☐行政業務	☐C	☐C	☐C	☐C

資通安全等級： ☐A ☐B ☐C

（本表可視需要自行延伸）

附件一之填表說明

註一：評估資通安全管理作業範圍之業務類別

業務類別	說明
關鍵業務	電信事業之核心網路設備（交換、傳輸、網管等）、接取網路設備、管線基礎設施等。
支援業務	指第二類電信轉售服務業務及支援電信事業營運所需之資訊處理設施，但非屬關鍵業務者，例如：客服管理系統、帳務管理系統，或是涉及客戶個人資料蒐集、處理及利用者。
行政業務	指電信事業內部輔助單位之業務項目，例如：人事、行政、總務等。

註二：影響構面／資通安全等級

安全等級 / 影響構面	A	B	C
1.影響業務運作	● 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全 ● 系統故障將造成關鍵業務執行效能非常嚴重降低，甚至業務停頓	● 系統故障對社會秩序、民生體系運作將造成嚴重影響 ● 系統故障將造成關鍵業務執行效能嚴重降低	● 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響
2.資料保護受到損害	● 機密性資料 ● 資料若外洩或遭竄改，將導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損	● 敏感性資料 ● 資料若外洩或遭竄改，將導致個人權益嚴重受損之資料	● 一般性資料 ● 資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損
3.法律規章之遵循	系統運作、資料保護、資訊資產使用等，若未依循相關規範辦理，將導致機關從根本上違反法律，並導致嚴重不良後果，如：損害賠償、罰金或是刑責	系統運作、資料保護、資訊資產使用等，若未遵循相關規範辦理，將導致機關違反法規命令，並伴隨輕微後果，如：行政處分或罰鍰等	系統運作、資料保護、資訊資產使用等，若未遵循相關規範辦理，不會導致機關違反法規命

附件二 電信事業資通安全等級自我評估說明表

公司名稱				
單位主管		評估日期：		
評估人員		評估日期：		
聯絡窗口	電話：	傳真：	行動：	
	Email：		頁次:第　頁/共　頁	

資產群組	業務類別	影響構面	資產安全等級 A、B、C		原　因　說　明
	☐關鍵業務 ☐支援業務 ☐行政業務	影響業務運作	前一年度		
			本年度		
		資料保護受到損害	前一年度		
			本年度		
		法律規章之遵循	前一年度		
			本年度		
（本表可視需要自行延伸）	☐關鍵業務 ☐支援業務 ☐行政業務	影響業務運作	前一年度		
			本年度		
		資料保護受到損害	前一年度		
			本年度		
		法律規章之遵循	前一年度		
			本年度		
資通安全等級	☐ A　☐ B　☐ C				

附件三 電信事業資通安全管理詳細風險評鑑表（範例）

NO.	部門	保管人	說明	資訊資產	資產類別	數量	機密性	完整性	可用性	資訊資產價值	威脅	脆弱性	風險估計			
													威脅等級	脆弱等級	風險值	風險等級
流水序號	機關部門別	資產保管人	業務補充說明	資產名稱	資產類別：區分為資訊記錄、電腦系統、實體設備、服務、人員、或是其他類別各目的事業可依據實務需要加以細分。	填註資產之數量	依其重要程度區分為普（1）中（2）高（3）三級	依其重要程度區分為普（1）中（2）高（3）三級	依其重要程度區分為普（1）中（2）高（3）三級	綜整計算資訊資產價值＝機密性＋完整性＋可用性	依據不同之資產類別選擇適用之資產威脅 各目的事業可以依據實際實務需要，訂定資產威脅列表	依據不同之資產威脅，選擇對應之脆弱性 各目的事業可以依據實際實務需要，訂定資產威脅列表	評定威脅等級區分為普（1）中（2）高（3）三級	評定脆弱性等級區分為普（（1）中（（2）高（（3）三級	綜整計算風險值＝資產價值*威脅等級*脆弱等級	決定風險等級 3~23 普級 24~53 中級 54~81 高級
1	人力資源	鍾先生	企業徵才	履歷表	資訊紀錄	2000	高	高	中	8	作業人員或使用者錯誤	使用者認知不足。	2	3	48	中
2	網路技術	陳先生	機房管理	交換設備	實體設備	100	高	高	高	9	作業人員或使用者錯誤	使用者認知不足。	3	3	81	高
3	行銷	江先生	客戶名單	個人資料	資訊紀錄	100000	高	高	高	9	未授權存取資料	軟體開發者與作業人員的職責未釐	3	3	81	高

											清。				
4	網路技術	陳先生	機房管理	交換設備	實體設備	100	高	高	高	9	地震	沒有回復資訊與資訊資產的營運持續管理與程序。	2	3	54	中
5	網路技術	陳先生	機房管理	交換設備	實體設備	100	高	高	高	9	作業人員或使用者錯誤	使用者認知不足。	2	3	54	中
6	資訊科技	王先生	資料庫管理	通聯記錄	資訊紀錄	6000000	高	高	高	9	委外作業失能	未釐清委外協議的權責。	3	3	81	高

附件四 資通安全管理實施計畫執行工作事項表

作業名稱 內容 等級	資訊處理設施 防護縱深	推動方式	稽核方式	資安教育訓練 時數
A	宜建置至少包括防毒閘道設備、網路型防火牆、入侵偵測防禦系統、網路型垃圾郵件過濾設備、路由交換器、乙太網路交換器、應用軟體控管設備、網頁應用防火牆等取得本會資通設備安全審驗證明之進階型設備。	以通過資訊安全管理系統第三方驗證為目標	每年至少執行一次內部稽核	主管、資通訊人員、業務人員、一般人員，每年至少達到 3、12、6、3 小時
B	宜建置至少包括防毒閘道設備、網路型防火牆、入侵偵測防禦系統、網路型垃圾郵件過濾設備等取得本會資通設備安全審驗證明之基礎型設備。	自行規劃並成立資通安全管理推動小組	每年至少執行一次內部稽核	主管、資通訊人員、業務人員、一般人員，每年至少達到 3、12、6、3 小時
C	宜建置至少包括防火牆、入侵偵測防禦系統、防毒軟體、垃圾郵件過濾設備等設備。	加強資通安全宣導	每年至少執行一次內部稽核	主管、資通訊人員、業務人員、一般人員，每年至少達到 3、12、6、3 小時

電信事業資通安全管理防護縱深檢查表						
資安設備	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
防毒閘道設備	◎	◎				
網路型防火牆	◎	◎				
網路型垃圾郵件過濾設備	◎	◎				
入侵偵測防禦系統	◎	◎	◎			
路由交換器	◎					
乙太網路交換器	◎					
應用軟體控管設備	◎					
網頁應用防火牆	◎					
防火牆			◎			
防毒軟體			◎			
垃圾郵件過濾設備			◎			

附件五 電信事業資通安全管理內部稽核表

公司名稱			
資通安全等級	□A □B □C		
單位主管		稽核日期：	
稽核人員		稽核日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
1.資訊安全政策						
1.1 是否依據相關法律、法規及營運要求，訂定資安政策？	◎	◎	◎			
1.2 是否考量組織整體業務活動及其相關風險，訂定資安政策？	◎	◎	◎			
1.3 是否識別違反資安政策之後果及訂定處理程序？	◎	◎	◎			
1.4 是否由管理階層核准資安政策文件，正式發布且轉知所有員工與各相關外部團體？	◎	◎	◎			
1.5 資安政策文件是否包括資安之定義、整體目標、範圍、實施內容、執行組織、權責分工、員工責任、事故通報處理流程？	◎	◎				
1.6 是否依據資安政策，訂定原則、標準及對組織特別重要之法規要求說明之文件及資料（如法律、法規命令、行政規則、契約、安全教育、訓練、認知、營運持續管理、作業程序、資安控管文件、使用者應遵守的安全規則）？	◎	◎				
1.7 資安政策是否就一般和特定責任之權責（包括通報資安事故）加以定義？	◎	◎				
1.8 是否對支援資安政策的文件建立補述文件？如針對特定資訊系統更詳盡的安全政策和程序，或使用者宜遵守的安全規則。	◎	◎				
1.9 資安政策是否由具有發展、審查及評估等核准權限之管理者，依規劃期間或有重大變更時，作必要之審查及調整？	◎	◎				
1.10 組織是否妥善維護資安政策之審查紀錄與訂定管理審查程序，包括審查時程及週期？	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
1.11 是否定期對組織人員及資訊設備進行安全評估，以確定其遵守資安政策及相關規定？	◎	◎				
1.12 是否指定專人或專責部門進行資安政策的維護及檢討？	◎	◎				
2.資訊安全之組織						
2.1 管理階層是否在組織內藉由清楚的指示、明確的指派及確認資安管理責任，主動地展現承諾以支持資安？	◎	◎	◎			
2.2 是否指派擁有權責之管理階層或成立跨部門組織負責推動、協調及監督資安管理事項？	◎	◎				
2.3 是否指定專人或專責部門，負責辦理下列資安管理工作事項（1）資安政策、計畫、措施之研議，（2）風險評鑑、資訊分類、系統安全控管措施，（3）資料及資訊系統之使用管理及保護，（4）資安認知訓練及資安稽核？	◎	◎				
2.4 資安管理責任的配置是否依據資安政策，並明確地識別需保護之個別資產與執行特定安全過程的責任，並加以文件化？	◎	◎				
2.5 是否依據員工之職務，訂定員工資安作業程序、權責規範或授權層級並予以文件化？（含經管使用設備及作業須知）	◎	◎				
2.6 是否訂定各項資訊處理設施之用途及使用授權，及安全之作業程序？	◎	◎				
2.7 是否識別並定期審查組織對資訊保護之機密性或保密協議之要求？	◎	◎				
2.8 是否訂定當發生資安事故時，如何及時與主管機關聯繫並通報之適當程序或規定？	◎	◎				
2.9 是否與各特殊利益團體、專家安全論壇及專業協會維持適當聯繫？	◎	◎				
2.10 是否定期或於資安作業環境發生重大變更時，召開管理審查會議，獨立審查組織之資訊安全管理之作法與其實作（如各項資安的控制目標、控制措施、政策、過程及程序）？	◎	◎				
2.11 因營運需要開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘雇人員及一般民眾）使用之資訊，是否執行風險評鑑與實作安全控制措施？是否於契約或規定中包含雙方權利、義務、資料保護、資訊保密、服務標的水準、智慧財產權、事故發生處理與違約處理等條款？	◎	◎				
2.12 是否對不開放外部團體存取的資訊進行必要的控制措施？	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
2.13 因營運需要開放給外部團體存取之資訊，是否定期審查其存取權限？	◎	◎				
2.14 組織因營運需要，開放給外部團體（含其他機關、往來業者、維護廠商、委外承包商、聘雇人員及一般民眾等）使用之資訊，於開放使用之前，是否明確說明所有之安全要求？	◎	◎				
2.15 委外契約中有關安全需求內容，是否包含法律要求（如個人資料保護法）、雙方有關人員權責、安全控管措施、作業程序、事故通報程序、服務水準、對委外廠商稽核權等資安責任與事宜，並得依實際需要適時修改安全控管措施及作業程序等？	◎	◎	◎			
3.資產管理						
3.1 是否明確識別所有資產，並製作與維持所有重要資產的清冊？	◎	◎				
3.2 是否有明確分辨重要資產之定義，並再依據該定義作資產盤點，建立與維護重要資產清冊？	◎	◎				
3.3 是否定期審查資產清冊，確保資產處於適切狀態？	◎	◎				
3.4 是否識別所有資訊資產之擁有者，並指派其依適切控制措施維護資訊資產之責任？	◎	◎				
3.5 是否識別及實作所有與資訊處理設施相關（含電子郵件、網路使用及行動設備等）之使用規則，並加以文件化？	◎	◎				
3.6 是否依據資訊對組織的價值、法律要求、敏感性及重要性加以分類？	◎	◎				
3.7 是否依據組織的分類法，訂定適當之資訊標示與處理程序？	◎	◎	◎			
3.8 是否對機密性資訊、敏感性之手稿資訊、影印公文之廢紙及已過保存期限之公文，於棄置前予以銷毀？	◎	◎	◎			
4.人力資源安全						
4.1 是否依照資安政策，訂定正式文件，規範所有員工、承包商或第三方使用者之安全角色與責任？	◎	◎	◎			
4.2 是否明確定義所有聘雇者、承包商及第三方使用者背景查證檢核之限制與程序，確保符合隱私權、個人資料保護及/或聘雇勞工保護相關法令之要求？	◎	◎				
4.3 被賦予機敏資訊存取權的所有員工、承包商及第三方使用者，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	◎	◎				
4.4 管理階層是否有要求員工、承包商及第三方使用者，依照組織已訂定的政策與程序執行安全事宜？	◎	◎				
4.5 是否對所有員工、承包者及第三方使用者工作職務有	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
關之安全程序及資訊處理設施，提供正確使用之認知、教育與訓練？						
4.6 是否訂定員工違反組織資安政策與程序之懲處規定？	◎	◎				
4.7 在與員工、承包商或第三方使用者所訂之契約內，是否規定在聘雇終止後與職務有關之責任仍然為有效的？	◎	◎				
4.8 所有員工、承包商及第三方使用者離職或聘雇終止時，是否依規定繳回其任職期間保管之資訊資產？（包含所有的軟體、公司文件、設備、行動裝置、信用卡、存取卡、軟體、手冊及儲存於電子媒體的資訊等所有其他組織資產）	◎	◎				
4.9 所有員工、承包商及第三方使用者之聘雇、契約或協議終止或因變更而調整時，是否迅速移除其對資訊及資訊處理設施之存取權限？	◎	◎				
5.實體及環境安全						
5.1 是否適當使用安全邊界（如圍牆、入口閘門或人員駐守的接待櫃檯等屏障),保護含有資訊與資訊處理設施的區域？	◎	◎				
5.2 組織管理之資訊處理設施（如通訊服務設施),在實體上是否與第三方管理（如客戶代管設備）之資訊處理設施有區隔？	◎	◎				
5.3 具有關鍵或敏感的資訊處理設施之安全區域，是否對授權進出人員作必要之限制及監督其活動？	◎	◎				
5.4 是否定期審查並更新其安全區域進出權限，並於必要時廢止？	◎	◎				
5.5 是否實施必要之辦公處所保護措施？	◎	◎	◎			
5.6 是否檢查及評估重要資通訊設備設置地點與鄰近場所之任何安全威脅，如火災、灰塵、水災、震動、化學效應、電力供應、電磁幅射、民間暴動及其他天然或人為災害等可能對設備之危害？	◎	◎				
5.7 是否設計並實施適當的控制措施，以保護敏感資訊處理設施之地點及內部人員通訊錄？	◎	◎				
5.8 是否嚴禁在電腦機房內使用未經核准之電器或其他物品？	◎	◎				
5.9 備援設備及備份媒體存放位置，是否與主要場地保持安全距離？	◎	◎				
5.10 安全區域是否與易燃物或危險物料保持安全距離，且無儲存大量的物資？	◎	◎				
5.11 是否設計並實施適當之控制措施，監督安全區域內之工作，並確保其須知原則？	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
5.12 是否訂定未經授權前，禁止拍照、錄影、錄音和以其他記錄性設備記錄之規定，如以行動裝置照相？	◎	◎				
5.13 是否對無人使用之安全區域上鎖並定期檢查？	◎	◎				
5.14 是否對收發、裝卸區及其他未經授權人員可進入之作業場所，有適當之進出控制措施，並應與資訊處理設施隔離，以避免未經授權的存取？	◎	◎				
5.15 是否明確訂定資通訊設備之控制措施（包括場外使用之設備，及財產之攜出），以降低資料未經授權存取、遺失及損壞之風險？	◎	◎				
5.16 是否特別保護並評估處理敏感資料的資通訊設備或資訊處理設施之有效性？	◎	◎				
5.17 是否採取適當控制措施，降低潛在實體威脅，如竊盜、火災、爆裂物、煙害、水災、水源停止供應、閃電、溫度、濕度、灰塵、振動、化學效應、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等？	◎	◎				
5.18 是否落實電腦作業區（含機房）禁止抽煙及飲食之規定？	◎	◎				
5.19 是否具備環境監控機制，掌握資通訊設備及資訊處理設施之溫度及溼度狀況？	◎	◎				
5.20 是否對支援性公共設施，如電源供應、水源供應、通風及空調，設計適當之保護措施，並施行之，以確保資通訊設備及資訊處理設施不受公共設施失效所導致之中斷？	◎	◎				
5.21 是否定期檢查並測試備援電源，確保其能在斷電期間正常運作？	◎	◎				
5.22 是否對電信機線設備（telecommunications lines）、網路佈纜（network cabling）及電源纜線設計適當之安全保護措施，並施行之？	◎	◎				
5.23 是否將通信纜線（communications cables）及電源纜線接地並隔離，以防止互相干擾？	◎	◎				
5.24 是否定期且正確的維護保養各項電信機線設備，確保其可用性及完整性？	◎	◎				
5.25 是否依據供應商建議的間隔與保養手冊，定期檢查並維護各項電信機線設備？	◎	◎				
5.26 是否由授權之維護人員執行各項電信機線設備之維護與修理？	◎	◎				
5.27 是否妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄？	◎	◎				
5.28 是否對送場外維修設備內儲存的資訊訂有安全保護措施？	◎	◎				

電信事業資通安全管理內部稽核表							
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
5.29 是否對攜出場所外之設備和媒體，訂有安全保護措施？	◎	◎	◎			
5.30 是否對行動裝置（設備）訂有嚴謹保護措施（如使用授權管理、設通行碼、檔案加密、專人看管）？	◎	◎	◎			
5.31 是否於汰除設備前將機密性、敏感性資料及有版權的軟體予以移除或實施安全覆寫？	◎	◎	◎			
5.32 含有敏感性資訊之設備於汰除後，是否根據風險評鑑決定銷毀其實體？	◎	◎	◎			
5.33 資訊資產如須攜出場外使用，是否經事前授權，並於攜出場外與歸還時，均進行安全查核及記錄？	◎	◎	◎			
6.通訊及作業管理						
6.1 資訊處理設施與資通訊設備之各項相關作業程序及活動，是否文件化並適當維護？如電腦開機與關機程序、備份、設備維護、資訊的處理與處置、異常情況之處理、緊急聯絡資訊、重新啟動及復原程序、稽核存底與日誌資訊之維護、電腦機房與郵件處理管理、生命財產安全（safey）等。	◎	◎				
6.2 資訊處理設施與資通訊設備之變更，是否有正式核准之程序，並向相關人員通報變更細節？	◎	◎				
6.3 資訊處理設施與資通訊設備之變更，是否詳實記錄，並重新進行風險評鑑？	◎	◎				
6.4 資訊處理設施與資通訊設備之變更，是否備有退回（fallback）程序，包括不成功的變更、意外事故的中止及復原之程序與責任？	◎	◎				
6.5 對安全要求較高的業務，是否區隔其職務與責任領域，以授與執行業務所需之最小權限為原則？	◎	◎				
6.6 業務資訊資產之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作，是否盡可能授權不同人員執行？	◎	◎				
6.7 設施、系統、軟體之開發、測試及運作，是否有分隔處理？	◎	◎				
6.8 是否對運作測試系統使用不同的使用者設定檔（profile），且功能選單需顯示適切的識別訊息，以降低錯誤風險？	◎	◎				
6.9 是否與第三方服務交付廠商簽訂適當之資訊安全協定，並納入契約條款，包含安全控制措施、服務定義及交付等級，並賦予相關安全管理責任？	◎	◎				
6.10 是否規劃必要轉換（資訊、資訊處理設施及其他任何需要移動者）之安全控制措施，並確保轉換期間安全的維	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
護？						
6.11 是否定期對第三方提供之服務、報告及紀錄等，進行適當之監視與審查，並定期稽核？	◎	◎	◎			
6.12 是否於第三方提供之服務有任何異動時，重新進行風險評鑑？	◎	◎	◎			
6.13 是否於設置資訊處理設施及資通訊設備前，進行容量規劃及預留安全容量，並於正式運作後，持續監控其容量狀態？	◎	◎				
6.14 是否建立新資訊系統、系統升級或安裝新版本之驗收準則，並在新資訊系統、系統升級及新版本正式驗收後，才移轉上線？	◎	◎				
6.15 是否全面使用防毒軟體，並即時更新病毒掃描引擎及病毒碼？	◎	◎				
6.16 是否定期對電腦系統及資料儲存媒體掃描惡意程式病毒及後門程式？	◎	◎				
6.17 是否頒訂正式政策，禁止使用未經授權的軟體？	◎	◎				
6.18 是否定期審查支援重要營運程序之系統軟體與資料？若出現任何未經核准的檔案或授權的修補程式時，是否進行正式調查。	◎	◎				
6.19 是否訂定使用電子郵件附件及下載之檔案前，檢查有無惡意程式軟體（含病毒、木馬或後門等程式）之程序？	◎	◎				
6.20 是否定義處理電腦病毒、木馬等惡意程式之管理程序與責任,並訓練員工如何通報惡意程式攻擊,及復原程序？	◎	◎				
6.21 是否準備遭惡意程式攻擊後復原之營運持續計畫，並包括所有必要之資料與軟體備份及復原準備工作？	◎	◎				
6.22 是否定期備份處理重要資訊及軟體，並定義備份資訊之必要等級？	◎	◎				
6.23 是否定期回復測試重要資訊及軟體，並將回復程序文件化，確保備份複本之可用性及有效性？	◎	◎				
6.24 重要及機敏資訊之備份程度及頻率是否反映組織的營運要求？	◎	◎				
6.25 是否將備份資訊儲存於足以避免主要場地發生災難時遭波及之遠端地點？	◎	◎				
6.26 是否給予備份資訊適切等級之實體與環境保護，並與主要場域使用一致之標準？	◎	◎				
6.27 是否將主要場域採用之控制措施延伸至備份作業場域？	◎	◎				
6.28 是否定期檢查及測試復原程序，確保有效性，且能夠在復原程序分配之時間內完成復原運作？	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
6.29 是否訂定網路及網路遠端設備之使用權責及程序？	◎	◎				
6.30 是否使用網路安全防禦設備，並適當的隔離外部網際網路與組織內部網路？	◎	◎				
6.31 組織建立之網路控制措施，是否能反映資訊之機密性、完整性與可用性要求？	◎	◎				
6.32 是否對於機敏性資訊之傳輸過程採取資訊加密等保護措施？	◎	◎				
6.33 是否訂定確保網路服務連線品質及可用性保護措施？	◎	◎				
6.34 是否定期檢討網路安全控制措施之執行？	◎	◎				
6.35 是否定期檢測網路運作環境之安全漏洞？	◎	◎				
6.36 是否使用適當之網路安全解決方案？如防火牆、入侵偵測系統？防火牆存取政策（security policy）設定是否適當？	◎	◎				
6.37 是否建立各種可攜式媒體之操作管理程序，防止文件、電腦媒體（如磁帶、磁碟）、輸入或輸出資料及系統文件，遭受未經授權的揭露、修改、移除及破壞？	◎	◎	◎			
6.38 是否以正式程序安全地汰除含有敏感性資訊之電腦媒體，如資料須經安全清除後，方可由組織內其他應用系統使用，或以焚化、絞碎等方式銷毀？	◎	◎	◎			
6.39 具機密性或敏感性資訊之媒體是否有安全之保存和報廢程序？	◎	◎	◎			
6.40 是否有安全處理程序及分級標示，以儲存或處理具機密性、敏感性之資訊？	◎	◎				
6.41 是否建立資訊的處理及儲存程序，以避免未經授權的揭露或誤用？	◎	◎				
6.42 對應用程式、程序、資料結構及授權過程等說明之系統文件，是否有適當的存取保護措施？	◎	◎				
6.43 是否對所有形式之資訊交換，訂定適當交換政策、程序及控制措施？	◎	◎				
6.44 是否對高度機敏性資訊在傳輸或儲存中使用加密技術？	◎	◎				
6.45 是否訂定組織與任何外部團體間交換資訊與軟體之協議？	◎	◎	◎			
6.46 運送重要電腦資訊、媒體（含報表），是否有安全保護措施及完整監控記錄（含收送人、時間及內容）？	◎	◎	◎			
6.47 是否訂定適當控制措施，以保護組織在實體邊界外傳送含有資訊之媒體時，不受未經授權的存取、誤用或毀損？	◎	◎	◎			

電信事業資通安全管理內部稽核表							
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
6.48 是否對採行電子交換之資訊視資安等級，運用識別碼與通行碼管制、電子資訊加密或電子簽章認證等保護措施，確保資訊的機密性、完整性、可用性及符合其他法律要求？	◎	◎				
6.49 是否對涉及敏感性資訊及機密文件之營運資訊系統提供適當之存取控制與保護？	◎	◎				
6.50 是否實施適當控制措施，保護在公眾網路上傳輸且涉及電子商務之資訊，使其不受詐欺行為、契約爭議及未經授權之揭露與修改？	◎	◎	◎			
6.51 是否對線上交易服務訂定適當控制措施，防止下列事項：(1) 不完整傳輸、(2) 誤選路徑、(3) 未經授權之訊息修改、揭露及 (4) 未經授權的訊息複製或重送 (replay) 等發生？	◎	◎	◎			
6.52 是否對開放供公眾取得之資訊訂定保護措施，以確保資訊完整性，防止未經授權之修改？	◎	◎				
6.53 是否依據法律要求，如個人資料保護法，實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故？	◎	◎	◎			
6.54 是否採用適切的存錄與監控設備，記錄資通訊相關活動？	◎	◎				
6.55 是否建立適當之控制措施，監控資訊處理設施之使用，及定期審查？	◎	◎				
6.56 是否對各項作業日誌 (log) 有適當的保護措施，不受竄改與未經授權之存取，並針對留存之通信資訊設定適當之留存期限 (如會計、帳務、客訴的處理、防止濫用及執法機關的要求)？	◎	◎				
6.57 是否定期稽查各項作業日誌？	◎	◎				
6.58 是否適當規劃存錄設施與作業日誌資訊之儲存媒體容量，避免無法記錄事故或覆蓋以往所記錄事故？	◎	◎				
6.59 作業日誌中是否留有管理者與操作者所涉及活動之詳細過程，並定期予以審查？	◎	◎	◎			
6.60 是否存錄使用者或系統程式通報之資訊處理或通信系統問題，並迅速處理及通報？	◎	◎				
6.61 是否根據議定之鐘訊來源校正所有系統鐘訊之時間，以確保時間紀錄正確？	◎	◎				
7.存取控制						
7.1 是否根據營運與安全要求，建立、文件化及審查資訊存取控制政策？	◎	◎				
7.2 是否在存取政策文件中明確陳述每個使用者或使用群組之資訊存取控制規則與權限？	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
7.3 資訊存取控制政策是否符合相關法律、法規命令及契約規定，如電信法、個人資料保護法等？	◎	◎				
7.4 是否對所有資訊系統與服務之核准和撤銷存取，訂定適當之使用者註冊與註銷程序？	◎	◎	◎			
7.5 是否於使用者變更角色、調職或離職後，立即移除或封鎖其存取權限？	◎	◎	◎			
7.6 是否維持所有使用者註冊服務、系統或資訊等之正式紀錄？	◎	◎	◎			
7.7 基於系統管理或特殊作業需要，需設定特殊權限時(如系統管理、高階管理者)，是否透過正式授權過程，控制特殊權限之配置？	◎	◎				
7.8 是否維護所有配置特殊權限之授權過程和紀錄，並於完成授權過程後才授予特殊權限？	◎	◎				
7.9 是否在提供使用者通行碼前，先進行身份鑑別程序？	◎	◎				
7.10 是否以安全之程序轉交預設之通行碼給使用者，且在使用者取得通行碼，並確認無誤後，回應系統管理者？	◎	◎				
7.11 是否於安裝軟體完畢後立即更新廠商預設之通行碼？	◎	◎				
7.12 是否要求使用者於聘雇任期與條件中，對個人通行碼簽署保密聲明？	◎	◎				
7.13 是否強制要求使用者，初次登入電腦系統後，必須立即更改預設通行碼，或於一定期限未登入後，使預設通行碼失效，必須重新申請建立？	◎	◎				
7.14 是否規定通行碼不得以無保護之型式儲存於電腦系統中？	◎	◎				
7.15 是否定期檢查所有使用者之存取權限,(建議每六個月一次、特權者每三個月一次)以及於有任何變更((如升職、降職、調職或聘雇終止等))後，亦審查其存取權限？	◎	◎				
7.16 是否規定通行碼長度須超過 6 個字元（建議以 9 個字元以上）？	◎	◎				
7.17 是否規定通行碼需以大小寫字母、特殊符號及數字組成？	◎	◎				
7.18 是否訂有通行碼輸入錯誤僅允許三次以內之限制？	◎	◎				
7.19 是否定期、依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼？	◎	◎				
7.20 是否規定不得在任何自動登入過程中內含通行碼，如儲存在巨集或功能鍵中？	◎	◎				
7.21 是否規定避免使用與個人有關資訊(如生日、身分證	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
統一編號、單位簡稱、電話號碼等）當做通行碼？						
7.22 是否避免保留通行碼的紀錄（如紙張、軟體檔案或手持裝置），除非其能被安全地存放，且該存放方式經過核准？	◎	◎				
7.23 應用系統是否具有於作業結束後或在一定未操作期間後，即自動登出之保護機制？	◎	◎				
7.24 是否避免將輸入之通行碼以明文方式顯示在螢幕上？	◎	◎				
7.25 是否對無人看管之資訊設施訂有適當保護措施？	◎	◎				
7.26 是否訂有桌面淨空及螢幕淨空政策？	◎	◎	◎			
7.27 是否於不使用主機、伺服器、個人電腦、終端機等電腦設備或人員離座時，即刻以保護措施，如關機、登出、設定螢幕保護密碼或其他控制措施保護電腦設備？	◎	◎	◎			
7.28 是否於下班後將經辦之機密性及敏感性資訊妥為收存？	◎	◎	◎			
7.29 是否訂定適當之控制措施，防止未經授權使用影印機和其他複製設備（如掃瞄器、數位相機）？	◎	◎	◎			
7.30 是否立即從印表機上取走敏感性或機密性資訊文件？	◎	◎	◎			
7.31 網路使用者（含外單位人員）是否取得正式之存取授權？	◎	◎				
7.32 是否於登入作業完成後，顯示前一次登入日期與時間，或提供登入失敗之詳細資訊？	◎	◎				
7.33 是否限制登入失敗次數於超過上限時，需強制延遲一段時間或重新取得授權後才允許再登入？	◎	◎				
7.34 是否訂定網路服務存取安全政策，確保使用者係經特定授權允許存取網路與網路服務？	◎	◎				
7.35 是否對外部連線使用者進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答（challenge/response）協定等安全技術？	◎	◎				
7.36 是否採用自動設備識別方法，鑑別存取敏感或機密資訊之設備，方允許其存取行為？	◎	◎				
7.37 是否對遠端使用者的存取控制訂有適當的鑑別機制？	◎	◎				
7.38 是否對需採用遠端診斷作業方式，訂有診斷埠之存取作業規範(如用金鑰管理及人員身份查驗或稽核等機制)?	◎	◎				
7.39 是否對無線網路之存取及應用訂有嚴謹之鑑別、加密方式及頻率選擇等控制措施？	◎	◎				
7.40 是否依據網路服務需要，區隔出獨立邏輯網域（如組	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
織內部網路或外部網路)，且每個網域皆有定義的安全邊界，及通訊閘道管制過濾網域間資料之存取（如網路防火牆）？						
7.41 是否對電子郵件、單雙向檔案傳輸、互動式存取或應用系統之存取期間作必要之限制？	◎	◎				
7.42 是否實施網路之路由控制，以確保電腦連線及資訊流不會破壞營運應用系統之存取控制政策？	◎	◎				
7.43 是否避免登入程序之系統輔助訊息提供未經授權使用者任何不必要之協助？	◎	◎				
7.44 是否依據系統機敏度，限制登入失敗次數之上限，並於登入失敗後立即中斷連線？	◎	◎				
7.45 是否對於異常登入之程序留有紀錄及定期檢視？	◎	◎				
7.46 是否對系統登入或存取重要資訊時之連線過程提供加密之程序與措施？	◎	◎				
7.47 是否對使用者採用具有唯一性之識別帳號（如使用者ID）？	◎	◎				
7.48 是否對重要系統使用者採用適切之身分鑑別技術，如一次性密碼、智慧卡、符記或生物特徵？	◎	◎				
7.49 是否以保護的形式儲存和傳送通行碼，並告知申請者？通行碼檔案是否和應用系統資料分開存放？	◎	◎				
7.50 是否對使用系統公用程式進行授權管制（如最低實務需求的授權）及身分鑑別程序？是否於需要職務區隔時，有管制措施不讓具備系統應用程式存取權限的使用者，取得系統公用程式之權限？	◎	◎				
7.51 是否設定網路會談結束或超過定義的無動作期限後，即中斷連線或關閉設備？	◎	◎				
7.52 是否對風險高之應用系統限制其連線時間，如限制在正常辦公時間內？	◎	◎				
7.53 是否訂定使用者及支援人員存取應用系統權限之管制措施？	◎	◎				
7.54 是否採用專屬（隔離）電腦作業環境處理機密及敏感性資訊？	◎	◎	◎			
7.55 是否訂定行動運算及通信設備之管理政策(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)？	◎	◎	◎			
7.56 遠距工作是否得到管理階層授權（如活動政策、計畫及流程等）和施予必要之保護措施？	◎	◎				
7.57 是否於遠距工作活動結束後，撤銷相關授權與存取權限及歸還管制設備？	◎	◎				
8.資訊系統獲取、開發及維護						

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
8.1 是否在規劃應用系統需求時將安全需求納入分析及規格文件中？	◎	◎	◎			
8.2 是否檢查輸入資料，並確認其正確性及適切性？	◎	◎				
8.3 是否對輸入錯誤設計及實作回應程序？	◎	◎				
8.4 是否對應用程式內部處理加入確認查核（validation check），偵測可能經由處理錯誤或故意行為之任何資訊毀損，並提供適當程式從失效中復原，確保資料之正確處理？	◎	◎				
8.5 是否使用密碼技術，鑑別與保護應用系統訊息之完整性？	◎	◎				
8.6 是否對輸出資訊具合理性查核及一致性控制計數（reconciliation control count），確保所有資料都已合理處理？	◎	◎				
8.7 是否設計與實作輸出確認測試與回應之程序？	◎	◎				
8.8 是否設計並實作資料輸出確認過程之活動日誌，並定義所有涉及資料輸出過程人員之責任？	◎	◎				
8.9 是否基於風險評鑑結果，識別所需的保護等級，設計所需加解密演算法之型式、強度及品質？	◎	◎				
8.10 是否基於風險評鑑結果，管理密碼金鑰，並發展適當之控制措施？	◎	◎				
8.11 是否於作業系統升級前，考量營運要求及該版本之安全性？	◎	◎				
8.12 是否由管理階層授權處理作業系統軟體更新之人員？	◎	◎				
8.13 是否限定由訓練合格之管理人員執行應用程式可執行碼更新作業？	◎	◎				
8.14 是否使用組態控制系統，以保持對所有已實作的軟體與系統文件之版本進行控制，且維護所有變更紀錄？	◎	◎				
8.15 是否避免以真實資訊進行系統開發與測試作業？如採用真實資訊進行測試，是否採取適當措施，避免程序或程式錯誤，導致不可預期之洩漏？	◎	◎				
8.16 是否對存取程式原始碼（program source code）訂有適當之控制措施，並留存稽核日誌？	◎	◎				
8.17 是否建立變更應用系統之管制程序？	◎	◎				
8.18 是否於應用系統變更後，立即更新系統文件？	◎	◎				
8.19 是否於作業系統變更後，對應用系統作技術性審查？	◎	◎				
8.20 是否於作業系統變更後，主動公告異動範圍、時間及可能的影響？	◎	◎				
8.21 是否於作業系統變更後，檢查其相關控管措施與程序	◎	◎				

電信事業資通安全管理內部稽核表							
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
仍然有效？						
8.22 是否對套裝軟體之變更僅限於必要之範圍，並嚴格管制所有變更項目？	◎	◎	◎			
8.23 是否檢查組織內可能之隱匿通道（covert channel），以降低資訊洩漏的風險？	◎	◎				
8.24 是否於委外開發之系統上線前，偵測有無惡意程式存在？	◎	◎				
8.25 是否於委外開發合約中，規範著作權之歸屬？	◎	◎				
8.26 是否於訂約時，簽訂安全履行條款與相關罰則？	◎	◎				
8.27 是否及時取得使用中電信系統之技術脆弱性資訊，並定期執行各項系統漏洞修補程式？	◎	◎				
8.28 是否於系統修補前，先作系統影響評估與測試，再採取必要措施？	◎	◎				
9.資訊安全事故管理						
9.1 是否建立資安事故或事件（含安全漏洞、系統弱點、病毒、非法入侵及系統異常）之正式通報應變程序？	◎	◎	◎			
9.2 是否建立資安事故回應小組單一聯繫窗口，授權在處理事故時採取立即之決定，並與外部團體（如執法機關、政府緊急應變中心、客戶、商業夥伴）建立聯繫管道？	◎	◎	◎			
9.3 是否留有資安事故處理過程之完整記錄，如有必要，應直接發送電子郵件及/或於網站首頁及時通知相關用戶？	◎	◎	◎			
9.4 是否建立資安事故通報之聯絡點，並確保全組織都知悉該聯絡點，以利隨時聯繫，且能夠有充分與及時的回應？	◎	◎	◎			
9.5 是否使機關員工及外部使用者知悉資安事故通報及處理程序，並要求依規定辦理？	◎	◎	◎			
9.6 是否要求資訊系統與服務的所有員工、承包商及第三方使用者，注意並通報任何觀察到或可疑的系統或服務之安全弱點？	◎	◎	◎			
9.7 是否依不同型式之資安事故，建立資安事故管理責任及應變程序？	◎	◎	◎			
9.8 是否建立資安事件或事故等事後管理會議，以協助單位能從資安事件或事故中學習到經驗？	◎	◎	◎			
9.9 是否擬定營運中斷後之各項風險處理優先順序或處理準則（含處理順序說明、最低營運水準定義）？	◎	◎	◎			
9.10 是否建立資安事故管理機制，如記錄事故型式、處理方法、處理成本及矯正預防措施？	◎	◎	◎			
9.11 是否已建立及使用各項指標，以協助偵測並預防資安事故？	◎	◎	◎			

電信事業資通安全管理內部稽核表							
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
9.12 是否在管理審查過程中將已發生之資安事故納入考量？	◎	◎	◎			
9.13 是否有適當保護措施保護資安事故中相關證據資料，以符合證據能力之要求，作為問題分析及法律必要依據？	◎	◎				
10.營運持續管理						
10.1 是否發展與實作營運持續計畫，以因應組織營運持續所需的資訊安全要求？	◎	◎				
10.2 是否對所有營運過程可能造成營運中斷之機率及衝擊進行風險評鑑？	◎	◎				
10.3 是否識別營運持續過程中關鍵資通訊設備及資訊處理設施？	◎	◎				
10.4 是否以人員安全為優先考量，並保護資通訊設備和組織財產，發展與實作營運持續計畫？	◎	◎				
10.5 是否訂定營運持續計畫（含啟動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來單位之應變規劃及合約適當性等）？	◎	◎				
10.6 是否維持營運持續計畫之單一架構，以確保所有計畫有一致性，持續一致地因應資訊安全要求，並識別測試與維護的優先順序？	◎	◎				
10.7 是否配合業務、組織及人員之變更而更新營運持續計畫（含緊急應變處理程序）？	◎	◎				
10.8 是否定期完整測試、演練並更新維護營運持續計畫？	◎	◎				
11.遵循性						
11.1 是否確保所有通訊系統與組織均不違反任何法律、法規命令、行政規則、契約義務及相關安全要求？	◎	◎				
11.2 軟體取得（含自行開發、委外開發、購置或租用）等可能涉及智慧財產權規定，是否符合法律、法規命令及契約的要求？	◎	◎				
11.3 是否公布智慧財產權遵循政策、定義軟體與資訊產品的合法使用、並告知違反政策者將遭懲處？	◎	◎				
11.4 是否維護使用版權、原版碟片、手冊等所有權之證明和證據，並定期檢核只安裝經授權之軟體與有使用版權之產品？	◎	◎				
11.5 是否依安全等級加以保護及儲存組織重要紀錄（如資料庫紀錄、系統日誌、操作日誌、稽核日誌)，如檔案加密或數位簽章？	◎	◎				
11.6 是否於稽核後產出稽核報告，並追踪改善情形（包括稽核發現之摘要、稽核區域、缺失說明及改進建議等）？	◎	◎				

電信事業資通安全管理內部稽核表						
檢查項目	資通安全等級			檢查結果		
	A	B	C	符合	不符合	不適用
11.7 是否對組織涉及個人隱私及個人資料保護之經管或處理資訊，有適當之保護機制？	◎	◎				
11.8 是否符合法律、法規及適用的契約條文發展和實作資料保護與隱私政策？	◎	◎				
11.9 是否依據個人資料保護法擬定適當資安維護措施？	◎	◎				
11.10 是否有監視設備或其他可偵測未經授權使用之設備，以防止資訊設施被不當使用？	◎	◎				
11.11 是否由管理人員定期審查其責任範圍內之資訊處理設施與其資安政策、標準及符合其他相關資安要求？	◎	◎				
11.12 是否確保相關人員能正確執行組織訂定之資安程序？	◎	◎				
11.13 是否定期進行資訊系統之資安技術符合性檢查(如滲透測試或系統弱點檢測）？	◎	◎				
11.14 技術遵循性之查核人員是否經過訓練，並作事前工作分配？	◎	◎				
11.15 是否由合格資安技術單位執行技術遵循性檢查？	◎	◎				
11.16 是否監控技術遵循性查核時之存取行為,並適當保存紀錄？	◎	◎				
11.17 是否將技術遵循性查核結果文件化？	◎	◎				
11.18 是否訂定資安內部稽核計畫（含稽核目標、範圍、時間、程序、人員）？	◎	◎				
11.19 是否定期辦理資安內部稽核？	◎	◎				
11.20 內部稽核範圍是否包含資通系統、供應商、資產負責人、使用者和管理階層？	◎	◎				
11.21 是否有保護資訊系統稽核工具之存取，以防止可能誤用或破解之措施？	◎	◎				
合計	265	265	51			

附件六 ISO/IEC 27011 增項稽核表

公司名稱			
資通安全等級	□A		
單位主管		稽核日期：	
稽核人員		稽核日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		

電信事業 ISO/IEC 27011 增項稽核表			
檢查項目	檢查結果		
	符合	不符合	不適用
1.資訊安全之組織			
1.1 電信事業對保密協議之內容，是否包含：對於通訊之有無、對象、日期時間及內容等，且定期審視該協議內容以確保不得有不當揭露之情事發生？			
1.2 組織是否訂定司法、檢調或研究機關（構）請求提供資訊時之控管程序，確認此申請係符合法規命令之合法程序？			
1.3 是否於提供用戶服務前訂定清楚之協議內容，要求用戶不得毀損電信設施或減低該設施之通訊服務能力？			
1.4 是否於提供第三方服務廠商存取權限前訂定清楚之協議內容，包含提供服務所需之相關安全政策與應注意事項？			
2.資產管理			
2.1 是否明確定義組織的電信設備，與其他組織相連結或相關之部份的管理責任，並加以文件化？			
2.2 電信事業是否對通訊之有無、對象、日期、時間及內容等，加以標示，並確保資訊存取之可歸責性？			
3.人力資源安全			
3.1 是否詳細檢查員工、承包商及第三方使用者職務上被授權能夠存取之必要服務：如：客戶個人資料或客戶通話內容等，並納入相關安全責任之中？			
3.2 是否對人員進用考量相關電信證照或具備適當的電信知識和技能？			
3.3 是否對所有聘雇之應徵者、承包商及第三方使用者之進用或委派，作適當之背景查驗工作，例如：工作職務涉及客戶個人資料或是通訊內容之存取者？			
3.4 是否於聘請第三方機構前，明確定義和溝通其安全角色和職責？			

電信事業 ISO/IEC 27011 增項稽核表			
檢查項目	檢查結果		
	符合	不符合	不適用
3.5 是否對委外承包商或第三方使用者，在合約中加入安全角色與職責的要求？			
3.6 是否要求組織內任何人於從事電信服務時，應保護職務上所知悉之營業秘密？（包含離職或退休後亦然）			
3.7 組織是否依據相關法律或法規命令，訂定服務或離退職員工，對於電信之有無及其內容，應嚴守秘密之責任規範？			
4.實體及環境安全			
4.1 權責人員是否可於電信營運中心之實體安全邊界發生異常狀況時立即處理？			
4.2 通訊系統之機房控制中心與操作室是否有適當強度之門禁管制措施（strong entry controls）？			
4.3 通信中心是否設置於適當地點（如避免易遭水災、風災、地震影響，或臨近強烈電磁及儲存危險物之場所），若不滿足此要求是否有因應措施？			
4.4 通信中心是否裝設自動消防系統？			
4.5 通信中心是否為抗震建物？樓層地板是否有足夠之承載能力？			
4.6 通信中心是否依據消防法規，使用防火材料，或使用消防設備，並經主管機關或專業技師查驗合格？			
4.7 電信設備機房是否於具備防範風災、水災、地震及火災之能力之適當地點設置，並配備適當之偵測、監視及門禁管制設備，防止未經授權之入侵？			
4.8 無人看管之隔離操作區，如無人機房，是否具備以下安全措施：（1）設備失效、電力失效之遠端偵測及消防警報，（2）適當之實體安全維護設施，防止未經授權之入侵等？			
4.9 是否將不同用戶之委託代管設備加以隔離，並配置適當保護措施，以避免未經授權之存取？			
4.10 電信網路設備集中設置區(如資訊、網管、傳輸交換電信機房)是否有不斷電系統及符合 SLA（服務層級協議）與 DRP（災害應變計畫）要求之備援電力保護？			
4.11 通訊系統放置於其他組織處之設備是否有足夠安全防護，且有定義清楚的邊界與介面，可以輕易加以隔離？			
4.12 放置於使用者端設備是否具備遠端監控功能？			
4.13 是否持續監控與其它電信事業之互連狀態，並有適當之控制措施，檢查與其它電信事業互連是否正常？發生問題時，是否有方法可以矯正？			
4.14 與其它電信事業之互連是否已妥善定義邊界與介面？是否已定義當用戶發生斷線時，如何處理之協議或合約？			
5.通訊及作業管理			

電信事業 ISO/IEC 27011 增項稽核表			
檢查項目	檢查結果		
	符合	不符合	不適用
5.1 通訊系統操作程序是否包含事故、緊急或危機處理程序？			
5.2 是否建立資通訊處理設施變更之管理程序？管理程序之紀錄是否包括設施之安裝、更改位置及移除？			
5.3 是否將系統開發、測試及正式運作區隔在不同的作業環境處理？若無法區隔是否有採取適當的管控措施?			
5.4 是否避免以敏感性資訊進行系統開發與測試？如採用敏感資訊進行測試，是否採取適當措施，避免程序或程式錯誤，導致不可預期之洩漏？			
5.5 是否對安裝行動碼（mobile code）作必要之授權處理或限制使用？是否評估內嵌行動碼之中介軟體（middleware）之限制使用？			
5.6 是否訂定網路服務供應商及客戶之服務協議，內容包含使用範圍、相關權責及程序？			
5.7 是否對不同營業項目提供客戶適當之安全水準，且於服務協議中描述提供之安全功能、服務水準及管理需求等？			
5.8 是否訂定相關政策，建置適切控制措施，防範垃圾郵件？			
5.9 是否訂定相關政策，建置適切控制措施防範，阻斷服務（DoS）或分散式阻斷服務（DDoS）攻擊？			
5.10 是否具備經由 IP 位置、通訊埠與通訊協定等個別過濾通訊或限制通訊頻寬之機制，適當的保護關鍵網路設施，如伺服器、路由器等？			
5.11 電信第三層（layer 3）網路設備是否具備防範偽造來源地址（IP spoofing）之能力？			
5.12 是否運用嚴格之密碼控制措施及/或高強度鑑別（strong authentication）功能，防範來源造假（source impersonation）？			
5.13 是否事先經由定期收集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊，並彙集關鍵知識？			
5.14 資通訊設備是否具備偵測網路壅塞及避免網路壅塞時通訊過度集中之機制？			
5.15 是否訂定作業程序，預先收集可能造成網路壅塞或是預期事件之資訊？			
5.16 是否採用分散式架構或機制，建置輔助設備及適當之組態，提升網路峰值處理能力，防範潛在網路崩潰或是災難之發生？			
5.17 是否能鑑別及給予必要的通訊優先權，協助災難發生後之交通維護、緊急通訊、電力供應或維持社會秩序？			
5.18 個人資料檔案之留存期限控管是否遵循相關法規命令？			
6.存取控制			
6.1 電信事業是否對用戶端設備訂定適切之存取控制規則(如控制的要求應基於資訊擁有者而非設備擁有者；採原則禁止、例外開放之規則）？			
6.2 是否提供使用者能有效識別與鑑別正確之電信服務營運商(如用戶無法證實時，應有的警示措施）的適切控制措施？			

電信事業 ISO/IEC 27011 增項稽核表			
檢查項目	檢查結果		
	符合	不符合	不適用
7.資訊系統獲取、開發及維護			
7.1 正式運作系統（operational systems）中之程式碼是否經核准，若有發展中程式碼與安裝編譯器程式之需求，是否有適當控制措施？			
7.2 是否於所有資訊系統變更實作前均有適當之回復策略？			
7.3 是否對所有運作中程式原始碼之異動留存稽核日誌？			
7.4 是否對屬敏感性系統（如交換器設備等）之作業系統軟體或應用軟體實施涵蓋所有功能之完整測試？			
7.5 是否對屬敏感性系統之應用軟體至少保留前三代版本相關備份？			
8.資訊安全事故管理			
8.1 是否建立資安事件（event）之通報及事故（incident）回應與提報處理程序的管理責任與職掌定義？			
8.2 是否建立資安事件或事故之事後處理機制或程序（如管理會議、統計分析），以協助組織能從資安事件、事故中學習經驗？			
9.營運持續管理			
9.1 是否對可能造成電信設施營運中斷之各項風險訂定處理優先順序或處理準則？			
9.2 營運持續計畫是否包含電信設施之緊急復原計畫，如電信設施所在處及其比鄰之建築物、場所等毀損或是要求撤離，應如何處置，以避免電信設施失去安全控制，而影響對於用戶之服務？			
合計 56 項			

註：1. 電信營運中心：指電信業務營運之園區。

2. 通信中心：指裝設提供電信業務的交換設施所在之建築。

3. 控制中心與操作室：指網路管理中心（Network Operation Center）。

4. 電信設備機房：指裝設提供電信業務的通信設施所在之房間。

附件七 國家通訊傳播委員會資通安全事故通報單

國家通訊傳播委員會通報小組 電話：(02) 2343-3552 傳真：(02) 2343-3699 或 e-mail：jmpd@ncc.gov.tw

國家資通安全會報政府資通安全組 電話：(02) 2733-9922 傳真：(02) 2733-1655 或逕送：106 臺北市大安區富陽街 116 號

填報時間：_____年_____月_____日_____時_____分　　編號：

一、發生資通安全事故之電信事業聯絡資料：

電信事業名稱：_____部門：_____

通報人：_____

電話：_____傳真：_____E-mail：_____

二、各電信事業因受外在因素所產生資通安全事故時通報事項：

1.事故發生時間：_____年_____月_____日_____時_____分

2.設備資料：

◎IP 位址（IP Address）：

外部 IP：_____內部 IP：_____ （無；可免填）

◎網際網路位址（Web-URL）：_____（無；可免填）

◎設備廠牌、機型：_____

◎作業系統名稱、版本：□Windows 系列□Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：□防火牆 □防毒軟體 □入侵防禦系統 □其他：_____

3.資通安全事故資料：

◎請分別評估資安事故造成之機密性、完整性以及可用性衝擊：

資安事故影響等級為機密性、完整性及可用性衝擊最嚴重者（數字最大者）

－機密性衝擊：(單選)

□機密資料遭洩漏（4 級）

□密級或敏感公務資料遭洩漏（3 級）

□非屬密級或敏感之關鍵業務資料遭洩漏（2 級）

□非關鍵業務資料遭洩漏（1 級）

□無資料遭洩漏（無需通報）

－完整性衝擊：(單選)

□重要資訊基礎建設系統或資料遭竄改（4 級）

□關鍵業務系統或資料遭嚴重竄改（3 級）

□關鍵業務系統或資料遭輕微竄改（2 級）

□非關鍵業務系統或資料遭竄改（1 級）

□無系統或資料遭竄改（無需通報）

－可用性衝擊：(單選)

□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（4 級）

□關鍵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（3 級）

□關鍵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（2 級）

□非關鍵業務運作遭影響或短暫停頓（1 級）

□無系統或設備運作受影響（無需通報）

◎事故分類：（單選）□非法入侵 □感染病毒 □阻斷服務 □其他：

◎破壞程度：(單選）□系統當機 □資料庫毀損 □網頁篡改 □其他：

◎事故說明：(請勿超過 200 中文字）

◎可能影響範圍及損失評估：(請勿超過 200 中文字）

◎是否影響其他機關（構）或重要民生設施運作：□是 □否

◎應變措施：(請勿超過 200 中文字）

三、期望支援項目：(文字勿超過 200 中文字）

◎是否需要支援：□是（請續填期望支援內容） □否（免填期望支援內容）

期望支援內容：(請勿超過 200 字）

四、解決辦法：

◎是否同時結案：□是（請續填解決辦法及解決時間） □否（免填解決辦法及解決時間）

解決辦法：(請勿超過 200 字）

五、已解決時間：　　年　　月　　日　　時　　分

附件八 資通安全管理矯正／預防措施一覽表

公司名稱			
單位名稱			
單位主管		評估日期：	
承辦人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		頁次：第　頁/共　頁

表單編號	檢查項目編號	矯正／預防措施概述	結案狀態		備註
			結案／未結案	完成日／預計完成日	

備註：本表如不敷使用時，請自行增加頁數。

附件九 資通安全管理矯正／預防措施單

<table>
<tr><td>公司名稱</td><td colspan="3"></td></tr>
<tr><td>單位名稱</td><td colspan="3"></td></tr>
<tr><td>單位主管</td><td></td><td>評估日期：</td><td></td></tr>
<tr><td>承辦人員</td><td></td><td>評估日期：</td><td></td></tr>
<tr><td rowspan="2">聯絡窗口</td><td>電話：</td><td>傳真：</td><td>行動：</td></tr>
<tr><td colspan="2">Email：</td><td>頁次：第　頁/共　頁</td></tr>
<tr><td>檢查項目內容</td><td colspan="3"></td></tr>
<tr><td>提出</td><td colspan="3">不符合事項說明（發現日期：　　年　　月　　日）：</td></tr>
<tr><td rowspan="3">矯正預防</td><td colspan="3">1.原因調查分析：</td></tr>
<tr><td colspan="3">2.矯正措施：</td></tr>
<tr><td colspan="3">3.預防措施：</td></tr>
<tr><td>確認</td><td colspan="3">結案與否：☐是（結案日期：　　年　　月　　日）
☐否（預定結案日期：　　年　　月　　日）

措施成效確認（未結案案件不需填寫）：</td></tr>
</table>

備註：本表如不敷使用時，請自行增加頁數。

附件十 內部稽核表檢查項目勾選不適用之說明

公司名稱			
單位名稱			
單位主管		評估日期：	
承辦人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		頁次：第　頁/共　頁
檢查項目編號	說明不適用理由或提出佐證資料		

備註：本表如不敷使用時，請自行增加頁數。

附件十一 增項稽核表檢查項目勾選不適用之說明

公司名稱			
單位名稱			
單位主管		評估日期：	
承辦人員		評估日期：	
聯絡窗口	電話：	傳真：	行動：
	Email：		頁次：第　頁/共　頁
檢查項目編號	說明不適用理由或提出佐證資料		

備註：本表如不敷使用時，請自行增加頁數。