教育部國民及學前教育署111年度校園資通安全業務管理輔導團
學校資通安全專責人員知能研習

目錄

壹、實施計畫

教育部國民及學前教育署111年度校園資通安全業務管理輔導團
學校資通安全專責人員知能研習

壹、依據

教育部國民及學前教育署111年度校園資通安全業務管理輔導團計畫辦理。

貳、目的

一、建立校園資通安全教育訓練制度及提升整體人才素養，藉由引導學校達成資通安全自主管理永續發展之目的。

二、實施校園資通安全業務專責人員專業課程訓練，提升校園資通安全管理人員之能力。

參、辦理單位

一、指導單位：教育部

二、主辦單位：教育部國民及學前教育署

三、承辦單位：國立臺南高級商業職業學校

肆、研習日期、地點及住宿

一、研習日期：111年9月19日(一)至9月20日(二)。

二、研習地點：9月19、20日-長榮大學國際會議廳。

三、住宿地點：台糖長榮酒店(台南)

伍、參加人員：本署所轄學校與特定非公務機關之資通安全專責人員。

陸、研習課程表：如附件

柒、報名日期及方式：

一、即日起－9/2(五)完成線上報名(報名網址https://forms.gle/Lxc4xRxsiFZCau3B6)，相關訊息將公告於教育部國民及學前教育署網站(https://www.k12ea.gov.tw/)中校園資安輔導團最新消息。

二、聯絡人-

國立臺南高商 秘書室鄭先生 06-2617123#762。

國立臺南高商 學務處謝先生 06-2617123#763。

三、全程參與之教師由主辦單位核發10小時研習時數，由承辦單位統一線上登錄時數。

捌、交通接駁資訊：

高鐵-111年9月19日(一)上午9:20於臺南高鐵站2號出口發車。

高鐵-111年9月20日(二)上午8:20於臺南高鐵站2號出口發車。

玖、本研習相關詳細內容公告於國教署校園資安輔導團專區

附件

教育部國民及學前教育署111年度校園資通安全專責人員知能研習日程表

第一天:111 年 9 月 19 日

時 間	會 議 程 序	主 持 人/主 講 人
09:30-10:00	報 到	國立臺南高商團隊
10:00-10:10	開幕式 重要業務報告	教育部國民及學前教育署長官
10:10-12:00	專題演講(一)	主持人：教育部國民及學前教育署長官 主　題：111 年資通安全維護計畫實施情形佐證資料提交說明及 ISMS 導入學校說明 講　師：國立華南高商 劉耀明主任
12:00-13:00	午餐	國立臺南高商團隊
13:00-14:30	專題演講(二)	主持人：教育部國民及學前教育署長官 主　題：111 年維護計畫查核表演練說明與資產盤點及風險評鑑 講　師：國立成功大學 鍾沛原委員
14:30-14:40	休息	國立臺南高商團隊
14:40-16:10	專題演講(三)	主持人：教育部國民及學前教育署長官 主　題：資通系統備份與回復演練實務 講　師：長榮大學 俞怡中組長
16:10-16:30	茶敘	國立臺南高商團隊
16:30-17:30	專題演講(四)	主持人：教育部國民及學前教育署長官 主　題：社群運作議題研討 講　師：國立台南高商 黃耀寬校長
17:30-	賦歸	國立臺南高商團隊

教育部國民及學前教育署111年度校園資通安全專責人員知能研習日程表

第二天:111 年 9 月 20 日

時間	會 議 程 序	主持人/主講人
08:30-09:00	報 到	國立臺南高商團隊
09:00-10:30	專題演講(五)	主持人：教育部國民及學前教育署長官 主　題：委外合約的訂定與管理 講　師：崑山科技大學 徐國鈞副教授
10:30-10:40	休息	國立臺南高商團隊
10:40-12:10	專題演講(六)	主持人：教育部國民及學前教育署長官 主　題：資通系統硬體管理實務 講　師：亞洲大學 陳偉嵩組長
12:10-12:40	綜合座談	教育部國民及學前教育署長官
12:40-	賦歸	國立臺南高商團隊

參、專業課程

一、111 年資通安全維護計畫實施情形佐證資料提交說明及 ISMS 導入學校說明

主講人/華南高商 劉耀明主任

111年資通安全維護計畫實施情形佐證資料提交說明

簡報大綱

- 實施情形檢核表
- 附表1-機關專職人力-填寫
- 附表2-經費配置
- 附表3-機關資通系統與服務資產清冊
- 機關應辦事項

實施情形檢查表1

實施項目	實施內容	佐證資料
1.核心業務及其重要性	1.1核心業務及重要性盤點？	1.110年資通安全維護計畫(核心系統)

實施情形檢查表2

實施項目	實施內容	佐證資料
2.資通安全政策及目標之訂定	2.1資通安全政策訂定及核定？ 註：資安政策參考範例如下 1.符合法令與法規要求 2.落實資通安全教育訓練，以提高員工之資訊安全意識 3.達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅	資通安全政策
	2.2 資通安全目標之訂定？	資通安全政策(目標)
	2.3 資通安全政策及目標宣導？	宣導方式包含：函知各單位、會議宣導、網站公告、教育訓練、辦理測驗、Email、人員安全守則等。
	2.4 資通安全政策及目標定期檢視	審理審查委員會會議紀錄。(需內含資安政策審查之紀錄)

實施情形檢查表1

實施項目	實施內容	佐證資料
1.核心業務及其重要性	1.1核心業務及重要性盤點？	1.110年資通安全維護計畫(核心系統)

實施情形檢查表4

實施項目	實施內容	佐證資料
5.資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	附表3-資通系統資產清冊
6.資通安全風險評估	6.1 資通安全風險評估及因應？	風險評鑑彙整表及風險處理計畫表
7.資通安全防護及控制措施	7.1 資通安全防護及控制措施	存取控制管理程序書、系統開發程序書通信與作業管理程序書
8.資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制？ (例如:臺灣學術網路各級學校資通安全通報應變作業程序)	國立XXXX學校資通安全事件通報及應變管理程序

實施情形檢查表5

實施項目	實施內容	佐證資料
8.資通安全事件通報、應變及演練相關機制	8.2 資通安全事件通報、應變及演練	1.資安事件通報：教育機構資安通報平臺111年資料(截圖) 2.111年社交工程演練：佐證資料(報告書含點閱率及開啟連結率) 3.111年通報應變演練：演練證明(演練平臺通報資料、簡訊、Email等)
9.資通安全情資之評估及因應機制	9.1資通安全情資之評估及因應措施？ 註：資安情資來源如上級機關、技服中心、ISAC等…	情資來源單位(上級單位、縣市網、區網、技服中心、廠商…等)公文、Email、網站公告…等。
10.資通系統或服務委外辦理之管理	10.1選任受託者應注意事項	合約書或契約書 選任受託者應注意事項(如要求ISMS導入、安全性檢測、稽核其執行等、資安事件通報等)已納入並明確標註於採購招標文件中。 未註明之原因。
	10.2監督受託者資通安全維護情形應注意事項	委外管理程序書

實施情形檢查表6

實施項目	實施內容	佐證資料
10.資通系統或服務委外辦理之管理	10.2監督受託者資通安全維護情形應注意事項	111年本機關計　份契約： 全部契約皆已納入前述規定。 其中　份契約已納入前述規定，其餘未納入之原因為： _____ 全部契約皆未納入相關規定，原因為：_____ 補充說明(選填)：_____
	10.3是否辦理委外廠商查核?	○ 本機關無資通系統或服務委外 ○ 本機關111年委外資通系統、服務廠商共計_____家 111年**自行辦理**委外廠商查核，計查核____家，受查核廠商為_____，查核方式為_____(例如實地查核、書面查核等)；111年**聯合其他機關**(包含等機關)**辦理**委外廠商聯合查核，計查核____ __家委外廠商，受查核廠商為_____，查核方式為_____。 ○ 111年未進行委外廠商查核，原因為： _____

實施情形檢查表7

實施項目	實施內容	佐證資料
11.資通安全教育訓練	11.1機關人員接受資通安全教育訓練情形	詳本機關應辦事項-資通安全教育訓練。
12.公務機關所屬人員辦理業務涉及資通安全事項之考核機制	12.1訂定考核機制並進行考核	111年資通安全考核獎懲情形：記獎 人、懲 人。
13.資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1資通安全維護計畫實施情形之稽核機制	(單選) A~C級機關：資通安全稽核 於 文件(編號、名稱及章節)內，稽核項目已納入資通安全管理法相關規定，執行情形載明於 文件(編號、名稱及章節)。 本機關內部稽核對象共有 個單位，稽核規劃為每年 個，預於年內可完成全部單位稽核。 稽核小組成員包含 個單位，共 人，每次稽核成員規劃為 (人數及組成規則)。 2.尚未訂定機關內部稽核計畫(A~C級機關)。本機關無資安內部稽核機制(D~E級機關)。 A~E級機關：補充說明(選填)：

實施情形檢查表8

實施項目	實施內容	佐證資料
13.資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1資通安全維護計畫實施情形之稽核機制	年度稽核計畫、稽核查檢表、稽核報告書。 2.尚未訂定機關內部稽核計畫(A~C級機關)。本機關無資安內部稽核機制(D~E級機關)。
	13.2資通安全維護計畫之持續精進及績效管理	本機關定期檢視及追蹤內部稽核改善執行情形 本機關不定期檢視及追蹤內部稽核改善執行情形，方法為 未追蹤
	13.3對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核	無
	13.4對所屬/所監督/所管機關(構)訂定稽核計畫	無
	13.5對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核	無

附表1-機關專職人力-填寫(C級)

- 姓名
- 職稱
- 公務信箱
- 人員屬性(正職、約聘、約僱、委外或約用)
- 是否專職(是/否)
- 有效專業資安證照張數
- 資安專業證照類型
- 資安專業證照名稱(如專業證照數非0則必填)
- 資安專業證照發證日期(如專業證照數非0則必填)*西元年/月/日
- 資安專業證照有效期限(如專業證照數非0則必填)*西元年/月/日
- 持有之有效職能評量證照張數

附表2-經費配置-填寫

110年機關預算配置：	111年機關預/概算配置(如已審議填預算)：	資安自主產品採購金額
1.機關年度經費-資本門	7.機關年度經費-資本門	109年資通安全硬體產品
2.機關年度經費-經常門	8.機關年度經費-經常門	109年資資通安全軟體產品
3.年度資訊經費-資本門	9.年度資訊經費-資本門	109年資資通安全服務
4.年度資訊經費-經常門	10.年度資訊經費-經常門	110年資通安全硬體產品
5.年度資安經費-資本門	11.年度資安經費-資本門	110年資資通安全軟體產品
6.年度資安經費-經常門	12.年度資安經費-經常門	110年資資通安全服務

附表3-機關資通系統與服務資產清冊1

- 財產編號：(非必填)
- 資產名稱(系統名稱)：(必填)
- 系統屬性：(必填，限填「行政」或「業務」)
- 版本類別：(必填，限填「共用」、「公版」或「機關自用」)，
  註：共用：2個以上機關共同使用之系統（如戶政、地政、財政、人事差勤系統)。
  公版：各機關依特定版本自行維運使用(如公務出國報告資訊網)。
- 系統建置方式：(限填「自行委外」、「租用服務」、「套裝軟體」、「自行開發」、「主管/上級機關提供」或「其他」)
- 系統主管機關名稱：（非必填，可輸入關鍵字過濾顯示）

附表3-機關資通系統與服務資產清冊2

- 系統管理者(部門)：(必填)
- 系統使用者(部門)：(必填)
- 主機設置於機關內(是/否)：（必填，限填「是」或「否」)
- 核心系統(是/否)：(必填，限填「是」或「否」)
- 含機敏資料(是/否)：(必填，限填「是」或「否」)
- 機敏資訊以非明文方式儲存(必填，是/否/無機敏資訊/其他機關維運)
- 機敏資訊類別
- 是否與民生權益相關(必填，是/否/其他機關維運)
- 防護需求等級：（必填，限填「普」、「中」、「高」或「其他」)
  註：「其他」表示可能為「系統建置於主管/上級機關處」或為「套裝軟體」。
  註：依據資安法責任等級分級辦法第11條，自行或委外軟體才需評防護需求等級。

附表3-機關資通系統與服務資產清冊3

- 是否包含於ISMS導入範圍：（非必填，限填「是」或「否」或空；註：「系統建置方式」為「主管/上級機關提供」得免填）
- 建置廠商：（非必填）
  註：「系統建置方式」為「主管/上級機關提供」得免填，否則必填。
  註：若為機關建置，則填寫機關名。
- 建置廠商之統一編號(必填)
- 維運廠商：
  註：「系統建置方式」為「主管/上級機關提供」得免填，否則必填。
  註：若為機關維運，則填寫機關名。
- 維運廠商之統一編號(必填)
- 最大可容忍中斷時間(小時)：（必填，限填整數，不含逗號）
- 是否符合防護基準：（必填，限填「符合」、「部分符合」、「不符合」或「不適用」）
- 不符合防護基準說明：(非必填；註：「是否符合防護基準」為「部分符合」及「不符合」則為必填項目、
  代碼參附件7-3，多項請以「/」隔開)

資通安全責任等級分級辦法
附表十資通系統防護基準

控制措施 構面	控制措施 措施內容	系統防護需求分級 高	中	普
存取控制	帳號管理	一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。

附表7-3

代碼	構面	驗證項目
C0101	存取控制	帳號管理
C0102		最小權限
C0103		遠端存取
C0201	事件日誌與可歸責性	記錄事件
C0202		日誌紀錄內容
C0203		日誌儲存容量
C0204		日誌處理失效之回應
C0205		時戳及校時
C0206		日誌資訊之保護

附表7-3

C0301	營運持續計畫	系統備份
C0302		系統備援
C0401	識別與鑑別	內部使用者之識別與鑑別
C0402		身分驗證管理
C0403		鑑別資訊回饋
C0404		加密模組鑑別
C0405		非內部使用者之識別與鑑別

C0501	系統與服務獲得	系統發展生命週期需求階段
C0502		系統發展生命週期設計階段
C0503		系統發展生命週期開發階段
C0504		系統發展生命週期測試階段
C0505		系統發展生命週期部署與維運階段
C0506		系統發展生命週期委外階段
C0507		獲得程序
C0508		系統文件
C0601	系統與通訊保護	傳輸之機密性與完整性
C0602		資料儲存之安全
C0701	系統與資訊完整性	漏洞修復
C0702		資通系統監控
C0703		軟體及資訊完整性

附表3-機關資通系統與服務資產清冊4

- 系統是否對外(必填，是/否/其他機關維運)
- 系統日誌保存時間是否超過6個月(必填，是/否/其他機關維運)
- 有無開放遠端連線維護(必填，有/無/其他機關維運)
- 是否禁用弱密碼(是/否/不適用/其他機關維運)(必填)
- 備註：

資通安全責任等級分級辦法

- 附表五 資通安全責任等級 C 級之公務機關應辦事項
- 附表七 資通安全責任等級 D 級之各機關應辦事項

C級單位應辦事項-管理面

制度面向	辦理項目	佐證資料
管理面	資通系統分級及防護基準	附表三
	資訊安全管理系統之導入及通過公正第三方之驗證	C級必需導入ISMS。 教育體系資通安全暨個人資料管理規範
	資通安全專責人員	附表1資安專職人力
	內部資通安全稽核	內部稽核報告書(每二年辦理一次)。
	業務持續運作演練	業務持續演練計畫、演練紀錄(核心資通系統每二年辦理一次)。

C級單位應辦事項-技術面1

制度面向	辦理項目	辦理內容
技術面	安全性檢測	弱點掃描、滲透測試報告(全部核心資通系統每二年辦理一次)。
	資通安全健診	資安健報告(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、目錄伺服器設定及防火牆連線設定檢視)每二年辦理一次
	資通安全弱點通報機制 (VANS)	一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 https://www.nccst.nat.gov.tw/Vans

C級單位應辦事項-技術面2

制度面向	辦理項目	辦理內容
技術面	資通安全防護	防毒軟體、防火牆、電子郵件過濾機制(授權書、截圖)

C級單位應辦事項-認知與訓練

制度面向	辦理項目	佐證資料
認知與訓練	資通安全教育訓練	教育訓練證明(簽呈、簽到單、研習證明等) 專職人員每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。 資訊人員每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。 一般人員每人每年接受三小時以上之資通安全通識教育訓練。

D級單位應辦事項

制度面向	辦理項目	辦理項目細項	佐證資料
技術面	資通安全防護	防毒軟體	防毒軟體、防火牆(授權書、截圖)
		網路防火牆	
認知與訓練	資通安全教育訓練	一般使用者及主管	(A、B、C、D、E、公務、特定非公務皆同) 每人每年接受三小時以上之資通安全通識教育訓練。

ISMS導入學校說明

ISMS導入標準

- 初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入
- 教育部臺教資(四)1090114352C函。依據行政院秘書長109年6月2日院臺護字第1090175614號函，資通安全責任等級非屬A、B級之教育機關（構）得照旨揭規範施行。
- 建議採用「教育體系資通安全暨個人資料管理規範」導入ISMS。

簡報大綱

- 基本概念及ISMS導入規劃
- 規劃資訊安全管理架構
- 執行風險評鑑與管理作業
- 規劃資訊安全管理系統實施
- 制度落實與實施稽核作業

31

資安基本觀念

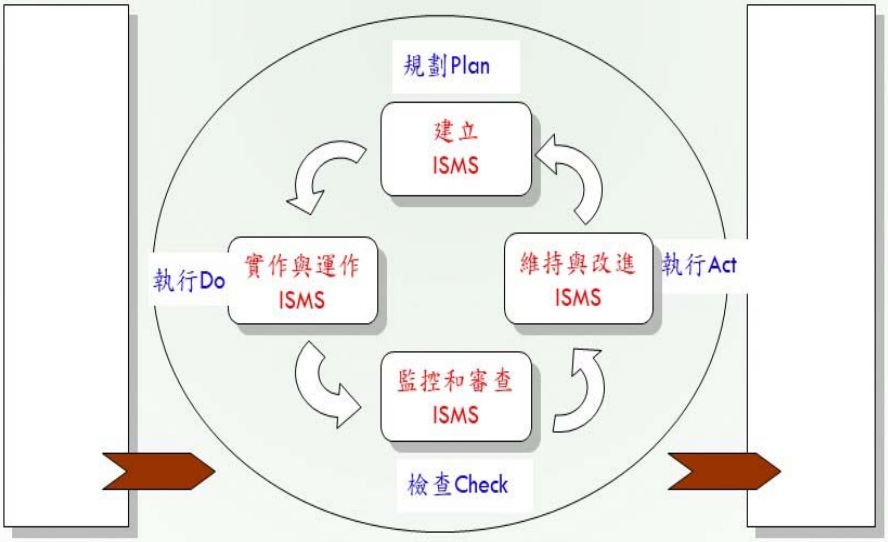
- 資安不僅僅是資訊或資安人員的責任，更是**組織內全體人員之責任**
- 資安**需要長官的大力支持**
- 資安之推動不能靠專案之型式
- 組織內每位成員都有可能成為資安的漏洞

資訊安全三大原則

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露。
- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性。
- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。

ISMS目的在於保護資訊資產的機密性、可用性與完整性。

PDCA 過程模式PROCESS MODEL



應用於ISMS過程之PDCA過程模式

ISMS建置執行概要

35

ISMS導入規劃說明(1/2)

階段	階段一：規劃資訊安全管理架構	階段二：執行風險評鑑與管理作業
時程	約2個月	約3個月
執行作業	1. 組織業務分析 2. 建立資訊安全政策 3. 成立資訊安全組織 4. 建立文件管理機制	1. 鑑別與評價資訊資產 2. 風險評鑑 3. 風險管理與產出風險評鑑報告
產出	1.啟始會議簡報及會議紀錄 2.資訊安全政策 3.資訊安全組織程序書 4.文件管理程序書	1.資訊資產管理程序書　5.風險改善計畫表 2.風險評鑑與管理程序書 6.風險評鑑報告 3.資訊資產清單 4.決定可接受風險值

36

ISMS導入規劃說明(2/2)

階段	階段三：規劃資訊安全管理系統實施	階段四：制度落實與實施稽核作業
時程	約4個月	約2個月
執行作業	1.建立資訊安全管理文件 2.建立資安事件應變處理程序及業務永續運作計畫 3.業務永續運作計畫演練	1.資安內部稽核計畫 2.執行資安內部稽核 3.進行管理審查會議
產出	1.資訊安全管理文件 2.資訊安全事件應變處理程序 3.業務永續運作計畫 4.業務永續運作計畫演練報告	1.內部稽核計畫 2.內部稽核報告 3.管理審查會議紀錄

37

- 基本概念及ISMS導入規劃
- 規劃資訊安全管理架構
- 執行風險評鑑與管理作業
- 規劃資訊安全管理系統實施
- 制度落實與實施稽核作業

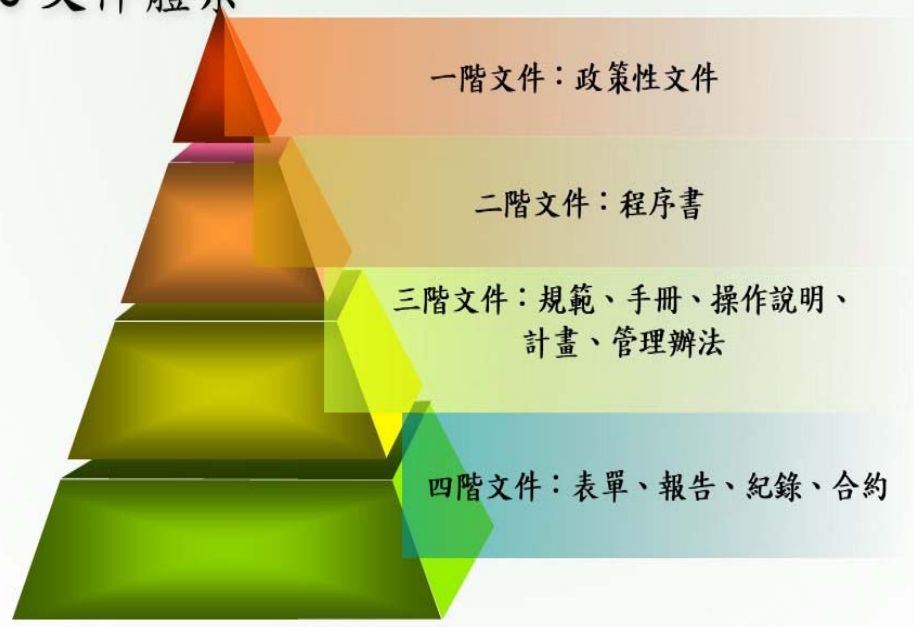
38

ISMS導入規劃說明

階段	階段一：規劃資訊安全管理架構	階段二：執行風險評鑑與管理作業
時程	約2個月	約3個月
執行作業	1. 組織業務分析 2. 建立資訊安全政策 3. 成立資訊安全組織 4. 建立文件管理機制	1. 鑑別與評價資訊資產 2. 風險評鑑 3. 風險管理與產出風險評鑑報告
產出	1.啟始會議簡報及會議紀錄 2.資訊安全政策 3.資訊安全組織程序書 4.文件管理程序書	1.資訊資產管理程序書　5.風險改善計畫表 2.風險評鑑與管理程序書 6.風險評鑑報告 3.資訊資產清單 4.決定可接受風險值

39

ISMS 文件體系



ISMS文件清單範例

文件編號	文件名稱	文件機密等級	相關表單編號	相關表單名稱	相關表單機密等級	發行/修訂日期	文件負責人
NIU-ISMS-A-001	資訊安全政策_V3.0	一般				106.12.01	
NIU-ISMS-B-001	資訊安全組織程序書_V3.0(106.12.01)	限閱	NIU-ISMS-D-001	資訊安全組織成員表_V1.1	限閱	102.11.20	
			NIU-ISMS-D-002	外來文件一覽表	限閱	98.03.04	
			NIU-ISMS-D-003	外部單位聯絡清單	限閱	98.03.04	
			NIU-ISMS-D-004	ISMS有效性量測表_V2.0	限閱	106.12.01	
			NIU-ISMS-D-008	資訊安全管理審查會議紀錄_V2.0	限閱	100.08.01	
NIU-ISMS-B-002	文件管理程序書_V3.0(106.12.01)	限閱	NIU-ISMS-D-005	文件調閱申請單	限閱	98.03.04	
			NIU-ISMS-D-006	文件修訂建議表	限閱	98.03.04	
			NIU-ISMS-D-007	資訊安全管理文件列表	限閱	98.03.04	
NIU-ISMS-B-003	資訊資產管理程序書_V3.0(106.12.01)	限閱	NIU-ISMS-D-009	資訊資產清單	限閱	98.03.25	
NIU-ISMS-B-004	風險評鑑與管理程序書_V3.1(107.01.17)	限閱	NIU-ISMS-D-010	威脅及弱點評估表	限閱	98.03.25	
			NIU-ISMS-D-011	風險評鑑彙整表	限閱	98.03.25	
			NIU-ISMS-D-012	風險改善計畫表	限閱	98.03.25	
			NIU-ISMS-D-013	適用性聲明書_V2.0	限閱	106.12.01	
NIU-ISMS-C-001	資訊資產異動作業說明書_V2.0(100.08.01)	敏感	NIU-ISMS-D-015	資訊資產異動申請表	限閱	98.07.07	
			NIU-ISMS-D-009	資訊資產清單	限閱	98.03.25	

本階段重要事項

- 建立資安組織，**召集人宜由機關副首長以上人員擔任**，以確保能獲得相關的資源
- 決定文管人員
- **召開資訊安全管理審查會議**，確認資訊安全政策、資訊安全組織程序書、文件管理程序書及相關表單，並完成發行及發佈

- 基本概念及ISMS導入規劃
- 規劃資訊安全管理架構
- 執行風險評鑑與管理作業
- 規劃資訊安全管理系統實施
- 制度落實與實施稽核作業

43

ISMS導入規劃說明

	階段一：規劃資訊安全管理架構	階段二：執行風險評鑑與管理作業
時程	約2個月	約3個月
執行作業	1. 組織業務分析 2. 建立資訊安全政策 3. 成立資訊安全組織 4. 建立文件管理機制	1. 鑑別與評價資訊資產 2. 風險評鑑 3. 風險管理與產出風險評鑑報告
產出	1.啟始會議簡報及會議紀錄 2.資訊安全政策 3.資訊安全組織程序書 4.文件管理程序書	1.資訊資產管理程序書　5.風險改善計畫表 2.風險評鑑與管理程序書 6.風險評鑑報告 3.資訊資產清單 4.決定可接受風險值

44

資產盤點

- 何謂「資產」？

  對組織有價值的任何事物

- 資產的分類
  - 實體資產，如電腦
  - 軟體資產，如應用系統
  - 資訊資產，如資料檔案
  - 書面文件，如合約
  - 人員、服務、組織的形象、…等
  - 環境
  - 通訊、網路
- 資產的價值

  依據機密性、完整性及可用性加以鑑別

資產清冊範例

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
NET-CM-001	CM	骨幹網路設備	骨幹 Cisco 6509 1部、Cisco 6506 2部 、Cisco ONS 2部、Cisco ASR9010 2部、Gigamon	網路組	網路組	網路組	2	2	3	3
NET-CM-002	CM	區域網路骨幹及服務	校園網路服務	網路組	網路組	網路組	2	2	3	3
NET-CM-003	CM	廣域網路骨幹及服務	網際網路服務、TANet網路服務	網路組	網路組	網路組	2	2	3	3
NET-CM-004	CM	網路安全設備	Firewall(CheckPoint 13500)1部、IPS(Cisco Firepower 8350)1部	網路組	網路組	網路組	3	3	3	3
NET-CM-005	CM	機房重要網路設備	H3C 5120 1部、HPE 5700 1部、HPE 1950 5部	網路組	網路組	網路組	2	2	3	3
NET-CM-006	CM	機房次要網路設備	Juniper EX2200 2部、Brocade FWS 624G 4部、Cisco C3750 2部、PoE Switch 3部	網路組	網路組	網路組	2	2	2	2
NET-CM-007	CM	負載平衡設備	Citrix Netscaler 8005 1部（含WAI	網路組	網路組	圖書資訊館	3	2	3	3
SYS-DA-001	DA	重要系統資料	教務系統資料庫	系統組	系統組	系統組	3	3	3	3
SYS-DA-002	DA	次要系統資料	教務系統備份資料庫、鏡像資料庫	系統組	系統組	系統組	2	2	2	2
SYS-DA-003	DA	個人電腦資料	系統開發人員電腦資料	系統組	系統組	系統組	2	1	2	2
NET-DA-004	DA	重要設備資料	骨幹交換器、防火牆、WAF等設定檔	網路組	網路組	網路組	3	3	2	3

風險評鑑與管理

- 依據資產本身的**威脅**及**弱點**計算風險值
- 威脅可能對系統、組織或資產造成一個有害的事件，如天災
- 弱點本身並不會造成傷害，如人員教育訓練不足。但如果沒有妥善管理，將促使威脅形成
- 風險處理方法
  - 避免風險
  - 降低風險到可接受的程度
  - 轉移風險
  - 接受剩餘的風險

資產威脅弱點評估表範例

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級（發生之可能性）			弱點等級（受到威脅利用之容易度）			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
NET-EV-002	EV	空調設備	3	火災	人員安全訓練不足	1			1			3
				火災	消防設施的不足或缺乏消防器材的保護	1			1			3
				火災	存放易燃物	1			1			3
				失竊	建築物、房間的實體進出控制不足	1			1			3
				失竊	缺乏安全警覺	1			1			3
				失竊	缺乏建築物、門、窗等物質的保護	1			1			3
				失竊	識別與認證機制的不足	1			1			3
				地震	缺乏建築物、門、窗等物質的保護		2		1			6
				灰塵	容易潮濕、有灰塵、穢物	1			1			3
				空調失效	沒有作好維護的工作		2		1			6
				空調失效	缺乏緊急應變機制		2			2		12
				電源供應中斷	不穩定的供電	1			1			3
				水災	位於易淹水的區域	1			1			3
				颱風	缺乏建築物、門、窗等物質的保護		2		1			6
				支援之公用設施失效	維護服務回應時間過長	1			1			3
				支援之公用設施失效	規格不清楚或未盡完善	1			1			3
				支援之公用設施失效	缺乏測試程序或測試不夠	1			1			3
				支援之公用設施失效	缺乏保養/維護程序或不足	1			1			3
				支援之公用設施失效	缺乏備援電力或備援電力不足	1			1			3

風險處理計畫範例

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險再評鑑			
							威脅	弱點		資產價值	威脅等級	弱點等級	風險值
1	NET-EV-002	EV	空調設備	機房冷氣主機2部、機櫃型精密式空調4部、UPS區冷氣送風機	網路組	3	空調失效	缺乏緊急應變機制	12				

教育體系資通安全管理規範或ISO 27001控制目標	現況說明	風險改善建議措施	教育體系資通安全管理規範或ISO 27001條文	建議權責單位	預計改善時間與處理方式	與高風險資產之風險評估彙整表對照
實體及環境安全	系統組機房僅有1部機櫃型精密式空調，有失效的風險	專案經費再增加1部機櫃型精密式空調	A.11.2.2	網路組	1.擬專案108年度校內經費改善(至108年12月31日止) 2.未達置前定期維護設備	1

- 基本概念及ISMS導入規劃
- 規劃資訊安全管理架構
- 執行風險評鑑與管理作業
- 規劃資訊安全管理系統實施
- 制度落實與實施稽核作業

ISMS導入規劃說明

階段	階段三：規劃資訊安全管理系統實施	階段四：制度落實與實施稽核作業
時程	約4個月	約2個月
執行作業	1.建立資訊安全管理文件 2.建立資安事件應變處理程序及業務永續運作計畫 3.業務永續運作計畫演練	1.資安內部稽核計畫 2.執行資安內部稽核 3.進行管理審查會議
產出	1.資訊安全管理文件 2.資訊安全事件應變處理程序 3.業務永續運作計畫 4.業務永續運作計畫演練報告	1.內部稽核計畫 2.內部稽核報告 3.管理審查會議紀錄

51

本階段產出文件及實作

- 人員安全與教育訓練程序書
- 實體安全管理程序書
- 通信與作業管理程序書
- 存取控制管理程序書
- 系統開發與維護管理程序書
- 委外管理程序書
- 安全事件管理程序書
- 業務永續運作管理程序書
- 資訊安全稽核作業程序書
- 矯正管理程序書

- 基本概念及ISMS導入規劃
- 規劃資訊安全管理架構
- 執行風險評鑑與管理作業
- 規劃資訊安全管理系統實施
- 制度落實與實施稽核作業

53

ISMS導入規劃說明

	階段三：規劃資訊安全管理系統實施	階段四：制度落實與實施稽核作業
時程	約4個月	約2個月
執行作業	1.建立資訊安全管理文件 2.建立資安事件應變處理程序及業務永續運作計畫 3.業務永續運作計畫演練	1.資安內部稽核計畫 2.執行資安內部稽核 3.進行管理審查會議
產出	1.資訊安全管理文件 2.資訊安全事件應變處理程序 3.業務永續運作計畫 4.業務永續運作計畫演練報告	1.內部稽核計畫 2.內部稽核報告 3.管理審查會議紀錄

54

內部稽核

- 擬定內部稽核計畫，並經權責主管核准
- 單位內若無適當稽核人員，可尋求外部人員協助
- 針對不符合項目進行矯正措施

管理審查會議審查內容-八大議題

- 過往管理審查之議案的處理狀態
- 資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項
- 資通安全維護計畫內容之適切性
- 資通安全績效之回饋，包括：
  A. 資通安全政策及目標之實施情形。
  B. 資通安全人力及源之配置實施情形。
  C. 資通安全防護及控制措施之實情形。
  D. 稽核結果。(內外稽結果、維護計畫實施情形)。
  E. 不符合項目及矯正措施。
- 風險評鑑結果及風險處理計畫執行進度
- 重大資通安全事件之處理及改善情形。
- 利害關係人之回饋。
- 持續改善之機會

管理審查會議之決議事項(建議)

- 資訊安全制度執行之各項改進措施
- 更新風險評鑑與風險改善計畫
- 針對可能影響資訊安全制度之內、外部事件，修正資訊安全管理流程與控制措施，包括：
  - 營運需求的變更
  - 安全需求的變更
  - 影響現行營運需求的業務程序變更
  - 管理或法規需求的變更
  - 契約要求的變更
  - 可接受風險等級或標準的變更
- 針對資訊安全制度之需要，協調所需之資源
- 控制措施有效性評量方式的改善

ISMS有效性量測範例

項次	量測項目	目標水準	量測方式或佐證資料	量測時間	量測人員	量測結果及差異說明	分析評估方式	分析評估時間	分析評估人員	分析評估結果及有效性說明
資訊安全目標	確保本館機房骨幹網路服務及核心資訊業務全年可用性	≧99.5%	1. 量測方式：12月底前自我檢查 2. 佐證資料：SMOKEPING紀錄	每年一次 107.12.28	網路組人員	符合 99.97%	1. 量測方式：透過內稽查核 2. 佐證資料：內稽報告	每年一次 108.02.27	內稽人員	符合。 經內稽檢查結果，可用性超過99.5%。
	為保護本館資訊資產之機密性與完整性，需進行風險評鑑及風險管理	≧1 次/年	1. 量測方式：12月底前自我檢查 2. 佐證資料：相關紀錄	每年一次 107.12.28	各組人員	符合 1 次	1. 量測方式：透過內稽查核 2. 佐證資料：內稽報告	每年一次 108.02.27	內稽人員	符合。 經內稽檢查結果，已執行風險評鑑及風險管理。
	為確保資訊需經權責單位授權才可存取，以確保其機密性，每年發生機密等級資訊外洩之事件	≦1 次/年	1. 量測方式：12月底前自我檢查 2. 佐證資料：相關紀錄	每年一次 107.12.28	各組人員	符合 0 次	1. 量測方式：透過內稽查核 2. 佐證資料：內稽報告	每年一次 108.02.27	內稽人員	符合。 經內稽檢查結果，未發生機密等級資訊外洩之事件。
	為確保本館教職員生資料之正確性與完整性，每年發生資料遭未經授權竄改之事件	≦0 次/年	1. 量測方式：12月底前自我檢查 2. 佐證資料：相關紀錄	每年一次 107.12.28	各組人員	符合 0 次	1. 量測方式：透過內稽查核 2. 佐證資料：內稽報告	每年一次 108.02.27	內稽人員	符合。 經內稽檢查結果，未發生資料遭未經授權竄改之事件。

ISMS工作清單

工作項目	頻率
資產盤點	至少每年一次
風險評鑑	至少每年一次
帳號清查	至少每半年一次
弱點掃描滲透測試	至少每二年一次
資安健診	至少每二年一次
BCP演練	核心系統至少每二年一次
ISMS有效性量測	至少每年一次
軟體清查	至少每年一次
內部稽核	至少每二年一次
有效性量測	至少每年一次
管理審查會議	至少每年一次

ISMS & 資通安全維護 施行應注意事項

- 說、寫、做一致
- 管理階層的支持
- 資通安全工作推動不是一個人的事
- 委外廠商的合約及管理
- 一般人員的教育訓練
- 融入變成日常的習慣

二、111 年維護計畫查核表演練說明與資產盤點及風險評鑑

主講人/國立成功大學 鍾沛原委員

111年維護計畫查核表演練說明與資產盤點及風險評鑑

鍾沛原 專案經理
成大資通安全研究與教學中心
2022/04/14

大綱

- 111年維護計畫查核表說明
- 資產盤點及風險評鑑
- 結論

資通安全責任等級分級辦法 (110/08/23修正)

- 第 6 條
  1. 各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。
  2. 前項所定自行或委外設置之資通系統，**指具權限區分及管理功能之資通系統**。
- 第 7 條
  1. 各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。

資通安全責任等級分級辦法修正草案內容

修正條文	現行條文
第六條 各機關維運自行或委外開發之資通系統、**或維運具權限區分及管理功能之非自行或委外開發系統**者，其資通安全責任等級為C。	第六條 各機關維運自行或委外開發之資通系統者，其資通安全責任等級為C級。
說明： 機關基礎資通環境或處理，使用市面既有資通系統，如**電子郵件、目錄服務系統，資料庫、帳務處理**等，仍應就其資安風險進行管控，為明確其資安責任等級要求，爰調修第六條 。→原資安責任等級D級之**「具有郵件伺服器，應備電子郵件過濾機制」**條款刪除。	

p.3

大陸廠牌資通訊產品盤點

受文者：教育部

發文日期：中華民國110年9月23日
發文字號：院臺護長字第1100186822號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：有關大陸廠牌資通訊產品盤點結果中，屬「在臺陸資廠商」之產品採購，請依說明事項辦理，請查照並轉知所屬公務機關。

說明：

一、為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，請各機關應於本(110)年12月31日前完成汰換大陸廠牌資通訊產品。

二、有關本院評估結果屬「在臺陸資廠商」者，如聯想集團(Lenovo)，雖非屬於本次盤點及汰換範圍，惟機關辦理採購時，如涉及經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」，應確實於招標文件中載明不允許在臺陸資廠商(陸資資訊服務業者)參與。

p.4

WHY資產盤點與風險評估！？

- 資通安全管理法施行細則第6條規定

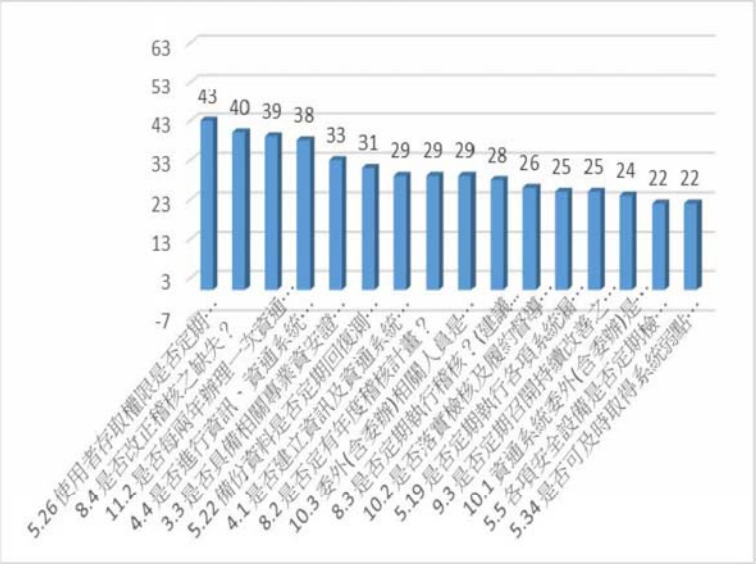
本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

一、核心業務及其重要性。
二、資通安全政策及目標。
三、資通安全推動組織。
四、專責人力及經費之配置。
五、公務機關資通安全長之配置。
六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。
七、資通安全風險評估。
八、資通安全防護及控制措施。
九、資通安全事件通報、應變及演練相關機制。
十、資通安全情資之評估及因應機制。
十一、資通系統或服務委外辦理之管理措施。
十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。
十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

111年維護計畫查核表說明

110年63校維護計畫實地訪視結果

- 前三名不符合問題統計
  1. 5.26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？
  2. 8.4 是否改正稽核之缺失？
  3. 11.2 是否每兩年辦理一次資通安全健診？ (本項C級機關列入評分，D級機關不列入評分)



資通安全政策之推動及目標訂定

查核內容	準備資料或客觀證據
1.1 是否定義符合組織需要之資通安全政策及目標？	資通安全政策或資通安全維護計畫
1.2 組織是否訂定資通安全政策及目標？	資通安全政策或資通安全維護計畫
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？	審核紀錄及公告紀錄
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？	管審會紀錄
1.5 是否隨時公告資通安全相關訊息？	公告紀錄

錯誤的範例

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列定性及定量目標：

4.1 定性目標：

4.1.1 確保相關資通安全措施或規範符合政策與現行法令的要求每年至少進行一次內部稽核。

4.1.2 每年至少進行一次業務持續計畫之測試或檢核。

4.2 定量目標：

4.2.1 確保資訊資產受適當之保護，每年未經授權或因作業疏失對資產所造成的損害降至最低。

4.2.2 確保所有資通安全事件或可疑之安全弱點，每年不依適當通報程序反應，並予以適當的調查及處理事件降至最低。

4.2.3 符合政府資通安全相關政策、規訂及相關法令要求。

4.2.4 定期實施資通安全教育訓練。

p.9

設置資通安全推動組織&配置適當之資通安全專業人員及適當之資源

查核內容	準備資料或客觀證據
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？	資通安全組織成員表
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？	資通安全組織成員表
2.3 是否訂定組織之資通安全責任分工？	資通安全組織成員表

查核內容	準備資料或客觀證據
3.1 是否訂定人員之安全評估措施？	人員安全守則
3.2 是否符合組織之需求配置專業資安人力(資安專責人員)？	資通安全維護計畫中敘明配置資通安全專責人員 (C級機關應辦事項：初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。)
3.3 是否具備相關專業資安證照或認證？(本項C級機關列入評分，D級機關不列入評分)	專業安證照及職能訓練
3.4 是否配置適當之資源？	資安或資訊相關經費情形(全年度與前年度經費之占比)

p.10

人員資通安全守則(範例)

1 目的：為落實本校資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。

2 範圍：本守則適用於正職人員與約聘（僱）人員。

3 作業守則

3.1 電腦應設定密碼確實保密。

3.2 電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘以內。

3.3 電腦之作業系統漏洞應即時更新修補。

3.4 電腦應安裝防毒軟體並即時更新病毒碼。

3.5 應定期將重要資料備份存放。

3.6 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.7 不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本校資訊細節。

3.8 在丟棄任何曾經儲存本校資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。

3.9 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

3.10 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼。

3.11 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

3.12 當有新象顯示系統可能中毒時，應儘速通知相關人員。

3.13 禁止濫用系統及網路資源，複製與下載非法軟體。

3.14 應遵守「個人資料保護法」規範，保護個人資料使用之合法性及機密性。

4 密碼使用原則

4.1 應保護通行密碼，維持通行密碼的機密性；資通系統之系統管理者應至少每 3 個月更換密碼一次，一般資通系統之使用者應至少 6 個月更換密碼，並禁止重複使用相同的密碼。

4.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

4.3 當有新象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

4.4 通行密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

4.5 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

4.5.1 個人姓名、出生年月日、身分證字號。

4.5.2 機關或單位名稱識別代碼或是其他相關事項。

4.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

4.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

4.5.5 電話號碼。

4.5.6 英文或是其他外文字典的字彙。

4.5.7 專有名詞。

4.5.8 空白。

5 電腦軟體版權之使用與管理

5.1 禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定。

5.2 本校資訊機房伺服器所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

5.3 本校人員若有安裝機房伺服器軟體需求時，需填寫「資通服務申請表」，經權責主管以上核准後，始得執行安裝。

6 保密協定

6.1 本校人員應填具「保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

7 公告與實施

7.1 本守則由本校資通安全委員會通過後公告實施，修訂時亦同。

7.2 本校員工若未遵守上述規定或資通安全政策及程序者，得依相關懲戒程序處置違紀人員。

簽署人：_____

中　華　民　國　　年　　月　　日

p.11

專職(責)人力及經費配置

- 經費配置
  - 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查

機關名稱	機關年度經費 -資本門	機關年度經費 -經常門	年度資訊經費 -資本門	年度資訊經費 -經常門	年度資安經費 -資本門	年度資安經費 -經常門
○○學校	1,000,000	700,000	40,000	30,000	10,000	8,000

計畫分級 / 年度	中長程計畫總經費		
	1 億以下(含)	1~10 億(含)	10 億以上
2020 年資安經費	至少為計畫之資訊建設經費 7%	至少為計畫之資訊建設經費 6%	至少為計畫之資訊建設經費 5%
2025 年資安經費	至少為計畫之整體經費 7%	至少為計畫之整體經費 6%	至少為計畫之整體經費 5%

資料來源：107~114年資安產業發展行動計畫

p.12

資訊及資通系統之盤點及風險評估

查核內容	準備資料或客觀證據
4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？(本項將列為實地稽核重點項目，並納入機關(校長)考核參考)	資訊資產清單
4.2 各項資產是否有明確之管理者及使用者？	資訊資產清單
4.3 是否定有資訊、資通系統分級與處理之相關規範？	維護計畫核心系統
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？	資訊資產清單風險評估表

資產盤點範例

A	B	C	D
資產編號	資產類別	資產名稱	資產說明
IS-CM-001	CM	負載平衡器	FortiADC 200F 負載平衡器 1部
IS-CM-002	CM	防火牆	FG-201E對外防火牆 1部
IS-CM-003	CM	頻寬控制	GSI內部上網行為管理 1部
IS-CM-004	CM	核心交換器	Cisco C4503-E 核心交換器 1部
IS-CM-005	CM	主幹網路中繼交換器(各棟樓)	Cisco C2650-S 交換器 4部 Cisco C2650-X 交換器 1部
IS-CM-006	CM	一般網路邊際交換器(各辦公室)	ZyXEL GS2200-24 交換器 17部 Cisco C2960-L 交換器 1部
IS-CM-007	CM	一般網路交換器(收容電腦與專科教室)	Cisco C3750G 交換器 1部
IS-CM-008	CM	無線網路邊際供電交換器(POE)	Cisco C3650G POE交換器 3部 Aruba 1930 POE交換器 1部
IS-CM-009	CM	無線網路控制器	Aruba 7030 控制器 1部
IS-DA-001	DA	重要系統資料	Core Switch設定檔
IS-DA-002	DA	一般系統資料	學校網站及公告資料
IS-DA-003	DA	一般系統資料	校園網路連線架構圖
IS-DA-004	DA	一般系統資料	無線AP點位圖與列表
IS-DA-005	DA	一般系統資料	各類資訊設備紀錄檔
IS-DC-001	DC	紙張文件(固定資產)	網路機房資訊設備清冊
IS-DC-002	DC	紙張文件(機房維護合約)	機房維護合約
IS-DC-003	DC	紙張文件(ISP合約)	TANET與兩條光纖線路合約
IS-DC-004	DC	紙張文件(設備採購與保固資料)	各項設備採購與授權保固等資料
IS-DC-005	DC	紙張文件(IP清冊)	全校設備、網段與IP清冊
IS-DC-006	DC	一般文件(各式申請表)	資通資產報廢銷燬處理申請表
IS-DC-007	DC	一般文件	機房進出紀錄、巡檢表
IS-EV-001	EV	穩壓器	穩壓器 1部
IS-EV-002	EV	不斷電系統	UPS 3部
IS-EV-003	EV	空氣設備	機房內2部及辦公區1部，共3部
IS-EV-004	EV	消防設施	滅火器二氧化碳，共2支
IS-EV-005	EV	監視設備	監視主機1部、監視鏡頭4支
IS-EV-006	EV	門禁設備	門禁主機1部
IS-HW-001	HW	重要系統主機	HP DL380 Gen10 伺服器 3部 VMware主機16部
IS-HW-002	HW	磁碟儲存陣列	NetApp E2812 儲存設備 2部 HP MSA2000 儲存設備 1部
IS-HW-003	HW	重要系統網路設備	Cisco MDS9148 HP StorageWorks 8/8 SAN switch
IS-HW-004	HW	網路附加儲存系統	Synology RS4017XS+ NAS 1部
IS-HW-005	HW	一般系統主機	HP DL380 Gen9 伺服器 1部(優質化網站)
IS-HW-006	HW	一般系統主機	HP DL380 Gen8 伺服器 1部(TQC檢定伺服器)
IS-HW-007	HW	無線網路AP主機	Aruba AP92 共16台、AP225共20台、AP325共10台、AP335共8台，共54台
IS-HW-008	HW	個人電腦	辦公區桌上型電腦共3部
IS-HW-009	HW	筆記型電腦	網管人員使用筆電(測線用)，共1部
IS-HW-010	HW	一般系統主機	DELL直立式伺服器 2部(TQC檢定伺服器)
IS-HW-011	HW	LOG管理分析系統	N-Reporter 1部
IS-PE-001	PE	設備維護人員	網管1位
IS-PE-002	PE	資訊設備委外維護人員	機房維護廠商工程師1位、業務1位
IS-PE-003	PE	一般使用人員	一般網路使用者
IS-PE-004	PE	資通安全組織	資通安全組織成員
IS-PE-005	SW	智慧網管軟體	Pixis
IS-SW-001	SW	作業系統(個人電腦用)	Windows OS(全校授權)
IS-SW-002	SW	作業系統(伺服器用)	Windows Server 2012R2 Windows Server 2019 標準版 x 2套
IS-SW-003	SW	套裝軟體(授權軟體)	MS Office辦公室應用軟體(全校授權)
IS-SW-004	SW	防毒軟體(個人電腦用)	ESET校園授權500U
IS-SW-004	SW	防毒軟體(伺服器用)	ESET伺服器授權1U(優質化主機用)
IS-SW-005	SW	備份軟體(系統備份)	Veeam
IS-SW-006	SW	備份軟體(行政備份)	Acronis 授權75套

核心業務及重要性

❑ 非核心業務及說明範例

非核心業務系統	業務失效影響說明	最大可容忍中斷時間
防火牆系統	可能使本校資安防護中斷	○小時
防毒系統	可能使本校資安防護中斷	○小時
監視系統等OT系統	可能使本校部分業務中斷	○小時
其他(不含親師生個人資料之資通系統)	可能使本校部分業務中斷	○小時

註：
1. 盤點對象為**具權限區分及管理功能之資通系統**
2. 最大可容忍中斷時間參考核心業務訂定原則，但**應大於或等於核心業務資通系統中最大值者**

資通安全管理措施之實施情況

查核內容	準備資料或客觀證據
5.1 人員進入重要實體區域是否訂有安全控制措施？	資訊設備主機機房門禁照片
5.2 重要實體區域的進出權利是否定期審查並更新？	進出人員清單
5.3 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？	人員進出紀錄表
5.4 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？	巡查紀錄表
5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	消防、CCTV、門禁設施檢查紀錄或保養資料。 設備使用訓練紀錄。
5.6 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？	陪同進出之紀錄及照片
5.7 重要資訊處理設施是否有特別保護機制？	實體安全管理制度
5.8 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？	例如：資訊機房偵煙、偵熱與滅火設備、漏水偵測等照片。

資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.9 電源之供應及備援電源是否作安全上考量？	電力保護設施照片(UPS、穩壓器接地線等)、緊急照明設備照片
5.10 通訊線路及電纜線是否作安全保護措施？	線路保護設施照片(如線槽、高架地板、套管等)
5.11 設備是否定期維護，以確保其可用性及完整性	系統主機及網路維護紀錄或合約、機房查檢紀錄表
5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	設備進出管理制度。(B-002 5.7.2) 設備進出紀錄表
5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	防毒軟體、登入等照片、設備領用紀錄。
5.14 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？	報廢管理制度及報廢紀錄
5.15 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？	管理制度及實體防護照片(例如：資料上鎖)。
5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	測試環境與正式環境照片、不適用則免附。

p.17

資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.17 是否全面使用防毒軟體並即時更新病毒碼？	至少2位一般使用者的個人電腦設定畫面
5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	至少2位一般使用者的個人電腦設定畫面
5.19 是否定期執行各項系統漏洞修補程式？	系統主機及個人電腦各兩臺設定畫面
5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	管理制度(B-007 5.3.5)
5.21 重要的資料及軟體是否定期作備份處理？	備份工作相關紀錄
5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	備份回復演練紀錄
5.23 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？	系統登作畫面、https、檔案加密。
5.24 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？	可攜式媒體管理制度

p.18

防毒軟體程序設定

快速掃描

建議的 () 快速掃描查看可能已註冊惡意程式碼的所有位置，例如登錄機碼和已知的 Windows startup 資料夾。結合 always on 即時保護，可在開啟及關閉檔時對其進行審閱; 每當使用者流覽至資料夾時，快速掃描可協助對以系統和內核層級惡意程式碼開頭的惡意程式碼提供強防護。

在大多數情況下，快速掃描足以滿足計畫掃描的建議選項。

完整掃描

完整掃描會從執行快速掃描開始，繼續執行所有已裝載固定磁片及移除/網路磁碟機的連續檔案掃描(如果完整掃描已設定為執行此作業)。
根據需要掃描的資料量和類型，完整掃描可能需要數小時或數天才能完成。

完成完整掃描之後，就可以使用新的安全性智慧，並必須進行新的掃描，以確保不會以新的安全性情報偵測到其他威脅。

由於完整掃描所涉及的時間和資源，在一般情況下，Microsoft 不建議排程完整掃描。

自訂掃描

自訂掃描是在您指定的檔案和資料夾上執行的快速掃描。例如，您可以選擇掃描 USB 磁片磁碟機，或裝置的本機磁片磁碟機上的特定資料夾。

Windows 系統管理工具→工作排程器→Microsoft→Widnows→Windows Defender→Windows Defender Schedule→觸發程序→新增→設定

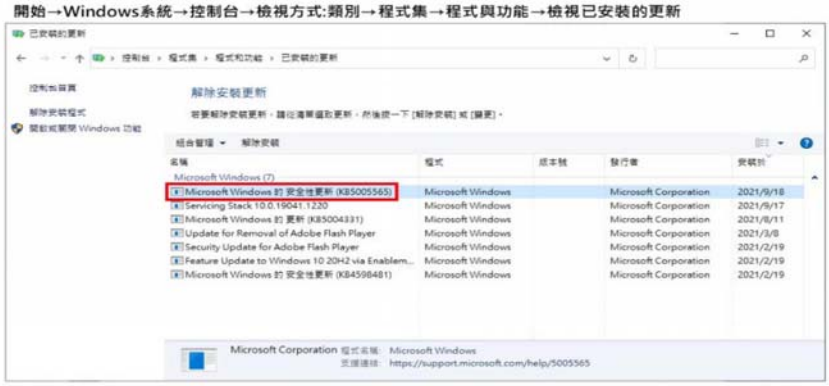
電腦使用之安全管理

- 微軟Windows之MSHTML引擎存在安全漏洞(CVE-2021-40444)

請各位同仁檢視自己的電腦並於中午12:00回填表單

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

開始→Windows系統→控制台→檢視方式:類別→程式集→程式與功能→檢視已安裝的更新



Win10的各版本中，只要有 KB5005565、66、68、69、73 其中一個，就表示有確實進行更新！

留意的已安裝的過舊軟體

- ❑ 7-Zip 18.05版本以上
- ❑ 防毒軟體
- ❑ Acrobat Reader
- ❑ Office軟體

End Of Life – Microsoft Windows and Office

Microsoft has a support lifetime for each of their products. Below is a list of software that has or soon will reach its end of life and support. You should not run software that is not supported, since it may contain security issues that are not fixed and can put your computer and information at risk. Michael Spice can help you with replacement and updating to a supported version of Office, Windows and Windows Server.

Microsoft Office

Microsoft Office 2003 – April 8, 2014
Microsoft Office 2007 – October 10, 2017
Microsoft Office 2010 – October 13, 2020
Microsoft Office 2011 for Mac – October 10, 2017
Microsoft Office 2013 – April 11, 2023
Microsoft Office 2016 – October 14, 2025
Microsoft Office 2016 for Mac – October 13, 2020
Microsoft Office 2019 – October 14, 2025
Microsoft Office 2019 for Mac – October 10, 2023
Microsoft Office 2021 – October 13, 2026
Microsoft Office 2021 for Mac – October 13, 2026

Microsoft Windows

Microsoft Windows XP – April 8, 2014
Microsoft Windows Vista – April 11, 2017
Microsoft Windows 7 – January 14, 2020
Microsoft Windows 8 – January 12, 2016 users must upgrade to Windows 8.1
Microsoft Windows 8.1 – January 10, 2023
Microsoft Windows 10 release 1507 from July 2015 – May 9, 2017

資料壓縮軟體 7-Zip 發現安全漏洞，儘速升級最新版本

- A Vulnerability in 7-Zip Could Allow for Arbitrary Code Execution
- A serious security vulnerability has been found in 7-Zip

Release Notes | Acrobat, Reader

Acrobat DC and Acrobat Reader DC Continuous Track release notes

Date	Release Notes	Release Type*	Focus
Oct 12, 2021	DC Oct 2021 (21.007.20099)	Continuous	Latest Release: This update provides security mitigations and bug fixes.
Sep 29, 2021	DC Sep 2021 (21.007.20096)	Optional Update	This patch fixes specific functionality issues.
Sep 14, 2021	DC Sep 2021 (21.007.20091)	Continuous	This update provides new features, security mitigations, feature enhancements, and bug fixes.
Jul 28, 2021	DC Jul 2021 (21.005.20060)	Optional Update	[Win Only] This patch fixes specific functionality issues.
Jul 13, 2021	DC Jul 2021 (21.005.20054)	Continuous	This update provides new features, security mitigations, feature enhancements, and bug fixes.
Jun 08, 2021	DC Jun 2021 (21.005.20048)	Continuous	This update provides new features, security mitigations, feature enhancements, and bug fixes.
May 11, 2021	DC May 2021 (21.001.20155)	Continuous	This update provides security mitigations and bug fixes.

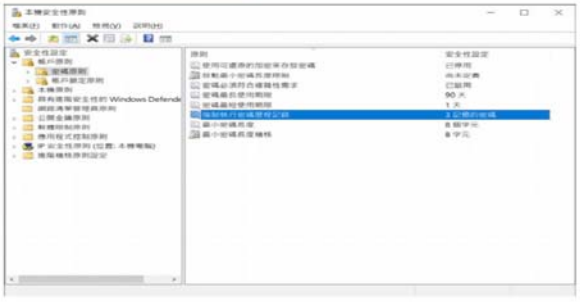
資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	帳號申請及註銷管理制度
5.26 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？	帳號
5.27 通行碼長度是否超過8個字元？	通行
5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	通行碼管理制度
5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	網路架構圖及業務與網段對應資料，內網區隔狀況、網路管理規定
5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	遠端連線作業
5.31 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)？	行動式電腦設備管理制度
5.32 重要系統是否使用憑證作為身份認證？	憑證使用認證佐證資料 (不適用者免附)

建議包含重要系統、主機、網路設備帳號清查佐證紀錄，並每年定期清查一次

密碼設定與查詢

- Windows 系統管理工具→本機安全性原則→安全性設定→帳戶原則→密碼原則



- CMD模式→net user 帳號

若上次設定密碼時間為當下時間，則表示從未設定密碼

p.23

資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	資訊服務變更管理制度及紀錄。
5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	弱掃報告及高風險弱點修補處理狀況
5.35 限制使用危害國家資通安全產品-大陸廠牌產品清冊列管及說明。	1.檢視資通系統及設備是否使用危害國家資通安全產品(如大陸廠牌) 2.大陸廠牌產品清冊(包含硬體、軟體、服務，請上傳可編輯檔案如excel,ods等)
5.36 限制使用危害國家資通安全產品-汰換大陸廠牌產品及說明。 1.110年12月31日前完成汰換大陸廠牌產品 2.如無法於期限內完成汰換，須於大陸廠牌產品清冊述明理由	1.大陸廠牌產品汰換紀錄 2.大陸廠牌產品清冊(包含硬體、軟體、服務，請上傳可編輯檔案如excel,ods等)

p.24

訂定資通安全事件通報及應變之程序及機制&定期辦理資通安全認知宣導及教育訓練

查核內容	準備資料或客觀證據
6.1 是否建立資通安全事件發生之通報應變程序	資通安全事件通報及應變管理程序。
6.2 機關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？	宣導及公告相關資料。
6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	安全事件報告單或矯正紀錄

查核內容	準備資料或客觀證據
7.1 是否定期辦理資通安全認知宣導？	資通安全公告、宣導及研習資料
7.2 是否對同仁進行資安評量？	資安評量或資安研習評量資料
7.3 是否對同仁依層級定期舉辦資通安全教育訓練？	資安教育訓練資料 資通安全認知訓練時數要求： 1.全體同仁每人每年須接受3小時以上一般資通安全教育訓練 2.專職(責)人員以外之資訊人員每人每年須接受3小時以上之資通安全專業課程訓練或資通安全職能訓練。 3.專職(責)人員每年須接受12小時以上資通安全專業課程訓練或資通安全職能訓練。
7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	公告、宣導、人員安全守責等資料。

p.25

資通安全維護計畫實施情形之精進改善機制&資通安全維護計畫及實施情形之績效管考機制

查核內容	準備資料或客觀證據
8.1 是否設有稽核機制？	內稽制度
8.2 是否定有年度稽核計畫？	內稽計畫書
8.3 是否定期執行稽核？(建議2年1次)	內稽紀錄
8.4 是否改正稽核之缺失？	內稽缺失矯正紀錄

查核內容	準備資料或客觀證據
9.1 是否訂定安全維護計畫持續改善機制？	矯正及預防管理制度
9.2 是否追蹤過去缺失之改善情形？	矯正及預防處理單
9.3 是否定期召開持續改善之管理審查會議？	管審會議紀錄

p.26

Why內部稽核(維護計畫範例)

- 資通安全維護計畫及實施情形之持續精進及績效管理機制(第拾節)
  - 本校資通安全維護計畫之實施
    - 為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本局之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。
  - 本校學校資通安全維護計畫實施情形之稽核機制
    - 稽核機制之實施
      - 資通安全推動小組應於12月前(至少每年一次)或於系統重大變更或組織改造後執行 1次內部稽核作業(自我檢查作業)，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

稽核計畫

- 資訊安全稽核小組成員
  - 組長
  - 組員
- 稽核時程
- 稽核日期

日期	時間	項目	稽核人員	地點
xxx/xx/xx	10:00-10:20	啟始會議	xxx Xxx xxx	
	10:20-10:30	高階主管訪談		
	10:30-12:00	一、核心業務及其重要性 二、資通安全政策及目標 三、設置資通安全推動組織 四、人力及經費之配置 五、資訊及資通系統之盤點及核心資通系統、相關資產之標示 六、資通安全風險評估 七、資通安全防護及控制措施		
	12:00-13:00			
	13:00-15:30	七、資通安全防護及控制措施 八、資通安全事件通報、應變及演練相關機制 九、資通安全情資之評估及因應機制 十、資通系統或服務委外辦理之管理 十一、資通安全教育訓練 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制 十三、資通安全維護計畫及實施情形之持續精進及績效管理機制	xxx xxx xxx	
	15:30-16:00	稽核結果彙整		
	16:00-16:30	結束會議		

資通系統委外(含委辦)案之履約檢核及督導管理(無則請填寫不適用)

查核內容	準備資料或客觀證據
10.1 資通系統委外(含委辦)是否簽訂協議書或契約？	委外(含委辦)案之協議書、契約書等文件，應符合資安法施行細第4款各項規定。
10.2 是否落實檢核及履約督導管理？	檢核受託單位繳交之資料，應附廠商承諾辦理資安相關事項之證明文件。
10.3 委外(含委辦)相關人員是否簽訂保密合約書？	保密切結書、保密合約書等文件

其他應辦事項

查核內容	準備資料或客觀證據
11.1 是否每年檢視一次資通系統(自有及委外)分級妥適性？	資通系統(自有及委外)分級相關文件(資通安全責任等級分級辦法附表九)
11.2 是否每兩年辦理一次資通安全健診？ (本項C級機關列入評分，D級機關不列入評分)	資通安全健診報告
11.3 是否完成資通安全防護(防毒軟體、網路防火牆、電子郵件過濾機制)？	1. 檢視資通設備是否安裝防毒軟體 2. 檢視網路防火牆建置情形 3. 具有電子郵件伺服器者，檢視電子郵件過濾機制
11.4是否完成資通安全弱點通報機制導入作業(111年尚在導入階段，暫不列入評分，C級機關應於2年完成導入)	C級機關：初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 資安法於110年8月23日修法，修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

資產盤點與風險評估

p.31

資產與資訊

- 資產是甚麼？
  - 組織直接賦予價值並需要組織的保護
  - 相關於資訊安全管理系統的範圍
- 資訊是組織資產的一部份，具有價值且需要持續被適切地保護

p.32

資產清冊建立

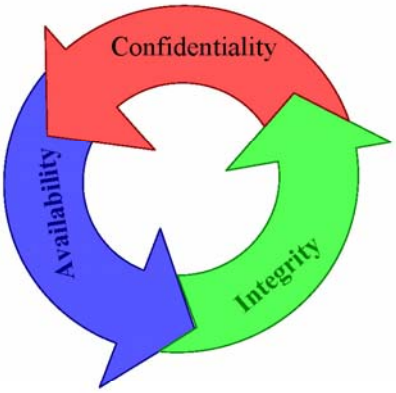
- 權責單位應建立「資訊資產清冊」
  - 清點及鑑別所管轄之資訊資產
  - 定期更新與維護
  - 彙整資訊資產清冊，陳報至資訊安全管理小組予以統一控管，確保資訊資產編號及清冊之完整性

資產鑑別

- 資訊資產分類
  - 人員：同仁、廠商
  - 文件：紙本存在之文書資料，公文、報表等
  - 資料：存放於儲存媒介之數位資訊
  - 軟體：作業軟體、套裝軟體、原始碼、資料庫等
  - 通訊：網路設備、資訊傳輸或服務
  - 硬體：主機設備
  - 環境：基礎設施與服務、環控、電力

資訊資產價值鑑別

- 不被洩露與確保機密（機密性，C）
- 資訊、系統、服務等正確性被扭曲（完整性，I）
- 系統不會因破壞而影響持續運轉（可用性，A）



機密性評估標準

- 範例

評估標準	數值
一般：此資訊資產無特殊之機密性要求	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用	2
敏感：此資訊資產僅供內部相關業務承辦人員存取	3
機密：此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

完整性評估標準

- 範例

評估標準	數值
資產本身完整性要求極低	1
資產本身具有完整性要求，但是完整性被破壞不會對本會造成傷害	2
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重	3
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止	4

p.37

可用性評估標準

- 範例

評估標準	數值
該資訊資產容許失效 3 天以上，不用被修復或是尋找替代品。	1
該資訊資產容許失效 8 小時以上，3 天以下，不用被修復或是尋找替代品。	2
該資訊資產容許失效 4 小時以上，8 小時以下，不用被修復或是尋找替代品。	3
該資訊資產容許失效 4 小時內不用被修復或是尋找替代品。	4

p.38

資產盤點範例

產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	擁有者	機密性	完整性	可用性	資產價值
PE-001	PE	管理階層人員	校長、教務主任、資訊組長	人事室	人事室	人事室	1	1	1	1
PE-002	PE	網路、系統維護人員	代理資訊教師	人事室	人事室	人事室	1	1	1	1
PE-003	PE	一般使用人員	教職員	人事室	人事室	人事室	1	1	1	1
IF-001	IF	作業文件	資料庫與資料檔案、備份資料	教務處	資訊組	資訊組長	1	1	1	1
IF-002	IF	系統文件	網路架構圖	教務處	資訊組	資訊組長	1	1	1	1
IF-003	IF	資訊紀錄 （電子/紙本）	啟用與報廢紀錄單、資訊工作日誌、系統特權帳號清單、設備進出紀錄表	教務處	資訊組	資訊組長	1	1	1	1
IF-004	IF	系統紀錄（Log）	防火牆Log紀錄(一個月一次)	教務處	資訊組	資訊組長	1	1	1	1
HW-001	HW	伺服器	學校Web主機	教務處	資訊組	資訊組長	1	1	1	1
HW-002	HW	其他硬體	印表機、影印機	總務處	總務處	總務處	1	1	1	1
HW-003	HW	個人電腦	桌上型電腦	教務處	資訊組	資訊組長	1	1	1	1
HW-004	HW	可攜式電腦	筆記型電腦	教導處	教導處	教導主任	1	1	1	1
HW-005	HW	資安設備	Zyxel防火牆	教務處	資訊組	資訊組長	1	1	1	1
HW-006	HW	網路設備	Zyxel交換器、L3交換器	教務處	資訊組	資訊組長	1	1	1	1
HW-007	HW	可攜式儲存媒體	USB、記憶卡、CD、DVD、投影機。	教務處	資訊組	資訊組長	1	1	1	1
SW-001	SW	作業系統	KMS	教務處	資訊組	資訊組長	1	1	1	1
SW-002	SW	資訊安全系統	防火牆軟體(Zyxel)	教務處	資訊組	資訊組長	1	1	1	1
EV-001	EV	一般辦公區域	辦公室、會議室。	學校	學校	學校	1	1	1	1
EV-002	EV	資訊機房	電腦機房	教務處	資訊組	資訊組長	1	1	1	1
EV-003	EV	建築保護設施	不斷電系統、穩壓器、機櫃、滅火器、發電機	總務處	總務處	總務處	1	1	1	1

別：人員 (PE)、資訊 (IF)、硬體 (HW)、軟體 (SW)、環境 (EV)

資產盤點重點建議

- 備份設備、資料
- 重要作業系統、資料庫、應用軟體盤點與版本註記
- 人員與環境資產盤點

資產價值標示與使用

- 實體設備(沒有一定要標示)
  - 資產價值1→紅色
  - 資產價值2→綠色
  - 資產價值3→黃色
  - 資產價值4→藍色
- 文件資料
  - 一般、限閱、敏感、機密
- 程序書
  - 實體安全管理、存取控制管理、系統開發與維護...

p.41

資產管理循環

p.42

資產複核與銷毀

- 權責單位每年至少進行1次資產盤點與資產清冊複核。
- 當範圍內有以下的狀況發生之時，則實施不定期的複核
  - 有新增、變更或移除資訊資產
  - 系統有重大異動
  - 作業環境改變
- 資訊資產之報廢（或銷毀）應視其機密等級，採取適當之方式進行銷毀

汰除儲存設備處理

[原件]大量行政文件洩露了硬盤轉售的稅收記錄等

神奈川硬盤流出

勝木茂 十二月6，2019 5:00

分享 鳴叫 0 書籤 970 電子郵件 印刷

包括朝日新聞採訪中發現的大量個人信息和機密信息（例如稅務局 神奈川縣 行政文件）已經被積累的 硬盤（HDD），網絡拍賣 被轉售出去。從縣服務器上卸下的HDD被作為二手物品出售，數據擦除不足。據該縣稱，一家公司的員工承擔著從擦除數據到丟棄數據的所有工作，並承認他們參與了轉售。

經縣確認，HDD用作共享服務器，用於累積有關縣辦公室內每個部門的信息。其中包括稅務檢查 後的公司名稱通知，帶有個人名稱和地址的 汽車納稅 記錄，公司提交的文件，縣職員的業務記錄以及日錄。..

據該縣稱，已轉售的HDD 被用於從富士通租賃公司（ 東京千代田區 ）租用的服務器，並在今年春天將要更換的服務器上將其從服務器中取出。根據與縣的合同，富士通租賃 將使 數據不可恢復的工作委託給 Brodrink （東京都中央區）進行處理，該公司負責信息設備的再現業務。富士通租賃已指示其銷毀它並使它無法使用，然後再丟棄它或完全擦除數據。

從縣到 Broadlink 交付時，HDD進行了簡單的數據擦除（初始化）。HDD 存儲在東京的 Broadlink 設施中，但是負責擦除數據的人員帶出了一部分數據，並將其放在拍賣現場。

一家經營IT公司的人成功地使用了9塊HDD進行工作。當該人檢查內容以確認使用前的安全性時，他注意到數據的存在。據說使用該恢復軟件保存了被認為是 神奈川縣的 正式文件的大量文件。

資料來源：招日新聞

資訊及資通系統盤點範例

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
1.	EVO 派送軟體	軟體資產	資訊教師	總務處	全校師生	電腦教室	1 套		
2.	個人電腦	實體資產	全體教職員	資訊教師	全體教職員	教室/辦公室	42 台		
3.	行動裝置	實體資產	全體教職員	資訊教師	全體教職員	教室/辦公室	33 台	筆電、平板、手機	
4.	可攜式媒體	實體資產	全體教職員	全體教職員	全體教職員	教室/辦公室	1 式	有資料的光碟、外接式硬碟、隨身碟	
5.	學校網站	軟體資產	資訊教師	資訊教師	全體教職員	教育局	1 式	局端雲端機房	
6.	NAS 儲存裝置	實體資產	資訊教師	資訊教師	全體教職員	主機房	1 台		
7.	AD 系統	軟體資產	資訊教師	資訊教師	資訊教師	教育局	1 套	局端雲端機房	
8.	主管人員	人員資產	校長	校長	校長	辦公室	1 式	主任以上	

p.45

風險評鑑範例

項次	資產名稱	類別	擁有者/職稱	機密性 ©	完整性 (I)	可用性 (A)	資訊資產價值(T) (C,I,A 取最大值)	潛在風險事件	風險發生可能性 (V)	風險值 資訊資產價值*(T*V)
1.	EVO 派送軟體	軟體資產	資訊教師	1	1	3	3	1.3.2	2	6
2.	個人電腦	實體資產	全體教職員	1	1	2	2	2.3.3	2	4
3.	行動裝置	實體資產	全體教職員	1	1	1	1	2.4.3	2	2
4.	可攜式媒體	實體資產	全體教職員	1	1	1	1	2.5.2	2	2
5.	學校網站	軟體資產	資訊教師	1	1	1	1	1.2.2	1	1
6.	NAS 儲存裝置	實體資產	資訊教師	2	1	2	2	2.1.3	1	2
7.	AD 系統	軟體資產	資訊教師	3	2	2	3	1.1.4	1	3
8.	主管人員	人員資產	校長	1	1	1	1	4.2.1	1	1

p.46

風險評鑑範例(cont.)

資產大類	資產小類	潛在風險事件	管控措施範例說明
1. 軟體資產類	1.1 作業系統	1.1.1 未落實作業系統更新/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-WSUS 機制失效 -定期檢查漏洞更新狀態 -資訊單位定期彙整提供發佈更新資訊(，供業務單位進行比對
1. 軟體資產類	1.1 作業系統	1.1.2 未購買妥適的作業系統授權/使用授權超過購買數，致使遭受廠商求償或抗議。	-作業系統授權清單
1. 軟體資產類	1.1 作業系統	1.1.3 未汰換原廠公告停止技術支援之作業系統，進而無法修補漏洞，致使遭受惡意攻擊、資料外洩或其他侵害。	
1. 軟體資產類	1.1 作業系統	1.1.4 未加入組織之網域，進而無法套用 GCB 或群組原則政策，致使無法有效管控。	-套用 GCB 設定，或設定適當權組原則
1. 軟體資產類	1.1 作業系統	1.1.5 個人電腦或伺服器等資訊設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
1. 軟體資產類	1.1 作業系統	1.1.6 作業系統最高管理權限管制不當，有共用或浮濫設定的情形。	
1. 軟體資產類	1.2 套裝軟體	1.2.1 未購買妥適的套裝軟體授權或使用超過購買授權數量，致使可能違反智慧財產權，遭受廠商求償。	-軟體管制清單 -軟體授權資料 -資產管理工具

p.47

風險評鑑範例(cont.)

資產大類	資產小類	潛在風險事件	管控措施範例說明
3. 資料資產類	3.1 紙本文件	3.1.1 資訊系統相關技術說明、設定或規劃文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-如文件櫃上鎖存放
3. 資料資產類	3.1 紙本文件	3.1.2 業務資料或其它包含機敏資訊之文件，未依安全等級控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依資訊資產安全等級限閱或敏感等級進行管理
3. 資料資產類	3.1 紙本文件	3.1.3 業務資料或其它包含一般資訊之文件，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循或損害組織信譽。	-依資訊資產安全等級一般或公開等級進行管理
3. 資料資產類	3.1 紙本文件	3.1.4 包含個人資料之文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依個人資料檔案機密等級進行管理
3. 資料資產類	3.1 紙本文件	3.1.5 逾保存期限之紙本文件、表單或紀錄，未能適度予以銷毀，造成保存之文件與資料過多，致使發生遺失或外洩情況時，增加組織遭損害求償之風險或損害組織信譽。	-依文件與紀錄管理程序書進行管理

p.48

風險評估注意事項

- 相關資訊資產是否皆納入風險評估範圍？
- 風險評估之影響程度、發生可能性之判斷原則。
- 可能面對的潛在風險因子(威脅、弱點)
- 是否識別出可接受風險值？
- 針對高於可接受風險值之項目採取改善措施！

- 戴口罩
- 實名制
- 區域消毒
- 居家隔離
- 人潮分流
- 施打疫苗
- 罰款
- .....

p.49

風險處理-計畫

- 風險處理計畫是定義行動以降低無法接受的風險，和實施所需的控制措施以保護資訊的一種「合作文件」
  - 針對高風險(超過可接受風險)項目或認為應該要處理的項目
  - 避免偶發、特殊或超過組織處理能力的風險
  - 預估風險處理後之殘餘風險(若無法低於可接受風險即應重新擬定風險處理計畫)

p.50

風險處理-方向

- 接受殘餘(剩餘)的風險
- 避免風險
- 轉移風險
- 降低風險到可接受程度

p.51

可接受風險的等級

- 要達到完全的安全是不可能的
- 總是有殘餘的風險
- 甚麼樣程度的剩餘風險能為組織所接受

〔即時新聞/綜合報導〕嚇死人！新竹竹北大風來襲，路上的紅綠燈被吹倒，有車輛當場受到波及，所幸車主沒有大礙。

在東北季風、熱帶性低氣壓外圍環流的影響下，北部多處地區下起豪大雨，全台18個縣市也出現強風，「我們新竹竹北的風不是開玩笑的大」，有網友在臉書社團「爆廢公社」分享新竹竹北某處道路的行車紀錄器畫面，可以看到道路中央的紅綠燈突然倒下，硬生生直接倒在車子上，擋風玻璃被砸出裂痕，駕駛嚇到當場飆髒話，所幸無人傷亡，恐怖畫面讓原PO不禁驚呼，「這個風都可以演絕命終結站了」。

資料來源：自由電子報

p.52

結論

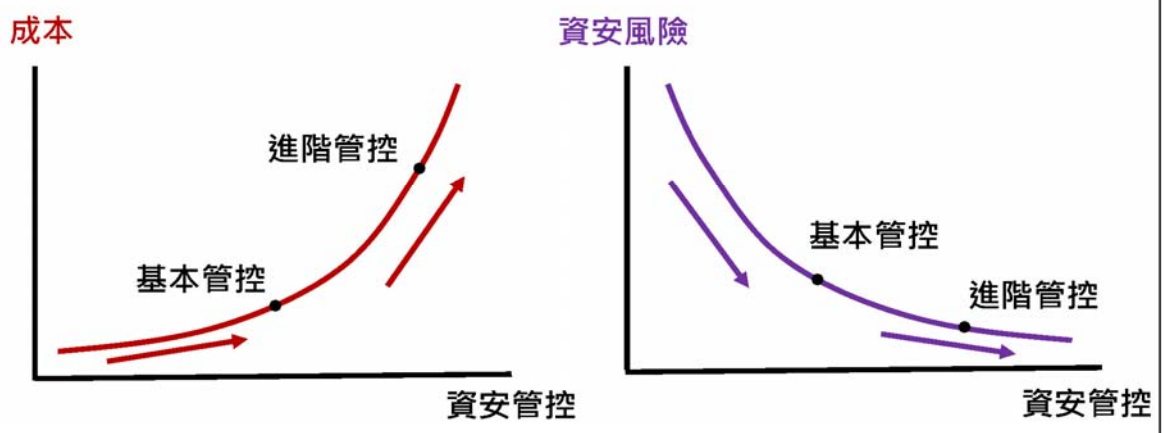
p.53

資安法的修訂與發展

- 修訂原則愈趨嚴格。
  - 資通系統認定包括電子郵件、目錄服務系統，資料庫、帳務處理。
  - 保留稽核事件紀錄至少六個月以上。
- 可能仍處於滾動式修正的狀態。
- 各級學校皆應積極應對與推動資安業務。

p.54

資安管控與成本考量



p.55

p.56

三、資通系統備份與回復演練實務

主講人/長榮大學 俞怡中組長

教育部國民及學前教育署
111年度校園資通安全專責人員知能研習

資訊系統備份與回復演練

長榮大學
圖書資訊處系統網路組
俞怡中

案例

學習歷程檔案硬碟被還原

https://www.youtube.com/watch?v=M-uMhLtQdX8&t=5s

公視新聞片庫遭刪除

https://www.youtube.com/watch?v=04DgxRp05nI&t=2s

備份很重要

備份資料是最後一道防線

業務營運持續

業務營運持續管理

- Business Continuity Management，BCM
- 遭逢天災或人禍等意外時，保護重要營運過程不受重大資訊系統失效或災害的影響，仍然可以繼續運作。
- 以風險管理為基礎，建立切合組織業務與目標的營運持續計畫，
- 依照適當的管理程序，定期測試與維護，使得營運持續管理不是紙上談兵而已，而是一套具體可行的方案。

業務營運持續管理

- 營運持續管理透過預防與復原控制措施的組合，將組織的衝擊最小化，把風險造成的影響降低到可以接受的等級。
- 而在規劃過程中，必須了解組織面臨風險發生的可能性與衝擊，能夠鑑別出影響組織成敗的重要業務，
- 維運這些重要業務時所需要的資產，包括：人員、軟硬體、行政資源、通訊資源等。
- 根據風險評鑑的結果發展營運持續策略，以決定營運持續的整體作法。

營運衝擊分析

- BusinessImpactAnalysis，BIA
- 找出關鍵業務、核心活動。
- 鑑別出在中斷事件發生時，那些業務、活動會影響到組織的運作
- 進而降低中斷發生之可能性，準備。
- 並建立緊急復原的機制。

BIAvs資通訊系統分級

- 資通安全責任等級分級辦法
  - 附表九資通系統防護需求分級原則
  - 鑑別系統等級：普、中、高
  - 識別核心系統 → 核心系統不限於【高】等級系統
- 界定RPO、RTO
  - 上級要求：主管機關、學校長官
  - 使用者需求
  - 系統重要性
  - 資料變更的頻率

業務流程/資訊系統	負責單位	負責人	復原時間目標（RTO）	資料復原時間目標（RPO）	重要分級	備註
學術網路連線	圖書資訊處(系統網路組)	[redacted]	4工作小時	N/A	高	
網域解析服務(DNS)	圖書資訊處(系統網路組)	[redacted]	4工作小時	24小時	高	
校務e化系統資料庫	圖書資訊處(軟體發展組)	[redacted]	4工作小時	6小時	高	
校務e化系統應用程式	圖書資訊處(軟體發展組)	[redacted]	4工作小時	8工作小時	高	
學生系統應用程式	圖書資訊處(軟體發展組)	[redacted]	4工作小時	8工作小時	高	
選課系統應用程式	圖書資訊處(軟體發展組)	[redacted]	4工作小時	8工作小時	高	
學校首頁	圖書資訊處(系統網路組)	[redacted]	4工作小時	24小時	高	

RPO

- Recovery Point Objective，可容許的最大資料損失量
- 與備份週期有關
- 數值要如何界定：
  - 與組織能夠承擔的風險
  - 擁有的資源
  - 資料異動的頻繁程度

EX

- 假設每天早上固定6:00備份，RTO為24小時

RTO

- Recovery Time Objective，讓系統重新上線的時間
- 系統回復所需的時間
  - 重新安裝?映像還原?
  - 設定檔案
  - 資料回復，最耗時的部分(有些認定RTO不含資料回復時間)

EX

- 上午8:00系統毀損後，在硬體設備沒問題的狀態下，下午2:00完成系統重建、資料回復，讓系統重新上限。RTO為6小時

MTPD

- Maximum Tolerable Periodof Disruption，最大可容忍中斷時間
- RTO把資料回復時間算入➔MTPD=RTO
- RTO不資料回復時間算入➔MTPD>RTO=RTO+資料回到時間

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間	資通系統分級
校務學生資料管理	校務行政系統	為本校依組織法執掌，足認為重要者	1.違反法遵義務：依個人資料保護法，應善盡個人資料保護責任。2.影響校務運作	24小時	中
官網	官網(已向上集中至成功大學)	為本校依組織法執掌，足認為重要者	影響校務運作	24小時	中
網域管理系統	DNS Server(已向上集中至區網中心)	為本校依組織法執掌，足認為重要者	影響校務運作	24小時	中
電子郵件系統	已向上集中至教育雲	為本校依組織法執掌，足認為重要者	影響校務運作	24小時	中
學生學習歷程系統	學生學習歷程系統	為本校依組織法執掌，足認為重要者	1.違反法遵義務：依個人資料保護法，應善盡個人資料保護責任。2.影響校務運作	24小時	中

業務持續演練計畫BCP

- 計畫
- 腳本
- 演練
  - 紀錄
    - 截圖
    - 紀錄時間
- 回復後測試與驗證
- 檢討

- 誰執行：
  - 自己做
  - 要求委外廠商、納入合約
- 每年至少Run一次

備份

備份種類

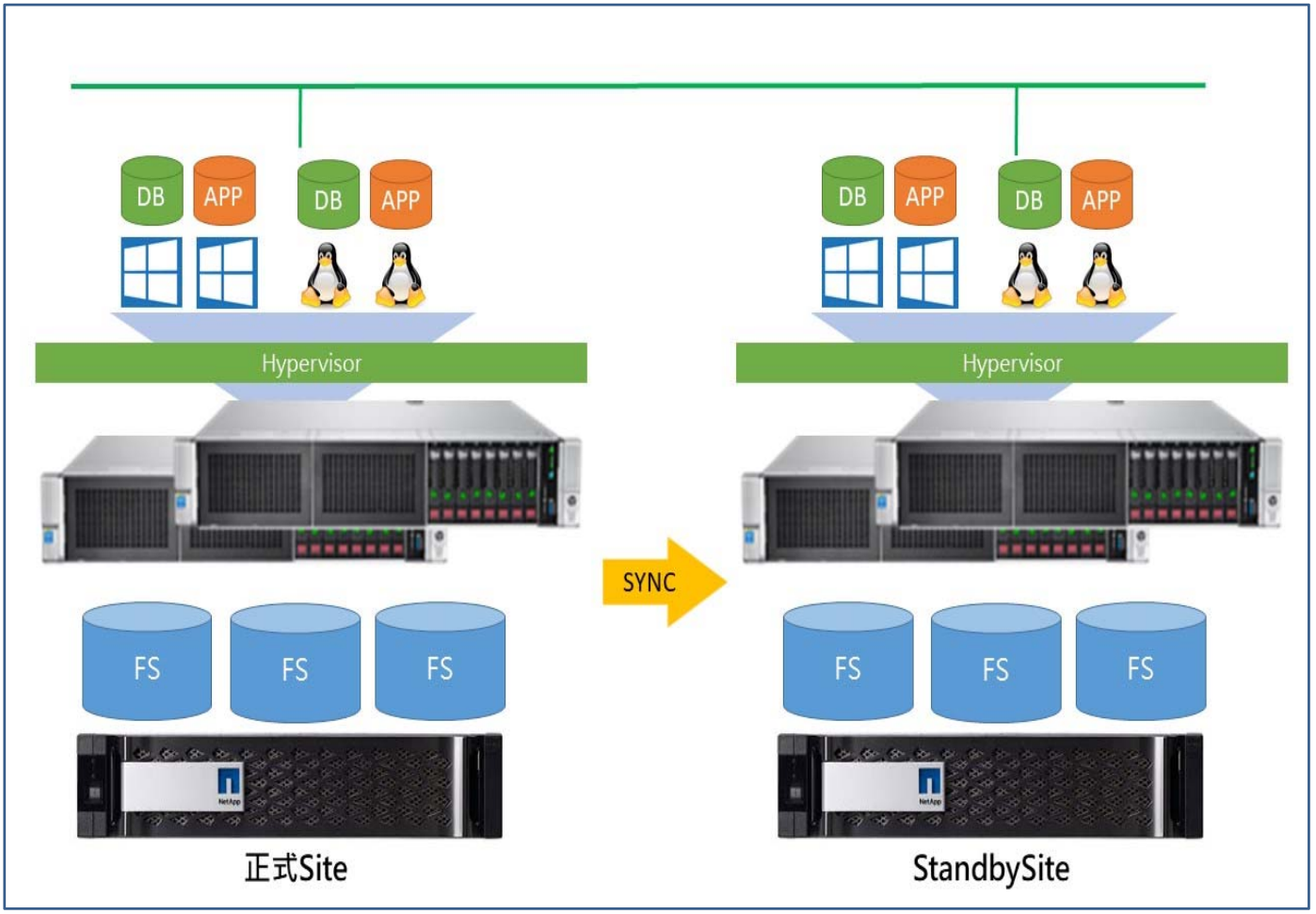
- **全部備份**（Full Backup）：即把硬碟或資料庫內的所有檔案、資料夾或資料作完整的複製。
- **增量備份**（Incremental Backup）：指對上一次完整備份或增量備份後更新的資料進行備份。
- **差異備份**（Differential Backup）：差異備份提供執行完整備份後變更的檔案的備份

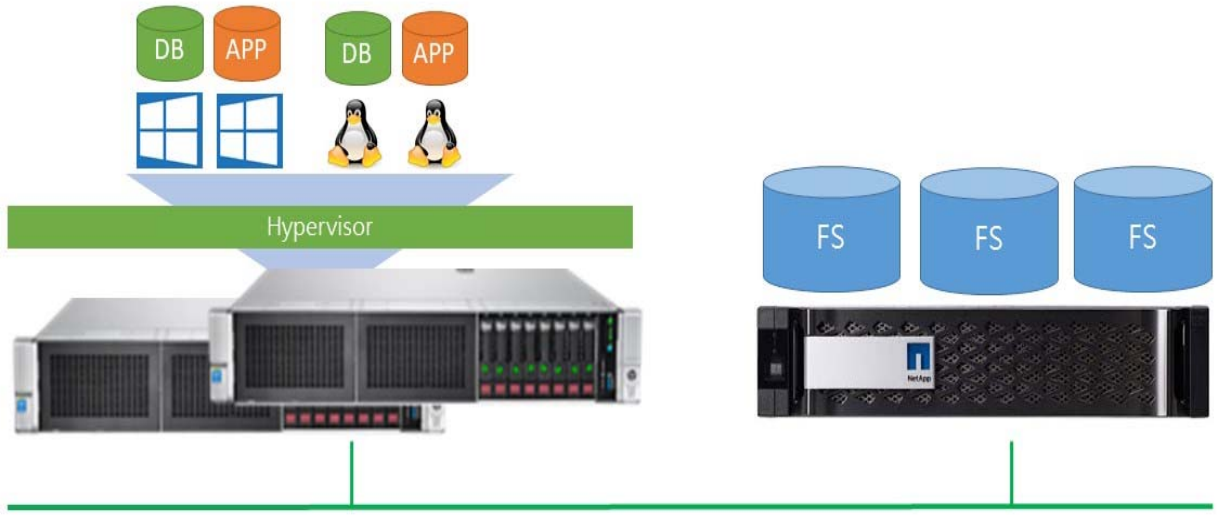
- **冷備份**（Cold Backup）：系統處於停機或維護狀態下的備份。這種情況下，備份的資料與系統中此時段的資料完全一致。
- **熱備份**（Hot Backup）：系統處於正常運轉狀態下的備份。這種情況下，由於系統中的資料可能隨時在更新，備份的資料相對於系統的真實資料可有一定滯後。
- **溫備份**（Warm Backup）：將備份系統已安裝組態成與當前使用的系統相同或相似的系統和網路執行環境，安裝了應用系統，定期備份資料。一旦發生災難，(1)直接使用定期備份資料，手工逐筆或自動批次追補孤立資料或(2)將終端使用者透過通訊線路切換到備份系統，恢復業務執行。

備份類型

- **線上備份**（On-line Backup）：需要及時還原的資料可以採用這總類型的備份，可以使用磁碟陣列、儲存區域網路、網路附加儲存或者是網路硬碟來保護資料安全。
- **離線備份**（Off-line Backup）：離線備份使用可離線媒體來備份，磁帶、光碟或是硬碟盒備份完成後離開備份媒體。

備份作業經驗分享


DB
APP
DB
APP
Hypervisor
FS
FS
FS
正式Site
SYNC
DB
APP
DB
APP
Hypervisor
FS
FS
FS
StandbySite



CJCU目前的作法

- 現況：

主要校務系統均虛擬化

- 複合式備份
  - +1的備份
- 異地備份
- 雲端備份
  - 壓縮、加密

類型	方式		週期
系統	Snapshot，匯出映像檔	每月完整備份	每月
程式碼	資料同步，壓縮備份	每月完整備份+每日差異備份	8個工作小時/24小時
檔案	資料同步，壓所備份	• 每日同步資料 • 同步後的資料：每月完整備份+每日差異備份	8個工作小時/24小時
資料庫	資料庫備份，複製到外部儲存	每日完整備份/每六小時差異備份	每六小時
網路設定	資料匯出	不定期	異動前或後
		每日	8個工作小時/24小時

系統備份

- 實體主機：
  - 磁碟系統備份工具
  - 第三方工具軟體
    - Ghost、Arconis、Veem、Nokivo....

- 全系統備份
- 快速還原

- 虛擬主機：
  - **VM工具、功能，快照**
  - **磁碟系統備份工具**
  - 第三方工具軟體
    - Arconis、Veem、Nokivo....

- 全系統備份
- 快速還原
- **快照匯出**

Hypervisor Crash!!

資料庫備份

- 資料庫系統工具
  - MS-SQL
  - MySql、MariaDB
- 第三方工具軟體
  - Arconis、Veem、Nokivo....

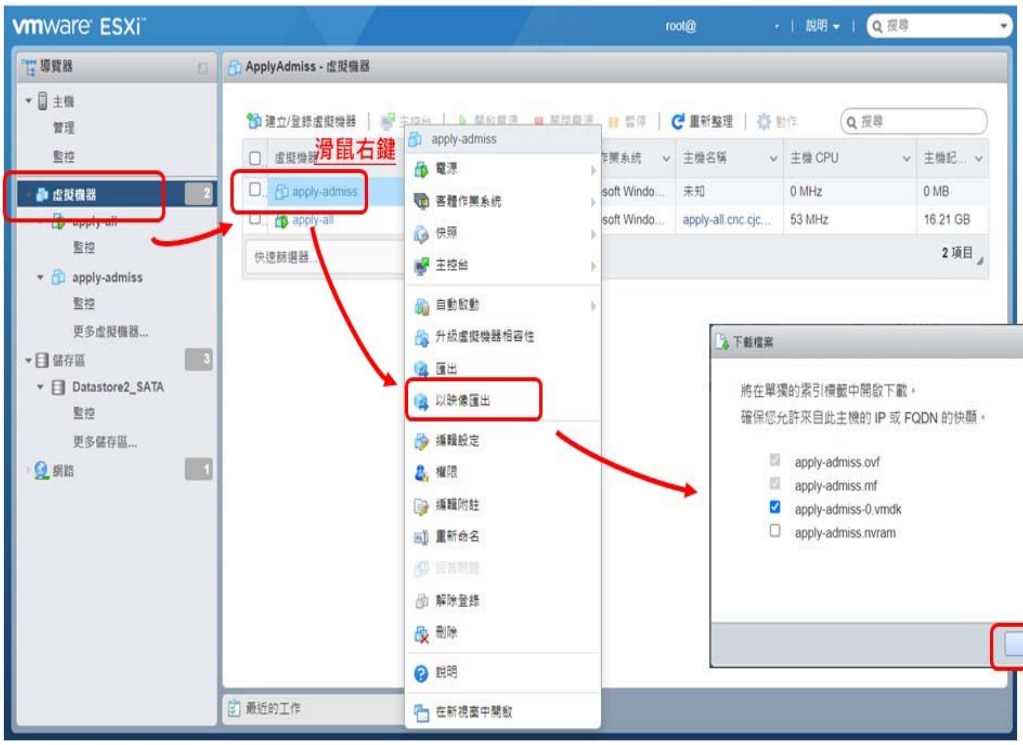
檔案系統備份

- 磁碟系統備份工具
- 第三方工具軟體

注意與提醒

- 磁碟系統備份
  - 硬體的設定?Raid5/6、還原模式?
  - 異地備份?
- 資料庫系統工具
  - 異地備份
- 檔案系統備份
  - 數量大、耗時
  - 耗費IO
  - 影響系統運作~

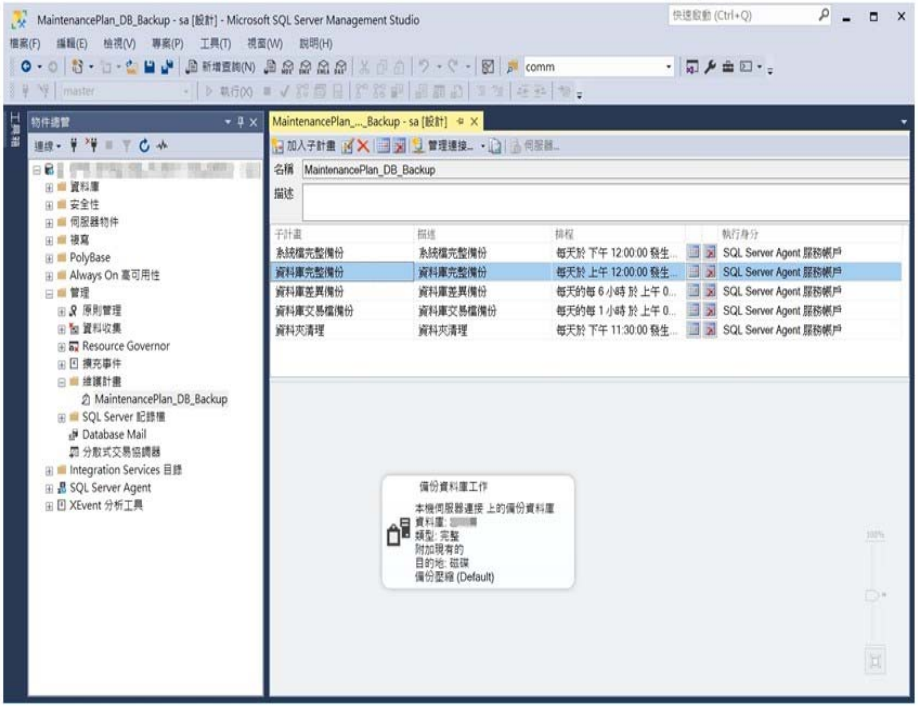
備份實務-VMimage



VM停機狀態下執行

備份實務-MS-SQL

- 完整+差異
- 六小時備份一次
- 定時利用工具軟體複製備份檔案



備份實務-MySQL

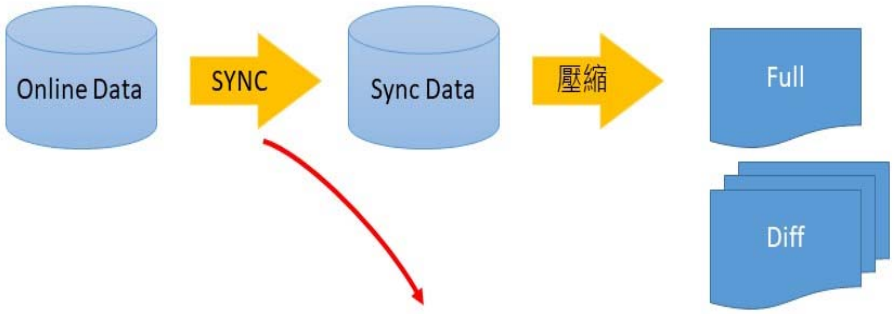
- 完整
- 建議在離峰執行
  - mysqldump -uusername –pXXXXXXXX DB_NAME > all.sql
  - Mysqlhotcopy –u username –p XXXXXXXX DB_NAME 目標目錄

目標目錄建議在不同硬碟

慘痛經驗

- 2008年，採用S牌備份軟體備份資料庫檔案
- 某次系統還原測試，發現所有資料都無法還原~~~
- 從此以後
  - 利用MS-SQL內建功能備份

備份實務-檔案系統



- 注意目錄結構
- 小檔案數量大、耗時
- 耗費IO
- 影響系統運作~

Linux檔案系統備份常用指令

- rsync
  - --bwlimit限制流量
  - --delete同步刪除
  - --exclude排除向
- 方法：利用script拆解目錄

```
cd /source_data
for dir1 in $(ls)
do
  mkdir –p /backup
  rsync -avug --bwlimit=1000 --delete --progress $dir1 /backup
done
```

#tar –zcvf /source_data /backup/backupfile.tgz

#zip –P password –D -9 backupfie.zip backupfie

營運持續演練的執行

- 用意
  - 驗證回復計畫
  - 驗證RPO、RTO有效
  - 驗證備份資料可用
- 週期
- 測試那一份
  - 異地的那一份~~~

營運持續演練回復測試驗證

- 系統功能驗證
- 資料庫資料驗證
  - 資料庫工具抽驗
- 檔案系統驗證
  - 檔案抽驗

- Microsoft SQLServer ManagementStudio
- phpmysqladmin
- HeidiSQL

營運持續演練**紀錄**的用意

- 紀錄時間
- 截圖

- 計時開始：演練開始
- 關鍵步驟的花費時間
- 驗證RTO有效性

- 紀錄
  - 關鍵步驟
  - 關鍵指令
- 建立緊急事件處理的SOP

Q and A

Thank You~~

四、社群運作議題研討

主講人/國立台南高商 黃耀寬校長

2022
9/19

111年資安輔導團社群運作議題研討

1

壹、社群運作計畫

2022
9/19

一、依據

教育部國民及學前教育署校園資通安全業務管理輔導團實施要點辦理。

二、目的

（一）鼓勵各校資安專責人員組成跨校專業學習社群，以資訊安全需求，實施校園資通安全業務專責人員訓練，提升校園資通安全管理人員之能力。

（二）促進資安專責人員經驗交流，以增進凝聚力與解決問題。

三、辦理單位

（一）主辦單位：教育部國民及學前教育署（以下簡稱國教署）。

（二）承辦單位：國立臺南高級商業職業學校。

四、辦理期程：自111年8月1日起實施。

五、成員對象：國教署所轄學校與特定非公務機關之資通安全專責人員。

2

壹、社群運作計畫

2022
9/19

六、實施方式

（一）**社群組成**：社群成員以地區資通安全專責人員為主要組成，以地區分配為原則，並以該地區輔導員為地區社群會議召集人，輔導團遴聘一位專家學者擔任社群諮詢委員協助設群運作。**本年度社群共分19組，每組需於111年8月1日至12月10日間辦理2場社群會議。**

（二）**社群議題**：學校網路安全、系統安全、應用程式安全、資安及個資管理、資料加密及身份認證授權、雲端安全及最新資安議題為主軸。

（三）**運作方式**：運作方式可包含資安實務觀察與回饋、主題探討、主題經驗分享、專題講座、標竿楷模學習、案例分析及專業領域研討等方式。

3

壹、社群運作計畫

2022
9/19

七、運作理念

（一）**自主規劃學習**：資通安全專責人員社群會議以合作方式共同進行探究或問題解決之學習社群。

（二）**提升校園資安防護成效**：透過資通安全專責人員經驗分享，討論各校資安防護作為，教學相長。

（三）**行政支持及資源整合協助**：社群會議時間資通安全專責人員得以公(差)假出席。

八、經費

本計畫所需經費由國教署下授國立臺南高商年度計畫經費支應。

4

參、社群運作議題分組討論

2022
9/19

一、社群成員聯絡方式

二、社群議題與運作方式

三、社群運作計畫

四、社群運作計畫範例

25

2022
9/19

感謝聆聽

26

五、委外合約的訂定與管理

主講人/崑山科技大學 徐國鈞副教授

大綱

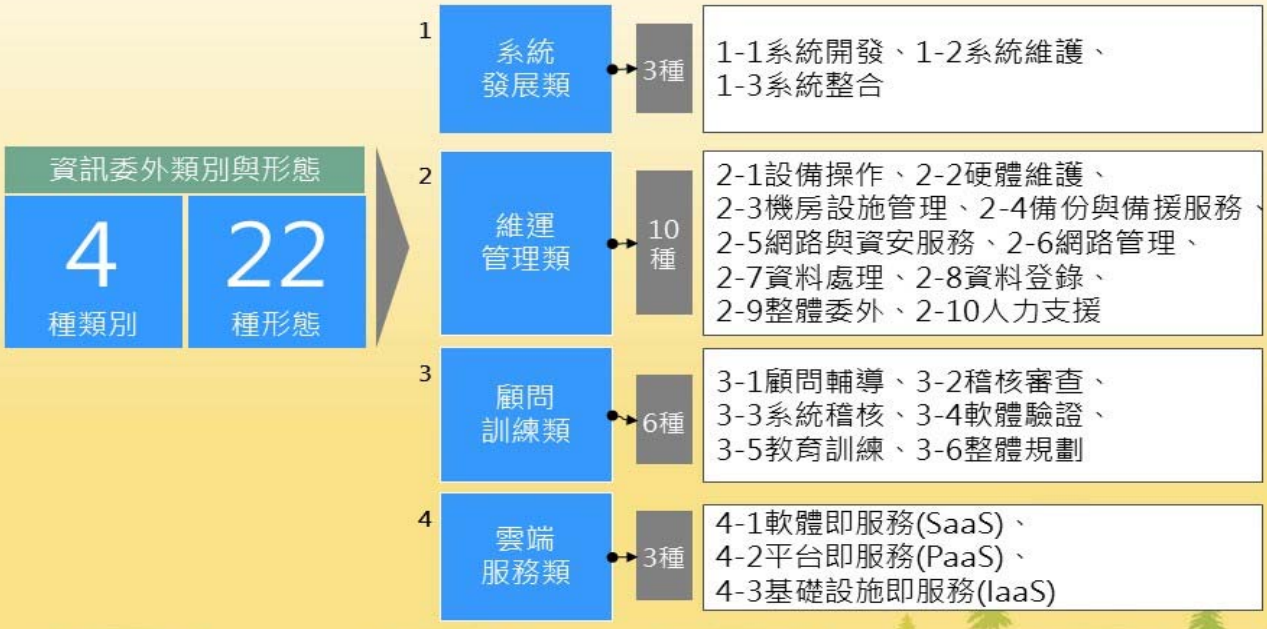
- 資訊委外類別與形態
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- 注意事項與常見缺失
- Q&A

大綱

- **資訊委外類別與形態**
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- 注意事項與常見缺失
- 政府資訊委外資安檢核表
- Q&A

資訊委外類別與形態

委外作業區分為：系統發展類、維運管理類、顧問訓練類及雲端服務類等 4 類，共 22 種作業形態。



5

系統發展類

1-1 系統開發

- 依機關規格需求，開發一套應用系統程式，並於開發完成後，進行測試、訓練、製作技術文件及上線之專案
- 其作業範圍包括新系統開發設計、舊系統汰舊換新、舊系統架構更改、系統移轉訓練及系統保固等工作

1-2 系統維護

- 應用軟體之維護服務與功能增修，包括軟體版本更新、應用程式錯誤與漏洞之排除及更正性服務等

1-3 系統整合

- 提供一套完整解決方案(Total Solution)之資通系統，涵蓋範圍包含整合網路、通訊及硬體設備，加上訂製軟體(Tailor-made Software)或套裝軟體，及新資通系統教育訓練等項目

6

維運管理類(1/5)

2-1 設備操作

委由委外廠商派員前來操作其資源設備，並依一定程序處理產出報告

2-2 硬體維護

- 在設備保固期滿後，為維持原硬體功能與正常運作，提供定期維護合約工作，統稱為硬體維護
- 購買硬體設備(如系統主機、終端機、工作站、個人電腦、印表機、繪圖機及連線設備等)於保固期限內，應由原供應廠商依購買時契約約定，提供各項售後服務，非屬硬體維護範圍
- 惟部分機關考量經常門預算編列不易，將設備維護費用一併納入採購案中，保固期限由1年延長3~5年不等

維運管理類(2/5)

2-3 機房設施管理

- 機房設施管理指電腦設備、機房設施及機房相關業務，運用外界提供之專業技術，協助執行設施管理任務
- 包含管理制度之規劃與執行，提供運作環境與軟硬體設備之規劃或管理等

2-4 備份與備援服務

- 備援指機關透過本地端備用之儲存空間與設備、遠端備用儲存空間、設備與網路，保存重要資訊資產與恢復系統正常作業。備援服務指委廠商提供資料儲存空間、主機運算能力、網路頻寬及備援場所(含辦公場所)等方式，協助機關保存重要之資訊資產與恢復正常作業
- 資訊委外之備援服務可有效降低機關資通系統無法運作之風險與成本，同時可降低災害復原所投資成本，減低因人員操作疏失造成資料遺失，或系統被攻擊造成系統網路無法運作等風險，並可縮短系統回復作業時間

維運管理類(3/5)

2-5 網路與資安服務

- 網路服務包含提供機關外部網路連線服務、私有網路服務、其他網路加值服務(含系統與應用)
- 資安服務則包含「資安健診服務」、「資安監控服務」、「弱點掃描服務」、「滲透測試服務」、「社交工程郵件測試服務」、「行動應用App檢測」及「應用程式原始碼安全檢測」等服務

2-6 網路管理

- 網路管理指監控機關內部網路活動，包含路由器、交換集線器、防火牆管理與網路流量分析及網路蠕蟲與病毒攻擊防護等服務，並提供問題診斷與產生各類網路活動統計資料，以協助機關之網路管理者維持網路正常運作

維運管理類(4/5)

2-7 資料處理

- 資料處理指協助電腦系統線上作業與批次作業之運作，機關將需要以電腦處理之工作，全部或一部分委由委外廠商以其自有設備，代為規劃、設計及處理，或委由委外廠商派員前來操作機關之設備，按一定程序與程式處理產出資料者

2-8 資料登錄

- 資料登錄指將機關之書面或微縮影片等原始文件，資訊委外以人工作業方式輸入、校對、彙整及轉換，產出電腦可處理之電子媒體檔案者

維運管理類(5/5)

2-9 整體委外

- 將全部或部分資通系統之整體運作，包含人員、環境設備、機器設施、作業程序、管理制度及其他相關或延伸之資訊委外管理
- 系統管理服務之方式可以是機關自備設備，由委外廠商派提供管理服務，或設備與管理服務皆由委外廠商提供，機關擁有使用權等不同之方式
- 工作內容包含整體資訊管理制度規劃與建置，擬定資通系統運作方式與執行，由機關訂定服務水準指標，以做為執行之要求與改善依據等工作

2-10 人力支援

- 依機關所需技術能力採人力派遣或業務承攬方式供機關使用

11

顧問訓練類(1/2)

3-1 顧問輔導

- 在特定主題範圍內，進行民眾需求調查、相關資訊法規制度研擬、新技術導入可行性、資訊技術服務及訂定專案相關採購案件之規格研擬等，如ISMS導入

3-2 稽核審查

- 為驗證管理程序或資通系統符合特定規範或標準而進行之專案，如政府機關資訊安全管理系統(ISMS)第三方驗證

3-3 系統稽核

- 為確保資訊單位內部作業資安控制，能有效建立並長期維持一定品質，協助評估並稽核資訊單位資安作業管制標準

12

顧問訓練類(2/2)

3-4 軟體驗證

- 透過一連串具稽核功能之特殊程式，驗證資通系統運用與功能是否正確與符合原始需求，通常由公正第三方執行

3-5 教育訓練

- 協助機關於業務資訊化過程中，有關各階層人員常態性或專案性資訊教育訓練之規劃與執行。訓練範圍可包含電腦軟、硬體技術、資訊管理技術、行政管理技術及資安等專業領域技術等

3-6 整體規劃

- 在政府整體業務、跨機關業務或機關業務範圍內，進行政府整體、跨機關業務或機關整體資通服務需求彙整、網路與資訊技術架構規劃、訂定相關系統間資訊交換規格及相關配套措施之規劃等

13

雲端服務類

4-1 軟體即服務(Cloud Software as a Service, SaaS)

- 透過網際網路提供軟體的一種服務模式，廠商將應用軟體統一部署在雲端伺服器上，客戶可透過瀏覽器使用廠商提供的應用軟體服務，使用者不用再購買軟體，且無須對軟體進行更新維護，服務提供商會全權管理和維護軟體，例如：Google DOCS、Microsoft Office Live、Facebook及Saleforce等。部分政府機關或企業使用Google Gmail即為SaaS的一種服務模式

4-2 平台即服務(Platform as a Service, PaaS)

廠商透過網際網路將雲端服務平台，例如：儲存設備、資料庫等開放給使用者，使用者可以自行部署應用程式，自行使用程式語言使用服務平台，但無須管理或控制雲端設備，包含網路設備、伺服器，例如：Google App Engine、Windows Azure及AMAZON AWS:S3 (Simple Storage Service)等

4-3 基礎設施即服務(Infrastructure as a Service, IaaS)

廠商透過網際網路，以虛擬主機方式提供完整的作業系統、資料庫存取，如Flexiscale、AWS (Amazon Web Services)等

14

大綱

- 資訊委外類別與形態
- **資訊委外資安策略**
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- 注意事項與常見缺失

- Q&A

資訊委外原則(1/5)

- 委外辦理資通系統之建置、維運或資通服務之提供，應考量廠商之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之廠商，並監督其資通安全維護情形
- 涉及國家機密業務不宜委外，惟若經評估仍須委外辦理，則執行廠商之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境
- 限制使用危害國家資通安全產品
- 委外廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證
- 委外廠商應配置充足且經適當訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員

資通安全專業證照請參閱行政院資通安全會報
之資通安全專業證照清單

16

資訊委外原則(2/5)

- 委外廠商辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施
- 若得複委託，機關應要求委外廠商對複委託廠商進行管理，包含設定一致的資安與個資保護目標、執行風險評鑑以達成該資安與個資保護之目標。機關甚至可與委外廠商協商，由委外廠商提出該些複委託廠商的監控管理報告
- 受託業務包括客製化資通系統開發者，委外廠商應提供該資通系統之第三方安全性檢測證明
- 該資通系統屬機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，機關應自行或另行委託第三方進行安全性檢測
- 涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明

資訊委外原則(3/5)

- 委託關係終止或解除時，應確認委外廠商返還、移交、刪除或銷毀履行委託契約而持有之資料(含委外廠商交付複委託之資料)
- 委託機關應定期或於知悉委外廠商發生可能影響受託業務之資安事件時，以稽核或其他適當方式確認受託業務之執行情形
- 具敏感性或國安(含資安)疑慮之業務範疇，於招標文件載明不允許投審會公告之陸資資通服務業者參與
- 應建立資安管理之事前規劃、事中招標及事後執行維運機制

資訊委外原則(4/5)

- 視需要以顧問導入，考量資安需求，並經由顧問標、規劃標、建置標及監督審驗標等程序辦理
- 擴大委外經濟規模效益，各機關得整合其他相關需求一次委外，朝最適合之標案規模辦理
- 重要資訊專案得視需要區分顧問標、規劃標、建置標及監督審驗標辦理
- 應透過RFI或RFC等方式，廣納各界意見，據以訂定合宜的資安需求(RFP)規格：
  - 公開徵求資訊(Request For Information，RFI)
  - 徵求修正意見(Request For Comments，RFC)
  - 徵求建議書文件(Request For Proposal，RFP)

資訊委外原則(5/5)

- 為提升資通安全服務品質，應用軟體宜與硬體分開招標，並先行辦理應用軟體招標建置，如需合併於同一標案辦理，應由各機關視個案性質訂定應用軟體與硬體經費比例上下限，列入計價，納入評選計分，遴選出能提供最佳整體解決方案之廠商
- 各機關應將應用軟體品質保證計畫列為委外必要工作項目，並要求廠商依照主管機關訂定之標準或規範發展系統，確保軟體品質與政府資訊的流通互用
- 廠商或團隊人員通過軟體相關資格評鑑或管理能力認證者，得列入評選加分項目
- 為確保委外服務績效，各機關應落實監督、稽核及管控服務水準，協助廠商溝通協調事宜，確保服務績效

資訊委外策略(1/2)

- 以政府機關採購招標觀點而言
  - 自行建構、採購硬體或訂製軟體轉為購買資通服務
  - 從開立軟硬體規格轉為設定服務水準(Service Level)
  - 從短期與一次性購買關係轉為中長期夥伴關係
  - 從重視價格轉為重視價值
  - 從解決個別問題轉為購買整體解決方案

資訊委外策略(2/2)

- 各機關得視委外個案性質決定，將資通安全需求所需費用列入成本分析計價項目

  例如：Web資安檢測服務與報告
- 規劃過程
  - 將機關的資安規範與對廠商(含複委託廠商)資安要求納入【契約書或RFP】
  - 將【資通安全需求】納入RFP中，列為委外需求與評比必要工作項目
- 執行過程

  要求廠商遵循主管機關訂定之標準或規範執行，並提供可行建議方案，確保委外作業安全
- 因應【個資法/施行細則】之施行
  - 廠商(被委託機關)增加多項義務與賠償責任，建議機關在估算成本時應一併考量
  - 委託機關必須負起「監督」職責

最近行動應用App的開發與運作越趨興盛，規劃委外安全時也可以考慮加入”工業局行動應用App基本資安自主檢測 “的相關要求。

大綱

- 資訊委外類別與形態
- 資訊委外資安策略
- **資訊委外風險說明與風險處理原則**
- 資訊委外各階段資安要求
- 注意事項與常見缺失

- Q&A

常見資訊委外風險

策略面

對於整個營運活動中有相當重要的影響力，特別是對於資訊作業委外服務內容之形態、範圍及管理方式等策略是否妥適，會直接或間接影響到機關資通安全

治理面

在合約關係生命週期中，對廠商(含複委託)缺乏管理，可說是資訊委外安全的主要風險。政府機關與廠商之間沒有定義適當的管理模式，可能增加資訊作業失誤、遵循性風險、作業風險及財務風險

需求面

不適當的需求規劃或描述可能對廠商可順利地執行服務產生衝擊，長期可能導致政府機關在營運、財務、法律及聲望上的問題，應該在計畫階段就必須考量資通安全需求，並納入需求規劃

合約面

未能完整涵蓋合約需要被管理的各種關係，即不完整的合約是整個合約關係中最大的風險。例如忽視款項支付細節、要求廠商不切實際的服務水準、缺乏合約終止規範與任何智慧財產權、個資等規範

廠商面

未適當選擇廠商可能出現履約期間廠商無法確實履行義務的風險，在簽訂合約前應採取適當的廠商盡責調查措施，以降低各類風險，使廠商能有更好的長期的履約能力與穩定性

參考CNS 27014資訊安全治理標準，獲得更多對治理面概念

24

機關常見的資訊委外風險

- 機關內因跨專案間之統合協調不佳，導致單一專案執行成效不彰
- 廠商因自身資通安全管理疏失，發生資安事件，連帶影響委外機關資通安全
- 委外機關需求無法確定或頻於修改，影響專案執行進度與驗收期程

25

常見資訊委外風險處理原則

以下為降低委外風險之主要原則，執行這些原則可以有效降低可能的風險與衝擊，然而風險依然存在，階段滾動進行風險評估仍然是必要的

- 多樣化來源策略，以避免過度倚賴或鎖定特定廠商
- 建立委外廠商管理程序
- 建立委外廠商的管理模式
- 建立委外廠商管理組織
- 預先規劃廠商的技術與能力需求
- 使用標準文件與範例
- 制定明確的需求
- 適當的選擇廠商
- 在合約草擬過程中涵蓋生命週期中所有相關項目
- 決定適當的資安控制措施
- 建立服務水準(SLAs)
- 建立執行水準協議(Operating Level Agreement, OLAs)及支撐合約(Underpinning contract)
- 建立適當的廠商績效或服務水準監控與報告機制
- 建立廠商獎懲模式
- 在合約生命週期中建立適當的廠商關係管理
- 檢視合約與服務水準
- 要求廠商風險管理
- 以政府機關政策檢視廠商法規遵循性
- 實施廠商內部控制評估
- 規劃與管理合約關係結束
- 訂定軟硬體處置規定

26

大綱

- 資訊委外類別與形態
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- **資訊委外各階段資安要求**
- 注意事項與常見缺失

- Q&A

計畫作業階段(1/8)

1	計畫作業
2	招標
3	決標
4	履約管理
5	驗收
6	保固作業

- 計畫作業階段涉及大量資訊蒐集與分析，評估個案之委外可行性與委外風險，以確認是否進行委外。當確認辦理委外時，機關應識別所有相關資安要求事項，而此部分將是委外作業中相對重要且複雜之環節
- 當機關確認辦理委外但於進行規劃活動前，宜優先確認工程會政府電子採購網中與資訊作業有關之採購項目，與經濟部工業局資訊服務採購網中與資安服務有關之採購項目。若無合適者，可參考其共同供應契約自行依需求辦理招標作業

計畫作業階段執行作業有3大重點：

- **資訊委外可行性分析**
- **資訊委外專案編成**
- **資訊委外資安需求識別**

28

計畫作業階段(2/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1.資訊委外可行性分析(1/3)

資訊委外可依「委外之作業形態不同、規模大小及專案機敏特性」參考下列步驟進行分析：

- 篩選適合委託辦理之業務項目

  就各預定委外業務項目檢討分析具資安作業能量之民間辦理部分，積極探詢可受委託辦理民間團體之參與意願，以確定該項業務委託民間辦理之資通安全可行性無虞

- 進行成本效益分析

  政府機關在決定業務委託民間辦理前，除一般成本分析外，宜將資通安全列入成本進行效益分析，以期確實有效執行。分析內容應包含「量化指標」與「非量化指標」

29

計畫作業階段(3/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1.資訊委外可行性分析(2/3)

– 量化指標

➢ 應考量：人力、時間、資產維護及資安保護等

◆專案自行開發之人事成本(包括薪資、保險及退休等費用)

◆專案自行開發之時間成本(包括業務需求時程與機關自行開發時程)

◆委外專案資訊設施資產成本(如設備、用地、建築等購置及維持成本)

◆因資安所增加之費用(如委託第三方資安弱點掃描，交付軟體資安驗證等成本)

◆大型(複雜)系統增加的監督人事成本(如委託第三方定期與不定期督導委外業務執行成本與委外業務成效評估成本)

◆如進行案件複雜度較高者，可聘請資安、財務及法律等專業顧問或專業機構依工程會所頒相關作業手冊協助辦理，其辦理程序應依採購法與評選及計費辦法等相關規定辦理

30

計畫作業階段(4/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1.資訊委外可行性分析(3/3)

– 非量化指標

➢ 應考量：受服務者滿意度與信賴度

◆對機關外部客戶之可用性提升，評估其可行性

◆對機關外部客戶之安全信賴度提升，評估社會成本效益

- 評估資訊委外資安風險與對策

  機關應確認委外資安風險評估之範圍，經由風險評估過程，得以較準確地將有限之成本與時間聚焦於風險熱點，對各階段應具備之防護措施亦有初步了解。而該風險評估與處置對策可做為委外契約協議輸入之一。但當所識別之資安風險無法降低至可接受風險等級時，則不宜取得此項產品或服務

31

計畫作業階段(5/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

2. 資訊委外專案編成

- 當確定進行委外後，機關首要任務則為指派適任之專案負責人。此人應對資訊委外專案性質或內容有充分了解之能力，並能對資訊委外專案所衍生之風險有控制與處置權力，故其位階不宜過低
- 在專案規劃期間，專案負責人除應了解委外產品與服務本質外，可視委外性質與規模諮詢與邀請採購(總務)、法務、會(主)計、業務、資訊及政風等單位人員，參與在資通安全、資訊技術、法規遵循、服務水準、專案細項預算及選商需求分析等工作
- 如因員工工作負荷過重或技術能力不足，宜遴聘外部顧問予以輔助。如因系統複雜或技術層次較高，則宜採取兩階段方式作業，即先委外進行系統規劃工作，再進行系統發展與建置工作

32

計畫作業階段(6/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3. 資訊委外資安需求識別(1/3)

當機關選派適當之專案負責人後，下一步則需了解與分析該資訊委外專案應有之資安要求事項。此分析之完善程度將深遠影響該資訊委外專案之成敗，機關不得不嚴謹視之

- 建立資訊委外資安策略

  應針對資訊委外個案，建立其資訊委外資安策略，包含：

  - 識別欲取得之產品與服務，包含其涉及範圍、使用對象、利害關係人、類型及本質評估資安負責人的專業能力
  - 上級機關與機關管理階層對資訊委外產品或服務之動機、需要及期望
  - 機關管理階層對配置必要資源之承諾
  - 持續因應資通安全風險之管理程序
  - 將採用之資安管理架構
  - 委外廠商評選準則項目
  - 用以定義下列項目時之高階資通安全要求事項
    - 移轉所採購產品或服務至不同資訊委外廠商之移轉計畫。
    - 資安變更管理程序。
    - 資安事件管理程序。
    - 遵循性監視與執行計畫。
    - 終止產品或服務獲取之終止計畫

33

計畫作業階段(7/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3.資訊委外資安需求識別(2/3)

- 識別委外廠商之限制

  在為個別資訊委外專案建立資訊委外資安策略後，此階段機關亦需視資訊委外產品或服務之本質，考量委外產品與服務是否涉及國家機密、影響國家安全或受世界貿易組織(WTO)政府採購協定之規範，以限制投標廠商或其人員之資格

- 邀請廠商提出對應措施方案

  機關辦理資訊委外作業時，可針對各項資通安全需求，於規劃時徵詢委外廠商提供相對應之建議措施，以符合我方最大利益，並經由RFI或RFC等方式，廣納各界意見，據以訂定實際可行之RFP；另為達到資訊委外透明與公平公開，重要資訊專案委外於正式公告招標前，亦可綜合RFI或RFC文件所蒐集之資料，研判各家廠商於資通安全防護做法與概略之經費需求

34

計畫作業階段(8/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3.資訊委外資安需求識別(3/3)

- 建立資訊委外資安管理計畫

  機關應依據資訊委外資安策略與來自廠商之回饋內容，對委外個案應具備之資安需求項目進行詳細分析，並將之具體化為資訊委外資安管理計畫，以提供擬訂委外契約書、RFP及 SLA之依據，確保資安要求之全面與一致性，應包含(但不限於)下列項目：

  - 所規劃取得產品或服務之規格
  - 於委外專案期間需存取之資訊資產
  - 委外廠商之資訊資產分類分級與資通系統防護需求分級等相關資安控制措施，至少應採取與機關資安管理水平相同之方法
  - 各階段應有之角色與責任
  - 依委外產品或服務之本質，確認過往同質委外專案資安事件之矯正預防措施，以做為本次委外資安強化之參考依據
  - 機關所屬管轄權內之法律法規要求事項，以及於選任委外廠商期間，應審查可能約束委外廠商之法律法規
  - 為可能取得之產品或服務指派特定資安角色與責任
  - 針對可能取得之產品或服務，機關能與潛在廠商分享之資訊

35

招標階段(1/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 本階段旨在遴選適宜之委外廠商，其資安管理熱點著重在RFP撰寫之完整度、評選準則中之資安要求符合度及在選商期間雙方資訊交換之安全性，本階段以招標過程之時序為架構，敘述各作業應注意之資安事項

招標階段執行作業有5大重點：

- **委外廠商評選準則之定義與實作**
- **保密協議書準備與簽訂**
- **招標文件之制定與發布**
- **服務建議書之蒐集**
- **服務建議書之評選**

36

招標階段(2/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

1. 委外廠商評選準則之定義與實作

- 招標階段之首要作業，需依資訊委外資安策略所定義之委外廠商評選準則項目與資訊委外資安管理計畫內容，定義並實作委外廠商評選準則，其應包含(但不限於)下列各項：
  - 委外廠商對招標文件定義之資安要求事項接受度
  - 委外廠商之資安能量
  - 委外廠商允許機關或經授權之第三方稽核，以確認所定義資安要求事項之遵循性
  - 先前由機關或不同委外廠商運作或製造之可能採購產品或服務之移轉計畫完整度
  - 於委外關係終止時，終止計畫之完整度
  - 委外廠商對其產品或服務之容量管理機制
  - 委外廠商之財務優勢
  - 委外廠商位置與提供產品或服務之位置，機關應特別考量此因素，以利識別機關與委外廠商間法律法規差異所造成之所有潛在法律法規風險，並確保適用於委外廠商之法律法規義務，在資安方面不致對委外關係協議有不利衝擊。此外，亦可評估諸如當地犯罪率或地理議題等環境威脅

37

招標階段(3/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

2. 保密協議書準備與簽訂

- 當選商過程中存在資訊資產移交(如資訊交換)，機關應備妥保密協議書，並於交換任何可能與採購產品或服務相關之資訊前簽署。若前述情況不允許，機關應定義得以交換之資訊類別或內容，並取得資訊擁有者同意，以避免過多或不必要機密資訊被揭露

38

招標階段(4/8)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

3. 招標文件之制定與發布(1/3)

- 招標文件包含項目眾多，機關在制定相關文件時，可參考工程會網站中「政府採購」→「招標相關文件及表格」連結下之相關文件與表格，包含「投標廠商聲明書範本」與「投標須知範本」等。而下列僅提出與資安相關內容之建議，包含採購契約、RFP及SLA等之撰寫注意事項
  - 採購契約
    - 係機關與委外廠商間就資訊委外契約所為之詳細規定。機關在借重廠商之專業資源處理自身資訊業務時，除要求廠商遵守相關法律法規(如個資法)外，更須明示廠商義務與責任，以降低機關須負擔之風險
    - 制定契約時，應衡量其公平性，並尋求機關內法務單位或具備資訊與法律專業之顧問協助，以免於契約履行出現紛爭時與廠商陷入僵局，甚至產生對己不利之狀況
    - 針對資訊委外，機關可參考工程會網站中「政府採購」→「招標相關文件及表格」連結下載最新版本，並依所識別之資安需求與限制，酌予修改

39

招標階段(5/8)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

3. 招標文件之制定與發布(2/3)

- 建議書徵求文件(RFP)
  - 徵求建議書文件(RFP)為廠商執行委外作業之需求依據，其中應明定委外廠商之責任與義務，而針對資安管理部分，機關應特別謹慎訂定相關規範要求，或要求投標廠商於投標之服務建議書中提出相對應做法。在此建議機關可依下列項目進行，以研擬妥適之RFP
    - ◆ 確認專案目標
    - ◆ 界定專案範圍
    - ◆ 掌握業務與資通系統現況
    - ◆ 蒐集現行資訊軟硬體作業環境
    - ◆ 釐訂需求內容
    - ◆ 制定服務水準指標
    - ◆ 規範交付項目與內容
    - ◆ 訂定專案管理需求
    - ◆ 訂定評選標準與方式
    - ◆ 參考機關契約條文、資訊服務採購相關手冊與指引

40

招標階段(6/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

3. 招標文件之制定與發布(3/3)

- 服務水準協議(SLA)
  - ➢ 在資訊委外作業中，「委外服務水準之管控」被視為委外服務成敗重要因素之一，於管控作業上，藉由明確服務項目與水準指標，建立清楚管理制度，確保服務水準，建立考核與輔助措施，有效掌控問題發生與處理過程結果，所有使用者在選擇服務水準上，享有符合服務水準規範之一致服務
  - ➢ 對於資訊委外作業而言，資安相關之服務水準管控以系統可用率、安全性及稽核作業為3大指標：
    - ◆ 系統可用率常被簡單地描述成系統在整個時段中，必須維持正常作業之特定時間，或者是可定量控管系統當機時間。對於使用者而言，系統可用率，常是影響他們對服務水準評量最重要因素，而系統可用率高低好壞，直接影響到使用者生產力與政府機關整體資訊管理作業。基於系統資安考量，可訂定系統可用率指標，以確保系統維持一定服務水準
    - ◆ 資訊管理作業，常藉由系統安全、通信安全、人員管制及作業管制等方式達成安全性目標，透過這些方式整合，確保資通系統(包含軟體、硬體、防火牆、資料庫及電信通訊等)之機密性與可用性，同時也可做為評斷政府機關現行作業整體安全性指標
    - ◆ 於服務水準協議中，提升績效並符合需求，必須持續不斷改善管理各項相關作業，因此稽核作業被視為是重要管理工具。如發現不符合事項時，訂定矯正或預防措施完成時限，以利追蹤稽核作業服務水準

41

招標階段(7/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

4. 服務建議書之蒐集

- 蒐集由可能之委外廠商所提交回應招標文件之服務建議書，並依委外廠商評選準則評選之。而對於非客製化服務之取得(例如ASP服務)，機關應驗核委外廠商所提供之資安管理、控制措施、實作及服務等級皆符合委外廠商評選準則

42

招標階段(8/8)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

5. 服務建議書之評選

- 招標之最後一步即對委外廠商所提出之服務建議書進行評選。但在評選服務建議書前，機關應選擇合格適任之評選委員，其中應考量其學經歷、相關領域實務經驗及利益迴避等條件，並向其強調有關遵守保密原則之事宜，具備適當評選人員後，評選內容分為2個重點，其一為投標廠商資格，另一個則為整體產品或服務之內容
  - 投標廠商資格
    - 機關應對投標廠商之背景資格限制進行嚴格審核。必要時，審核欲採購產品或服務所涉及之供應鏈廠商背景資料
  - 整體產品或服務內容
    - 機關應考量整體產品或服務供應鏈中有較佳透明度，且保證符合機關於招標文件中所定義之資安要求事項者

43

決標階段(1/2)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 決標階段之重點即與得標廠商進行簽約作業，即機關與委外廠商雙方依據招標文件與廠商回應之服務建議書進行最終協議
- 於雙方協議並確定契約內容後，即進行簽約作業。簽約程序中應確認廠商是否完成保密切結與完成專案編組等事宜，例如：廠商在簽約前須依據招標文件之規定，提出各項保密切結，並依據規定訂定資通安全防護計畫，廠商專案組織人員之遴選與質量需考量重新調整，並賦予適當職掌，以利承辦單位依據合約執行各項查核，並做成紀錄
- 相關文件要求：
  - 得標廠商與其專案工作成員應簽訂保密約定至少1式3份，並於指定期限內送交甲方1份備查
  - 得標廠商應就專案建置過程中之文件資料與人員管控訂定保密安全規範，並應於契約生效日起一定期間(例如：2週)內送交甲方，其後如有不足，並應適時修正之

44

決標階段(2/2)

1. 計畫作業
2. 招標
3. **決標**
4. 履約管理
5. 驗收
6. 保固作業

- 最有利標之注意事項
  - 以最有利標辦理之委外業務，應依招標文件所規定之評審標準，就廠商投標之技術、品質、功能、商業條款及價格等項目，作序位或計數之綜合評選，評定最有利標
  - 於此階段應將資安要求納入評定項目，藉以實際反映廠商資安作業能量

45

履約管理階段(1/23)

1. 計畫作業
2. 招標
3. 決標
4. **履約管理**
5. 驗收
6. 保固作業

- 當雙方確認契約內容並簽署後，委外專案將正式啟動，機關則應依據契約內容進行委外關係管理。其主要活動可能包含(但不限於)下列項目：
  - 確保委外廠商收到最終協議，並完全了解其中包含之資安要求事項
  - 於專案期間，當未預期事件發生時，依議定之移轉計畫進行產品或服務移轉，並及時通知另一方
  - 依議定程序管理資安變更與處置資通安全事件
  - 對可能參與終止計畫執行之人員進行定期訓練
  - 於委外廠商通知時，管理未涵蓋於資安變更管理程序中，但可能影響委外專案之其他變更，應對相關變更進行風險評估與管理，以確保變更所產生之資安風險於可接受之等級
  - 與委外廠商議定協議之變更，並核准更新之
  - 進行遵循性監視與專案執行活動符合度確認，並確保不符合事項矯正處置之執行或使用違約罰則條款。在此，機關應規劃監視之範圍、執行頻率及執行方式等

46

履約管理階段(2/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

下列為進行委外關係管理期間可能適用之資安控管項目，機關應就委外專案之性質，參考適用之事項

管理重點	
資通安全組織	資訊委外風險持續識別
資訊委外人力資源安全	資訊委外實體與環境安全
資訊委外管理	資訊委外使用者存取管理
資訊委外資通安全事件管理	

47

履約管理階段(3/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資通安全組織

- 機關與委外廠商皆應指定專案管理人員，負責推動、協調及督導下列資通安全管理事項
  - 資通安全責任分配與協調
  - 資訊資產保護事項監督
  - 資通安全事件檢討與監督
- 委外專案視需要成立跨部門資通安全推動小組，推動下列事項
  - 協調跨部門資通安全事項權責分工
  - 協調研議應採用之資通安全技術、方法及程序
  - 協調研議整體資通安全控制措施
  - 協調研議資通安全計畫
  - 協調研議其他重要資通安全事項

48

履約管理階段(4/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外風險持續識別(1/2)

- 經由委外作業過程中產生之風險，在核准廠商存取內部設施前加以識別，並作適當的控制措施
- 若允許委外廠商存取機關資訊處理設備或資訊時，執行風險評鑑識別特定控制措施的要求
- 委外廠商存取風險之識別，應考慮下列事項
  - 委外廠商攜帶存取的資訊處理設備與儲存媒體
    - 處理設備：手機與電腦
    - 儲存媒體：磁片、磁碟、光碟、隨身碟及報表
  - 委外廠商對資訊與資訊處理設備之存取形式
    - 實體存取：辦公室、機房及檔案櫃
    - 邏輯存取：機關的資料庫與資通系統的連結與存取
    - 機關與委外廠商的網路連接：固定連接或遠端存取
    - 存取發生於現場(On-Site)或場外(Off-Site)
    - 涉及資訊的價值與敏感性及對營運的關鍵性
    - 保護不打算被廠商存取的資訊，必要的各項控制措施

履約管理階段(5/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外風險持續識別(2/2)

- 委外廠商對資訊與資訊處理設備之存取型式(續)
  - 如何識別被授權存取的委外廠商或人員，如何查證授權與多久需再確認一次
  - 與廠商在儲存、處理、通信、分享及交換資訊時，所採用的各種不同方法與控制措施
  - 當委外廠商需存取而無法存取時，及因登錄或收到不精確或誤導資訊時的衝擊
- 委外廠商人員異動風險
  - 考慮廠商專案成員調整與異動時，限期調整其權限

履約管理階段(6/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(1/9)

- 為確保委外員工與廠商能勝任其角色，以降低竊盜、詐欺或設施誤用的風險，應於委外前，依契約條款闡明廠商應負之安全責任(尤其是敏感性工作)，並進行適當篩選，例如：人員背景查證審核、簽訂保密切結書及完成適當教育訓練

人員僱用前	僱用期間
● 角色與責任 – 篩選 – 僱用條款與條件	● 管理階層責任 ● 資通安全認知、教育及訓練 ● 懲處作業程序 ● 僱用終止或變更 ● 終止責任 ● 資產歸還 ● 存取權限移除

51

履約管理階段(7/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(2/9)

- 人員僱用前-委外人員資安角色與責任(1/3)
  - 資訊作業委外時應對機關相關業務人員、委外廠商及分包與轉包商之資安角色與責任，依照資通安全政策加以界定與文件化，並包含下列要求
    - ➢ 依據機關資通安全政策實作與行動
    - ➢ 保護資產不受未授權存取、揭露、修改、銷毀及干擾
    - ➢ 執行特定的各項資安過程與活動
    - ➢ 確保已指派責任給採取行動之個人
    - ➢ 向機關通報資安事件、潛在事件或其他資安風險
    - ➢ 資安角色與責任定義時機
    - ➢ 資安角色與責任宜於資訊委外作業人員僱用前事先定義，且明確地傳達給受僱用者，工作描述能用以書面佐證其資安角色與責任

52

履約管理階段(8/23)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

資訊委外人力資源安全(3/9)

- 人員僱用前-委外人員資安角色與責任(2/3)
  - 篩選
    - ➢ 委外人員背景查證檢核

      查證檢核時考量所有隱私權與個人資料保護等相關法令，參酌下列控制措施：
      - ◆是否有合格的品格推薦信或可諮詢的人員
      - ◆進用人員的學經歷檢核
      - ◆確認應徵人員學歷與專業資格
      - ◆獨立身分檢核，例如：護照或類似文件
      - ◆更詳細的核對，例如：信用核對或犯罪紀錄檢核
    - ➢ 定義查證檢核準則與限制程序
      - ◆宜定義查證檢核準則與限制程序，例如：誰有資格篩選人員，如何、何時及為何執行查證檢核

53

履約管理階段(9/23)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

資訊委外人力資源安全(4/9)

- 人員僱用前-委外人員資安角色與責任(3/3)
  - 僱用條款與條件
    - ➢ 保密切結書

      為保障委外作業安全，宜針對參與廠商之作業員工，經由個人同意並簽署僱用同意書。該同意書陳述其與機關對資通安全的責任
    - ➢ 僱用同意書，反映機關資安政策
      - ◆ 被賦予敏感資訊存取權之委外人員，在被允許存取資訊處理設備前，簽署機密性或保密協議
      - ◆ 委外人員法定責任與權利，例如：著作權法或個資法規定
      - ◆ 委外人員所處置資通系統與服務相關資訊分類及機關資產管理之責任
      - ◆ 委外人員處理來自其他公司或外部團體資訊之責任
      - ◆ 延伸至機關外與正常工作時間外之責任，例如：在家工作
      - ◆ 委外人員違犯機關資安要求時，所採取之行動
    - ➢ 確保委外人員同意機關資通安全條款與條件，及其將會取得資通系統與服務之存取權限範圍與限制

54

履約管理階段(10/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(5/9)

- 僱用期間-管理階層責任
  - 管理階層應要求委外人員，依照機關制定的政策與程序施行資安事宜
    - 確保委外人員在被核准存取敏感資訊或系統前，正確地說明資通安全角色與責任
    - 提供指導綱要予委外人員，述明對其角色的安全期望
    - 激勵委外人員符合機關資安政策
    - 激勵委外人員達到所扮演角色與責任的資安認知等級
    - 激勵委外人員符合僱用條款與條件，包括符合資安政策與適切的工作方法
    - 激勵委外人員持續擁有技能與資格
  - 激勵工作之重要

    若委外人員未認知資安責任，可能導致對機關巨大損害。受激勵的人員較少引起資通安全事件，而拙劣管理可能令委外人員感覺被輕視，導致負面衝擊

55

履約管理階段(11/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(6/9)

- 僱用期間-資通安全認知、教育及訓練
  - 機關宜對委外相關承包者與作業人員，使其接受與工作職務相關之認知與訓練作業，且定期更新機關政策與程序內容之適切性，並於核准存取資訊或服務之前進行認知訓練，內容以介紹機關之資安政策與期望
  - 持續不斷之訓練宜包含資通安全要求、法律責任及營運控制措施，以及資訊處理設施之正確使用訓練，例如登入程序、軟體套件之使用、安全程式之設計及懲處過程資訊
  - 有關資安認知、教育及訓練活動宜適切且相關於該人員之角色、責任及技術，並包含已知威脅資訊、更進一步建議聯絡人與通報資通安全事件之適當管道

56

履約管理階段(12/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(7/9)

- 僱用期間-懲處作業程序
  - 委外人員如有違反資通安全，宜有正式的懲處過程，對於未查證資安違例已發生前，不宜執行懲處作業程序
  - 懲處過程宜確保涉嫌違反資安政策員工，得到正確與公平之處理，並考量違例之性質與嚴重性、對營運衝擊、是否為初犯或累犯、是否經過適當訓練、相關法律、營運契約及其他因素等，採取累進處罰
  - 在嚴重的不當行為狀況下，宜允許立即停止其職務、存取權限及特權，必要時立即護送離開場域，懲處過程應適當，以預防委外人員違反資安政策、程序及其他資安違例
  - 有關廠商因違反契約，機關採取罰款之懲處方式，如不符合委外案件承作金額比例原則，可由廠商自行至工程會請求仲裁

57

履約管理階段(13/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(8/9)

- 僱用期間-僱用終止或變更

  為確保委外人員依程序離開機關或變更僱用條件，確保離開時受到管理，並完成資訊業務移轉交接、歸還設備及移除所有存取權限
- 僱用期間-終止責任

  委外專案終止責任，宜包含持續之資安要求、法律責任及機密性協議內之責任，以及於結束委外作業後持續一段界定期間之僱用條款與條件

58

履約管理階段(14/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外人力資源安全(9/9)

- 僱用期間-資產歸還

  委外作業完成、契約或協議終止時，應歸還所有機關資產，包括歸還所有軟體、機關文件及設備。其他如：存取卡、軟體、手冊及儲存於電子媒體的資訊等，也需一併歸還，並保留執行紀錄

  – 若委外作業由廠商提供或使用設備時，將所有相關資訊移轉回機關，並安全地從設備上清除

  – 若廠商擁有進行中之運作重要的知識，將該資訊文件化，並移轉回機關

- 僱用期間-存取權限移除

  – 委外人員對資訊與資訊處理設備之存取權限，在契約、協議終止或因變更而調整時，宜重新考量資通系統與服務相關之資產存取權限

  – 應注意若由管理階層發起之僱用終止，情緒不悅員工可能蓄意毀損資訊或破壞資訊處理設備；若為員工自行請辭，可能企圖為將來用途而蒐集資訊

履約管理階段(15/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外實體與環境安全

- 為防止機關場所內資訊，因委外作業而遭未經授權之實體存取、損害及干擾
- 關鍵或敏感之資訊處理設備，宜置放於安全區域，經由適當的資安屏障與進出控制措施加以保護，確保設備免受未經授權之存取、損害及干擾

安全區域

使用安全周界，例如：牆、卡控入口閘門或有人員駐守的接待櫃檯等屏障，以區隔委外作業與內部資訊處理設備的區域

設備安全

委外設備安全，應考量機關內因委外所需存取或委外人員攜入之資訊設備，包括個人電腦、個人數位助理、行動電話、智慧卡及其他形式，並注意由機關工作地點攜出與機關外攜入的各項風險

履約管理階段(16/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(1/6)

- 文件化作業程序

  機關內操作程序宜加以文件化與維持，並讓委外人員依其被指派工作項目，可隨時或經要求取得資訊處理與通信設施相關系統活動之文件化程序

- 變更管理
  - 因委外作業所產生之資訊處理設施與系統變更宜受控制，對於運作中之系統與應用軟體之變更，應嚴格管理控制
  - 宜有正式管理責任與程序，以確保對設備、軟體或程序之所有變更符合控制要求，變更完成後，宜保留一份內含所有相關資訊之稽核日誌

- 職務的區隔

  職務區隔是降低意外或蓄意系統誤用風險方法之一，對於委外職務與責任領域宜加以區隔，以降低機關資產遭未經授權或非意圖之修改或誤用產生，並注意無任何人員可未經授權或未受偵測之存取、修改或使用資產

61

履約管理階段(17/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外管理(2/6)

- 委外開發、測試及運作

  宜分隔開發、測試及運作之設施，以降低對運作系統未經授權存取或變更之風險，並識別出於運作、測試及開發環境間可能產生之資安問題，採取適當之控制措施
  - 於軟體開發階段導入安全程式開發，製作一套資安測試與評估計畫，實作此計畫，並將結果文件化
  - 將軟體由開發移轉到運作狀態之規則，宜加以定義與文件化
  - 開發與運作之軟體宜在不同系統或電腦處理器上運轉，且位於不同網域或目錄
  - 不能由現行運作之系統，存取編譯器(Compiler)、編輯器(Editor)及其他開發工具或系統公用程式
  - 委外測試系統環境宜儘可能逼真地模擬運作之系統環境
  - 對運作測試系統，宜使用不同使用者測試帳號，功能選單宜顯示適切之識別訊息以降低錯誤風險
  - 敏感資料不宜複製至測試系統環境
  - 系統需求評估
  - 適當之測試作業
  - 第三者執行查核與驗證

62

履約管理階段(18/23)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

資訊委外管理(3/6)

- 委外廠商服務交付管理

  委外廠商服務交付管理旨在確保資通安全與服務交付與委外廠商所議定之協議一致，包含對委外廠商服務之監視與審查，與管理委外廠商服務之變更

  – 委外廠商服務之監視與審查
    - 機關宜定期監視與審查由委外廠商提供之服務，以確保委外廠商遵守協議中資通安全條款與條件，且資通安全事件與問題均受到妥適管理
    - 依專案之性質與資安防護等級評估該資訊委外專案，依委外專案之重大性施行與其相稱之監視與審查活動，在有限資源下獲得最高之監視與審查效益
    - 對於委外產品或服務最有效與及時之審查方式，即是要求委外廠商定期產出服務報告，並安排定期進度會議，以即時反映與管理相關議題
  – 委外廠商服務變更管理
    - 對於委外廠商所提供服務之變更，包含維持與改進現有資通安全政策、程序及控制措施，應加以管理，並考量所涉及之營運系統與過程，並重新評鑑風險

63

履約管理階段(19/23)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

資訊委外管理(4/6)

- 防範惡意碼與行動碼

  機關於委外作業需要採取預防措施，防止與偵測惡意程式與未經授權行動碼之植入，以保護軟體與資訊完整性，管理者宜適時導入與實作控制措施，防止、偵測及移除惡意程式與控制行動碼

- 委外媒體的處置
  – 為防止資產被未經授權揭露、修改、移除或破壞而導致營運活動中斷，與委外作業有關之媒體宜加以控制與實體保護，並建立適切操作程序，以防止文件、電腦媒體(如磁帶與磁碟)、輸入、輸出資料及系統文件被未經授權揭露、修改、移除及破壞
  – 委外作業過程中之資料(含書面與磁性媒體)，應進行妥善控管與處理，避免機敏資訊外洩，造成重大損害與賠償事件發生

64

履約管理階段(20/23)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

資訊委外管理(5/6)

- 委外媒體的處置(續)
  - ➢ 可攜式媒體的管理
    - ◆可攜式媒體包括磁帶、磁碟、快閃磁碟、外接式硬碟、光碟(CD)、隨身碟、數位視訊影碟(DVD)、手機、數位相機及印出的媒體，宜採取適當程序以管理資訊委外作業人員使用之可攜式媒體，以避免資訊外洩或惡意程式入侵
    - ◆管理可攜式媒體，應考量下列原則
      - ■若不再需要，任何從機關移除之可再利用媒體內容，宜使其無法復原(如備份之磁帶與可覆寫光碟片)
      - ■若需要與實際可行時，從機關移除媒體應需授權，並保存該筆移除紀錄，以維持稽核存底
      - ■委外廠商攜入可攜式媒體進機關應受程序管制或限制
      - ■宜明確以書面記載所有程序與授權等級

65

履約管理階段(21/23)

1 計畫作業
2 招標
3 決標
4 履約管理
5 驗收
6 保固作業

資訊委外管理(6/6)

- 委外媒體的處置(續)
  - ➢ 系統文件的安全
    - ◆經委外產製的系統文件宜加以保護，免遭未經授權存取，並採行下列管控措施：
      - ■文件化相關資通安全控制措施
      - ■更新系統文件，並妥善保管與處理舊版文件
      - ■確保操作文件與使用者程序根據需要作適切變更。例如：資料庫與資料檔案、系統文件、使用者手冊、訓練教材、作業性與支援程序、營運持續管理計畫及預備作業計畫
      - ■辦公桌面的淨空政策
      - ■正式委外人員離職程序，確保繳回機關資產，並保留執行紀錄
      - ■電腦與網路之日常管理作業，應有正式文件，變更應經權責單位核准
      - ■保全委外作業系統文件應考慮：安全存放、版本控管、存取控制

66

履約管理階段(22/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

資訊委外使用者存取管理

- 為確保未經授權資訊委外作業人員對資通系統存取，機關宜有正式程序，以控制資通系統與服務存取權限配置作業，這些程序應從開始登記使用註冊，到最終不再需要存取資通系統與服務註銷
- 宜特別注意特權存取權限配置是否有控制必要，使用者註冊與註銷之存取控制程序包括：
  - 檢核是否經過系統擁有者授權，或由管理階層另行個別核准存取權限
  - 檢核所授予的存取權限等級，是否符合營運目的，是否與機關資安政策一致，例如：不違反職務區隔
  - 給予委外人員存取權限的書面聲明
  - 要求委外人員簽署聲明
  - 確保服務提供者在完成授權程序前，不會提供存取
  - 維持一份含所有註冊使用服務之使用者的正式紀錄
  - 機關可透過帳號、識別證及卡片等機制，管理委外人員帳號，使每一位委外人員具有「唯一」識別，並可依識別驗證使用者身分
  - 委外人員因變更角色、調職或離職後，應立即移除或封鎖其存取權限

67

履約管理階段(23/23)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

委外資通安全事件管理

- 為確保與委外作業相關之資通安全事件與弱點，能夠被採取及時矯正措施之方式傳達，委外機關宜備妥正式之事件通報與提報程序供委外廠商配合並施予合宜訓練，委外廠商宜認知可能對機關資產安全造成衝擊不同型式事件與弱點之通報程序，並要求所有人員儘快向指定聯絡點通報任何資通安全事件與弱點
- 通報程序應包含：
  - 適當記錄資安事件的作業處理程序，確保資安事件回報處理或撰寫資安事件檢討(或結果)報告
  - 資通安全事件報告格式可支援回報行為，並幫助回報人員記錄在資通安全事件所有必要的行為狀況
  - 發生資通安全事件後的正確行動
    - 記錄所有重要細節
    - 應儘速通知相關人員處理，不隨意執行任何動作
  - 反映資通安全弱點
  - 反映軟體功能不正常

68

驗收階段(1/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 執行「驗收階段」係依據契約文件與「履約管理」階段執行成果辦理，並得以書面或召開審查會議方式辦理
- 依下列建議，要求廠商專案驗收內容與進度：
  - 廠商於簽約後一定時間內提交「專案工作計畫書」
  - 廠商須定期召開工作進度報告會議，並提交工作報告
  - 於資訊委外作業執行過程中，配合各階段需求，規劃並實施充足教育訓練
  - 完成履約管理階段之廠商服務交付管理，依機關要求格式，交付契約內要求之各項文件
  - 除上述專案文件外，廠商應衡酌各工作項目性質與內容，詳述擬交付的文件或資料，並負責製作專案進行過程中每次會議紀錄，交由機關確認
  - 製作結算驗收證明書，驗收完畢後規定時間(例如：15個日曆天)內填具。(採購法施行細則第101條)
  - 進行功能檢測，包括：系統(網路)架構、人機介面及系統介面
  - 進行非功能檢測，包括：效能檢測、承載力檢測及資安檢測
  - 除資安檢測外，其他各項檢測需求，非資安範圍，請機關依需求自行規劃

69

驗收階段(2/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 資安驗收內容(1/2)
  - 顧問訓練類
    - 為純粹提供管理與技術服務，在完成顧問服務時即可得知是否符合機關要求。對於某些需由顧問使用軟體輔助才可完成專案之情況，應確認委外廠商是否使用最適之檢測工具與版本；而大多數本類之專案驗收可以滿意度訪問與調查來確認其執行成效測
  - 系統發展類
    - 通常除功能與效能測試外，應要求委外廠商提供該資通系統之安全性檢測證明，其中可包含確認無程式後門、進行程式原始碼檢測、弱點掃描或滲透測試等，避免日後因系統漏洞造成傷害。此外，當資通系統使用非委外廠商自行開發之元件時，宜要求委外廠商揭露第三方程式元件之來源與授權證明，以確保其元件非來自大陸地區或其他限制地區

70

驗收階段(3/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 資安驗收內容(2/2)
  - 維運管理類
    - 與顧問訓練類之服務類似，若維運過程有新發現程式漏洞，需進行程式修補者或定期進行程式弱點掃描外，一般狀況是每年定期執行系統弱點掃描
  - 雲端服務類
    - 與系統發展類相似，除確認功能與效能外，對於產品或服務之資安保證大多來自於委外廠商所提供之證明。機關應確認與評估雲端服務供應商宣稱之證認範圍，包含控制與評估涵蓋功能及服務

71

驗收階段(4/4)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 委外關係終止
  - 當專案如預期順利結束後，機關應立即停止委外廠商所涉及之實體與邏輯存取權限，並回收或請委外廠商銷毀屬於機關之資訊資產，必要時可要求委外廠商出具銷毀證明
  - 若因該委外專案具有保固期，而無法執行上述項目時，機關應詳細審查委外廠商所擁有之存取權限適當性，以及委外廠商所持有屬於機關之資訊資產必要性
  - 若專案因未預期之情況，由契約其中一方決定終止，在驗收階段除依上述之驗收流程確認已完成之專案活動外，對於未預期終止之情況應至少執行下列事項：
    - 釐清機關決定終止專案決策背後之資安動機。若有，機關應識別與評鑑與該資安動機相關之風險，並定義與實作其相對應之處置選項
    - 確認產品或服務之移轉程序
    - 定義與實作溝通計畫，以通知因委外專案終止而受衝擊之內部人員與第三方
    - 指派專人依終止計畫處理委外專案之終止
    - 確保委外專案過程中所涉及之所有資訊資產，並更新於資產清冊中
    - 確認使用於委外專案中所涉及之資訊資產之歸還、轉交予另一個委外廠商或銷毀
    - 確認委外廠商專案期間所取得之實體與邏輯存取權限之及時移除

72

保固作業(1/2)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 軟硬體系統完成驗收程序後進入保固期，期間不論軟硬體資產，應以維持驗收完成時之狀態為主要目的。各機關如因後續維護預算(經常門)編列有困難，而將部分系統維護工作整併於系統發展類之系統整合或軟體開發工作項目中，其所列方式應比照系統發展類之軟體維護或維運管理類服務方式處理，不宜與保固服務混為一談；例如其後續資安檢測作為，可比照列為維運管理類服務方式執行，不宜列為保固服務範圍

73

保固作業(2/2)

1. 計畫作業
2. 招標
3. 決標
4. 履約管理
5. 驗收
6. 保固作業

- 保固期間對於運作中之資訊處理設施和應用軟體系統，均應受到嚴格之變更管理控制，如系統有重大資安顧慮或瑕疵，經與委外廠商協調後，如屬委外廠商責任，需由委外廠商另提變更計畫
- 保固期間系統如有委外廠商派駐人員協助者，發生異常事件時，應由派駐人員負責反映至資訊業務承辦人員，再循正常程序陳報，否則仍應由資訊業務承辦人員循序陳報
- 機關宜有正式管理責任與程序，以確保對設備、軟體或程序之所有變更，符合控制要求。變更完成後，宜保留一份內含所有相關資訊之稽核日誌

74

大綱

- 資訊委外類別與形態
- 資訊委外資安策略
- 資訊委外風險說明與風險處理原則
- 資訊委外各階段資安要求
- **注意事項與常見缺失**
- Q&A

計畫作業階段注意事項(1/5)

政府資訊委外資安檢核表

1	委外作業資安要求		4項
2	計畫作業		9項
3	招標		11項
4	決標		13項
5	履約管理		58項
6	驗收 & 保固作業		8項
			共103項

政府資訊作業委外安全管理注意事項或常見缺失

1 專案編成：專案編組不恰當或專業人力不足

- 解決方案
  - 適時向資安主管反應，以明確律定各單位權責
    - 尤其是資訊委外之個資清查與風險評鑑，通常需要各業務單位的全力協助
  - 儘量爭取經費以安排適當之教育訓練課程，提升資安專業能力，或外聘顧問解決資安專業人力不足問題

計畫作業階段注意事項(2/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

2 資訊風險評估：未確實評估潛在風險或虛應故事

- 解決方案
  - 參閱「資通系統風險評鑑參考指引」，根據時間與資源限制，選擇合適風險評鑑方式，評估資訊委外資安風險
    - ➢ 高階風險評鑑
    - ➢ 詳細風險評鑑

77

計畫作業階段注意事項(3/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

3 廠商提出對應措施方案：無法有效評鑑廠商提出對應措施建議方案是否符合需要

- 解決方案
  - 對於複雜或大型資訊專案，解決方法是遵循RFI、RFC及RFP之作業程序，配合廠商相互競爭實況，提升方案適用性與有效性
  - 對於簡單或小型資訊專案，則外聘顧問協助審查

78

計畫作業階段注意事項(4/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

4 建立委外資安管理制度：常以抄襲代替建立符合單位實況之資訊安全管理制度

- 解決方案

依據機關屬性、規模及資源，確實建立符合機關實際需求之「資訊委外資安政策」與相對應程序與表單

計畫作業階段注意事項(5/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

5 資通安全服務水準定義：資通安全服務水準定義不當或不明確

6 委外服務契約項目規劃：委外服務契約項目規劃不當或不明確

- 解決方案

依時間與資源，適當評估資訊委外資安風險，並遵循RFI、RFC及RFP之作業程序辦理

履約管理階段注意事項(1/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

1. 執行契約規範項目：未能依據合約與RFP要求，確實執行契約規範項目
2. 採行控制措施：未能依據合約與RFP要求，確實執行契約規範項目

- 解決方案

依時間與資源，適當評估資訊委外資安風險，並遵循RFI、RFC及RFP之作業程序辦理

81

履約管理階段注意事項(2/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

3. 新系統上線作業審查措施：未能確實執行新系統上線作業審查，並依相關作業程序辦理

- 解決方案

確實要求執行新系統上線審查，如有專業或人力不足時，應及早請求協助，或委請第三方協助解決專業與人力不足問題

82

履約管理階段注意事項(3/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

4 資安事件之反應與處理：發生資安事件時隱匿不報

- 解決方案
  - 在資通安全管理政策、規範或程序中，訂定適當獎懲措施，以建立資安作業紀律
  - 定期或不定期實施抽查與演練

履約管理階段注意事項(4/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

5 營運持續管理：營運持續管理計畫未依據實際狀況修訂，或事件發生時無法有效執行

- 解決方案

  定期或不定期實施演練，並檢討實際執行與計畫間差距，適時修訂營運持續管理計畫，做為後續矯正預防參考

履約管理階段注意事項(5/5)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

6 緊急應變計畫檢查缺失的改善：未能確實追蹤管制缺失改善情形

- 解決方案

建立追蹤機制，並納入定期會議中檢討改善

驗收階段注意事項(1/4)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

1 定期評估與稽核廠商資安控管績效：未能確實執行定期評估與稽核廠商資安控管績效

- 解決方案

將評估與稽核廠商資安相關工作，納入工作要項與機關工作行事曆

驗收階段注意事項(2/4)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

2 會議與文件資料：會議與文件資料建立不確實或不完整

- 解決方案

委請第三方協助解決專業與人力不足問題

87

驗收階段注意事項(3/4)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

3 軟體委外開發稽核：軟體委外開發稽核能力不足

- 解決方案

委請第三方協助解決專業與人力不足問題

88

驗收階段注意事項(4/4)

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

政府資訊作業委外安全管理注意事項或常見缺失

4 異動稽核措施是否符合預期效能：未能確實執行異動稽核措施

- 解決方案

確實執行異動稽核措施，如有專業或人力不足時，應及早請求協助，或委請第三方協助解決專業與人力不足問題

其他注意事項

政府資訊委外資安檢核表

1	委外作業資安要求	4項
2	計畫作業	9項
3	招標	11項
4	決標	13項
5	履約管理	58項
6	驗收 & 保固作業	8項
		共103項

1 廠商資格審查是否依RFP與契約書規定辦理(含外國或大陸地區廠商)

2 遴選評選委員時，是否考量其學經歷、相關領域實務經驗及利益迴避等條件

1 評選廠商投標建議書時，評選委員是否將資安列入評選項目

1 廠商是否定期召開工作進度報告會議，並提交工作報告

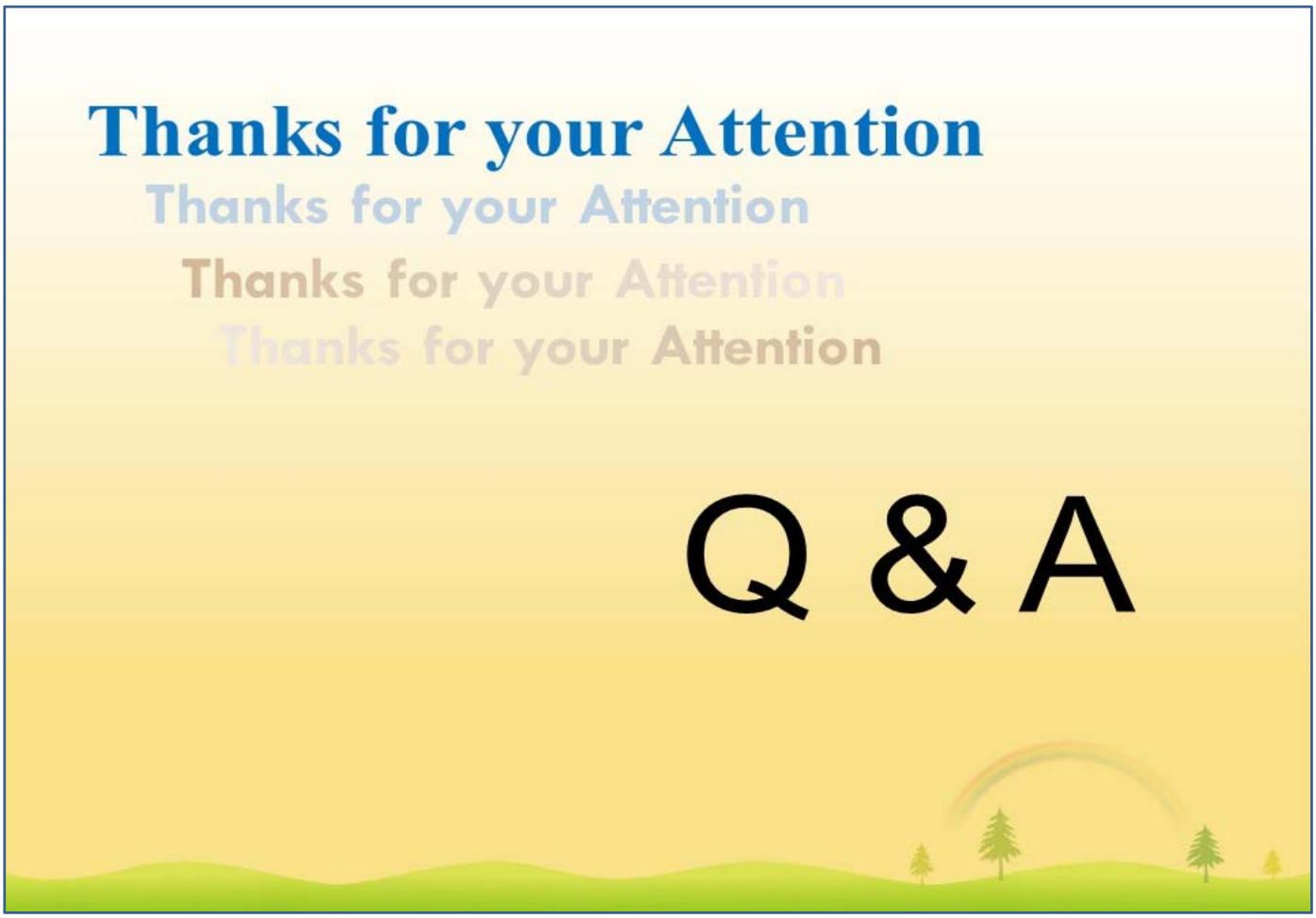
2 配合各階段需求，規劃並實施充足之教育訓練，推動並提昇委外人員資安知識與技能

3 是否完成程式源碼檢測，執行程式弱點掃描

4 是否定期執行系統弱點掃描

5 發現資安弱點與可能面臨的威脅，是否請原設計廠商提供變更計畫

6 執行中之資通系統發生異常或系統漏洞時，機關對是否詳細評估廠商所提之變更計畫對系統的影響並獲得批准


Thanks for your Attention
Thanks for your Attention
Thanks for your Attention
Thanks for your Attention
Q & A

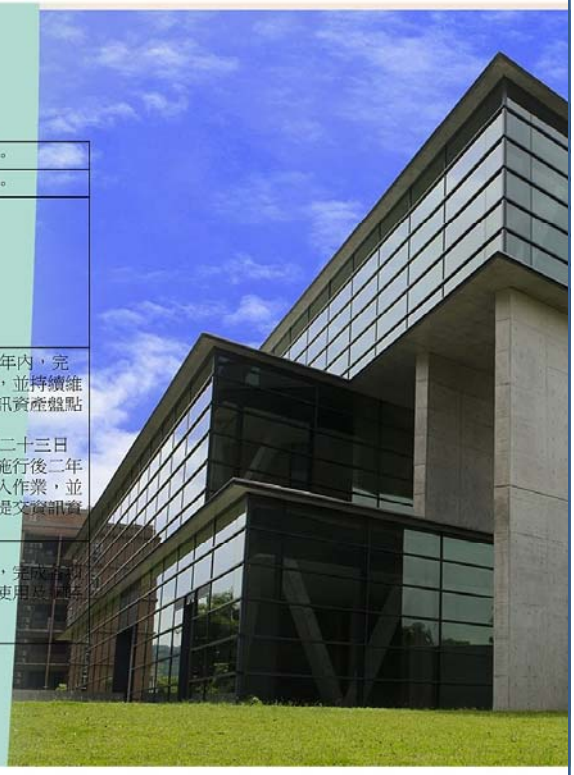
六、資通系統硬體管理實務

主講人/亞洲大學 陳偉嵩組長

法規依循

技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

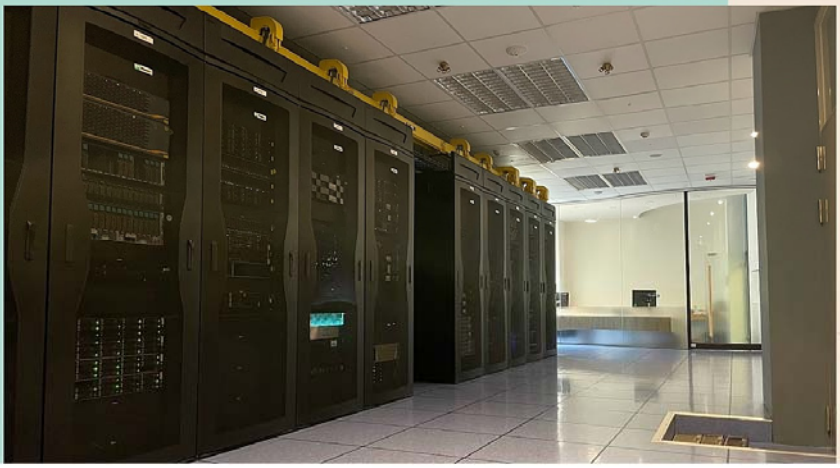
相關內容可參閱110年研習課程



Prezi

資通系統之硬體設備

資通系統所涵蓋之硬體設備以資訊機房為主，對包含環境支援、伺服器設備、儲存設備、網通設備及個人設備。



環境支援

伺服器設備

儲存設備

網通設備

個人設備

Prezi

設備應定期執行維護及保養作業，並留存紀錄（5.11）

環境設備

空調設備

電力設備

消防設備

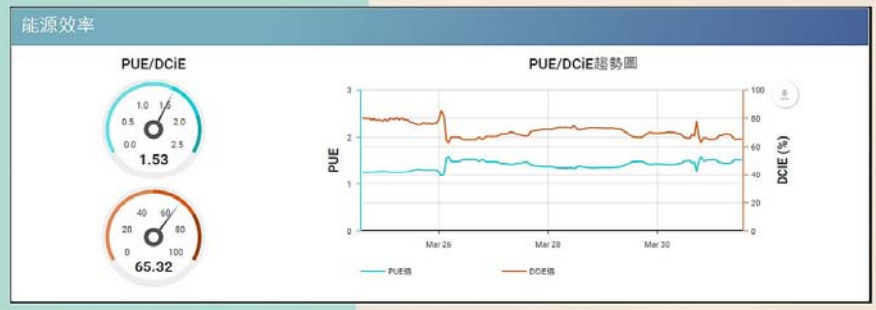
其他設備

Prezi

記錄溫度變化，有助於預警設備異常狀況 5.4

Prezi

電力系統 5.9



UPS

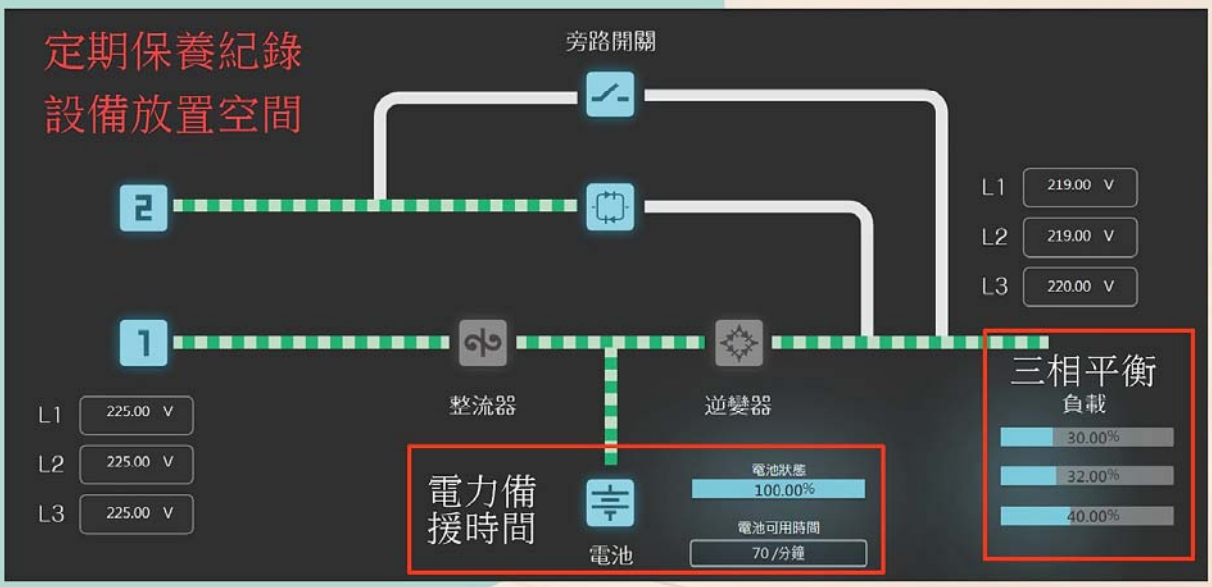
發電機

接地系統

電力監控是機房節能的第一步

Prezi

不斷電系統之維護重點



Prezi

發電機之維護重點

自動切換
定期維護
油量監測
有載運轉測試

Prezi

等電位接地系統配置

透過以建築物本身之等電位接地系統配置，降低建築物內可能出現的電位差以確保人員安全

Prezi

消防系統之維護重點

5.8

定期申報及維護(有效性確認)
選擇適當的滅火設備
C02 海龍 FM200 氬氣

Prezi

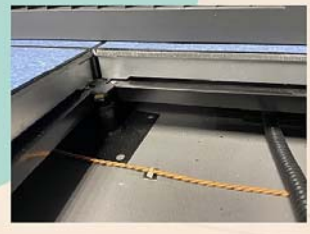
其他環境設備

CCTV 監視設備 5.3

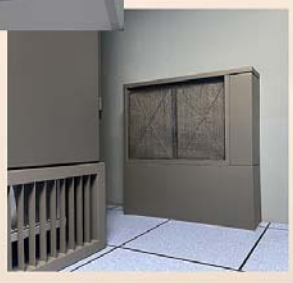
門禁管理設備 5.1 5.2

設備進出登記 5.7 5.12
人員進出登記 5.6

漏液偵測



換氣系統



Prezi

伺服器設備維護作業

定期帳號清查作業　5.25 5.26

網站、系統弱點掃描、資安健診　5.19

鐘訊同步設定

Web Server Https 通訊協定　5.23

Prezi

儲存設備之管理維護

備份政策制定 (RPO)　5.21 5.22

設備異常告警(Log Review)

備份結果通知

Prezi

網路設備之維護

資安設備

線路管理

無線網路

建立網路架構圖

管理權限

設定檔之備份　　防火牆政策清查

IP派送與管理
網路區隔配置　5.16 5.29

遠端連線管理
(RDP、Anydesk)　5.30

Prezi

資安設備

防火牆&入侵偵測系統

網頁防火牆

資料庫稽核系統

Prezi

防火牆

FW_Policy

- 應採用正面表列
- 避免開啟RDP 等遠端桌面連入
- 防火牆政策的申請(S_IP、D_IP、Port_NO、Time)
- 防火牆政策的定期清查
- 防火牆政策群組化分類
- 特殊連線作業宜再定義可連線時段

Prezi

項目	來源IP	目的IP	連線Port	備註
1	Any	140.120.X.1	Tcp_80、Tcp_443	
2	Any	140.120.X.2	Tcp_80、Tcp_443	
3	Any	140.120.X.3	Tcp_80、Tcp_443、Tcp_8080	
4	168.1.1.1	140.120.X.3	Tcp_1433	
5	Any	140.120.X.4	Tcp_8080	

項目	來源IP	目的IP	連線Port	備註
1	Any	140.120.X.1 140.120.X.2 140.120.X.3	Tcp_80、Tcp_443	
2	Any	140.120.X.3 140.120.X.4	Tcp_8080	
3	168.1.1.1	140.120.X.3	Tcp_1433	

Prezi

良好的線路管理提供高可靠度的網路服務及快速的故障排除 5.10

Prezi

無線網路管理重點

5.29 5.30

須提供具備驗證機制之無線環境

無線網路使用者之連線限制

Thin AP / Fat AP 特性

Prezi

個人設備之管理

可攜式電腦設備之管理 5.13 5.24

作業系統之版本、防毒軟體更新、軟體授權 5.17 5.18 5.19 5.20

NB及平板電腦之管理 5.13 5.31

Prezi

其他配合作業項目

演練作業 5.22

重大異動及變更管理 5.33

危害國家資通安全設備清查及對應作法 5.35 5.36

人員資訊安全管理之落實 5.15 5.27 5.28

資通設備報廢流程 5.14

資安通報平台 5.34

Prezi

稽核重點

5.26 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?

5.22備份資料是否定期回復測試，以確保備份資料之有效性?

5.19是否定期執行各項系統漏洞修補程式?

5.5各項安全設備是否定期檢查? 同仁有否施予適當的安全設備使用訓練?

5.34是否可即時取得系統弱點的資訊並作風險評估及採取必要措施?

總結

硬體配置及規劃宜整體規劃

防火牆規則應重整並定期審查

資安風險及弱點應盡速完成修補

落實日常巡檢紀錄

肆、附件

教育部國教署所轄公務機關111年度資通安全維護計畫實施情形查核表

單位：

查核日期：　年　月　日

查核人員：

查核項目	查核內容	查核結果			準備資料或客觀證據
		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？	□	□	□	資通安全政策或資通安全維護計畫
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	資通安全政策或資通安全維護計畫
	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？	□	□	□	審核紀錄及公告紀錄
	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？	□	□	□	管審會紀錄
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	公告紀錄
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？	□	□	□	資通安全組織成員表
	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？	□	□	□	資通安全組織成員表
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	資通安全組織成員表
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？	□	□	□	人員安全守則
	3.2 是否符合組織之需求配置專業資安人力(資安專責人員)？	□	□	□	資通安全維護計畫中敘明配置資通安全專責人員(C級機關應辦事項：初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。)
	3.3 是否具備相關專業資安證照或認證？(本項C級機關列入評分，D級機關不列入評分)	□	□	□	專業安證照及職能訓練
	3.4 是否配置適當之資源？	□	□	□	資安或資訊相關經費情形(全年度與前年度經費之占比)
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？(本項將列為實地稽核重點項目，並納入機關(校長)考核參考)	□	□	□	資訊資產清單
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	資訊資產清單
	4.3 是否定有資訊、資通系統分級與	□	□	□	維護計畫核心系統

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	處理之相關規範？				
	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？	□	□	□	資訊資產清單風險評估表
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	□	□	□	資訊設備主機機房門禁照片
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	進出人員清單
	5.3 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？	□	□	□	人員進出紀錄表
	5.4 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？	□	□	□	巡查紀錄表
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	□	□	□	消防、CCTV、門禁設施檢查紀錄或保養資料。 設備使用訓練紀錄。
	5.6 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？	□	□	□	陪同進出之紀錄及照片
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	實體安全管理制度
	5.8 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？	□	□	□	例如：資訊機房偵煙、偵熱與滅火設備、漏水偵測等照片。
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	電力保護設施照片(UPS、穩壓器、接地線等)、緊急照明設備照片
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	線路保護設施照片(如線槽、高架地板、套管等)
	5.11 設備是否定期維護，以確保其可用性及完整性？	□	□	□	系統主機及網路維護紀錄或合約、機房查檢紀錄表
	5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	□	□	□	設備進出管理制度。(B-002 5.7.2) 設備進出紀錄表
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	□	□	□	防毒軟體、登入等照片、設備領用紀錄。
	5.14 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？	□	□	□	報廢管理制度及報廢紀錄
	5.15 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？	□	□	□	管理制度及實體防護照片(例如：資料上鎖)。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	測試環境與正式環境照片、不適用則免附。
	5.17 是否全面使用防毒軟體並即時	□	□	□	至少2位一般使用者的個人電

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	更新病毒碼？				腦設定畫面
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	至少2位一般使用者的個人電腦設定畫面
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	系統主機及個人電腦各兩臺設定畫面
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	□	□	□	管理制度(B-007 5.3.5)
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	備份工作相關紀錄
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	備份回復演練紀錄
	5.23 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？	□	□	□	系統登作畫面、https、檔案加密。
	5.24 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？	□	□	□	可攜式媒體管理制度
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	帳號申請及註銷管理制度
	5.26 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？	□	□	□	帳號申請單及帳號清查表
	5.27 通行碼長度是否超過8個字元？	□	□	□	通行碼管理制度
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	通行碼管理制度
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	□	□	□	網路架構圖及業務與網段對應資料，內網區隔狀況、網路管理規定
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	□	□	□	遠端連線作業
	5.31 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)？	□	□	□	行動式電腦設備管理制度
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	憑證使用認證佐證資料 (不適用者免附)
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	□	□	□	資訊服務變更管理制度及紀錄。
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	□	□	□	弱掃報告及高風險弱點修補處理狀況
	5.35 限制使用危害國家資通安全產品-大陸廠牌產品清冊列管及說明。	□	□	□	1.檢視資通系統及設備是否使用危害國家資通安全產品(如大陸廠牌) 2.大陸廠牌產品清冊(包含硬

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
					體、軟體、服務，請上傳可編輯檔案如excel, ods等）
	5.36 限制使用危害國家資通安全產品-汰換大陸廠牌產品及說明。 1.110年12月31日前完成汰換大陸廠牌產品 2.如無法於期限內完成汰換，須於大陸廠牌產品清冊述明理由	□	□	□	1.大陸廠牌產品汰換紀錄 2.大陸廠牌產品清冊(包含硬體、軟體、服務，請上傳可編輯檔案如excel, ods等）
6.訂定資通安全事件通報及應變之程序及機制	6.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	資通安全事件通報及應變管理程序。
	6.2 機關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？	□	□	□	宣導及公告相關資料。
	6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	□	□	□	安全事件報告單或矯正紀錄
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	□	□	□	資通安全公告、宣導及研習資料
	7.2 是否對同仁進行資安評量？	□	□	□	資安評量或資安研習評量資料
	7.3 是否對同仁依層級定期舉辦資通安全教育訓練？	□	□	□	資安教育訓練資料 資通安全認知訓練時數要求： 1.全體同仁每人每年須接受3小時以上一般資通安全教育訓練。 2.專職(責)人員以外之資訊人員每人每年須接受3小時以上之資通安全專業課程訓練或資通安全職能訓練。 3.專職(責)人員每年須接受12小時以上資通安全專業課程訓練或資通安全職能訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	□	□	□	公告、宣導、人員安全守責等資料。
8.資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？	□	□	□	內稽制度
	8.2 是否定有年度稽核計畫？	□	□	□	內稽計畫書
	8.3 是否定期執行稽核？(建議2年1次)	□	□	□	內稽紀錄
	8.4 是否改正稽核之缺失？	□	□	□	內稽缺失矯正紀錄
9.資通安全維護計畫及實施情形之績效管考機制	9.1 是否訂定安全維護計畫持續改善機制？	□	□	□	矯正及預防管理制度
	9.2 是否追蹤過去缺失之改善情形？	□	□	□	矯正及預防處理單
	9.3 是否定期召開持續改善之管理審查會議？	□	□	□	管審會議紀錄
10.資通系統委外(含委辦)案之履約	10.1 資通系統委外(含委辦)是否簽訂協議書或契約？	□	□	□	委外(含委辦)案之協議書、契約書等文件，應符合資安法施行細第4款各項規定。
	10.2 是否落實檢核及履約督導管	□	□	□	檢核受託單位繳交之資料，應

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
檢核及督導管理(無則請填寫不適用)	理？				附廠商承諾辦理資安相關事項之證明文件。
	10.3 委外(含委辦)相關人員是否簽訂保密合約書？	□	□	□	保密切結書、保密合約書等文件
11.其他應辦事項	11.1 是否每年檢視一次資通系統(自有及委外)分級妥適性？	□	□	□	資通系統(自有及委外)分級相關文件(資通安全責任等級分級辦法附表九)
	11.2 是否每兩年辦理一次資通安全健診？(本項C級機關列入評分，D級機關不列入評分)	□	□	□	資通安全健診報告
	11.3 是否完成資通安全防護(防毒軟體、網路防火牆、電子郵件過濾機制)？	□	□	□	1. 檢視資通設備是否安裝防毒軟體 2. 檢視網路防火牆建置情形 3. 具有電子郵件伺服器者，檢視電子郵件過濾機制
	11.4是否完成資通安全弱點通報機制導入作業(111年尚在導入階段，暫不列入評分，C級機關應於2年完成導入)				C級機關：初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 資安法於110年8月23日修法，修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

備註 1:核心資訊系統須進行本表各個項目查核。
備註 2:本表參考行政院資通安全會報之資通安全維護計畫制定。

資通安全管理法

公布日期：民國 107 年 06 月 06 日

第 一 章 總則

第 1 條

為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，特制定本法。

第 2 條

本法之主管機關為行政院。

第 3 條

本法用詞，定義如下：

一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

四、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

五、公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。

六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

七、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。

八、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關指定，並報主管機關核定者。

九、政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。

第 4 條

1 為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：

一、資通安全專業人才之培育。

二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。

三、資通安全產業之發展。

四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。

2 前項相關事項之推動，由主管機關以國家資通安全發展方案定之。

第 5 條

1 主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。

2 前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。

第 6 條

1 主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。

2 前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。

第 7 條

1 主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之。

2 主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。

3 特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。

第 8 條

1 主管機關應建立資通安全情資分享機制。

2 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。

第 9 條

公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

第 二 章 公務機關資通安全管理

第 10 條

公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

第 11 條

公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

第 12 條

公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。

第 13 條

1 公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。

2 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。

第 14 條

1 公務機關為因應資通安全事件，應訂定通報及應變機制。

2 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。

3 公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。

4 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。

第 15 條

1 公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。

2 前項獎勵事項之辦法，由主管機關定之。

第 三 章 特定非公務機關資通安全管理

第 16 條

1 中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。

2 關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

3 關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。

4 中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。

5 關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關。

6 第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。

第 17 條

1 關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

2 中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。

3 中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。

4 前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。

第 18 條

1 特定非公務機關為因應資通安全事件，應訂定通報及應變機制。

2 特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。

3 特定非公務機關應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。

4 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由主管機關定之。

5 知悉重大資通安全事件時，主管機關或中央目的事業主管機關於適當時機得公告與事件相關之必要內容及因應措施，並得提供相關協助。

第 四 章 罰則

第 19 條

1 公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。

2 前項懲處事項之辦法，由主管機關定之。

第 20 條

特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰：

一、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫必要事項之規定。

二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。

三、未依第七條第三項、第十六條第五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條第六項或第十七條第四項所定辦法中有關改善報告提出之規定。

四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八條第四項所定辦法中有關通報及應變機制必要事項之規定。

五、未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。

六、違反第十八條第四項所定辦法中有關通報內容之規定。

第 21 條

特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

第 五 章 附則

第 22 條

本法施行細則，由主管機關定之。

第 23 條

本法施行日期，由主管機關定之。

資通安全管理法施行細則

修正日期：民國 110 年 08 月 23 日

第 1 條

本細則依資通安全管理法（以下簡稱本法）第二十二條規定訂定之。

第 2 條

本法第三條第五款所稱軍事機關，指國防部及其所屬機關（構）、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款及第二項規定之機關。

第 3 條

公務機關或特定非公務機關（以下簡稱各機關）依本法第七條第三項、第十三條第二項、第十六條第五項或第十七條第三項提出改善報告，應針對資通安全維護計畫實施情形之稽核結果提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形：

一、缺失或待改善之項目及內容。

二、發生原因。

三、為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施。

四、前款措施之預定完成時程及執行進度之追蹤方式。

第 4 條

1 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

八、受託者應採取之其他資通安全相關維護措施。

九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其

他適當方式確認受託業務之執行情形。

2 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項：

一、曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

二、曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

三、曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

四、其他與國家機密保護相關之具體項目。

3 第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。

第 5 條

前條第三項及本法第十六條第一項之書面，依電子簽章法之規定，得以電子文件為之。

第 6 條

1 本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

一、核心業務及其重要性。

二、資通安全政策及目標。

三、資通安全推動組織。

四、專責人力及經費之配置。

五、公務機關資通安全長之配置。

六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。

七、資通安全風險評估。

八、資通安全防護及控制措施。

九、資通安全事件通報、應變及演練相關機制。

十、資通安全情資之評估及因應機制。

十一、資通系統或服務委外辦理之管理措施。

十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。

十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

2 各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。

3 第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關經其上級或監督機關同意，得由其上級、監督機關或其上級、監督機關所屬公務機關辦理；特定非公務機關經其中央目的事業主管機關同意，得由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關或中央目的事業主管機關所管特定非公務機關辦理。

第 7 條

1 前條第一項第一款所定核心業務，其範圍如下：

一、公務機關依其組織法規，足認該業務為機關核心權責所在。

二、公營事業及政府捐助之財團法人之主要服務或功能。

三、各機關維運、提供關鍵基礎設施所必要之業務。

四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第五款涉及之業務。

2 前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

第 8 條

本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告，應包括下列事項：

一、事件發生或知悉其發生、完成損害控制或復原作業之時間。

二、事件影響之範圍及損害評估。

三、損害控制及復原作業之歷程。

四、事件調查及處理作業之歷程。

五、事件根因分析。

六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

七、前款措施之預定完成時程及成效追蹤機制。

第 9 條

中央目的事業主管機關依本法第十六條第一項規定指定關鍵基礎設施提供者前，應給予其陳述意見之機會。

第 10 條

本法第十八條第三項及第五項所稱重大資通安全事件，指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。

第 11 條

1 主管機關或中央目的事業主管機關知悉重大資通安全事件，依本法第十八條第五項規定公告與事件相關之必要內容及因應措施時，應載明事件之發生或知悉其發生之時間、原因、影響程度、控制情形及後續改善措施。

2 前項與事件相關之必要內容及因應措施，有下列情形之一者，不予公告：

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或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。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。

二、其他依法規規定應秘密、限制或禁止公開之情形。

3 第一項與事件相關之必要內容及因應措施含有前項不予公告之情形者，得僅就其他部分公告之。

第 12 條

特定非公務機關之業務涉及數中央目的事業主管機關之權責者，主管機關得協調指定一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。

第 13 條

1 本細則之施行日期，由主管機關定之。
2 本細則修正條文自發布日施行。

資通安全責任等級分級辦法

修正日期：民國 110 年 08 月 23 日

第 1 條

本辦法依資通安全管理法（以下簡稱本法）第七條第一項規定訂定之。

第 2 條

公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。

第 3 條

1 主管機關應每二年核定自身資通安全責任等級。

2 行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。

3 直轄市、縣（市）政府應每二年提交自身、所屬或監督之公務機關，與所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級，報主管機關核定。

4 直轄市及縣（市）議會、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會應每二年提交自身資通安全責任等級，由其所在區域之直轄市、縣（市）政府彙送主管機關核定。

5 總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核定自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，送主管機關備查。

6 各機關因組織或業務調整，致須變更原資通安全責任等級時，應即依前五項規定程序辦理等級變更；有新設機關時，亦同。

7 第一項至第五項公務機關辦理資通安全責任等級之提交或核定，就公務機關或特定非公務機關內之單位，認有另列與該機關不同等級之必要者，得考量其業務性質，依第四條至第十條規定認定之。

第 4 條

各機關有下列情形之一者，其資通安全責任等級為A級：

一、業務涉及國家機密。

二、業務涉及外交、國防或國土安全事項。

三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。

四、業務涉及全國性民眾或公務員個人資料檔案之持有。

五、屬公務機關，且業務涉及全國性之關鍵基礎設施事項。

六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。

七、屬公立醫學中心。

第 5 條

各機關有下列情形之一者，其資通安全責任等級為 B 級：

一、業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。

二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。

三、業務涉及區域性或地區性民眾個人資料檔案之持有。

四、業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。

五、屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。

六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。

七、屬公立區域醫院或地區醫院。

第 6 條

1 各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。

2 前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。

第 7 條

各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。

第 8 條

各機關有下列情形之一者，其資通安全責任等級為E級：

一、無資通系統且未提供資通服務。

二、屬公務機關，且其全部資通業務由其上級機關、監督機關或上開機關指定之公務機關兼辦或代管。

三、屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關或出資之公務機關兼辦或代管。

第 9 條

各機關依第四條至前條規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。

第 10 條

各機關之資通安全責任等級依前六條規定認定之。但第三條第一項至第五項之公務機關提交或核定資通安全責任等級時，得考量下列事項對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級：

一、業務涉及外交、國防、國土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者，其中斷或受妨礙。

二、業務涉及個人資料、公務機密或其他依法規或契約應秘密之資訊者，其資料、公務機密或其他資訊之數量與性質，及遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害。

三、各機關依層級之不同，其功能受影響、失效或中斷。

四、其他與資通系統之提供、維運、規模或性質相關之具體事項。

第 11 條

1 各機關應依其資通安全責任等級，辦理附表一至附表八之事項。

2 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。

3 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

4 公務機關之資通安全責任等級為A級或B級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。

5 中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。

第 12 條

1 本辦法之施行日期，由主管機關定之。

2 本辦法修正條文自發布日施行。

資通安全責任等級 C 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依 附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、 其他具有同等或以上效果之系統或標 準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內， 配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		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	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、 初次受核定或等級變更後之二年內，完成資通安全弱點通報機制 導入作業，並持續維運及依主管 機關指定之方式提交資訊資產盤 點資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者， 應於修正施行後二年內，完成資 通安全弱點通報機制導入作業， 並持續維運及依主管機關指定之 方式提交資訊資產盤點資料。
	資通安全	防毒軟體	初次受核定或等級變更後之一年內，

	防護	網路防火牆	完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能 訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別持 有證照及證書各一張以上，並持續維 持證照及證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機 關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執 行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情 勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

資通安全責任等級 C 級之特定非公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依 附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、 其他具有同等或以上效果之系統或標 準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		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	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、 關鍵基礎設施提供者初次受核定或等級變更後之二年內，完成資 通安全弱點通報機制導入作業， 並持續維運及依主管機關指定之 方式提交資訊資產盤點資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者， 應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之 方式提交資訊資產盤點資料。
	資通安全	防毒軟體	初次受核定或等級變更後之一年內，

	防護	網路防火牆 具有郵件伺服器者，應備電 子郵件過濾機制	完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
認知與訓練	資通安全教育訓練	資通安全專責人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專責人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，至少一名資通安全專責人員持有證照一張以上，並持續維持證照之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機 關判斷是否屬於核心資通系統。

二、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及 時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上 效用之措施。

三、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情 勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

四、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資 通安全證照。

五、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定 之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

資通安全責任等級 D 級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

資通安全情資分享辦法

修正日期：民國 110 年 08 月 23 日

第 1 條

本辦法依資通安全管理法（以下簡稱本法）第八條第二項規定訂定之。

第 2 條

本辦法所稱資通安全情資（以下簡稱情資），指包括下列任一款內容之資訊：

一、資通系統之惡意偵察或情蒐活動。

二、資通系統之安全漏洞。

三、使資通系統安全控制措施無效或利用安全漏洞之方法。

四、與惡意程式相關之資訊。

五、資通安全事件造成之實際損害或可能產生之負面影響。

六、用以偵測、預防或因應前五款情形，或降低其損害之相關措施。

七、其他與資通安全事件相關之技術性資訊。

第 3 條

1 主管機關應就情資分享事宜進行國際合作。

2 主管機關應適時與公務機關進行情資分享。

3 公務機關應適時與主管機關進行情資分享。但情資已依前項規定分享或已經公開者，不在此限。

4 中央目的事業主管機關應適時與其所管之特定非公務機關進行情資分享。

5 特定非公務機關得與中央目的事業主管機關進行情資分享。

6 前項分享之情資，經中央目的事業主管機關認定足以防止其他機關資通安全事件之發生或降低其損害者，中央目的事業主管機關得予以獎勵。

第 4 條

1 情資有下列情形之一者，不得分享：

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。

二、其他依法規規定應秘密或應限制、禁止公開之情形。

2 情資含有前項不得分享之內容者，得僅就其他部分分享之。

第 5 條

公務機關或特定非公務機關（以下簡稱各機關）進行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。

第 6 條

各機關應就所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。

第 7 條

1 各機關進行情資整合時，得依情資之來源、接收日期、可用期間、類別、威脅指標特性及其他適當項目與內部情資進行關聯分析。

2 公務機關應就整合後發現之新型威脅情資進行分享。

第 8 條

各機關應就所接收之情資，採取適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。

第 9 條

1 各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。

2 各機關因故無法依前項規定方式進行情資分享者，分別經主管機關或中央目的事業主管機關同意後，得以下列方式之一為之：

一、書面。

二、傳真。

三、電子郵件。

四、資訊系統。

五、其他適當方式。

第 10 條

1 未適用本法之個人、法人或團體，經主管機關或中央目的事業主管機關同意後，得與其進行情資分享。

2 主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享，應以書面與其約定應遵守第四條至前條之規定。

第 11 條

1 本辦法施行日期，由主管機關定之。

2 本辦法修正條文自發布日施行。

資通安全事件通報及應變辦法

修正日期：民國 110 年 08 月 23 日

第 一 章 總則

第 1 條

本辦法依資通安全管理法（以下簡稱本法）第十四條第四項及第十八條第四項規定訂定之。

第 2 條

1 資通安全事件分為四級。

2 公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：

一、非核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

3 各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：

一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

4 各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：

一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

5 各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件：

一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

第 3 條

資通安全事件之通報內容，應包括下列項目：

一、發生機關。

二、發生或知悉時間。

三、狀況之描述。

四、等級之評估。

五、因應事件所採取之措施。

六、外部支援需求評估。

七、其他相關事項。

第 二 章 公務機關資通安全事件之通報及應變

第 4 條

1 公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

2 前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。

3 公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

4 公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

第 5 條

1 主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。

二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。

2 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。

3 前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審核結果通知主管機關，並提供審核依據之相關資訊。

4 總統府、國家安全會議、立法院、司法院、考試院、監察院及直轄市、縣（市）議會，應於其自身完成資通安全事件之通報後，依第一項規定時間完成該資通安全事件等級之審核，並依前項規定通知主管機關及提供相關資訊。

5 主管機關接獲前二項之通知後，應依相關資訊，就資通安全事件之等級進行覆核，並得依覆核結果變更其等級。但主管機關認有必要，或第二項及前項之機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。

第 6 條

1 公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：

一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

2 公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。

3 前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。

4 上級、監督機關或主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。

第 7 條

1 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，就所屬、監督、所轄或業務相關之公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。

2 主管機關就公務機關執行資通安全事件之應變作業，得視情形提供必要支援或協助。

3 公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。

第 8 條

1 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。

2 前項演練作業之內容，應至少包括下列項目：

一、每半年辦理一次社交工程演練。

二、每年辦理一次資通安全事件通報及應變演練。

3 總統府與中央一級機關及直轄市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。

第 9 條

公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

一、判定事件等級之流程及權責。

二、事件之影響範圍、損害程度及機關因應能力之評估。

三、資通安全事件之內部通報流程。

四、通知受資通安全事件影響之其他機關之方式。

五、前四款事項之演練。

六、資通安全事件通報窗口及聯繫方式。

七、其他資通安全事件通報相關事項。

第 10 條

公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

一、應變小組之組織。

二、事件發生前之演練作業。

三、事件發生時之損害控制機制。

四、事件發生後之復原、鑑識、調查及改善機制。

五、事件相關紀錄之保全。

六、其他資通安全事件應變相關事項。

第 三 章 特定非公務機關資通安全事件之通報及應變

第 11 條

1 特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。

2 前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。

3 特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

4 特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

第 12 條

1 中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。

二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。

2 中央目的事業主管機關依前項規定完成資通安全事件之審核後，應依下列規定辦理：

一、審核結果為第一級或第二級資通安全事件者，應定期彙整審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。

二、審核結果為第三級或第四級資通安全事件者，應於審核完成後一小時內，將審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。

3 主管機關接獲前項資料後，得就資通安全事件之等級進行覆核，並得為等級之變更。

第 13 條

1 特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：

一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

2 特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。

3 前項調查、處理及改善報告送交之時限，得經中央目的事業主管機關同意後延長之。

4 中央目的事業主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。

5 特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應於審查後送交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。

第 14 條

1 中央目的事業主管機關就所管特定非公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。

2 主管機關就特定非公務機關執行資通安全事件應變作業，得視情形提供必要支援或協助。

3 特定非公務機關知悉第三級或第四級資通安全事件後，應召開會議研商相關事宜。

第 15 條

特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

一、判定事件等級之流程及權責。

二、事件之影響範圍、損害程度及機關因應能力之評估。

三、資通安全事件之內部通報流程。

四、通知受資通安全事件影響之其他機關之時機及方式。

五、前四款事項之演練。

六、資通安全事件通報窗口及聯繫方式。

七、其他資通安全事件通報相關事項。

第 16 條

特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

一、應變小組之組織。

二、事件發生前之演練作業。

三、事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。

四、事件發生後之復原、鑑識、調查及改善機制。

五、事件相關紀錄之保全。

六、其他資通安全事件應變相關事項。

第 四 章 附則

第 17 條

主管機關就各機關之第三級或第四級資通安全事件，得召開會議，邀請相關機關研商該事件之損害控制、復原及其他相關事宜。

第 18 條

公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：

一、社交工程演練。

二、資通安全事件通報及應變演練。

三、網路攻防演練。

四、情境演練。

五、其他必要之演練。

第 19 條

1 特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：

一、網路攻防演練。

二、情境演練。

三、其他必要之演練。

2 主管機關規劃、辦理之資通安全演練作業，有侵害特定非公務機關之權利或正當利益之虞者，應先經其書面同意，始得為之。

3 前項書面同意之方式，依電子簽章法之規定，得以電子文件為之。

第 20 條

1 公務機關於本辦法施行前，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安全事件之通報及應變。

2 前項通報及應變機制如有變更，應送主管機關重為核定。

第 21 條

1 本辦法之施行日期，由主管機關定之。

2 本辦法修正條文自發布日施行。

公務機關所屬人員資通安全事項獎懲辦法

修正日期：民國 110 年 08 月 23 日

第 1 條

本辦法依資通安全管理法（以下簡稱本法）第十五條第二項及第十九條第二項規定訂定之。

第 2 條

公務機關就其所屬人員辦理業務涉及資通安全事項之獎懲，得依本辦法之規定自行訂定獎懲基準。

第 3 條

有下列情形之一者，予以獎勵：

一、依本法、本法授權訂定之法規或機關內部規範，訂定、修正及實施資通安全維護計畫，績效優良。

二、稽核所屬或監督機關之資通安全維護計畫實施情形，或辦理資通安全演練作業，績效優良。

三、配合主管機關、上級或監督機關辦理資通安全維護計畫實施情形之稽核或資通安全演練作業，經評定績效優良。

四、辦理資通安全業務切合機宜，防止資通安全事件之發生，避免本機關、其他機關或人民遭受損害。

五、主動發現新型態之資通安全弱點或入侵威脅，並進行資通安全情資分享，防止資通安全事件之發生或降低其損害。

六、積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。

七、對資通安全業務提出具體建議或革新方案，並經採行。

八、辦理資通安全人才培育事務，有具體貢獻。

九、辦理資通安全科技之研發、整合、應用、產學合作或產業發展事務，有具體貢獻。

十、辦理資通安全軟硬體技術規範、相關服務及審驗機制發展等事務，有具體貢獻。

十一、辦理資通安全政策、法制研析或國際合作事務，有具體貢獻。

十二、辦理其他資通安全業務有具體功績。

第 4 條

有下列情形之一者，予以懲處：

一、未依本法、本法授權訂定之法規或機關內部規範辦理下列事項，情節重大：

（一）資通安全情資分享作業。

（二）訂定、修正及實施資通安全維護計畫。

（三）提出資通安全維護計畫實施情形。

（四）辦理資通安全維護計畫實施情形之稽核。

（五）配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。

（六）訂定資通安全事件通報及應變機制。

（七）資通安全事件之通報或應變作業。

（八）提出資通安全事件調查、處理及改善報告。

二、辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。

三、其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

四、對業務督導不力，致其屬員、所屬或所監督機關之人員有前三款情形之一。

第 5 條

公務機關辦理其所屬人員之平時考核，應審酌前二條所定獎勵及懲處情形，依事實發生之原因、經過、行為之動機、目的、手段、表現、所生之影響等因素為之；其所屬人員為聘用人員、約僱人員或其他與機關有僱傭關係之人員者，其獎勵及懲處之情形並應納入續聘之參考。

第 6 條

公務機關對所屬人員作成第四條各款情形之懲處前，應給予當事人申辯之機會；必要時，得就所涉資通安全專業事項，徵詢相關專家學者之意見。

第 7 條

1 本辦法之施行日期，由主管機關定之。

2 本辦法修正條文自發布日施行。

我的筆記

我的筆記