



國立臺南大學

113年度資通系統防護基準以 及委外廠商自評教育訓練



顧問諮詢

漢昕科技 楊雯珺

輔導顧問

20240711

BCCS 漢昕科技

資安整備專家



本校結構

系統管理者與資安人員

- 擁有自行開發或委外之系統之管理人員
- 系統放置位置於廠商或南大機房

全校人員

- 一般使用者或單位主管人員



全校資訊安全稽核(113.07.29~30、113.08.13~14)

- 稽核行程



Microsoft Word
文件

- 稽核內容



OpenDocument
文字

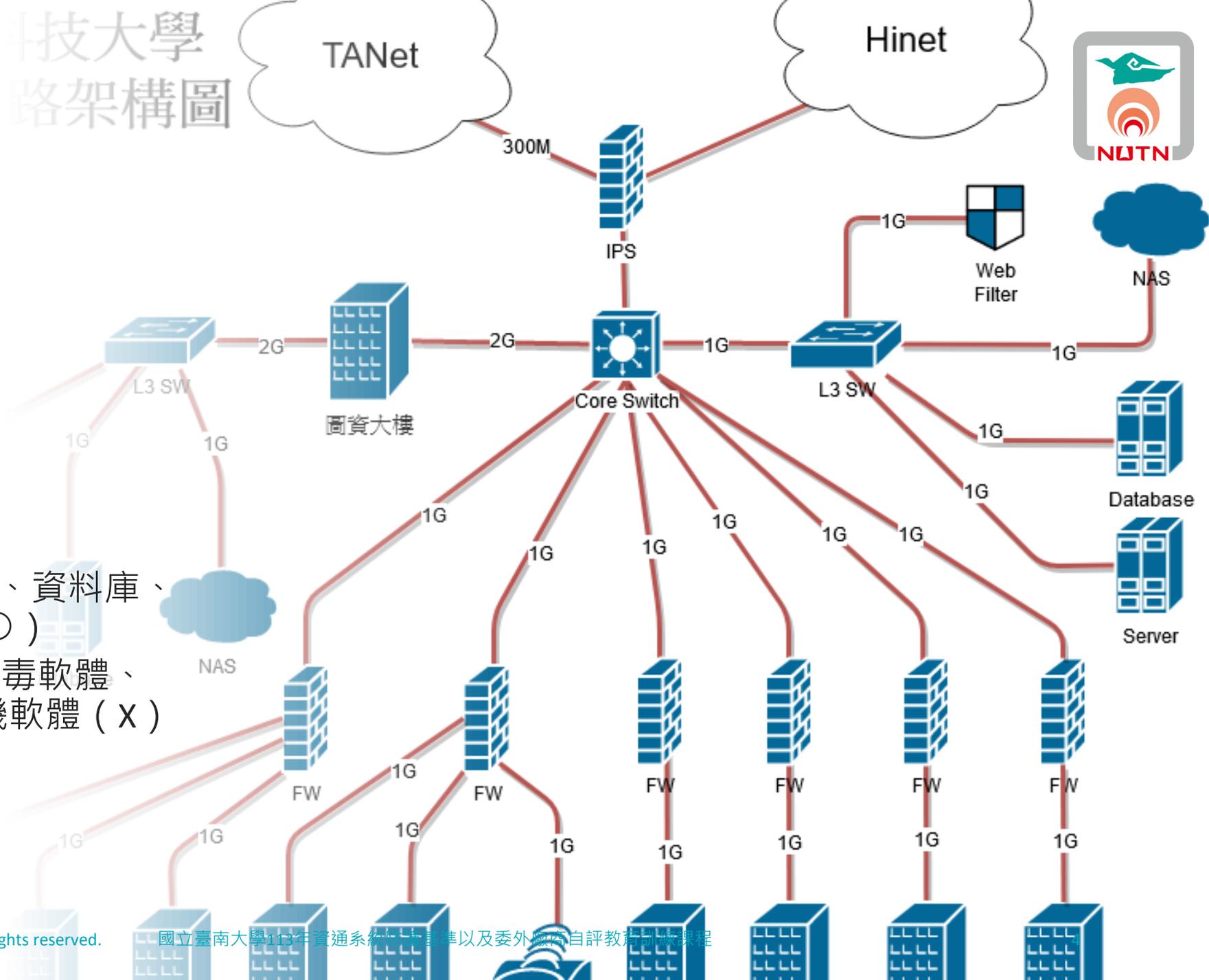
資訊系統

- 資通系統

- 自行開發
- 委外開發
- 可以設定與管控權限

- 例如

- 系統、網站(頁)、平台、資料庫、AD、電子郵件系統 (○)
- Windows作業系統、防毒軟體、個人電腦軟體、印表機軟體 (X)



資訊系統

- 何謂委外開發
 - 有**合約關係**，包含開發或維護(委託南大除外)
 - 可以客製化修改系統
 - 有叫修人員與聯絡方式
 - 權責在本校



大綱



資通系統等級評估

- 資訊系統安全等級評估表



防護基準以及委外廠商自評說明

- 資通系統妥適性檢視及防護基準實施情形評估表
- 委外廠商查核項目表



課後測驗



資訊系統安全等級評估表



南大入回

登出系統

計中首頁

南大首頁

資通安全管理法應辦事項 -- 資通系統防護需求分級鑑別

法規說明 分級原則 MTPD 說明

個人常用榜

熱門排行榜

資訊系統列表

資通系統防護需求分級鑑別

資訊系統查詢

問題與建議

2024/06/21

系統名稱：

--請選擇--

業務屬性：

-- 請選擇 --

原因說明：

業務屬性 原因說明

設定影響構面之防護需求等級

分別考量資訊系統於發生資安事件時可能造成之衝擊，即衡量資訊系統資料外洩、資料遭竊改、系統故障等情事時可能造成的後果嚴重程，並據以評估、設定安全等級

1.機密性：

防護需求等

原因說明

2.完整性：

防護需求等

原因說明

3.可用性：

防護需求等

原因說明

4.法律遵循性：

防護需求等

原因說明

防護需求等級：

最大可容忍中斷時間(MTPD)：

--請選擇--

儲存

防護基準以及委外廠商自評說明

資通系統妥適性檢視及防護基準實施情形評估表



- 依據：

資通安全法等級分級辦法 附表五 資通安全責任等級C級之公務機關應辦事項要求執行

- 辦理方式：

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（資責§11.11前段）

- 資料來源：
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304&kw=%e8%b3%87%e9%80%9a%e5%ae%89%e5%85%a8%e8%b2%ac%e4%bb%bb%e7%ad%89%e7%b4%9a%e5%88%86%e7%b4%9a%e8%be%a6%e6%b3%95>

委外廠商查核項目表



- 依據：

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。（資責§4.9）

- 資料來源：
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030303&kw=%e8%b3%87%e9%80%9a%e5%ae%89%e5%85%a8%e7%ae%a1%e7%90%86%e6%b3%95%e6%96%bd%e8%a1%8c%e7%b4%b0%e5%89%87>

資通系統妥適性檢視及防護基準實施情形評估表 範例說明

普級



Microsoft Excel
工作表

中高級



Microsoft Excel
工作表

委外廠商查核項目表

限公司受託者查核項目表

編號：
填表日期：113年 月 日
查核人員： 邱 偉

8.1	資訊安全事故管理程序	2024/4/6 下午 12:17
8.2	資訊安全事故處理程序教育訓練簽到表	2024/4/6 下午 12:17
3.4	配置適當之資通安全專業人員及適當之資源	2024/4/6 下午 12:17
4.1-4.2	資訊資產清冊	2024/4/6 下午 12:17
4.3	文件與紀錄管理程序	2024/4/6 下午 12:17
4.4	風險清單	2024/4/6 下午 12:17
5.1	年度教育訓練計畫(2023)	2024/4/6 下午 12:17
5.2	年度稽核報告(2023)	2024/4/6 下午 12:17
5.3-5.4	教育訓練簽到表1	2024/4/6 下午 12:17
5.3-5.4	教育訓練簽到表2	2024/4/6 下午 12:17
5.3-5.4	教育訓練簽到表3	2024/4/6 下午 12:17
6.1	內部稽核管理程序	2024/4/6 下午 12:17
6.2	年度稽核計畫(2023)	2024/4/6 下午 12:17

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1. 資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	依規定按時進行教育訓練之宣導。
	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？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	將資安訊息公告於布告欄。
2. 設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	指派高階主管擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議、資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	公司內部訂有資安責任分工組織。
3. 配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有訂定人員錄用之安全評估措施。
	3.2 是否符合組織之需求配置專業資安人力？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	公司依規定配置資安人員。
	3.3 是否具備相關專業資安證照或認證？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	專業人員具備ISO27001之證照。
	3.4 是否配置適當之資源？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	公司已投入足夠資安資源。
4. 資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	資產依規定指定管理者及使用者。
	4.3 是否有資訊、資通系統分級與處理之相關規範？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	已進行風險評估及擬定相應之控制措施。
5. 定期辦理資通安全認知宣導及教育訓練	5.1 是否定期辦理資通安全認知宣導？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有定期辦理宣導。
	5.2 是否對同仁進行資安評量？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	按期進行資安評量。
	5.3 同仁是否依層級定期舉辦資通安全教育訓練？	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	有定期辦理教育訓練。
	5.4 同仁是否瞭解單位之資通安全政策、目標及應	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	同仁均瞭解單位之

課後測驗





問題與討論