

大雅國中 109 年資通安全數位研習講義 (數位學習資源整合平臺與教學)

1. 網址: <https://elearn.hrd.gov.tw/mooc/index.php>



2. 學校網頁:

二、帳號申請與時數上傳設定 1. 進入網站後，按下左側【登入】鈕，然後選擇左邊「我的 e 政府」



2. 先確認有沒有我的 E 政府帳號



3. 輸入身分證字號進行查詢，如果已有帳號，請直接登入

3. 輸入身分證字號進行查詢，如果已有帳號，請直接登入，接下來**請看第 5 點**

公務帳號查詢

身分證字號: ☐ 顯示身份證字號

姓名:

以下所列為與此身分證字號和姓名關聯之帳號: (帳號已經過遮蔽處理)

帳號	姓名	身分別
sm****uh	杜建忠	公務人員

建議使用簡訊取回密碼

4. 若沒有帳號，請按下「申請公務帳號」進行帳號的申請

4. 若沒有帳號，請按下「申請公務帳號」進行帳號的申請

以下所列為與此身分證字號和姓名關聯之帳號：(帳號已經遠端處理)

查無相關公務帳號

 申請公務帳號

(1) 按下申請公務帳號



(2) 然後填寫必要的資料，按下建立我的帳戶



(3) 點選最下面的連結「申請成為公務帳號」



(4) 下面這個頁面，請輸入大雅國中的 OID 「2.16.886.111.90027.100045」，然後輸入你的 手機號碼，按下「我同意」

www.cp.gov.tw 顯示

您的自然人籍公務員案件進行中，請參預我的E政府公務帳號申請證之注意事項完成後續申請作業。

確定

我的E

會員登入

辦理公務帳號

我的E政府公務帳號申請書

會員帳號: may6303	申請日期: 民國 109年08月21日
姓名: 葉聖英	案件編號: 264311
申請項目: 自然人籍公務員(待審中)	
新帳號名稱: (臺中市立雙英國民中學)	
新帳號OUID: 2.16.886.111.90027.100047	

[illegible]

您係以 EGOV 帳號登入本平台，您在本平台帳號為：
K7512082401

請設定您於本平臺要顯示的頭幅，此頭幅會顯示於討論區、
我的學習王國排行榜、共學夥伴區...等資訊頁面。

* 頭幅：

* Email：

登入是否顯示學額狀態

將顯示其上學生數額   如果您的學校行政人員，但也必須取得全體教務處領導學員將數，請勾選。



本次課程 9 月 30 日截止

三、選課方式

1. 在 e 等公務員 首頁，請在查詢欄位輸入「109年第一次政府資通安全防護巡迴研討會」



2. 選擇報名課程，然後按「確定」



進入課程畫面後，選擇「上課去」



接下來左側點選「開始上課」，從選單中各章節逐一觀看，累積時數



3. 閱讀時數夠了之後，請點選左側「測驗／考試」



4. 完成測驗之後，要填問卷，先回到課程首頁，選擇「問卷／投票」



5. 要了解目前學習情況，可以從網站首頁點選個人專區，然後選擇「學習紀錄」



在頁面最下方，會有目前已參加的項目，以及有沒有通過，或是那個該做的沒做

No.	課程類型	課程名稱	上課期間	閱讀時數	測驗	問卷	通過條件	通過狀態	認證時數	終身學習時數上傳狀態	終身學習時數上傳時間	環境教育時數上傳狀態	環境教育時數上傳時間	教師研習時數上傳狀態	教師研習時數上傳時間
1	開放式	109年第一次政府資源安全防護巡迴研討會(FCEN-TER109100858)	2020-08-07 16:47:09 2020-09-05 10:21:25	03:12:07	100	未填	課程測驗：60分(含)以上 閱讀時數：01:30:00(含)以上 填寫問卷：是	--	3.0	--	--	--	--	--	--

- 可至【學習記錄】點【列印證書】



四、測驗題庫

- X 1. 針對資訊資產弱點進行修補後，不需要再到 VANS 系統進行資訊資產版本資料更新。
 - X 2. 機關 ISMS 的「導入」與「驗證」應該放在同一個採購案，以便要求通過驗證，取得證書。
 - O 3. TWGCB-ID 是我國政府組態基準編碼方式，可快速識別與查找政府組態基準(GCB)設定 項目。
 - X 4. 規模較小且無資訊(資安)人力的機關，無須成立或加入資通安全推動小組。
 - X 5. 帳號密碼設定只有自己知道，所以即使密碼很簡單也不怕被破解。
 - O 6. 駭客喜歡用最新議題搭配社交工程郵件進行攻擊。
 - X 7. 若只是瀏覽網頁並不會遭到挖礦程式所利用。
 - O 8. 駭客可用加密 VPN 連線串起多個不同網段並增加自身隱蔽性。
 - O 9. 駭客除了直接攻擊機關，也經常透過供應鏈進行攻擊。
 - O 10. LOTL 技術指駭客使用系統內建的服務或工具進行攻擊。
-
- X 1. 因電力中斷導致系統無法使用，不屬於駭客入侵行為，所以不用通報資安事件。
 - X 2. 機關 ISMS 的「導入」與「驗證」應該放在同一個採購案，以便要求通過驗證，取得證書。
 - O 3. VANS 系統可將已登錄的資訊資產項目與弱點資料庫自動比對，當重大弱點發生時可即時得知與應變處理。
 - X 4. 公營事業與政府捐助之財團法人，不是資通安全管理法納管對象。

- X 5. 政府組態基準(GCB)針對 Windows Server 2016 伺服器劃分不同角色，為方便部署，每個 角色所套用群組原則物件皆是相同的。
- O 6. 公務機關應該在知道資通安全事件後「1 小時」內通報。
- O 7. 目前已發展之政府組態基準(GCB)類別包含作業系統、瀏覽器、網通設備及應用程式。
- X 8. 若只是瀏覽網頁並不會遭到挖礦程式所利用。
- O 9. 機關應該要訂定機關內部與對所屬機關的資安稽核機制。
- X 10. 監視器之類的 IOT 設備，只要能用好，不需要進行更新。

- O 1. VANS 系統可將已登錄的資訊資產項目與弱點資料庫自動比對，當重大弱點發生時可即時得知與應變處理。
- O 2. 公務機關資安專責人員要專職擔任，即該人員只能辦理資安業務。
- O 3. 駭客透過 LOTL 技術，可以執行不在硬碟中的惡意程式。
- X 4. Dropbox 僅提供檔案儲存服務，不可能被駭客用來遠端操控系統。
- X 5. 機關首長公務繁忙，不受到資通安全管理法每年 3 小時資安通識教育訓練的規範。
- O 6. 駭客除了直接攻擊機關，也經常透過供應鏈進行攻擊。
- O 7. 依「資通安全責任等級分級辦法」規定，A 級與 B 級公務機關在初次受核定或等級變更 後之「一年」內，須依主管機關公告項目，完成政府組態基準(GCB)導入作業並持續維運。
- X 8. 政府組態基準(GCB)針對 Windows Server 2016 伺服器劃分不同角色，為方便部署，每個 角色所套用群組原則物件皆是相同的。
- O 9. 公務機關應該在知道資通安全事件後「1 小時」內通報。
- O 10. 駭客可用加密 VPN 連線串起多個不同網段並增加自身隱蔽性。

- X 1. 監視器之類的 IOT 設備，只要能用好，不需要進行更新。
- O 2. 公務機關應該在知道資通安全事件後「1 小時」內通報。
- X 3. 帳號密碼設定只有自己知道，所以即使密碼很簡單也不怕被破解。
- X 4. VANS 系統可針對目標主機進行弱點掃描，並產出弱點掃描結果報告。
- X 5. 機關 ISMS 的「導入」與「驗證」應該放在同一個採購案，以便要求通過驗證，取得證書。
- O 6. 駭客透過 LOTL 技術，可以執行不在硬碟中的惡意程式。
- O 7. 政府機關資安弱點通報機制(VANS)納管範圍包含 Windows 平台資通系統與使用者電腦 之軟體資產。
- X 8. 規模較小且無資訊(資安)人力的機關，無須成立或加入資通安全推動小組。
- X 9. 政府組態基準(GCB)針對 Windows Server 2016 伺服器劃分不同角色，為方便部署，每個 角色所套用群組原則物件皆是相同的。

O 10. 機關應該要訂定機關內部與對所屬機關的資安稽核機制。

O 1. VANS 系統可將已登錄的資訊資產項目與弱點資料庫自動比對，當重大弱點發生時可即時得知與應變處理。

X 2. VANS 系統可針對目標主機進行弱點掃描，並產出弱點掃描結果報告。

X 3. Dropbox 僅提供檔案儲存服務，不可能被駭客用來遠端操控系統。

X 4. 駭客帶來的資安威脅並不會影響日常生活。

O 5. 公務機關應該在知道資通安全事件後「1 小時」內通報。

X 6. 因電力中斷導致系統無法使用，不屬於駭客入侵行為，所以不用通報資安事件。

O 7. 駭客喜歡用最新議題搭配社交工程郵件進行攻擊。

O 8. TWGCB-ID 是我國政府組態基準編碼方式，可快速識別與查找政府組態基準(GCB)設定項目。

O 9. 目前已發展之政府組態基準(GCB)類別包含作業系統、瀏覽器、網通設備及應用程式。

O 10. 駭客透過 LOTL 技術，可以執行不在硬碟中的惡意程式。

X 1. 導入政府組態基準(GCB)時，須以 GCB 設定值為標準，無論如何都不能變更。

X 2. 政府組態基準(GCB)針對 Windows Server 2016 伺服器劃分不同角色，為方便部署，每個角色所套用群組原則物件皆是相同的。

O 3. 政府機關資安弱點通報機制(VANS)之五大作業流程為資訊資產盤點、資訊資產正規化、資訊資產登錄、弱點比對與修補、資訊資產更新。

O 4. 政府機關資安弱點通報機制(VANS)納管範圍包含 Windows 平台資通系統與使用者電腦之軟體資產。

X 5. 資通安全責任等級為 E 級或資通安全維護計畫已經併入上級機關辦理，便無須提報資通安全維護計畫實施情形。

X 6. 機關 ISMS 的「導入」與「驗證」應該放在同一個採購案，以便要求通過驗證，取得證書。

O 7. 目前已發展之政府組態基準(GCB)類別包含作業系統、瀏覽器、網通設備及應用程式。

O 8. 駭客喜歡用最新議題搭配社交工程郵件進行攻擊。

X 9. 帳號密碼設定只有自己知道，所以即使密碼很簡單也不怕被破解。

X 10. 監視器之類的 IOT 設備，只要能用就好，不需要進行更新。

O 1. 目前已發展之政府組態基準(GCB)類別包含作業系統、瀏覽器、網通設備及應用程式。

X 2. 駭客帶來的資安威脅並不會影響日常生活。

O 3. 駭客可用加密 VPN 連線串起多個不同網段並增加自身隱蔽性。

O 4. 依「資通安全責任等級分級辦法」規定，A 級與 B 級公務機關在初次受核

定或等級變更 後之「一年」內，須依主管機關公告項目，完成政府組態基準(GCB)導入作業並持續維運。

X 5.帳號密碼設定只有自己知道，所以即使密碼很簡單也不怕被破解。

O 6.政府機關資安弱點通報機制(VANS)之五大作業流程為資訊資產盤點、資訊資產正規化、 資訊資產登錄、弱點比對與修補、資訊資產更新。

O 7.LOTL 技術指駭客使用系統內建的服務或工具進行攻擊。

X 8.資通安全責任等級為 E 級或資通安全維護計畫已經併入上級機關辦理，便無須提報資通 安全維護計畫實施情形。

X 9.Dropbox 僅提供檔案儲存服務，不可能被駭客用來遠端操控系統。

X 10.監視器之類的 IOT 設備，只要能用就好，不需要進行更新。

O 11.公務機關初次受核定或等級變更後之一年內，C 級以上資通安全專責人員每人應持有 1 張 以上資安專業證照與 1 張以上資安職能評量證書。

O 12.駭客透過 LOTL 技術，可以執行不在硬碟中的惡意程式。

X 13.機關 ISMS 的「導入」與「驗證」應該放在同一個採購案，以便要求通過驗證，取得證 書。

O 14.駭客除了直接攻擊機關，也經常透過供應鏈進行攻擊。

X 15.導入政府組態基準(GCB)時，須以 GCB 設定值為標準，無論如何都不能變更。

X 16.因電力中斷導致系統無法使用，不屬於駭客入侵行為，所以不用通報資安事件。

O 17.駭客喜歡用最新議題搭配社交工程郵件進行攻擊。

X 18.若只是瀏覽網頁並不會遭到挖礦程式所利用。

O 19.VANS 系統可將已登錄的資訊資產項目與弱點資料庫自動比對，當重大弱點發生時可即時得知與應變處理。

O 20.公務機關應該在知道資通安全事件後「1 小時」內通報。 X 21.公營事業與政府捐助之財團法人，不是資通安全管理法納管對象。

X 22.政府組態基準(GCB)針對 Windows Server 2016 伺服器劃分不同角色，為方便部署，每個 角色所套用群組原則物件皆是相同的。

X 23.VANS 系統可針對目標主機進行弱點掃描，並產出弱點掃描結果報告。

X 24.針對資訊資產弱點進行修補後，不需要再到 VANS 系統進行資訊資產版本資料更新。

X 25.機關首長公務繁忙，不受到資通安全管理法每年 3 小時資安通識教育訓練的規範。

X 26.規模較小且無資訊(資安)人力的機關，無須成立或加入資通安全推動小組。

O 27.公務機關資安專責人員要專職擔任，即該人員只能辦理資安業務。

O 28.TWGCB-ID 是我國政府組態基準編碼方式，可快速識別與查找政府組態基準(GCB)設定 項目。

O 29.政府機關資安弱點通報機制(VANS)納管範圍包含 Windows 平台資通系統與使用者電腦 之軟體資產。

O 30.機關應該要訂定機關內部與對所屬機關的資安稽核機制。