資通安全管理法修法說明會（北區第 4 場次）

逐字會議紀錄

時間：109 年 12 月 14 日（星期一）下午 2 時 30 分

地點：臺大醫院國際會議中心 402AB 會議室（台北市徐州路 2 號 4 樓）

【主席致詞】(略)

【資通安全管理法施行情形及整體修法重點】(略)

【交流討論】

柯旻圻助理設計師：

有關簡報的部分，大家有沒有什麼看不懂、聽不懂或者疑問的部分，請提出來？（無）我們逐一從母法到各六個子法，我們看修改的部分。

首先母法的部分，這邊我們改的主要在財團法人、公法人的名詞定義，還有實施情形，公所及代表會給上級政府是比較大的改變，針對母法的修法大家有沒有什麼問題？（無）

細則的部分，這邊比較少，主要是公所、代表會它的實施情形是給上級政府，再來是實施情形的提報方式，由主管機關指定，上行政院管考系統去做提報，提報整個流程跟提報內容我們有做一個修改，讓大家可以比較方便填內容，即使機關沒有資訊人員，也會比較好填報，另外上級機關也可以幫所屬機關提報他們機關的實施情形，這個是細則比較大的改變，細則的部分，還有沒有其他修法有關的問題要詢問的？（無）

接下來是分級辦法，我們改了不少東西，影響最大的改變就是第 6 條 C 級的定義，針對 Mail Server 與 AD 的高防護需求，可是它沒辦法被定義為自行開發或委外開發的資通系統，這種 Mail Server 拉到 C 級，主要是維運，使用不算，如果上級機關有 mail server，你使用，這樣不算 C 級，有維運 Mail Server 或 AD 才會是 C 級。接下來是 VANS 與 EDR 端點防護機制的導入，這是比較大的改變，其他就是附表的調修，譬如說遠端連線，還有稽核的留存，針對分級辦法我們改這幾條，機關有沒有問題想要詢問？

勞動部勞工保險局：

因為最近 1 月 15 日要回一個資通安全等級調查表，剛好跟這個修法有關係，要填責任等級的調查表，其中有 1 個欄位就是剛才第 6 條具權限區分及管理功能之非自行或委外開發系統，欄位後面寫「必填」（如 Mail Server、AD 等），他在這個修正條文裡面，目的是為了要定義 C 級機關，因為其他原因已經被列為 A、B 級機關，這個欄位可以寫「無」嗎？

第 2 個小問題，這個具權限區分及管理等等的系統，類似有點像套裝軟體，像這邊舉的例子，微軟的 exchange 或者是微軟的 windows server，這些套裝軟體，既然是套裝軟體就是百百種，一般人對具權限區分及管理等等的系統，認定就會不一樣，是不是可以就調查表列舉的範例，譬如說 mail server、AD 或資料庫管理系統，是不是寫這些列舉的就好了？

柯旻圻助理設計師：

資安處有發 1 個責任等級的調查表，上面有 1 欄是寫分級第 6 條權限區分及管理功能非自行開發或委外開發的資通系統，這 1 項，主要 A、B 級本來就是 A、B 級，如果有的話，不能填「無」，因為你們有就要寫，這個主要是 AD、Mail Server，修法後我們就不用再調查一次，看 C 級以下的機關有沒有 Mail Server、AD，我們直接以各機關提報上來的這份資料，去做責任等級調整，有關於權限區分及管理功能，這個文字我們還在修，我們在想法要怎麼訂，把文字清楚一點劃分出來，像 office、Windows 那些也算是套裝軟體，我們還在想怎麼去做文字上的定義。

第 2 個是有關套裝軟體，為什麼文字寫這麼複雜？寫「具權限區分及管理功能」而不是直接寫「套裝軟體」？就像是我剛剛講的，一些比較小的套裝軟體是不是就會到 C 級？所以這邊才會寫它不是自行開發或委外開發的系統，像有些系統就是開發出來的，這沒有什麼好說，在自己機關的盤點就要盤進去，可是 Mail Server 或 AD 這種界限比較不像傳統的資通系統，這邊就會特別去做一個定義。

在填寫上我們為什麼會多加一個「其他」？因為這種類型的系統百百款，比較常見的是列表上有列的，Mail Server、AD、DBMS 與帳務處理，這邊列了「其他」，如果機關有想到類似這種情況，它不是自行或委外開發的，它也很重要，這 1 種比較偏套裝的系統，也可以填上去，可能會有我們比較沒有想到的，樣態比較特殊的系統，這個是第 2 題的部分。

主席林春吟高級分析師：

我補充一下，那一段主要是 C 級機關的研判，如果你是 A、B 級那一欄對你的重要性比較沒有那麼大，可是也不能寫「無」，就寫「等」就好了。

我們在切哪一條線以下是C級，我們沒有要讓C爆增，因為C級的要求比較多，大家不要自己建系統，以目前的定義是管理性的套裝軟體，我們希望把那一塊補足，如果像文書編輯，那不是我們要的東西，所以你們可以在那一欄，你們機關是屬於可能 C、可能 D，那一欄建議儘量把可能會符合的寫上去，因為我們現在也在蒐集大家有什麼樣的系統，我們也怕一刀劃下去讓大家不小心跑到 C 級，那邊我們目前在衡量，有關那一欄，A、B級寫幾個，然後寫「等」，如果可能是C或D，覺得可能會落進去，我們會建議幫我們寫上去，回來我們會彙整去看，看怎麼樣是比較好的衡量方式，這邊也要麻煩大家一下。

柯旻圻助理設計師：

分級辦法部分還有機關有問題嗎？

桃園署立醫院：

我想要問的是分級辦法附表一有分職能證書與證照，行政院有沒有建議資安長是屬於專職人員，他是不是需要去取得證書或證照？因為這問題對我們真的很重要。另外我這邊還想要問，因為修法完後是每個人要有一張，可是剛剛有舉例，如果團隊是 10 個人，裡面 4 個人有證書、4 個人有證照，那我可以分別是 8 個人嗎？這個問題我也想要釐清一下。

因為人員取得證書或證照這件事情，對於機關說是一個成本，我們在徵才的時候，其實不容易找到這樣具有證書或證照的人，我們也要請求行政院這邊給我們參考的準則或證照的排序，就是國際間有很多知名的證照，有些是來自於技術面、有些是管理面，他們怎麼去做等級的排序這個也希望給我們一些幫助。

柯旻圻助理設計師：

第 1 個問題，如果資安長是機關的資安專責人員的話，依法源要求，要取得至少 1 張以上證照。

主席林春吟高級分析師：

我們在資安法上，資安長建議是機關副首長，原則上機關副首長就不可能是資安專職人力，有時候我們去稽核的時候，我們也發現他們就把資

訊科的科長報出來當資安專職人力，可是那個是資訊科，所以裡面有資安作業跟資訊作業，用這樣去研判就知道資訊科長就不可能是專職，可是如果他是資安科長就可以當專職人力。所以你剛才的問題回到，除非你那個機關是資安的機關，你們機關副首長或資安長就有可能是專職人員，再來就看你們要不要把他提報為專職人員，如果提報為專職人員就會有相關的法遵議題。

桃園署立醫院：

是，我可以解讀為行政院其實沒有要求資安長是專職人員嗎？

主席林春吟高級分析師：

對，一般來說資安長不會是專職人力，我們為什麼要框在副首長，因為資安作業一定是全機關的事，全機關要做一定有跨單位協調，所以資安長一定要跨單位以上的人員擔任，才比較能夠協調不同的單位，所以照這個邏輯，的確我們沒有期待資安長會是一個資安專職人員。

柯旻圻助理設計師：

第 2 題，你的資安專職人員有 8 人？

桃園署立醫院：

我的團體有 10 個人，其中 4 個人有專業證照，另外 4 個人有職能證照，剛好分布為 8 個人，這樣是允許的嗎？

主席林春吟高級分析師：

原則上我們會先扣法遵，如果你們是 A 級應該配 4 位，我們要求這 4 位要具備執行資安的職能，所以我們會希望證書跟證照是落在這 4 位身上，不是聯合起來的，可能是剛剛同仁講時候沒界定太清楚，就算你有 10 個人，如果確定 A、B、C、D 是法定上的專職人員，你當然可以 6 位沒問題，可是我們稽核的時候，會去看這 4 位的證書跟證照有沒有達到法遵的要求，如果有就 OK，其他多的都是優於法遵，會變成優點。

再來人才訓練的部分，我們公布出來的證照清單有分類，1 個是管理的，1 個是技術類，因為機關裡面的專職人員，不見得都可以處理技術那邊，技術相對門檻會高一點，所以那些證照的排序會比較不容易，可是原則上可以把專職人力，先定位為管理面或技術面，如果兩邊都可以的話，對他來講議題不大，每個資安人員，我建議必須要拿到 ISO 27001LA 那一張，那一張算很基本，他等於把資安處理概念都融會貫通，那一張相形之

下要取得也比較簡單，讓大家可以快速符合法遵的要求，這是實務上我們看到很多機關是這樣的處理方式。

至於是不是技術方面，要看你們的同仁到底是對哪一塊比較有天分，因為訓練是一個成本、考證照也是一個成本，大家評估一下自己可以處理的方式。

桃園署立醫院：

還有 1 個問題，其實我是想要問這些證照的取得，員工取得證照之後，他可能會向機關提出需求要做加薪或者是獎金的要求，因為機關這邊沒有參考的基準，不知道怎麼樣的證照它的取得是有價值的，或者 27001 是基本的，在 27001 之上，我們應該要怎麼獎勵同仁下班之後進修、念書，鼓勵他繼續有更高的證照？

主席林春吟高級分析師：

比較專業一點，資通電軍那邊有 1 個可以參考的做法，他那邊會衡量，就是考到哪些證照可以加薪多少，那個資訊可以找來參考一下，就會對證照的難易度有一些區分，或許可以作為你們機關的參考。

柯旻圻助理設計師：

分級辦法大家還有問題嗎？

新北市社會局：

請教一下，去年我在台北市府服務，今年到新北市府，台北市與新北市在資訊人力配置差蠻多的，台北市很多單位有資訊室，新北市只有 1 個科裡面有資訊股，我們自己在資訊股正職人員只有 2 位，股長、管理師與約聘僱人員共 4 位，如果到 111 年 12 月 31 日，資安專職人員只能有 2 位，我們相信資訊股長不能是資安的人，因為他是資訊，像剛剛資訊科長不是資安科長，到那個期限之後，約聘僱又不是資安專職人員，這時候新北市這些單位在遵法性就會有問題，是不是在這上面可以把新北市比照台北市變資訊室，這當然不太可能，但是有這樣的問題，再請教資安處。

主席林春吟高級分析師：

有關機關的組織配置，權責在機關首長，我們很難從法或哪個層面去規範，因為會跟既有的法定權責有扞格，我們把過渡時間拉出來，期待機關從內部做員額或資源爭取的動作，我們這邊也是同步跟人事總處去協調，我們之前談的方案是外加，至少員額最快到位，人再想辦法到位，因

為整體國家的機關組織就是一個總員額法，目前也是框在那邊，最近扣合數位專責部會機關，一併考量資安人力的議題，我們也在看那一塊有怎樣的處理方式，才會把過渡時間延 2 年。

這位同仁是新北市社會局，首先在社會局裡面局長資源的配置方式，或者以整個新北市政府做通盤的考量，可是因為他的權責，要嘛就是你們局長，那如果涉及市府含所屬的話，可能要到市長那邊，都可以做一些協調，因為有一些縣市也有提出整體縣市增加員額的方案，都是有的。各機關作法不太一樣，有一些縣市他們有順利的跟他們的市長要到員額去聘人，這邊提供一些機關的做法給你們參考，這個問題還是要回到機關那邊去做一個處理。

財團法人聯合信用卡中心：

我們是屬於特定非公務機關，有 2 個問題，第 1 個是資通安全專責人員的部分，資通安全專業課程要受 12 個小時，每年至少 12 個小時，資通安全專業課程比較沒有什麼問題，但是資通安全職能，目前都只提供給公務機關，像我們這種特定非公務機關有沒有可能可以報名上這樣的課程，這是第 1 個。

第 2 個，資通安全專責人員以外的資訊人員，每人每 2 年要接受 3 個小時以上的資通安全專業訓練或資通安全職能訓練，3 小時的資通安全教育訓練這個比較沒有什麼問題，如果從 11 月 24 日那個 FAQ 裡面有提到，每 2 年至少接受 3 個小時以上專業教育訓練，這個部分有規定哪些施行單位？FAQ 3.15 吧，這個部分因為資訊人員都要去上的話，那個就不是 7,000 多個，這一塊我覺得應該很難達到這個要求，因為有規定是哪些單位施行才算是資通安全專業訓練課程，在 FAQ 3.15 上面，以上是我的問題。

主席林春吟高級分析師：

首先是我們職能訓練的部分，有 2 種班，一種有補助的，一種沒有補助，補助我們會從技術服務中心出錢，有補助我們只開放給公務機關報名，所以特定非公務機關可以報名沒補助那塊，其實也有機關反應那邊報不進去，也有機關會統整他所屬，去找辦訓練的機構，到他們機關來辦專班，然後開放讓其他人來上課，也有這樣的做法。

剛才講到資訊人員每 2 年 3 小時的做法，其實也是類似的，我們開放專業訓練有 4 類的資格，原則上那個扣合我們希望他是辦訓練的機構，找

辦訓練的機構來幫你們辦，那樣的課也是可以的，因為我們考量訓練品質的議題，也有機關在講可不可以他的廠商幫忙上課，廠商有時候找他的工程師，工程師可能技術很厲害，可是教學不是他的強項，雖然他很專業，我們這邊強調那個訓練是有專業性在的，像有一些訓練機構，不管是大學、巨匠、恆逸都是立案的訓練機構，那邊的課程就可以做一個訓練處理。

桃園署立醫院：

我想要延續剛剛這位長官的問題，資訊人員的定義，可不可以請行政院給我們明確的定義？

柯旻圻助理設計師：

資訊人員就是在機關的資訊單位。

主席林春吟高級分析師：

我們資訊人員的定義是採比較廣義的，在我們FAQ上有，他應該是從事資訊相關的，有一些機關業務單位會開發系統，他在維運那個系統的同仁，我們也定義成資訊人員，所以在我們稽核的時候，也會要求他必須要達到資訊人員這邊需要有的訓練時數。

桃園署立醫院：

請問駐點的 MIS 算嗎？可能只是那個地方、診所負責維運電腦？

主席林春吟高級分析師：

他是廠商？

桃園署立醫院：

是我們的同仁，他就是駐點在那邊。

主席林春吟高級分析師：

可是處理他們的 MIS 嗎？

桃園署立醫院：

是。

主席林春吟高級分析師：

那就算。

新北市教育局：

我們之前有特別寫信請問 1 個問題，私立國中小、高中職的學校因為走的是 TANET 的骨幹，可是我們卻無法進行管轄，是不是在這次資安法

修法把私立學校涵蓋在這個範圍之內？

主席林春吟高級分析師：

因為目前私立的國中小、高中職不在資安法納管對象。你是透過什麼方式詢問？

新北市教育局：

透過 mail 到資安處。

主席林春吟高級分析師：

TANET 是指教育部那個，教育部常常對使用它們骨幹網路會有一些規範要求，他有沒有把這些私立的納進去？

新北市教育局：

他現在就是說要問行政院這邊，因為我們之後要做行政院的填報。

主席林春吟高級分析師：

這一點我們跟教育部確認一下，可能漏接了，畢竟它有讓私立學校在那個 TANET 骨幹上做運作。

新北市教育局：

如果不在管轄範圍內，他們的資安漏洞，包含向上集中都沒有辦法做，我們進行弱掃，又發覺他學校伺服器特別多、掃出來的弱點特別多，我們如果又無法管轄，這一塊是很大的漏洞。

主席林春吟高級分析師：

這一塊我們跟教育部討論一下，因為你們在相同的網路骨幹上運作，就像是大家都在 GSN 上面 RUN，理論上我們會確保大家都要有同樣的防護能量，不然就會感染給大家。

新北市教育局：

所以之後私立學校是不是走行政院的填報方式？

主席林春吟高級分析師：

我們跟他確認一下，因為它目前不在我們的納管清單裡面。

北區國稅局：

剛剛提到資通安全專責人員以外的資訊人員，每年要 3 小時的資通安全專職的教育訓練，因為我們在 8 月中有收到行政院資通安全發 1 個文，109 年政府防護巡迴研討會，因為有作成線上的課程，所以認列上面所寫的規定，因為作成線上課程，我們本來都是要去上課，可否建議每年至少

有錄製這樣的課程？因為用線上課程，公務人員本來就在上課，所以可以節省經費，剛剛您講，恆逸、巨匠，我們一個人上課的錢大概要 3,000 到 8,000 元，我們機關資訊人員 50 幾個，對我們來說是非常龐大的預算，我們建議是否可以比照每年錄製類似這樣的課程，讓我們資訊人員去線上上課。

主席林春吟高級分析師：

你的建議我們再帶回去研議一下，今年上半年情況比較特殊，所以才會有那樣的議題，因為我們會認列專業時數，原則上大家會有一定的參與情形，是不是適合用線上的方式，我們再回去研議一下。

台東地方法院：

剛剛簡報有提到其他相關事項裡面，有關資安專職人員配置，機關以約聘僱或委外人員擔任過渡性做法，延長到 111 年 12 月 31 日，現在的問題是台東還有離島金門、澎湖，有時候正職人員異動很多，這些離島或偏鄉的機關，可不可以不要在這個限制裡面，可以長期用約僱或委外的作為資安專職人力？

主席林春吟高級分析師：

原則上我們會希望各機關爭取正式的員額來處理資安這件事，因為資安的作業常常會涉及一些機敏性，所以我們建議還是爭取正式員額，我們過渡期間是為大家爭取這個時間，就目前的政策方向是沒有要開放的，謝謝。

中央研究院：

有關資安教育訓練可不可以增加在職比例？因為我們機關大概 6,000 人，也有很多人會在 11、12 月報到，目前實務上有一些困難點。

第 2 個，在附表十各營運持續的系統備份，應在運作系統不同地點，之前是不同處，照之前的定義是同一個機房不同機櫃就可以符合，那現在不算。另外地點可不可以再有一個明確的定義，譬如說距離多少，可以去跟其他的單位說如何去配合。

主席林春吟高級分析師：

您是希望增加一個在職期間沒有滿多少，可以排除在計算的數字外？這個我們回去研究一下。之前是用「不同處」不是表示在這個空間的這一邊跟那一邊就符合，的確有人看到不同處，就認為一個放東邊一個放西邊

就符合，所以我們這一次才讓它更精準，讓大家不要誤解，不是表示之前可以，之前就是不可以，現在只是用字精準，讓大家不要誤解。至於加上距離我們回去研議一下是要不要加進去，因為以前做異地備援，有時候會有參考的距離，超過多少公里，那時候沒有放進去，可能有一些考量，這個我們回去再做一下研議。

中央研究院：

再補充一下，因為我們這邊老師級的人特別多，他們會反映他們已經到那個層級還在上這個東西，有點浪費時間，有沒有其他的替代方案可以讓他們滿足這個時數的要求，又不要強迫他們的上課。

主席林春吟高級分析師：

如果你們有建議的做法可以提供給我們參考看看，我們目前想到的做法是上課取得時數，這是一般正規做法，如果有其他...

中央研究院：

因為他們已經在幫別人上課，他派出去以後，他在別的地方幫別人專業課程，可是我們這邊卻要求他上 3 小時基本的課程。

國立台灣藝術教育館：

正職專責人員人力配置這部分，就目前資料看起來，只有簡報部分有提到，但是法或是正式的公文都沒有提到這一塊，這個部分，將來有沒有可能以正式的發函或什麼方式，讓長官知道到 112 年後就不能以約聘僱或委外的方式去替代專職的人員，這樣長官才會知道如何因應。

柯旻圻助理設計師：

我們有同步更新在資通安全會報網站資安法常見問題，我們有寫剛剛簡報上的內容，這部分可以參考，用我們 FAQ 上面的內容。

主席林春吟高級分析師：

那一邊主要會比較機動性的調整，有一些比較細部的解釋，或者一些滾動修正，目前的做法是在 FAQ 上處理，比較不可能入法，因為入法後每次光要修法，會緩不濟急，比較不適合大家使用，你們內部要簽陳可能先拿 FAQ 做陳核或報告，有一些機關他們會在定期會議中，把一些要討論的議題放到簡報裡，你們可以先拿資安會報網站上 FAQ 的內容先去做處理。

中央研究院：

我要問的是資安弱點通報機制與端點偵測與回應機制的問題，這個導

入要導入全院的系統，我們裡面還有一些研究單位，裡面還有分行政電腦跟研究用的電腦，研究用的電腦也要導入的話，老師會說我在監控他，我們要怎麼回應他們這一點？

主席林春吟高級分析師：

有一些機關裡面的成員會需要比較花時間溝通，在學術單位有，之前曾經在法制單位也有反映過，我們提供法制單位的處理方法給你參考，原則上會拿這個法的依據過去，當你要跟他做什麼事情的時候，要他人在現場，跟他說明是依法要處理的事情，他們原則上會用這個動作處理。因為他們也曾經發生過，在沒有落實讓他本人在現場的情況，造成後續一些爭議，再來讓那個成員的主管去處理成員那邊的溝通議題，因為你剛才講的都是屬於一些溝通遵循那方面的議題，那個在法，可能比較難處理。

至於剛才講就是他導入的範圍，尤其是 EDR 的部分，我們目前走的方式，在這邊先列出來，主要方便大家爭取相關的預算資源，因為每一個機關可以取得的資源不太一樣，所以我們這邊的規範就沒有定死說你的範圍，這種定法比較像目前在一般事項裡面資安健診的做法，曾經在說明會的時候，有機關有提出他們的建議，提供大家參考，如果沒辦法全機關佈建的時候，那個機關其實是比較有資源的機關，所以試了 2 套 EDR，他那一天提的建議是，他們覺得 EDR 佈在主機端效果比較大，你們可以看看你們優先序，個人電腦這邊至少一些具管理者權限要先佈，1 個是你的資源、1 個是你佈的策略，再來逐步去做有效果的防護出來，提供一些建議給你們，萬一你們沒有辦法順利的爭取到比較充足的資源的話。

中央研究院：

補充一下，我們這邊剛好有法制加研究的法律所，如果說牴觸到個資議題的時候，有辦法嗎？因為我們之前發生過案例，真的在 log 調閱就出現問題，可能會有更大的爭議。

主席林春吟高級分析師：

原則上我們處理的是處理公務的設備，它原則上應該是一個公務環境安全的維護，我們先不要講電腦，有一些機關的實體環境，你要進出是要出示證件才能進出，有一些門禁管制的，如果要擴充到比較多的議題，可能比較難在這邊討論，我知道你們目前面臨的難處，可是原則上回到我們現在處理的是公務運作環境，我們在執行的，也是在維持公務環境的安

全，理論上應該有一些可疑的跡象會引發下一個動作，很多東西可能要做一些溝通，或由管理層去做一些處理，不然有些機關，我不確定你們機關能不能做，就是你要接上機關的網路，就必須達到一定的安全要求，你才有可能接上我們的網路，當我偵測到你可能有危害的話，有些機關可能讓他先斷網，可是你們機關可以怎麼樣處理，可能還是要回到機關裡面大家討論跟共識。

財團法人中小企業聯合輔導基金會：

我想問 e 等公務園時數可以認列嗎？

柯旻圻助理設計師：

e 等公務園上面有關資安相關課程，我們在 FAQ 也有寫，就是認資安通識時數，跟資安專業時數是 2 個時數，認列不同。

柯旻圻助理設計師：

分級辦法還有什麼問題嗎？

集保結算所：

請問附表 10，有關於存取帳號管理有新增 1 條，閒置時間與使用時間應該是對應以往的閒置時間與使用時間，可是後面有 1 個資通系統之使用情形與條件，這樣子是很廣的，請解釋一下使用情形及條件的定義範圍是多廣？

主席林春吟高級分析師：

這一條主要我們要講的是明確定義，像是帳號類型、功能限制、操作時段、來源位置、連線數量、存取資源，你剛才講的使用條件及狀況，可以參考我們說明那邊列的一些項目去做考量。

集保結算所：

因為說明的內容是一般的時候會有，可是法出來的時候，會放在備註欄嗎？放在最下面的部分？

主席林春吟高級分析師：

一樣也會在右邊，照我看到的，在右邊會有一些說明，對法的一些定義去做比較細部的描述，不然有一些文字，大家在解讀上會有一些困惑，就是透過後面的說明處理，您看看我們目前說明的內容，讓你們在執行上有沒有問題，如果還是有一些不明確，可以再反映給我們，我們再看怎麼補強，這個我們到時候都會一塊出來。

桃園市政府主計處：

想請教有關專職課程，資安人才培訓服務網，他們在 8 月有公告推廣 e 等公務園的線上課程，說明是為人員資安職能，編制 4 門有關資通安全管理相關的課程，那 4 門的課程也不能算是專業課程嗎？其實 e 等公務園上有課程是括弧專業課程，可是是限制中央才可以上，其他單位不能報名上課，如果數位課程不能算，那些課程也算嗎？

主席林春吟高級分析師：

有關於你剛剛反映的狀況，我們回去整個在盤一下，我們不能認列為專業課程的話，那個「專業」放在那邊可能不太適合，至於技服放上去的 4 門資安相關課程，我們還是依照我們目前的邏輯，e 等公務園上，我們目前認列都是通識課程，剛剛你講的技服那 4 門課，還有標註專業的課程，我們回去確認一下，做一個統一的調整，謝謝。

中央研究院：

新版的 FAQ 有提到 e 等公務園那邊會增加資安通識與資安專業課程代碼，有這樣的前提之下，是不是代表以後 e 等公務園也可以認列資安專業？

主席林春吟高級分析師：

那邊主要是方便大家計算資安時數，因為在學習時數系統裡沒有辦法分開，有機關反映是不是在系統裡算，大家上課的時候都會匯進去學習時數，2 個代碼的標註是幫助大家在匯入學習時數的時候標好，匯進去後就可以從系統撈出來，可以很快知道哪一個同仁專業或通識時數多少，主要是在處理時數統計那一塊，目前 e 等公務園那邊，我們還是用通識時數的方式處理。

土地銀行：

請問 VANS 導入，1 年內要導入 VANS，我們要導入 VANS 的話是不是已經有規格或做法，是不是已經開過說明會，是只有公務機關嗎？

主席林春吟高級分析師：

去年我們就辦說明會，今年 6、7 月的時候也有辦說明會，那時候發的通知對象，是我們會納進來做規範的對象，如果你們已經錯過那一段的話，在我們技服網站上有 1 個 VANS 專區，不管是教材還是作業方式，目前大家比較可行的做法，機關裡面有盤資產的一個工具，把資產資訊盤集

中以後，讓它轉 CPE 格式，對接到 VAN 那邊幫你比對，比對後會把資料 PASS 回來給你們，讓你們清楚目前類似 1,000 筆資產裡面，有哪些弱點、有多少筆，至於類似 100 筆弱點分布在機關的哪邊，要到機關自己的資產系統去看，我們也不會知道那 100 筆弱點在哪裡。我們要掌握大家弱點的情況，我們真的會去追是重大的事件，像今年 10 月初因為那個會影響 AD，所以我們就會去追，要把他修補做處理，其他的部分就回歸機關處理，因為那個風險會在機關裡面，你們要評估可以修補或做什麼防護，去控制風險，大概整個處理是這樣，你可以看看，如果你們還不清楚，上面應該有一些聯絡資訊，在技服中心的網站。

外交部領事事務局：

想請教一個，這邊提到增加端點偵測及回應機制，所謂 EDR 機制，在資通安全防護也歸列 1 個防毒軟體，防毒軟體與 EDR 產品它的費用蠻貴的，主要我想問像市面上有防毒軟體，本身聲稱有 EDR 功能，像這樣的防毒軟體也認列 EDR 的部分嗎？

主席林春吟高級分析師：

原則上我們強調是它達到的功能效果，的確市面上有一些防毒軟體有預見到這個技術趨勢，他有把相關功能融到產品內，只要你們的工具有這樣的功能，原則上是可以的，沒有說你一定要另外買一套。

柯旻圻助理設計師：

分級辦法就到這邊。接下來是通報應變辦法，我們主要改了 2 個點，1 個是有關聯的多起資安事件，一定時間內陸續發生，由上級機關額外通報做統籌的規劃調度；第 2 個，上級機關可以請發生資安事件的機關，對他們事件的調查處理改善報告提出一些修正或是一些說明，這邊我們明訂，在中間損害控制跟復原作業，可以請所屬機關提出說明，通報應變辦法除了這邊之外，還有沒有什麼問題想要了解？（無）

下一個特定非公務機關的稽核辦法，比較重要是 OT 的部分，因為現在開始 IT 的稽核已經做差不多，再來有些特定非公務機關，CI 提供者、公營事業，這種類型的資安稽核會需要該領域的專家，所以這部分有因應做稽核團隊組織上的調整，特定非公務機關稽核辦法有沒有問題？（無）

情資分享辦法，鼓勵特定非公務機關主動分享情資，中央目的事業主管機關可以鼓勵，情資分享這邊有問題嗎？（無）

獎懲辦法，這個主要是針對經上級機關跟主管機關一直催辦，比較重大的情形，如果真的需要動用到獎懲的話，原則上我們會以獎勵為主，我們不會希望做這個懲處，如果有很重大的資安缺失要做懲處的話，檢視範圍，法明訂上級機關也一併做檢視，獎懲辦法這一條各位有沒有問題？（無）對於獎懲其他項目有沒有問題？

新北市社會局：

我記得好像是上個月，前1、2個月行政院資安處來文有新進人員宣導範例，上面有提到一點，如果同仁有發現資安問題回報的話，有獎勵的辦法，這個立意是很好的，用獎勵的方式，但是剛剛有提到，希望機關不要列入 KPI，確實發生這樣的案例，市府評估各局處，因為有通報資安事件所以有被扣分，所以是不是有機會在條文中敘述到這一點？

主席林春吟高級分析師：

條文比較難對於人員那一塊做處，目前我們沒有想到比較好的方式，如果有建議的條文內容，可以給我們，我們跟法規那邊研究一下。有關資安事件通報，原則上相信大家作業層面，其實不會有我通報資安事件反而被受處罰的概念，的確有一些管理層級的人員，其實他們不太清楚資安事件是一個不可控的，就算做得再好，就像人會不會生病一樣，每天早睡早起、運動、吃得健康，也沒有辦保證不生病，發現資安事件這件事情，原則上第一時間的責任不在機關這邊，可是後面會去看你是不是有應作為未作用的事情，就可能會引發一波獎懲，可能有獎也有懲，因為你發現得早，讓其他人沒有受害，其實應該獎勵；可是也曾經發生過，已經上新聞的事件，你的帳號密碼已經洩漏出去了，大家知道後第 1 個動作是改帳密，但是還沒有改，像那種情況，雖然他們前面通報算快，可是後面處理是不 OK，所以後面那件事情就應該去追究，可能大家沒有放在心上。所以通報資安事件不太適合只因為你通報資安事件就去做負面的處理，我知道有 1 個部會在做社交工程演練，大概點了以後就記下來，那個部會多 1 個，如果你發現了，覺得是可疑信件去通報，就是用加分處理，社交信件就很擬真，訓練大家資安意識，那是另一個切入點。有關資安事件，大家要有比較正確的處理概念，可能需要用宣導的方式，不然那個文化或認知沒有改變的話，其實法定在那邊，一樣還是會發生我們覺得不是那麼合理的事情。我們在資安長會議，一直宣導資安事件不要納入 KPI，我們出去

稽核的時候，發現那個機關把資安事件納 KPI，我們一定會寫待改善事項，可能需要用另外的方式去做對應處理，我們嘗試讓大家的觀念可以慢慢扭轉過來，如果用 COVID-19 來講，如果有人確診又不講，又在這邊出沒，是很讓人害怕的，你們再內部看看怎麼樣多溝通，辛苦了。

柯旻圻助理設計師：

獎懲辦法還有問題嗎？（無）整個資安法的修法還有沒有什麼問題？

主席林春吟高級分析師：

大家如果不在這邊發問，我們也有紙本提供做意見表示，或者是會後再交流，今天謝謝大家參加這個說明會，說明會到這邊，謝謝。