資通安全管理法修法說明會（中區第 2 場次）

逐字會議紀錄

時間：109 年 12 月 17 日（星期四）下午 2 時 30 分

地點：集思台中新烏日會議中心富蘭克林廳

（臺中市烏日區高鐵東一路 26 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：

開始進行交流討論的階段，我們這個會議有逐字紀錄，所以請大家舉手的時候報一下自己的機關，再提出問題。針對剛剛簡報的部分，施行情形還有修法，有沒有什麼問題想要提出的？

臺中市政府地方稅務局：

第 1 個，想問一下專職人員的證照，因為我們都是派非資訊專業的人去考，所以難度相當高，或者考上的人因為異動又走了，又要派人去考，所以我覺得這個對我們一般的行政機關取得這樣的證照是有點困擾。上課拿證照錢也不少，因為機關都規定要拿到證照才能核銷，如果沒有拿到證照就要自行吸收，所以大家接到這個任務都壓力很大，我不知道這個部分在國家資通安全會報這邊是不是有一些解決方法？這是第 1 個問題。

第 2 個，剛剛簡報有提到事件通報是知悉起 1 個小時，這個「知悉起」的定義可不可以講清楚一點？

第 3 個，有關 GCB 例外管理的定義跟列管，像 GCB 例外我們是不斷的在檢討，但是有時候實體環境或者有一些服務的限制，所以在開例外我們的確有點不知道那個標準在哪裡。

第 4 個，EDR 的部分，從去年開始，我們終端本來只有裝防毒跟去更新，未來可能有一些端點安全檢測機制要 ON 起來。就我所知，我們是還沒規定的時候就開始做，但是因為我們家的電腦數蠻多的，有 1,800 多台，算起來每年光 EDR 的經費就要 5、600 萬，這個對稽徵機關也是一個很大的負荷，不知道國家資通安全會報是不是有一個通用的東西，譬如是

運用你們既有的資源，否則我們這個經費非常龐大，以上是我的疑問，謝謝。

主席林春吟高級分析師：

我先回答一下，第 1 個，有關證照的部分，原則上機關的人才還是要培養，所以還是要麻煩機關要編相關的教育訓練費用。另外你們機關的核銷其實是有一點問題，之前也曾經有機關反映過，同仁考到照才可以核銷，其實不應該是這樣，之前新北市某個局處有反映過這個問題，再回頭去看一下新北市自己的規定，其實訓練的費用是機關要支付的，它要付 1 次，如果後面考照沒有考到，的確沒有考到的錢是要自己付，可是訓練跟考照分 2 段，訓練的部分在他們機關的規定是由機關負擔，除非你們機關明文不行，因為這是法定要的訓練，所以這可能要回去跟機關的主會計溝通一下，因為這是法定要的，要同仁自己花自己的錢不合理。

臺中市政府地方稅務局：

沒有，他沒有辦法拿到證照，所以他必須再去訓練。

主席林春吟高級分析師：

原則上機關只會幫你出 1 次錢，這是目前的規定沒有錯，要不然如果同仁一直考，機關也會受不了，雙方會各有立場，可是目前我們知道一些會計的核銷還是支付的制度，的確會幫你出 1 次錢。

臺中市政府地方稅務局：

因為我們自己派員去上課拿證照可能要經費，技服中心是不是可以定期開一些課程，我們主動去上？我們可能就不會有經費上的壓力。

主席林春吟高級分析師：

在現在的法令規定上，資安專職人力有 2 個要求，一個是專業證照、一個是職能證書，專業證照就是一些國際上的證照，其實最基本的那 1 張 ISO 27001 LA。

臺中市政府地方稅務局：

那個沒問題。

主席林春吟高級分析師：

在證照方面，你已經有 1 個基本的保障門檻了，如果同仁想要再拿更進階、更高階的證照，那就是更多的事情。職能證書那一塊，技服中心那邊我們有投注一些資源，有一些教育訓練是補助班，資源還是有限，沒有

辦法達到每個人都可以滿足，儘量大家可以報那個補助班。

臺中市政府地方稅務局：

補助班好像也要繳一半的費用。

主席林春吟高級分析師：

對，那個還是要機關支應，我知道有一些縣市或上級的部會會統一去開班，等於訓練的費用是上級支應，調訓所屬機關，等於找人來機關這邊開班，這樣有可能在經費上比較節省。台中則看市府那邊是不是可以統一辦教育訓練，理論上它不應該排除稅務單位，我知道有些縣市政府出來辦，他所屬的機關，不管是民政、戶政就是去報名，只要是A、B、C級機關，你們有資安專職人力訓練的需求，就是去報名，讓它統一去支付那些錢，這都是實務上的一些做法，先提供你參考。

第 2 個，資安事件知悉 1 小時，原則上「知悉」是給大家有一個處理上的緩衝，「知悉」的確沒有一個比較明確的定義，到底你什麼時候知道，不見得你知道就是發生的時候，可能發生一陣子才發現，當你知道這件事，就要去通報。我們在實務上最常發生的爭議，你的資安事件都上報了，你還不去通報，要怎麼說你不知悉？實務上也有人說「資安人員知悉才算」，不是，是這個資安事件他們家的主管，反正誰看到報紙，原則上那個時間就會開始起算，所以不要把它限縮。因為只要有一些公開特定的時間，就可以拿那個時間當依據，當然機關裡面自己有時候會覺得服務異常，你會去確認一下，如果你覺得是資安事件，就趕快先去通報，我們要請大家掌握這個處理原則，因為 1 個小時時間有時候不小心就超過了，或者你們平常就記好，如果要通報，它的網站、網址、帳號密碼在誰手上，常常發生真的要通報的時候，找不到那個人來通報，所以每個機關應該都有幾個人、有那個帳號可以進去通報。

第 3 個，有關 GCB 例外管理，原則上 GCB 會做一些管控上的設定，會採比較嚴格的方式，所以在有一些業務執行上，必須做一些條件上的放寬，我們實務上會做這個提醒，主要就是，它可能是某一個單位用某個系統需要放寬，可是那個機關是全機關放寬，這樣就不 OK，我們提的其實是這個。原則上用到的再去放寬，不要有一個放寬就大家一律放寬，這是我們要提醒的部分。在實務上必須要放寬，它才能做應用，這是可以的。你們有持續在檢討、注意這件事情，這很好、這就是我們鼓勵的，看看客

觀環境有沒有改變，如果改變就去做調整、檢視，有時候我們可能為了在處理某一件事情暫時把它放寬，可是後來忘記關起來，常常後面就會開始出事，所以定期檢視這件事很重要，大家有很多細瑣的事情必須做處理。

第 4 個，EDR 的部分，你們之前已經開始做，這是很好的，因為現在很多的攻擊，其實防毒軟體越來越抓不到，為什麼導 EDR？因為 EDR 可以就一些流量去做截取，後面經由它的 AI 或不管什麼樣的分析，先找出一些可疑的，先在它還沒有發作前擋下來，這就是我們為什麼要導這件事情。EDR 目前在整個經費上，如果是採共契去下訂，經費是非常高的，可是我們也有訪過幾個機關的案例，他們統合所屬單位，以量制價的概念，它的價錢跟共契上差非常大，它是有議價空間的，國內也有一些新創團體有提供 EDR 的服務。所以採購策略上大家可能要注意，大家聯合去談，他們會有一些可行的方案出來，共契原則上處理的就是讓你採購很方便，兩個是不一樣的。

臺中市政府地方稅務局：

其實你講的我們當然知道，誰能統籌這件事情？一定是縣市政府，但是因為我們算是府外單位，我們可能就要自己處理，我相信有一些稅務單位應該也都是府外單位，我發現那個價格嚇死人，我們去年是正好有一些結餘款，當然我們也採用了那個策略，跟廠商做 1 個策略，我們外網優先，我們有做實體更新，就先做外網。但是今年開始變成強制規定的時候，我們就有點擔心，以前我們還可以說先做外網，內網反正有實體隔離。但是如果未來這都是強制規定，連內網都要做，那個價格我們有點無法負擔。也許我們也會試著先提，去爭取經費，但是我覺得這個經費真的很可怕，如果以 1 個授權 2,000 的話，我們 2,000 台電腦就 5、600 萬了，我想其他單位應該也會有這種困擾，誰能夠去統籌這個資源，我覺得應該需要有中央的單位給我們一些支援。

主席林春吟高級分析師：

我們一直以來跟國發會推動的都是資訊/資安資源向上集中，這一段要嘛縣市政府、要嘛部會，我們會希望它統籌處理這件事，稅務單位其實對到中央，還有 1 個財稅資訊中心，沒關係，這個訊息都可以跟上級機關反應，像財稅資訊中心，就我們去訪視的時候，他們也有說他們會幫大家統籌一些事情，這件事情我們還沒有談到，這個東西可以去反映。因為我們

去訪機關，目前這件統籌的話，它出來的價錢跟共契上就有差距，他們佈建的數量是上萬台，如果照共契的價錢，佈建上萬台，你可以估算大概是多少錢，可是他們一定不是那個價錢，這個是有點市場機制，我們這邊其實也不方便去做處理。可是就我們去訪現實的狀況，用一個量跟他們談價是有機會的。而且EDR不管是國外的產品，還是國內的產品都有，當供應商多的時候，就有一些議價空間在。目前也有一些既有的防毒軟體是有搭EDR功能，我覺得都可以訪看看。

因為就機關來說，可能是經費支出；可是就廠商來說，其實它也有市場占有率的議題，這一段可能還是麻煩大家多協助一下，我們這邊也會跟那些廠商做一些溝通，因為當他們的產品在多一點場域運作的時候，其實對他們產品的優化也是有幫助的，這個是雙方要共同合作的。先回應到這邊，還有沒有其他機關針對簡報部分要提出問題？（無）

柯旻圻助理設計師：

簡報部分如果沒有問題的話，我們就進修法，首先看母法，我們主要改的就是名詞定義，公法人跟財團法人。另外一個重點，公所、代表會實施情形提報給上級政府，比照地方制度法精神。針對母法修法的部分有沒有機關有問題？（無）

施行細則的部分，修正比較重要的部分，實施情形的提報方式由主管機關指定，統一用一個系統，針對細則修改的部分，有沒有機關有問題的？（無）

分級辦法，有幾個大重點，第1個，C級機關的定義，有關Mail Server跟AD應該C級，這部分的文字我們會再修，機關如果有比較好的界限劃定，也歡迎提出一些建議。第2個，VANS跟EDR的導入，1年內跟2年內。針對分級辦法，有沒有機關有問題？

臺中市政府地方稅務局：

這個導入，因為其實那個授權是1年、1年的，導入是持續一直都要有？看起來是這樣。

主席林春吟高級分析師：

持續營運，我說明一下，您的問題主要是屬於弱點通報？還是端點防護？還是2個？

臺中市政府地方稅務局：

端點。

主席林春吟高級分析師：

原則上，在我們修正條文發布後 2 年內，大家要做這個導入的作業，要持續的營運，後續如果我們有規定一些偵測資料提交的話，必須要照我們那個規格提交，當我們要請大家提交偵測資料的時候，這邊我們會去跟業者談，跟他們把規格確認清楚再過來，不會讓各機關各自去弄。

其實之前其他場次提到的問題，我在這邊跟大家分享一下。有沒有規定一些佈建的範圍？目前我們沒有明確的佈建範圍，可是大家要去思考，一個是你可以爭取到的資源有多少，再來把資源花在刀口上，把它先佈在你覺得最重要、影響最大、要保護的資產上。

之前有 1 個縣市政府，他們比較幸運，他們已經試用至少 2 套不同的 EDR 佈在他們機關裡面，那時候給的建議，因為我自己沒有佈過，只能把別人的經驗提供給大家，他們覺得 EDR 佈在主機端效果比較好，可能因為他們的主機應用服務是非常多的，可是在稅務可能相對單純，在你們的機關說不定就不是你們的優先選項，對他們來說，他們覺得佈在主機端效果是比較好的，佈在使用端效果沒那麼好，可是有可能他們的使用者端環境單一控管，就相對單純。所以每個機關要評估一下，你要保護的資產，複雜度比較高的，到底是在主機端還是使用者端？或者特定的哪幾台電腦？這都是可以去考量的。

也有機關今年因為有發生資安事件，所以他們馬上爭取到一筆錢，把他們所有設備通通佈了，各個機關的狀況其實不太一樣。

臺中市政府地方稅務局：

我想問未來你們在看我們落實佈建的部分，譬如我們有一些規劃，我們是外網的電腦先佈，或者是您剛剛講的佈 Server，來不及佈在我們全部的設備，在這個遵循性上，不知道你們是怎麼看這個事情？

主席林春吟高級分析師：

我請問一下，你有沒有上過 ISO 27001 LA？

臺中市政府地方稅務局：

有，我本身有證照。

主席林春吟高級分析師：

所謂「稽核」重點在哪裡？它會去管理你的佈建方式嗎？它原則是就

你的處理方式去做一個確認是否達到這個。再來，你是否有更好的建議。

臺中市政府地方稅務局：

我知道，這個部分是我們在寫的時候，但是因為你們現在採取的機制是我們要主動告訴你我們的執行情形，有可能我的執行情形，譬如 2,000 台電腦，就外網先佈一半，可能是 50%有佈建，不知道這樣寫回去的時候會不會認為這樣佈建不完備，但是因為我們已經解釋，我們是實體隔離的，可能內網沒有立即的危險，所以我們就沒有第一時間佈。

主席林春吟高級分析師：

所以你們就要把它寫清楚。

臺中市政府地方稅務局：

我們把它寫清楚，但是不知道你們在看我們回報的東西會不會有影響。

主席林春吟高級分析師：

你是跟你的上級機關提報，所以你要溝通的對象是上級機關。在我們的立場，我們會希望大家可以保護、爭取到相關的資源做處理，在實務上為什麼這麼做？你的規劃原因、理由是什麼？資安是一個風險管理的概念，我們現在可以做的就是想辦法降低風險，你是不是有降低你的風險？

臺中市政府地方稅務局：

但我怕的是我們沒有全部佈建就是違反法令。

主席林春吟高級分析師：

我剛才有沒有提到任何你違反法令的事情？沒有吧，因為每一個處理的程序，我沒有辦法在這邊跟你保證什麼，但是做這些事情都要資源，我們現在先把文字落出來，方便大家去爭取資源；當我們沒有列出來的時候，大家去爭取資源可能就要看，像你們之前可能就有運用到一些資源去做處理，可是有些機關可能就沒有辦法。可是當我們法列出來，我知道有的機關就會拿這個，說法規定要這麼做，所以編這些經費去爭取，這件事情就是這樣。至於有些處理上的細節，如果還需要進一步討論，我們會後再處理。

柯旻圻助理設計師：

剛剛是針對 VAN、EDR 的部分，責任等級分級辦法修法的部分還有機關有問題嗎？（無）

通報應變辦法，主要改的點有 2 個，1 個是有發現相似、相關的資安事件，或是針對同一的體系、同樣攻擊手法，這種額外提報 1 個資安事件做統籌規劃。另外 1 個，在資安事件的處理上，事中的損害控制、控管，上級機關或中央目的事業主管機關可以請所屬提出說明或做修改。針對通報應變辦法這兩點機關有沒有問題想要詢問的？（無）

特定非公務機關資通安全維護計畫實施情形稽核辦法，這邊比較單純一點，針對 OT 稽核，因為現在開始會有一些 OT 的稽核，在小組的組成上、比例上有做一些調整，針對特定非公務機關稽核辦法的擬修正內容，有沒有機關有問題或建議？（無）

再來是情資分享，主要改的內容就是鼓勵特定非公務機關主動分享資安相關的情資。針對這一條有什麼想法或問題想詢問的？（無）

最後是獎懲辦法，主要就是法條明訂在主管跟上級機關的部分一併做檢視。獎懲辦法這一條有問題嗎？

南投縣教育處：

獎懲辦法的部分主要是針對公務機關，其實學校獎懲的處理部分，除了行政人員之外，並沒有辦法用一般公務人員的獎懲辦法來處理，學校大部分都是由學校的老師做資安的管理，這個部分我們在推動的時候，其實會造成一些老師覺得我的本質工作就是教書，跟老師的獎懲有關的是教師的獎懲辦法，在教師法裡面，跟這個相衝突的時候，取決於誰？它的法源依據是什麼？這是我的建議。

主席林春吟高級分析師：

教師那一塊我們跟教育部之後研議一下，看那一塊怎麼處理會比較好。據你剛剛所說的，教師的部分，原則上不適用公務人員獎懲辦法？非常謝謝你提供這個建議，我們後續會跟教育部討論一下怎麼處理，可以幫助大家，謝謝。

柯旻圻助理設計師：

獎懲辦法之外，其他的母法跟子法整個修法如果還有問題的話，請大家舉手提問，或者有什麼建議想提供的也可以提出。（無）

主席林春吟高級分析師：

如果大家暫時沒有要在現場發言提問的話，也歡迎大家用紙本的方式提供相關建議給我們，或者會後我們可以做進一步的交流跟討論，我們今

天說明會就到這邊，謝謝大家參與。