「推動證券商導入金融零信任架構問卷」

問題與討論

更新日期 民國 114 年 3 月 19 日

前言

本文件整理了本公司在實體會議和電子郵件等場合中，從各業者蒐集來之問題、以及相應的回答。這些問題和回答已根據主題進行分類，包含以下幾個方面：場域及系統篩選、遠距辦公場域、雲端存取場域、系統維運管理場域、應用系統管理場域、服務供應商場域、跨機構協作場域等常見問題。此文件旨在供證券業者參考。

如本文件內容有未盡事宜，業者仍應依據「金融業導入零信任架構參考指引」的相關規定進行辦理。

目錄

0. 場域及系統篩選

編號	問題(Q)	回應內容(A)
1.	題目中的應用系統是否指的是評估的系統？	是，請以填寫於「說明」分頁的系統為評估對象。
2.	如果未達到題目說明之所有條件，是否應選擇「其他」？	若未達到選項1，請以選項2至5為主進行選擇。如需補充說明（例如：詳述說明已執行部分），請直接在「補充說明」欄位中回答。
3.	導入過程是否有針對不同等級券商作區分？	未針對不同等級券商而有所不同。
4.	在低衝擊情境中，什麼是「非自動化提供客戶服務」？	此文字來自於「金融機構辦理電腦系統資訊安全評估辦法」。惟挑選系統的方法僅為參考，挑選系統的方法因公司規模和系統數量不同而異，並沒有標準化的方法。我們可將提供客戶服務的系統歸類為衝擊較高的系統，例如：核心系統，以排除對公司影響較大的系統。
5.	如果公司沒有含有客戶資料、或其恢復時間目標（RTO）超過8小時的系統，是否就沒有可供評估的系統？	挑選系統的方法僅為參考，挑選系統的方法因公司規模和系統數量不同而異，並沒有標準化的方法。若公司系統較少，無法使用參考之方法論，則只要任一系統符合六個場域中的任一條件，即可做為評估對象。
6.	是否能再說明「雲端存取」、「服務供應商」、「跨機構協作」的意思？	雲端存取場域：指的是系統或服務建置於雲端（即公有雲，例如 AWS、Azure、GCP）。因此，如果系統不是雲端系統，未建置於雲端，則不適用於雲端存取場域。 服務供應商場域：指的是系統允許提供公司資訊系統服務的廠商員工直接存取，例如作業系統維運、網路設備維運等。亦即，系統或設備存在廠商員工使用之帳號。 跨機構協作場域：指的是系統允許公司的業務協力廠商員工使用。亦即，系統存在非同一法定個體之員工使用的帳號。
7.	以客服系統套用至題目為例： 一、「雲1，存取雲端系統在進行身份驗證時是否使用多因子認證」。這是指存取客服系統時是否使用多因子認證嗎？如果客服系統不是雲端系統，這題是否就	如果客服系統不是雲端系統，未建置於雲端，則不適用於雲端存取場域。請選擇一個預計導入零信任的系統，該系統需符合六個場域中的一個，然後根據該場域進行回答即可。不適用的場域可直接回答不適用。 雲端存取場域：指的是系統或服務建置於雲

	不適用？還是這題是指客服系統存取雲端系統時，是否在身份驗證時使用多因子認證？ 二、部分題目詢問是否有使用IAM、SIEM、SOC等，這些問題是否需要先確認客服系統是雲端系統，否則應皆為不適用？	端（即公有雲，例如 AWS、Azure、GCP）。因此，如果系統不是雲端系統，未建置於雲端，則不適用於雲端存取場域。
8.	若以VPN系統作為此次評估系統，有涵蓋四個場域，是否能先就填完其中一個場域的問卷來繳交？	可以，選一個場域先行回答。
9.	如果我們挑選的「高風險低衝擊」應用系統僅供內部使用，並且無遠距辦公、無雲端存取、無跨機構協作，是否只需填寫「場域_系統維運管理」和「場域_應用系統管理」這兩個頁籤？	是的。在這種情形下，只需填寫「場域_系統維運管理」和「場域_應用系統管理」兩個場域。
10.	評估的系統僅供內部網路使用，但通過遠距連線進入公司後，即算是連接到公司內部網路並可登入該系統。這種情況是否可以跳過「遠距辦公」場域的問卷？	以您目前的描述來說，該系統適用於遠距辦公場域。只要透過VPN、VDI等方式從公司外部進入公司內部網路並存取的系統，均適用於遠距辦公場域。「僅能在公司內部網路使用」的意思是指無法使用VPN或VDI方式進行遠端存取。
11.	遠距辦公的場域中，仍是有提到應用程式支柱及資料支柱，是否係指應用程式或資料可以在Internet上存取或是僅透過VPN/VDI的連線方式?	是否使用VPN/VDI的連線是用來判斷是否適用於遠距辦公場域的標準。因此，如果任一系統可以在連入VPN/VDI後使用，那麼此系統則適用於遠距辦公場域。 如果應用系統不需要連入VPN/VDI即可在網際網路上使用，則不適用於遠距辦公場域。

1. 身份		
編號	問題(Q)	回應內容(A)
12.	問題1： 在「0_場域系統篩選」中，我們選擇高風險低衝擊系統（假設為系統A）。如果系統A需要進行登入，我們在1.1中是否需要確認從登入VPN開始到系統A之間所有的登入資訊是否使用了多因子認證（MFA）？還是只需確認登入VPN是否使用了MFA即可？如果只需確認VPN的話，原因是什麼？ 問題2： 同理，在指引項次1.6的日誌蒐集中，是否需要確認所有中間的身份驗證日誌都需蒐集？	問題1： 本問卷是基於高風險低衝擊原則設計。因為VPN/VDI是遠距辦公場域的範圍，回答遠距辦公場域問卷時只需確認登入VPN這段是否使用了MFA即可。後續經過的其他系統（包括系統A本身）係屬於其他場域的範疇。 問題2： 指引項次1.6涉及可視性分析，等級為III。重點在於需要有完整的日誌以進行關聯分析，因此所有身份驗證日誌都需要納入蒐集範圍。
13.	指引中僅提到OTP，但問卷中使用的是TOTP。PWC的定義是否相同？	在指引項次1.2中提到「排除簡訊、語音及電子郵件OTP」，這些類型的OTP被認為是無法抵抗網路釣魚的MFA機制。而TOTP是一種可以綁定實體載具的MFA機制，能夠抵抗網路釣魚攻擊。 以參考原則1.2來說TOTP僅為舉例，各券商應考量是否使用實體載具。
14.	我們的遠端使用 AnyDesk 並搭配otpcode，這樣的配置是否符合1.1？	以此情境，若 AnyDesk 以使用帳號密碼及OTP進行身分驗證，是有符合1.1。但應考量AnyDesk 的使用是否適當，於未來導入零信任架構，係不適合用此類工具。

2. 設備		
編號	問題(Q)	回應內容(A)
15.	在零信任架構問卷中，有許多部分提到「EDR」。如果我們導入的是「MDR」，是否符合問卷中EDR的要求？	請確認您的MDR解決方案具有偵測端點行為的功能，若有，即為符合。MDR（Managed Detection and Response）是一種資安事件偵測與回應的服務。要確保符合問卷中對EDR（Endpoint Detection and Response）的要求。
16.	參考原則項次2.4「偵測到設備」，是指連線的設備還是我們正在評估的伺服器？	「偵測到設備」指的是連線設備，而非評估標的伺服器。係依據參考原則項次2.4，關於控管設備之動態屬性若有不合規時的處理方式，指引提到三種：「授權審核條件」、「隔離機制」或「限制須經VDI」。

3. 網路

編號	問題(Q)	回應內容(A)
17.	參考原則項次3.2「是否已建置SDN/SDP 網路管理機制」，依照參考原則的原意，是否也可以採用微分段（Micro-Segmentation）作為解決方案？SDN 和 SDP 在指引中並未出現。	是的，任何可以實現微分段（Micro-Segmentation）之解決方案皆可以。由於微分段的實作方式有很多種類，其中一些方法在實作方法比較難以擴展，因此題目以較高標準為基準。如果需要補充您公司的具體作法，可以在「補充說明」欄位中填寫。
18.	參考原則項次3.6「公司是否建立如下資安事件偵測與應處機制: SIEM、NDR、SDN/SDP、SOC、可依據IOC分析」，SDN/SDP是否可以使用微分段（Micro-Segmentation）作為替代方案？	是的，任何可以實現微分段（Micro-Segmentation）之解決方案皆可以。由於微分段的實作方式有很多種類，其中一些方法在實作方法比較難以擴展，因此題目以較高標準為基準。如果需要補充您公司的具體作法，可以在「補充說明」欄位中填寫。
19.	參考原則3.5 題目為「SDN 是否能根據 NDR 提供的入侵指標（IOC）來管理設備接入後可存取的網段」，倘若NDR已具備如參考原則所述具有動態調整網路設定或即時告警功能，是否可不串接SDN，直接將NDR作為解決方案?	可以。由於各種資安設備和解決方案的功能各不相同，若需要補充貴公司的具體作法，請填寫在「補充說明」欄位中。
20.	如果所選系統為SaaS，是否所有關於SDN/SDP的問題都不適用？	是的。可參考「雲端存取」頁籤中，參考原則項次3.1和3.2的問卷已有說明：SaaS和PaaS不適用。因此，無需使用 SDN/SDP 相關解決方案，日誌蒐集也無需包含其日誌。

4. 應用程式與工作負載

編號	問題(Q)	回應內容(A)
無		

5. 資料

編號	問題(Q)	回應內容(A)
21.	根據參考原則5.7，假設公司已完成項目a、b和d的建置，並預計在3到5年內完成項目c和e，回答欄位是否只需填寫c和e？	項目a、b、c、d和e均為必須建置的內容。因此，如果c和e預計在3到5年內完成，則在5.7的回答中應填寫「4」。
22.	在參考原則5.7中，「公司是否建立以下資安事件偵測與應處機制: 已建置SIEM、SIEM已收容應用程式之日誌、已建置SDN、已建置SOC、資料管理系統」，是否可以用Micro-Segmentation替代SDN/SDP作為解決方案？	是的，任何可以實現微分段（Micro-Segmentation）之解決方案皆可以。由於微分段的實作方式有很多種類，其中一些方法在實作方法比較難以擴展，因此題目以較高標準為基準。如果需要補充您公司的具體作法，可以在「補充說明」欄位中填寫。