推動證券商導入金融零信任架構作業問卷說明會

資誠智能風險諮詢管理有限公司
三月 2025

Agenda

一、問卷簡介
二、場域及系統篩選
三、各場域題目說明(以「1.場域_遠距辦公」為例)
四、後續工作項目
五、 Q&A

1

問卷簡介

簡介

本問卷係依據2024/07/15「金融業導入零信任架構參考指引」評估各證券商導入零信任架構之進度。

系統盤點
(方法論僅供參考)

- 盤點公司全部系統
- 考量各系統是否適用於六個場域

篩選系統
(方法論僅供參考)

- 判斷各系統是否含高風險情境、低衝擊情境
- 篩選屬於高風險且低衝擊的系統

填寫問卷

選擇一套系統回答問卷：

1. 場域_遠距辦公
2. 場域_雲端存取
3. 場域_系統維運管理
4. 場域_應用系統管理
5. 場域_服務供應商
6. 場域_跨機構協作

2

場域及系統篩選

填寫問卷

#	領域	題數
1	0_場域及系統篩選	0
2	1.場域_遠距辦公	30
3	2.場域_雲端存取	32
4	3.場域_系統維運管理	24
5	4.場域_應用系統管理	30
6	5.場域_服務供應商	27
7	6.場域_跨機構協作	33
	總題數	176

填寫問卷

「推動證券商導入金融零信任架構問卷」問卷使用說明

本問卷係依據2024/07/15「金融業導入零信任架構參考指引」評估各證券商導入零信任架構之進度。

本問卷以自評進行：

1. 各券商應依據「金融業導入零信任架構參考指引」中的零信任架構實作建議：「風險導向，優先處理高風險場域」，選擇導入零信任架構的範圍。因此，本問卷提供辨識**高風險**、**低衝擊系統**的方法論供各券商參考。請參考下述的「高風險、低衝擊系統方法論參考」。然而，本方法論僅供參考，與後續評估無直接關聯。
2. 券商可**自行選擇**並說明依據**一套系統**回答「六大場域與『零信任架構實作參考原則分級表原則』的評估」。請考量「高風險、低衝擊系統方法論參考」中六大場域的定義，並選擇符合該系統的場域的進行回答。

高風險、低衝擊系統之方法論參考

第一階段 0 場域及系統篩選

方法論參考：盤點公司所使用之**全部系統**，並請考量這些系統是否適用於「金融業導入零信任架構參考指引」所定義的**六個場域**。

第二階段 0 場域及系統篩選

方法論參考：依高風險系統篩選方法，識別每個場域適用系統中屬於**高風險**之系統。

方法論參考：依低衝擊系統篩選方法，識別每個場域適用系統中屬於**低衝擊**之系統。

第一階段 – 盤點所有系統，以及其適用之六大場域

遠距辦公	使用者及設備位於傳統資安防護邊境外，如：人員透過VPN存取系統、人員透過VPN使用公司個人電腦存取、人員透過網際網路可存取
雲端存取	雲端資源(SaaS、PaaS及IaaS)位於傳統資安防護邊境外，如：M365、Google Workspace、自建於雲端之伺服器、自建於雲端之微服務
系統維運管理	含重要主機設備及系統軟體（作業系統、資料庫等）之特權帳號管理
應用系統管理	重要應用系統之管理者或高權限使用者帳號，如：帳號管理員、可接觸大量個資或機敏資料者
服務供應商	委外廠商之遠端維運管理，該系統設有維護廠商帳號，且透過遠端方式進行設備與系統軟體（作業系統、資料庫等）之維護
跨機構協作	重要應用系統開放予外部使用者從外部存取，用以共同協作企業業務，其人員到離或使用設備非屬本機構管控範圍者

同一套系統可能會適用多個場域，但每個場域則不一定有適用系統

第二階段 – 篩選高風險、低衝擊系統

高風險系統(符合任一情境)

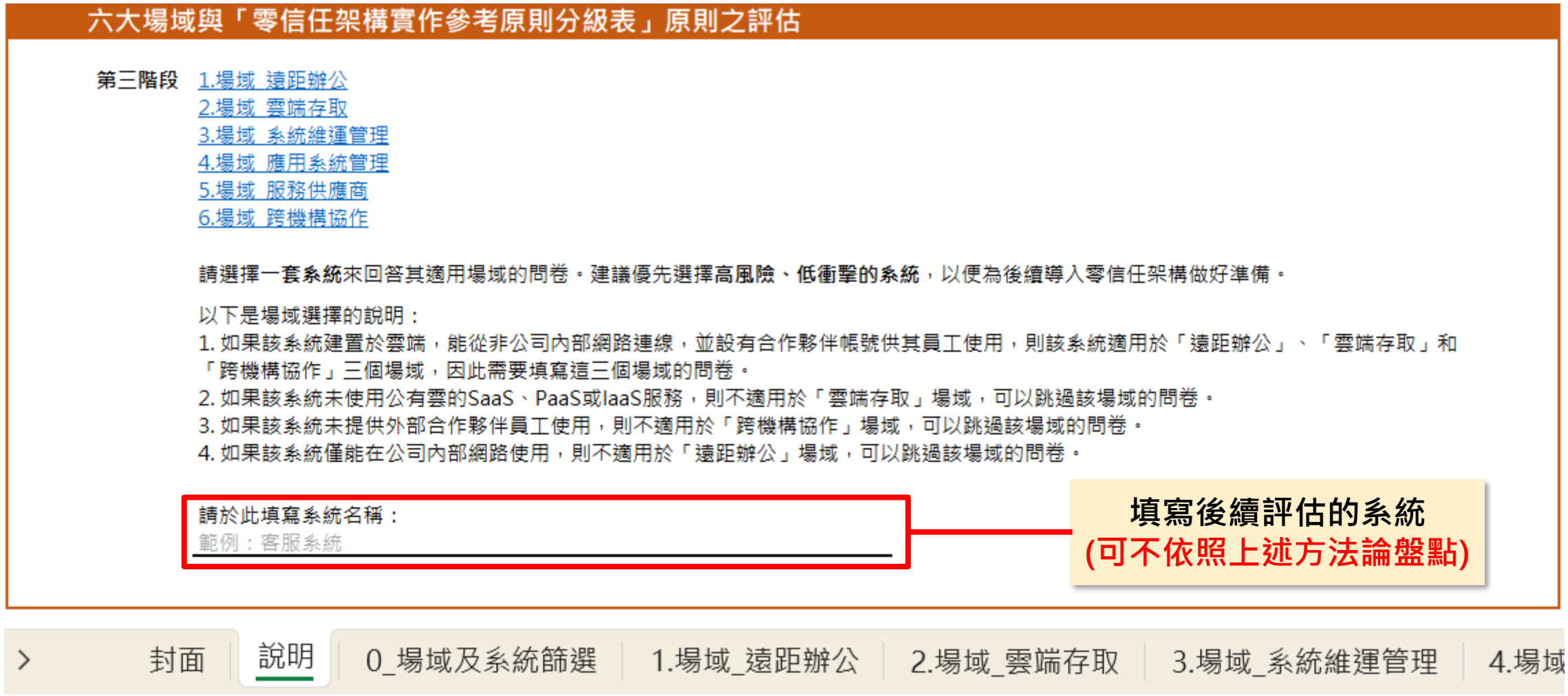
- 這些系統是否存有客戶個資？
- 這些系統是否存有客戶交易資料？
- 這些系統是否存有員工個資？

低衝擊系統(符合任一情境)

- 這些系統是否為非自動化提供客戶服務？
- 這些系統之回復時間目標 (RTO) 是否超過8小時？

適用「金融業導入零信任架構參考指引」六大場域、為高風險且低衝擊的系統

決定填寫問卷之對象系統



3

各場域題目說明
(以「1.場域_遠距辦公」為例)

填寫問卷 – 欄位說明 (1)

建議回答者：
可參照此請權責人員回答問題

支柱	參考原則項次 參考原則	等級	題號	題目	建議回答者 選項	回答	補充說明
身分	1.1 採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險。	I	遠1	遠距存取系統在進行身份驗證時是否使用多因子驗證（MFA）： 若透過VPN/VDI存取系統，登入VPN/VDI之身分驗證是否需MFA? □■是 □■否	網管/Infra (MFA) 1. 是，已完成 2. 否，預計1年內完成 3. 否，預計1年至3年內完成 4. 否，預計3年至5年內完成 5. 否，且未來也不執行，原因請於「補充說明」欄位說明 6. 不適用，原因請於「補充說明」欄位說明 7. 其它，請於「補充說明」欄位說明		

封面 | 說明 | 0_場域及系統篩選 | 1.場域_遠距辦公 | 2.場域_雲端存取 | 3.場域_系統維運管理 | 4.場域_應用系統管理 | 5.場域_服務供應商

根據自身執行情況填寫題目執行情況
- **「回答」：依選項填寫數字(1~7)**
- **「補充說明」：視回答進行補充說明**

填寫問卷 – 欄位說明 (2)

支柱	參考原則項次 參考原則	等級	題號	題目	建議回答者 選項	回答	補充說明
身分	1.3 對外部使用者(如服務供應商或跨機構協作)提供或採用不低於內部使用者信賴等級之身分鑑別機制。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I	遠3	遠距辦公之定義為公司員工於企業網路外部進行辦公作業，無外部使用者(如服務供應商人員或跨機構協作人員)，故本原則不適用於本場域。	應用程式系統負責人(應用程式系統帳號、身分驗證) 或網管/Infra (VPN、VDI、MFA) (各自回答負責部分) 不適用	不適用	本場域不適用此參考原則

封面 | 說明 | 0_場域及系統篩選 | 1.場域_遠距辦公 | 2.場域_雲端存取 | 3.場域_系統維運管理 | 4.場域_應用系統管理 | 5.場域_服務供應商

綠底表示不需填寫內容
(該場域不適用此參考原則)

身分支柱

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
身分	1.1	採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險。	I

遠1

遠距存取系統在進行身份驗證時是否使用多因子驗證（MFA）：
若透過VPN/VDI存取系統，登入VPN/VDI之身分驗證是否需MFA?　□■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司可透過VPN/VDI遠端存取系統，並採用多因子驗證，使用者須輸入帳號密碼後透過手機TOTP登入VPN/VDI。

回答	補充說明
1	

情境2：

公司允許透過VPN/VDI遠端存取系統，目前登入VPN/VDI的方式為輸入帳號密碼，預計於1年內新增其他MFA身分驗證方式。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
身分	1.2	採用包含綁定實體載具(如FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對APP等，排除簡訊、語音及電子郵件OTP)的多因子驗證機制，可抗網路釣魚風險。	II

遠2

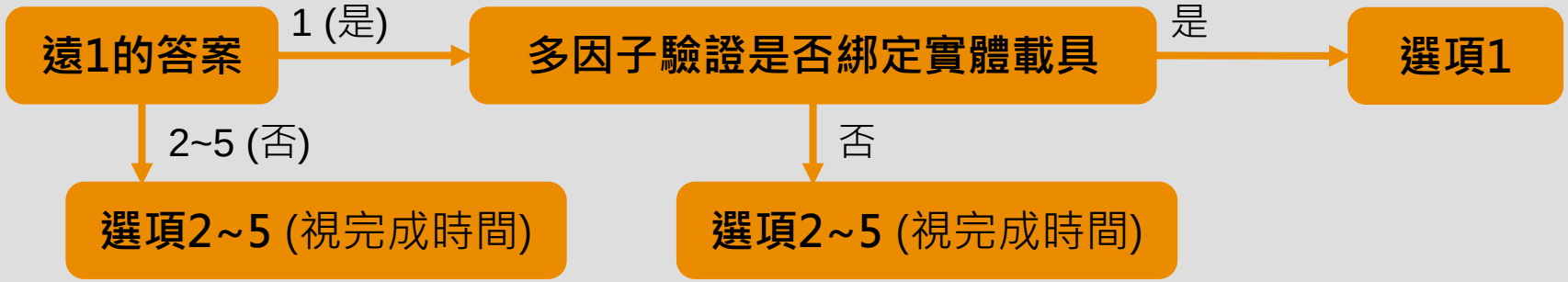
若遠1之答案為「否」的系統，本題即為「否」。
如果遠距存取系統在身份驗證時有多因子驗證機制，該機制是否綁定實體載具？ □■是 □■否

實體載具包括：
1. 硬體憑證載具
2. 手機TOTP APP驗證(如MicroSoft Authenticator、Google Authenticator)

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)



填寫範例

情境1：

公司可透過VPN/VDI遠端存取系統，並採用多因子驗證，使用者須輸入帳號密碼後透過手機TOTP登入VPN/VDI。

回答	補充說明
1	

情境2：

公司透過VPN/VDI遠端存取系統，目前採用帳號密碼及手機簡訊OTP登入，預計於2年內將OTP改為TOTP驗證方式。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
身分	1.3	對外部使用者(如服務供應商或跨機構協作)提供或採用不低於內部使用者信賴等級之身分鑑別機制。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I

遠3

遠距辦公之定義為公司員工於企業網路外部進行辦公作業，無外部使用者(如服務供應商人員或跨機構協作人員)，故本原則不適用於本場域。

選項

不適用

填寫範例

該場域不適用此參考原則，不需填寫。

回答	補充說明
不適用	本場域不適用此參考原則

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
身分	1.4	如具多元身分鑑別機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I

遠4

遠距辦公之定義為公司員工於企業網路外部進行辦公作業，無外部使用者(如服務供應商人員或跨機構協作人員)，故本原則不適用於本場域。

選項

不適用

填寫範例

該場域不適用此參考原則，不需填寫。

回答	補充說明
不適用	本場域不適用此參考原則

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
身分	1.5	完成身分鑑別後，除依角色屬性存取控制(RBAC)落實最小授權原則外，並具基於屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點等)納為授權審核條件，動態撤銷、限縮存取授權或即時告警。	II

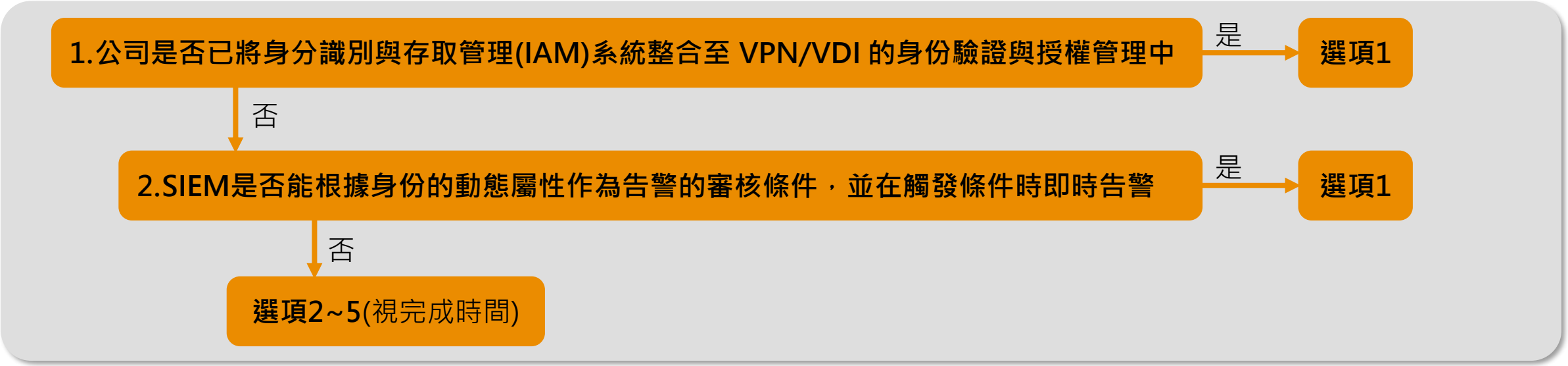
遠5

1. 公司是否已將 IAM 系統整合至 VPN/VDI 的身份驗證與授權管理中？ □■是 □■否
   補充說明：該IAM系統具有依據屬性(如身分、設備、網路、應用程式、資料)，動態調整授權之能力。
   若本題答「是」，則為符合；若本題答「否」，則請回答第2題。
2. 公司尚無建置IAM，但SIEM是否能根據身份的動態屬性（如存取的時間、存取的地點等）作為告警的審核條件，並在觸發條件時即時告警？ □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)



填寫範例

情境1：

SIEM能根據身份的動態屬性（如存取的時間、存取的地點等）作為告警的審核條件，並在觸發條件時即時告警。

回答	補充說明
1	

情境2：

公司未建置IAM系統，且SIEM也無法根據存取時間、地點等條件進行即時告警，預計於1年內修改SIEM系統之觸發條件。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
身分	1.6	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或SOAR Playbook等)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III

遠6

公司是否已建立以下資安事件偵測機制：

a. 建置 SIEM
b. 建置 SOC
c. 將 VPN（如有）和 VDI（如有）的**身份驗證**日誌傳送至 SIEM 進行分析，並可提供即時告警
d. 將 VPN（如有）和 VDI（如有）的**身份驗證**日誌傳送至 SOC，並可根據入侵指標（IOC）或攻擊行為樣態進行分析，提供即時告警

---

e、f為等級IV之必要實作項，故下列選項為選填，供參考用

---

e. 建置SOAR
f. SOAR已整合SIEM、SOC之告警並已建立自動化之即時回應機制

題目說明(以「1.場域_遠距辦公」為例)

選項

1. a、b、c、d均已建置或達成，已完成
2. 預計1年內完成a、b、c、d
3. 預計1年至3年內完成a、b、c、d
4. 預計3年至5年內完成a、b、c、d
5. 不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已建置SIEM和SOC等資安事件偵測機制，並將VPN的身份驗證日誌傳送至SIEM和SOC進行分析，以提供即時告警。

回答	補充說明
1	

情境2：

公司已建置SIEM和SOC等資安事件偵測機制，但VPN的身份驗證日誌尚未整合至SIEM及SOC，預計於2年內修改SOC的分析範圍。

回答	補充說明
3	

設備支柱

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.1	具有效盤點且可唯一識別(如TPM等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。	I

遠7

是否使用以下任一方式來識別連線至 VPN/VDI的設備（如電腦、手機、平板）： □■是 □■否

1. 使用 MAC 地址識別
2. 將唯一識別碼存放於設備的 TPM（可信平台模組）中，以識別公司設備

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司採用MAC地址識別連線至VPN的設備。

回答	補充說明
1	

情境2：

公司未採用MAC地址或將唯一識別碼存放於設備的 TPM中，預計於一年內採用MAC地址識別

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.1	具有效盤點且可唯一識別(如TPM等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。	I

遠8

是否具備偵測設備組態設定的機制：
□■是 □■否

組態設定應包括以下方面：
1. 病毒碼更新狀態
2. 作業系統更新狀態
3. 安全組態設定是否符合公司政策

注意：如果僅允許使用電腦進行連線，則只需描述電腦的情境。但若允許使用多種設備（如電腦、手機、平板）進行連線，則所有設備都需具備偵測機制，方可選擇「是」。

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司具備偵測設備之組態設定的機制，例如：病毒碼更新狀態、作業系統更新狀態。

回答	補充說明
1	

情境2：

公司未具備偵測設備之組態設定的機制，預計於5年內修改相關規範。

回答	補充說明
4	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.2	具納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。	II

遠9

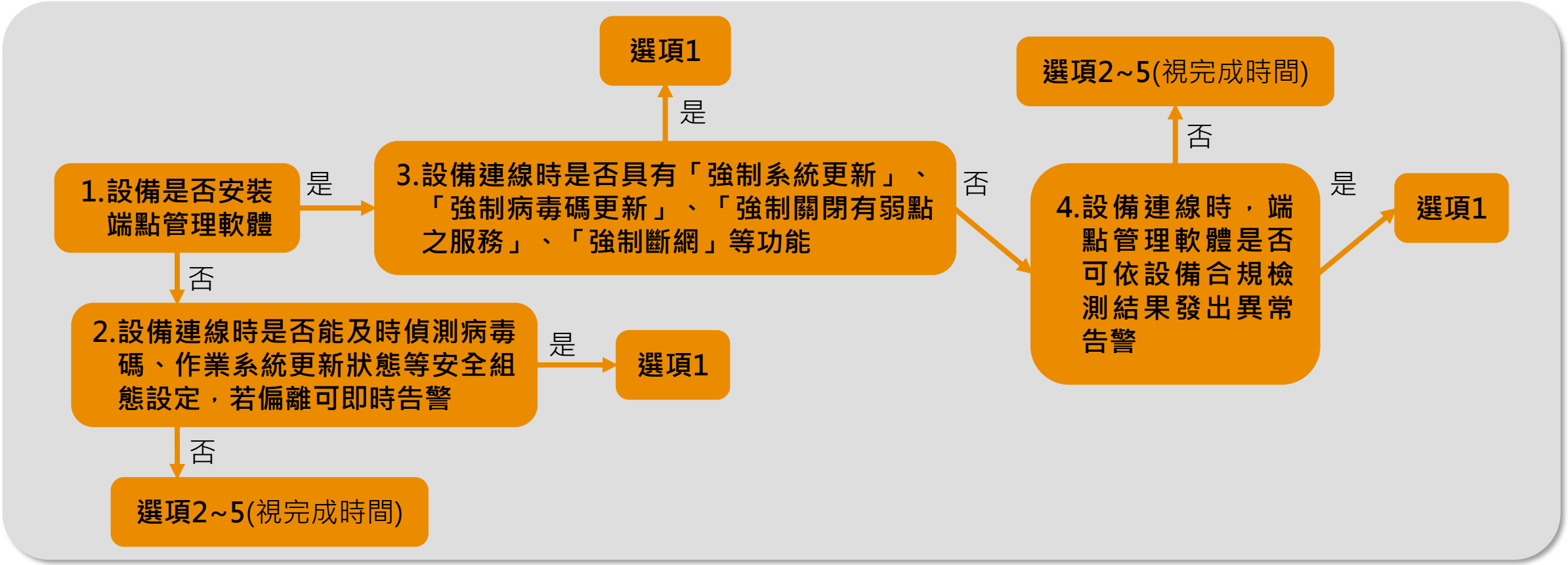
設備：可透過VPN/VDI連線至公司內網之電腦、手機或平板。

1. 公司是否在管理的設備上安裝端點管理軟體? □■是 □■否
   若本題答「是」，則依序回答第3~4題；若本題答「否」，則繼續答第2題。
2. 公司若無端點軟體，是否能於設備連線時，及時偵測設備之病毒碼更新狀態、作業系統更新狀態，安全組態設定未與公司政策偏離，若有發生偏離可即時告警? □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。
3. 設備連接系統時(透過VPN/VDI)，是否具有「強制系統更新」、「強制病毒碼更新」、「強制關閉有弱點之服務」、「強制斷網」等功能 □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則請回答第4題。
4. 若第 3 題選「否」，當設備連接系統時(透過VPN/VDI)，若無法「強制系統更新」、「強制病毒碼更新」、「強制關閉有弱點之服務」、「強制斷網」，是否可發出設備異常告警? □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

題目說明(以「1.場域_遠距辦公」為例)

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明



題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司已於可遠端連線之電腦安裝端點管理軟體，於遠端連線時強制更新系統版本、並強制斷網，或雖無法強制執行僅會發送告警通知給權責單位。

回答	補充說明
1	

情境2：

公司未安裝端點管理軟體，於設備連線時未能及時偵測病毒碼、作業系統更新狀態等安全組態設定，並發送即時告警，預計於5年內新增偵測及異常通知告警機制。

回答	補充說明
4	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.3	對外部設備(如BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之合規中繼閘道(如VDI等)存取。	I

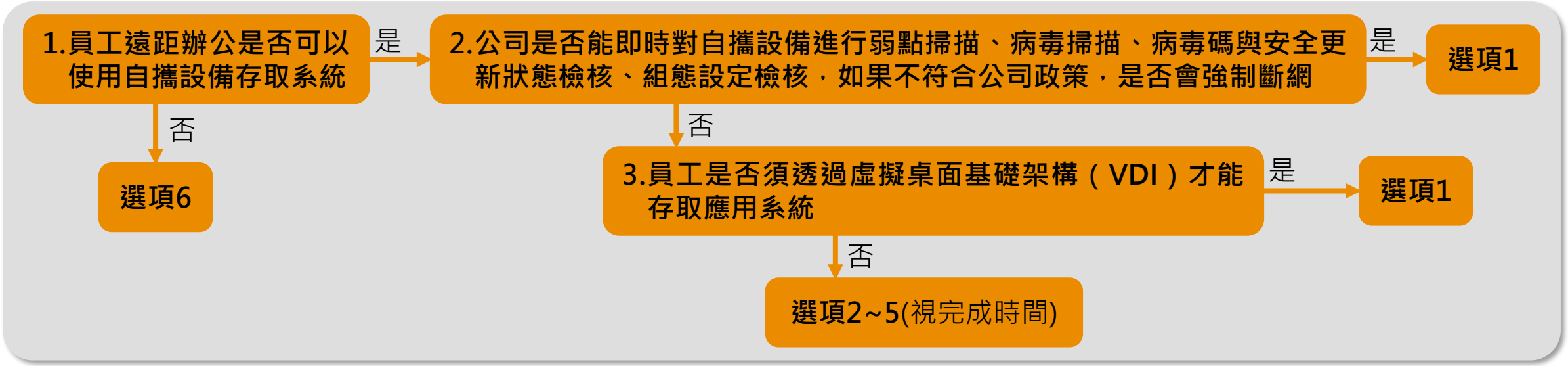
遠10

1. 員工遠距辦公是否可以使用自攜設備（BYOD，包括電腦、手機、平板）存取系統 (透過VPN/VDI)?
   □■是 □■否
   若回答「是」，需繼續回答2～3，若本題答「否」，則不適用。
2. 針對員工遠距辦公持BYOD存取系統前，是否能即時對其進行弱點掃描、病毒掃描、病毒碼與安全更新狀態檢核、組態設定檢核，如果不符合公司政策，是否會強制斷網？ □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則請回答第3題。
3. 是否已限制員工持BYOD進行遠距辦公時，必須透過虛擬桌面基礎架構（VDI）才能存取應用系統？
   □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)



填寫範例

情境1：

員工無法使用自攜設備存取系統。

回答	補充說明
6	員工無法使用自攜設備遠端存取系統

情境2：

員工可以使用自攜設備存取系統，目前未針對自攜設並進行安全更新狀態、組態設定檢核，但員工須透過VDI才能存取應用系統。

回答	補充說明
1	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.4	可將設備之動態屬性(如是否納管及合規、設備位址、或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼閘道(如VDI等)存取。	II

遠11

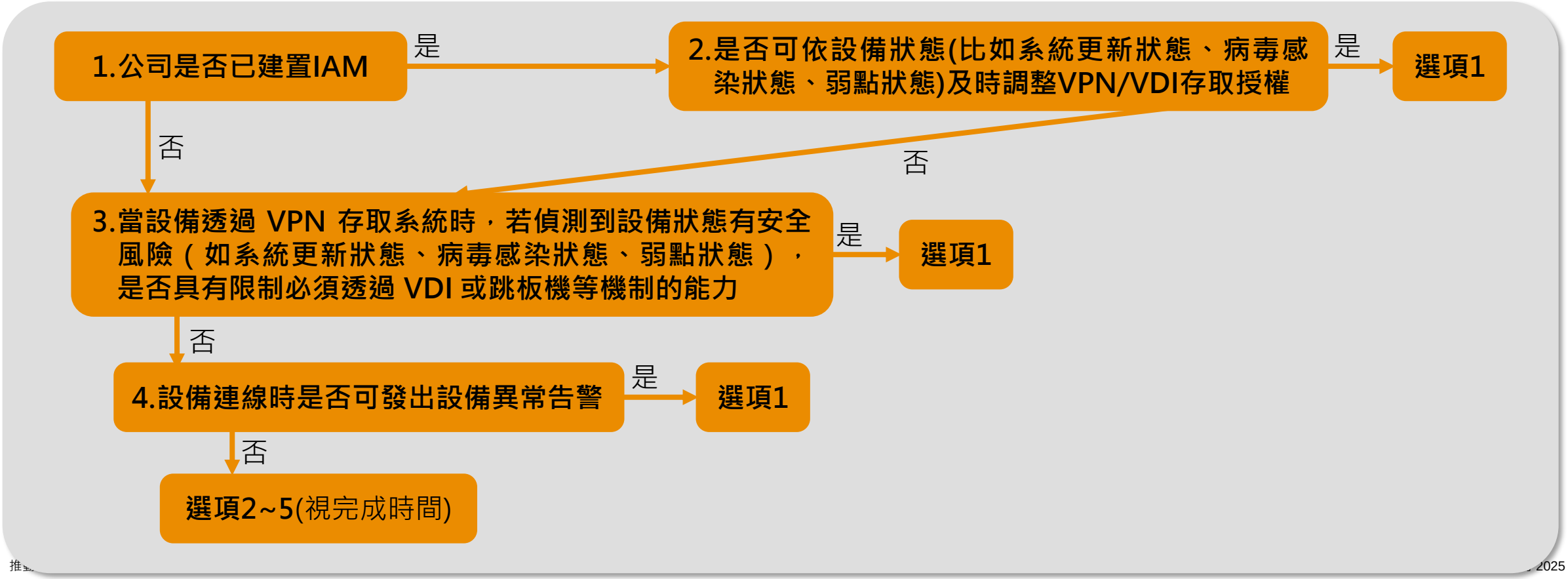
公司是否已建置 IAM 並整合以管理公司設備的存取權限？請依序回答下列問題：

1. 公司是否已建置IAM? □■是 □■否
   若本題答「是」，需繼續回答第2題；若本題答「否」，則請回答第3~4題。
2. 若已建置IAM，請說明其是否可依設備狀態(比如系統更新狀態、病毒感染狀態、弱點狀態)及時調整VPN/VDI存取授權? □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則請回答第3~4題。
3. 當設備透過 VPN 存取系統時，若偵測到設備狀態有安全風險（如系統更新狀態、病毒感染狀態、弱點狀態），是否具有限制必須透過 VDI 或跳板機等機制的能力？ □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則請回答第4題。
4. 當設備透過 VPN 存取系統時，若偵測到設備狀態有安全風險（如系統更新狀態、病毒感染狀態、弱點狀態），是否能即時發出告警？ □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

題目說明(以「1.場域_遠距辦公」為例)

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明



題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司尚未建置身分識別與存取管理(IAM)系統，但具有於設備連線時偵測設備系統更新狀態、病毒感染狀態、弱點狀態之機制，並可及時限制該設備必須透過VDI存取。

回答	補充說明
1	

情境2：

公司未建置身分識別與存取管理(IAM)系統，且透過VPN存取系統，也未於偵測到設備狀態有安全風險時限制透過VDI等機制，也未有安全風險的告警機制，預計於5年內新增機制。

回答	補充說明
4	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.5	對設備活動紀錄具有即時偵測及回應機制(EDR)，在偵測到威脅指標(IOC)時，可自動隔離或即時應處(如發出事件單即時追蹤處置)。	III

遠12

公司是否已建立以下**所有**資安事件偵測機制：　□■是 □■否

a. 已建置SIEM或已建置EDR

b. EDR、IPS、防火牆、VPN(若有)、VDI(若有)之日誌已拋SIEM，並可依據入侵指標(IOC)或攻擊行為樣態進行分析，且可依據SIEM之告警即時隔離設備之能力，或由SIEM提供即時告警。

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司已建置SIEM，收容範圍涵蓋EDR、IPS、防火牆、VPN、VDI之日誌，並可依據攻擊行為樣態進行分析，SIEM告警後可即時隔離設備。

回答	補充說明
1	

情境2：

公司已建置SIEM，惟收容範圍未涵蓋EDR之日誌，預計於1年內完成。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
設備	2.6	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III

遠13

公司是否建立如下資安事件偵測與應處機制

a. 已建置SIEM
b. 已建置EDR
c. 已建置SOC
d. EDR、IPS、防火牆、VPN(若有)、VDI(若有)之日誌已匯入SIEM與SOC，並可依據入侵指標(IOC)或攻擊行為樣態進行分析。系統可根據 SIEM 與 SOC 偵測到的威脅即時隔離設備，或由 SIEM 提供即時告警功能。

---

e、f為等級IV之必要實作項，故下列選項為選填，供參考用

---

e. 已建置SOAR
f. SOAR已整合SIEM、SOC之告警並已建立即時回應機制

題目說明(以「1.場域_遠距辦公」為例)

選項

1. a、b、c、d均已建置或達成，已完成
2. 預計1年內完成a、b、c、d
3. 預計1年至3年內完成a、b、c、d
4. 預計3年至5年內完成a、b、c、d
5. 不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已建置SIEM、EDR、SOC等資安事件偵測與應處機制，並將EDR、IPS、防火牆、VPN、VDI之日誌匯入SIEM與SOC，依據入侵指標(IOC)進行分析，如有異常，系統可即時隔離設備。

回答	補充說明
1	

情境2：

公司已建置SIEM、EDR、SOC等資安事件偵測與應處機制，惟未將VPN之日誌匯入SIEM與SOC，故無法提出告警，預計於2年內修改SOC的分析範圍。

回答	補充說明
3	

網路支柱

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
網路	3.1	具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。	I

遠14

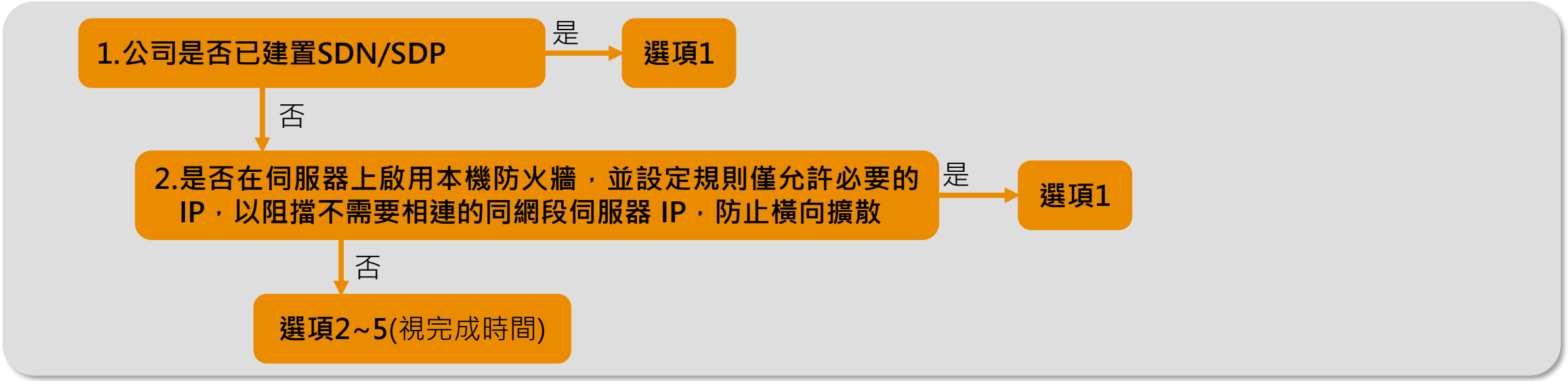
公司網路設定是否具備限制同網段伺服器之間存取的能力？

1. 已建置SDN/SDP： □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則請回答第2題。
2. 是否在伺服器上啟用本機防火牆，並設定規則僅允許必要的 IP，以阻擋不需要相連的同網段伺服器 IP，以防止橫向擴散？ □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)



填寫範例

情境1：

公司已建置SDN/SDP。

回答	補充說明
1	

情境2：

公司未建置SDN/SDP，且未啟用伺服器之本機防火牆，預計於1年內完成啟用。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
網路	3.2	具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。	II

遠15 是否已建置 SDN/SDP 網路管理機制？ □■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：
公司已建置 SDN/SDP 網路管理機制。

回答	補充說明
1	

情境2：
公司未建置 SDN/SDP 網路管理機制，預計1年內完成建置。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
網路	3.3	呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。	II

遠16 公司是否已建置以下功能：可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制（如NDR或可監控應用系統topology之機制）？ □■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：
公司已建置 NDR 。

回答	補充說明
1	

情境2：
公司未建置NDR或可監控應用系統topology之機制，預計1年內完成建置。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
網路	3.4	於資源存取路徑之資料傳輸加密(如採https等加密協定)。	I

遠17

系統的存取介面是否採用以下任一加密方式？ □■是 □■否
1. 若系統是透過網頁存取，是否已限制僅能使用 HTTPS（443），並關閉 HTTP（80）
2. 若系統可使用非網頁瀏覽器方式存取，該網路協定是否為加密傳輸協定

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：
系統可使用非網頁瀏覽器方式存取，且網路協定為加密傳輸協定。

回答	補充說明
1	

情境2：
系統透過網頁存取，已啟用HTTPS（443），但未關閉 HTTP（80），預計1年內完成。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
網路	3.5	對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。	III

遠18 SDN/SDP 是否能根據 NDR 提供的入侵指標（IOC）來管理 VPN 接入後可存取的網段？ □■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

SDN/SDP可根據NDR提供的入侵指標來管理VPN 接入後可存取的網段。

回答	補充說明
1	

情境2：

SDN/SDP無法根據NDR提供的入侵指標來管理VPN 接入後可存取的網段，預計1年內完成。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
網路	3.6	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook等)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III

遠19

公司是否建立如下資安事件偵測與應處機制

a. 已建置SIEM
b. 已建置NDR
c. 已建置SDN/SDP
d. 已建置SOC
e. SDN/SDP、NDR、IPS、防火牆、VPN(若有)、VDI(若有)之日誌已匯入SIEM與SOC，並可依據入侵指標(IOC)或攻擊行為樣態進行分析

---

f、g為等級IV之必要實作項，故下列選項為選填，供參考用

---

f. 已建置SOAR
g. SOAR已整合SIEM、SOC之告警並已建立即時回應機制

題目說明(以「1.場域_遠距辦公」為例)

選項

1. a、b、c、d、e均已建置或達成，已完成
2. 預計1年內完成a、b、c、d、e
3. 預計1年至3年內完成a、b、c、d、e
4. 預計3年至5年內完成a、b、c、d、e
5. 不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已建置SIEM、NDR、SDN/SDP、SOC等資安事件偵測與應處機制，將SDN/SDP、NDR、IPS、防火牆、VPN、VDI之日誌匯入SIEM與SOC，並依據入侵指標(IOC)進行分析。

回答	補充說明
1	

情境2：

公司已建置SIEM、 NDR、SDN/SDP、SOC等資安事件偵測與應處機制，惟未將VPN之日誌匯入SIEM與SOC，依據入侵指標(IOC)進行分析，預計於2年內修改SOC的分析範圍。

回答	補充說明
3	

應用系統支柱

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
應用程式	4.1	以作業屬性及風險區隔角色，並依角色風險等級定義授權條件(如身分及設備鑑別之等級)，採最小授權原則定義授權範圍；並針對特權作業採獨立角色授權(不混用於非特權作業)，減少特權帳號之濫用及風險。	I

遠20

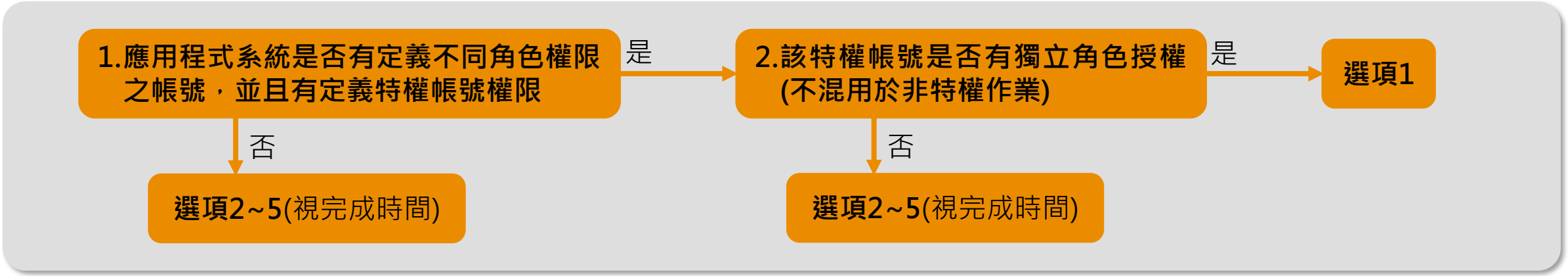
應用程式系統是否有依角色定義權限，並針對特權帳號設立獨立角色授權。請依序向下回答。
補充說明：獨立角色授權指的是特權角色僅限於特權操作（如帳號新增/修改/刪除/授權），不應包含其他作業權限。

1. 應用程式系統是否有定義不同角色權限之帳號，並且有定義特權帳號權限? □■是 □■否
   若本題答「是」，則繼續回答問題2；若本題答「否」，則為不符合。
2. 應用程式系統之特權帳號是否有獨立角色授權(不混用於非特權作業)? □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)



填寫範例

情境1：

應用程式系統已依職責給予帳號權限，並針對特權作業採獨立角色授權。

回答	補充說明
1	

情境2：

應用程式系統已依職責給予帳號權限，惟特權帳號權限混用於非特權作業，預計1年內調整。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
應用程式	4.2	可將帳號動態屬性(如MFA強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。	II

遠21

是否能即時偵測存取應用系統之設備的屬性(如MFA強度、設備合規、時間、地點等)，並已建置自動審核之機制，請依序向下回答。

1. 具有即時偵測設備在存取應用系統時所具有的屬性（如MFA強度、設備合規、時間、地點等）的能力，並在發現設備的動態屬性未達設定標準時，是否具備即時告警機制? □■是 □■否
【必須所有可連線之設備皆可偵測，本題才可答「是」】

「可存取應用系統之方式」包括透過VPN/VDI或網際網路存取。
「設備」包括所有可存取應用系統的設備，該設備透過VPN/VDI也包括在內。
MFA強度舉例：是否綁定實體載具?實體載具包括：1. 硬體憑證載具；2. 手機TOTP APP驗證[如MicroSoft Authenticator、Google Authenticator]
設備合規舉例：病毒碼更新至最新病毒碼、安全組態設定符合公司規範、弱點掃描無高風險弱點、安全更新狀態
時間舉例：定義不合理的存取時間
地點舉例：定義不合理的存取地點[IP地理位置]

題目說明(以「1.場域_遠距辦公」為例)

遠21

2、3為等級IV之必要實作項，故下列選項為選填，供參考用

---

2. 是否已建置IAM?　□■是 □■否
   若答「是」，請繼續回答3。若本題答「否」，則可跳過第三題。
3. 若設備之動態屬性審核未達設定標準，是否具有動態撤銷權限之功能?　□■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

具有即時偵測設備在存取應用系統時所具有的屬性（如MFA強度、設備合規、時間、地點等）的能力，並在發現設備的動態屬性未達設定標準時，具備即時告警機制。

回答	補充說明
1	

情境2：

尚未建置可將能存取應用系統之設備的屬性(如MFA強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件，預計於3年內調整。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
應用程式	4.3	對應用程式活動紀錄具有即時偵測及回應機制，並可依據使用者行為或使用模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警。	III

遠22

應用程式系統之授權是否依據使用者之高風險異常操作行為即時撤銷權限，或根據定義的高風險異常操作行為即時通知告警。請依序向下回答。

補充說明：高風險操作行為由公司依應用系統之特性自行定義，舉例：

a. 交易系統非常規交易：若某客戶主要在凌晨交易美股，但偶發白天大金額高頻率港股交易，則定義為異常。
b. 複委託後台系統非常規查詢：若某營業員大量查詢客戶交易資料並試圖複製，則定義為異常。

以上僅舉例，非真實建議。惟應設計高風險情境，不以不適用跳過本原則。

1. 是否已有機制分析應用程式的高風險異常資料存取行為，並可即時告警？（透過 SIEM 或其他方式）
   □■是 □■否

題目說明(以「1.場域_遠距辦公」為例)

遠22

2~4為等級IV之必要實作項，故下列選項為選填，供參考用

---

2. 公司是否已建置IAM系統?　□■是 □■否
   若本題答「否」，3、4不需回答。
3. 應用程式系統之帳號身分驗證與授權是否透過IAM系統?　□■是 □■否
4. IAM系統是否可依據應用程式系統高風險異常操作行為即時撤銷應用程式授權?　□■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司已將應用系統操作日誌匯入SIEM，並依據高風險異常資料存取行為進行分析，如有異常會即時通知權責人員。

回答	補充說明
1	

情境2：

公司未將應用系統操作日誌匯入SIEM，預計於3年內改善。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
應用程式	4.4	從網際網路及防護邊界內部對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放經Internet存取之防護能力。	II

遠23

應用程式系統所進行之資安測試是否包括源碼檢測、弱點掃描、滲透測試。其中弱點掃描與滲透測試需在防護邊界內部（無任何資安防護）或繞過防護設備（如防火牆、IPS、WAF 等）的條件下進行。
下列問題有任一題回答「是」，即為符合；三題皆回答「否」，即為不符合：

1. 應用程式系統是否定期執行源碼檢測? □■是 □■否
2. 應用程式系統是否定期執行弱點掃描(本弱點掃描指應用層弱點掃描及作業系統層弱點掃描)? □■是 □■否
3. 請回答應用程式系統是否定期執行滲透測試? □■是 □■否

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司已針對應用程式定期執行滲透測試。

回答	補充說明
1	

情境2：

公司未針對應用程式執行源碼檢測、弱點掃描或滲透測試，預計於3年內改善。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
應用程式	4.5	為應用程式開發、測試及部署建立持續整合及部署(CI/CD) 通道，分階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行落實權責分離。	II

遠24

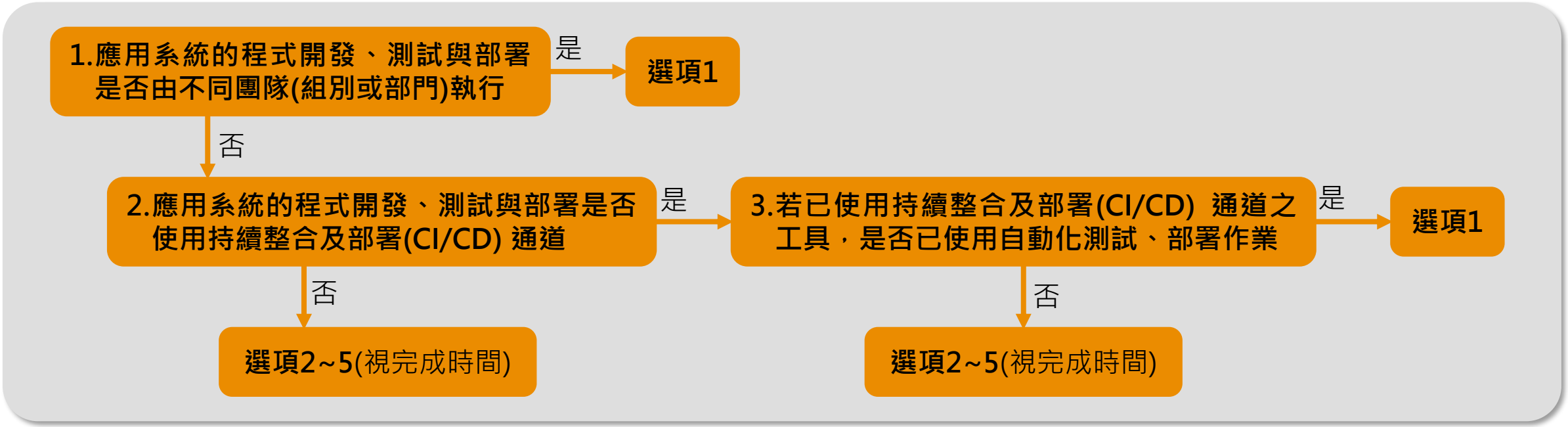
應用程式系統的程式開發、測試與部署是否已採自動化機制，或由不同團隊執行開發、測試、部署作業。請依序向下回答。

1. 應用系統的程式開發、測試與部署是否由不同團隊(組別或部門)執行? □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則繼續回答第2~3題。
2. 應用系統的程式開發、測試與部署是否使用持續整合及部署(CI/CD) 通道(CI/CD工具可參考下列)：□■是 □■否
   工具範例：Jenkins、GitLab、Bamboo、TeamCity、Buildkite、Spinnaker、Argo CD、Octopus Deploy、Buildkite等。
   若本題答「是」，則繼續回答第3題；若本題答「否」，則為不符合。
3. 若已使用持續整合及部署(CI/CD) 通道之工具，是否已使用自動化測試、部署作業? □■是 □■否
   若本題答「是」，則為符合；若本題答「否」，則為不符合。

題目說明(以「1.場域_遠距辦公」為例)

選項

1. 符合，已完成
2. 不符合，預計1年內完成
3. 不符合，預計1年至3年內完成
4. 不符合，預計3年至5年內完成
5. 不符合，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明



題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司已將應用系統的程式開發、測試與部署之職責交由不同組別執行。

回答	補充說明
1	

情境2：

公司未將應用系統的程式開發、測試與部署之職責分離，且未使用持續整合及部署(CI/CD) 通道，預計於3年內改善。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
應用程式	4.6	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III

遠25

公司是否建立如下資安事件偵測與應處機制

a. 已建置SIEM
b. SIEM已收容應用程式之日誌
c. 已建置SDN
d. 已建置SOC
e. **應用程式**、NDR、IPS、防火牆、VPN(若有)、VDI(若有)之日誌已拋轉至SIEM與SOC，並可依據入侵指標(IOC)或攻擊行為樣態進行分析，SDN可依SIEM與SOC偵測之威脅即時隔離，或由SIEM提供即時告警

---

f、g為等級IV之必要實作項，故下列選項為選填，供參考用

---

f. 已建置SOAR
g. SOAR已整合SIEM、SOC之告警機制，並已建立即時回應機制

題目說明(以「1.場域_遠距辦公」為例)

選項

1. a、b、c、d、e均已建置或達成，已完成
2. 預計1年內完成a、b、c、d、e
3. 預計1年至3年內完成a、b、c、d、e
4. 預計3年至5年內完成a、b、c、d、e
5. 不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已建置SIEM、SDN、SOC等資安事件偵測與應處機制，且將應用程式、NDR、IPS、防火牆、VPN、VDI之日誌拋轉至SIEM與SOC，並依據入侵指標(IOC)進行分析，如有異常會提供即時告警。

回答	補充說明
1	

情境2：

公司已建置SIEM、SDN、SOC等資安事件偵測與應處機制，惟未將應用程式之日誌匯入SIEM與SOC，依據入侵指標(IOC)進行分析，預計於2年內修改SOC的分析範圍。

回答	補充說明
3	

資料支柱

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.1	針對機敏資料部署防止資料外洩防護機制，如依據資料特徵之DLP、資料不落地等。	I

遠26

資料管理系統 (如Database、檔案共享系統、文件管理系統、ftp server、NAS...等) 是否設計資料外洩防護機制。請依序向下回答。

1. 資料管理系統是否已定義機敏資料，並建置資料外洩防護(DLP)機制? □■是 □■否

補充說明：DLP機制包含但不限於以下方法：

a. 資料管理系統匯出資料，採加密方式。
b. 資料管理系統匯出資料，採浮水印機制(於匯出之資料加註匯出人員，且浮水印無法移除)
c. 資料管理系統於伺服器端裝設DLP防護機制，可防護已定義需防止外洩的機敏資料。
d. 於可存取資料管理系統的設備皆裝設端點DLP防護，可防護已定義需防止外洩的機敏資料。

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)

填寫範例

情境1：

公司已定義資料管理系統內的機敏資料，並於可存取資料管理系統的設備皆建置DLP防護。

回答	補充說明
1	

情境2：

公司已定義資料管理系統內的機敏資料，但未針對機敏資料建置DLP機制，預計於3年內新增相關機制。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.2	具監控資料存取和使用情況機制，可依據資料存取行為或資料處理模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行為。	III

遠27

資料管理系統(如Database、檔案共享系統、文件管理系統、ftp server、NAS...等)之資料存取授權是否依據使用者之高風險異常資料存取行為予以即時撤銷權限，或能依據定義之高風險異常操作行為，即時告警通知。請依序向下回答。

(高風險操作行為由公司依應用系統之特性自行定義，舉例：

a. 某營業員於非營業時間大量查詢客戶交易資料，並試圖複製，定義為異常。

以上僅舉例，非真實建議。惟應設計高風險情境，盡可能不以不適用跳過本原則)

1. 是否已有分析資料管理系統高風險異常資料存取行為之機制，並可即時告警?(透過SIEM或其他任何方式) □■是 □■否

2~4為等級IV之必要實作項，故下列選項為選填，供參考用

---

2. 公司是否已建置IAM系統? □■是 □■否
   若本題答「否」，3、4不需回答，可以直接跳過。
3. 資料管理系統之帳號身分驗證與授權是否透過IAM系統? □■是 □■否
4. IAM系統是否可依據資料管理系統高風險異常操作行為即時撤銷資料存取授權? □■是 □■否

題目說明(以「1.場域_遠距辦公」為例)

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已將資料管理系統操作日誌匯入SIEM，並依據高風險異常資料存取行為進行分析，如有異常會即時通知權責人員。

回答	補充說明
1	

情境2：

公司未將資料管理系統操作日誌匯入SIEM，預計於3年內改善。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.3	建立資料盤點、分類及、標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。	I

遠28 資料管理系統（如資料庫、檔案共享系統、文件管理系統、FTP 伺服器、NAS 等）中的資料存取是否落實角色基礎存取控制（RBAC）原則，即根據資料機敏度限制可存取的使用者？ □■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：
資料管理系統已根據資料機敏度限制可存取的使用者。

回答	補充說明
1	

情境2：
資料管理系統未根據資料機敏度限制可存取的使用者，預計3年內改善。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.4	建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如離線備份、儲存於隔離環境、防止寫入等)及有效還原。	I

遠29

資料管理系統(如Database、檔案共享系統、文件管理系統、ftp server、NAS...等)是否建置高可用性?
資料管理系統的相關伺服器是否設有高可用性（HA）備援機制，並定期進行異地備份與還原演練？
□■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

資料管理系統已採用HA備援機制，並定期執行異地備份與還原演練。

回答	補充說明
1	

情境2：

資料管理系統未採用HA備援機制，預計3年內改善。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.5	可將資料存取的動態屬性(如MFA強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警。	II

遠30

是否能即時偵測存取資料管理系統(如Database、檔案共享系統、文件管理系統、ftp server、NAS...等)之設備的屬性(如MFA強度、設備合規、時間、地點等)，並已建置自動審核之機制，請依序向下回答。

1. 是否具即時偵測可存取資料管理系統之設備(如偵測MFA強度、設備合規、存取時間、IP所在地理位置等屬性)的能力?　□■是 □■否
   【必須所有可連線之設備皆可偵測，本題才可答「是」】
   若本題答「是」，則繼續答2。若本題答「否」，則為不符合。

「可存取資料管理系統之方式」包括透過VPN/VDI或網際網路存取。
「設備」包括所有可存取應用系統的設備，該設備透過VPN/VDI也包括在內。
MFA強度舉例：是否綁定實體載具?實體載具包括：1. 硬體憑證載具；2. 手機TOTP APP驗證[如MicroSoft Authenticator、Google Authenticator]
設備合規舉例：病毒碼更新至最新病毒碼、安全組態設定符合公司規範、弱點掃描無高風險弱點、安全更新狀態
時間舉例：定義不合理的存取時間
地點舉例：定義不合理的存取地點[IP地理位置]

題目說明(以「1.場域_遠距辦公」為例)

遠30

2. 參考遠27，若發生高風險異常資料存取行為與設備之屬性審核未達設定標準時，是否皆已建置即時告警之機制? (發生高風險異常資料存取，或存取之設備屬性未達標準，是否已建置即時告警機制)
   □■是 □■否
   若本題答「是」，則為符合。若本題答「否」，則為不符合。

3、4為等級IV之必要實作項，故下列選項為選填，供參考用

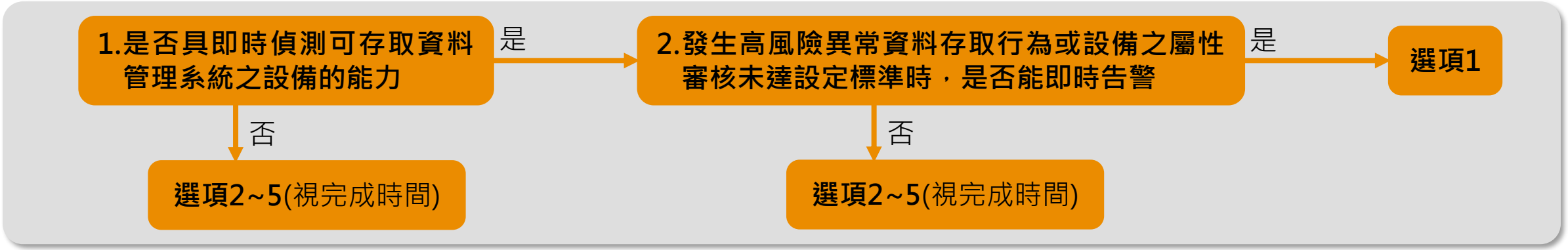
---

3. 是否已建置IAM? □■是 □■否
   若答「是」，請繼續回答4。若本題答「否」，則可跳過第四題。
4. 若存在高風險資料存取行為與設備之屬性審核未達設定標準之情事，是否可於資料管理系統停用授權?
   □■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

題目說明(以「1.場域_遠距辦公」為例)



填寫範例

情境1：

可於設備連線時，偵測存取資料管理系統之設備的安全屬性(如MFA強度、設備合規、時間、地點等)，若有偵測到不合規能即時告警。

回答	補充說明
1	

情境2：

未能即時偵測存取資料管理系統之設備(如MFA強度、設備合規、時間、地點等)，納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警，預計於3年內完成。

回答	補充說明
2	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.6	依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。	I

遠31

資料管理系統（如資料庫、檔案共享系統、文件管理系統、FTP 伺服器、NAS 等）是否已識別並定義機敏性資料，並對這些資料進行加密儲存？且已建立加密金鑰的安全管理機制？ □■是 □■否

選項

1. 是，已完成
2. 否，預計1年內完成
3. 否，預計1年至3年內完成
4. 否，預計3年至5年內完成
5. 否，且未來也不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已於資料管理系統定義並加密儲存機敏資料，且設有加密金鑰的安全管理機制。

回答	補充說明
1	

情境2：

公司已於資料管理系統定義並加密儲存機敏資料，但未適當保管加密金鑰，預計於3年內完成。

回答	補充說明
3	

題目說明(以「1.場域_遠距辦公」為例)

支柱	項次	參考原則	等級
資料	5.7	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III

遠32

公司是否建立以下資安事件偵測與應處機制：

a. 已建置SIEM
b. SIEM已收容應用程式之日誌
c. 已建置SDN
d. 已建置SOC
e. **資料管理系統（如Database、檔案共享系統、文件管理系統、FTP server、NAS等）**、NDR、IPS、防火牆、VPN（若有）、VDI（若有）之日誌已拋至SIEM與SOC進行分析，SDN依據SIEM與SOC偵測之威脅進行即時隔離

---

f、g為等級IV之必要實作項，以下選項為選填，供參考用：

---

f. 已建置SOAR
g. SOAR已整合SIEM、SOC之告警機制，並已建立即時回應機制

題目說明(以「1.場域_遠距辦公」為例)

選項

1. a、b、c、d、e均已建置或達成，已完成
2. 預計1年內完成a、b、c、d、e
3. 預計1年至3年內完成a、b、c、d、e
4. 預計3年至5年內完成a、b、c、d、e
5. 不執行，原因請於「補充說明」欄位說明
6. 不適用，原因請於「補充說明」欄位說明
7. 其它，請於「補充說明」欄位說明

填寫範例

情境1：

公司已建置SIEM、SDN、SOC等資安事件偵測與應處機制，且將資料管理系統、NDR、IPS、防火牆、VPN、VDI之日誌拋轉至SIEM與SOC進行分析，如有威脅SDN將進行即時隔離。

回答	補充說明
1	

情境2：

公司已建置SIEM、SDN、SOC等資安事件偵測與應處機制，惟未將資料管理系統之日誌匯入SIEM與SOC進行分析，預計於2年內修改SIEM與SOC的分析範圍。

回答	補充說明
3	

4

後續工作項目

調查問卷及說明會時程

1. 寄發與回收「零信任架構導入進度調查問卷」
2. 零信任架構參考指引解析說明會

三月

五月

落實零信任系列說明會
第一場 身分

六月

落實零信任系列說明會
第二場 設備

七月

1. 落實零信任系列說明會 第三場 網路
2. 先行機構零信任架構導入分享研討會 第二場

八月

落實零信任系列說明會
第四場
應用程式

九月

落實零信任系列說明會
第五場 資料

Q & A

1. 後續相關問題，請以書面方式Email至 rella.liu@pwc.com 及 albert.l.li@pwc.com。
2. 關於零信任問卷問題，請使用Email標題為「[零信任問卷問題] ....」起頭來信，以免信多可能造成漏信。
3. 請特別注意 3/18 中午12點為我們的最後收信時間點，往後的信件將不繼續整理至常見問題 FAQ。
4. 常見問題 (FAQ) 將於 3/19 公布，以減少類似的問題來回討論。
5. 本次僅為第一次問卷回收，已了解目前各位的現況，後續將於所有說明會結束後再次回收一次問卷。
6. 繳交問卷時，請使用Email標題為「[零信任問卷繳交] ....」起頭來信，以免信多可能造成漏信。

Q & A

pwc.com