KPMG

財團法人金融聯合徵信中心

辦理融資租賃公司代理當事人線上申請信用報告作業說明暨實地查核實務分享會

輔導與審查及實地查核實務分享

廠商名稱：安侯建業聯合會計師事務所

民國113年3月6日

大綱

1. 個資保護與資安宣導
2. 代理當事人線上申請信用報告
   –作業流程及資訊環境
3. 代理當事人線上申請信用報告
   –常見缺失及改善建議事項
4. 代理當事人線上申請信用報告
   –重要事項提醒

KPMG

個資保護與資安宣導

個資保護

《個人資料保護法》修法

2023.5. 16三讀通過《個人資料保護法》部分條文修正案

(1) 修正個資法第48條

非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，**處新臺幣（下同）2萬元以上200萬元以下罰鍰，若是情節重大者，處15萬元以上1,500萬元以下罰鍰。屆期未改正者，按次處15萬元以上1,500萬元以下罰鍰。**

(2) 增訂個資法第1條之1

推動設置個資保護獨立監督機關，由『**個人資料保護委員會**』擔任個資法主管機關，解決目前個資法分散式管理下之實務監管問題。

籌備處已於2023年12月5日揭牌；2025年8月以前正式成立個資保護委員

近期個資外洩事件

上海商銀1.4萬戶客戶個資外洩，遭重罰千萬

上海商銀因為客戶個人資料遭到外洩共1萬4千戶（已歸戶），顯示該行有未完善建立及執行內部控制制度，致客戶資料外洩，因此，予以開罰1千萬元。。

WEAK：

- 未訂定妥適個人電腦管理者權限規範：
- 未訂定完善可攜式設備管理規範
- 系統未記錄個人資料使用情況，留存軌跡資料或相關證據
- 作業系統上線前及更新時，未能測試出資安監控軟體漏洞

ACTION：

- 盤點涉及個人資料之各類電腦系統是否均建置留存個人資料使用稽核軌跡
- 查詢個人資料相關權限是否符合最小化權限原則
- 建置應用系統稽核機制及權限範圍內不正常查詢及下載情形監控分析機制

近期個資外洩事件

統聯遇駭洩個資，害女大生被詐判賠5萬

統聯客運網站五月遭駭，三個月內有四萬多筆個資遭竊，利用網路訂票系統訂票的劉姓女大生個資因此被竊，並遭詐騙集團騙走八萬餘元。她依個資法提訴求償，新北地院三重簡易庭法官認為，統聯網站防火牆十六年沒更新有過失，但女大生也要自負三成責任，判賠五萬餘元。

WEAK：

- 防火牆是2006年產品，至今未持續更新，無法確實有效阻擋或隔離來自網路的惡意攻擊

ACTION：

- 防火牆更新，強化資安防護。
- 訂票改採無個資方式處理，由民眾設定一次性的取票號碼與密碼

近期個資外洩事件

“Line母公司遭遇網路攻擊，44萬用戶、合作夥伴、員工個資恐外洩。

即時通訊軟體Line母公司LY Corporation發布資安通告，指出他們偵測到未經授權的第三方於10月9日存取該公司系統，而有可能導致使用者、業務合作夥伴、員工等人士的資訊遭到洩露。

WEAK：

- 韓國雲端業者Naver的承包商遭駭，員工電腦感染惡意軟體。
- 由於LYC和Naver共用處理員工及其他個資的身分驗證系統，駭客藉由Naver的系統入侵先前屬於Line Corporation的內部系統

ACTION：

- LYC強制重設員工內部系統的密碼、雙因素身分驗證機制
- 透過使用者註冊的電子郵件，以及Line官方帳號發送訊息等方式，來通知當事人。

近期個資外洩事件

「移工一站網」甫上線400筆個資外洩 勞動部檢討資安

勞動部「在台移工一站式申請聘僱及居留整合服務」今天上線，但申辦網站卻發生個資外洩。勞動部指出，接獲通報後已下架檢測，目前已重新上線提供服務。

WEAK：

- 因為程式設計瑕疵，導致部分雇主個人資料在頁面露出。

ACTION：

- 勞動部後續將進行檢討、強化整個申辦系統。
- 未來新增服務時都會檢測、驗證。

近期個資外洩事件

日本遊戲商 雲端空間權限錯設 百萬玩家個資外洩 6年才發現

開發出《神域召喚》等手機遊戲的日本手機遊戲商Ateam傳出個資外洩事件，，導致935,779筆個人資料外洩，其中98.9%是客戶。外洩的資訊包含姓名、電子郵件地址、電話號碼、公司名稱和地址等敏感資料。

WEAK：

- 自2017年3月起，內部錯誤地將Google Drive雲端硬碟設定為「任何知道這個連結的人都能查看」

ACTION：

- 目前Ateam已經完成了對此一事件的調查，承諾將加強個人資訊的管理

近期個資外洩事件

> 二手網上買賣平台個資外洩犯下根本性失誤

網上買賣平台Carousell去年進行系統遷移期間發生資料外洩事件，令到260萬名 Carousell全球用戶的個人資料遭到外洩。

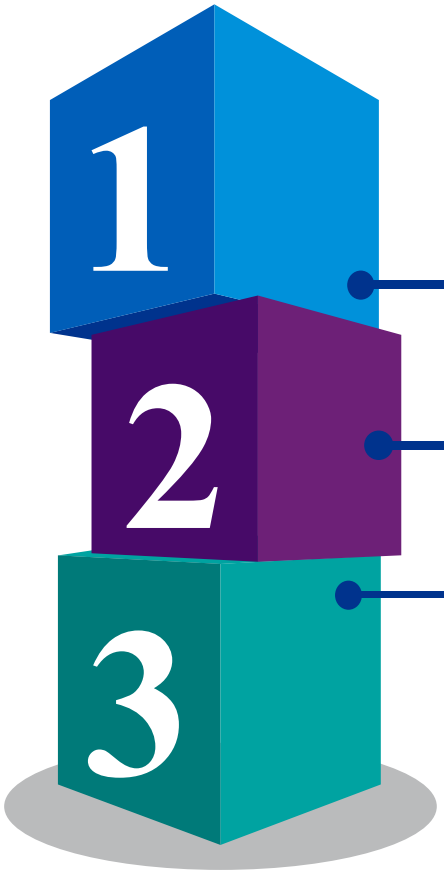
WEAK：

- 未有在系統遷移前進行私隱影響評估
- 不全面的編碼覆檢程序、
- 欠缺有效的偵測異常活動，導致未能防止或偵側用戶的個人資料，在相關應用程式被擷取

ACTION：

- Carousell為一項新功能進行標準覆檢時才發現該保安漏洞，已即時修復
- 指示平台採取多個步驟糾正，以及防止有關違規情況再次發生

個資外洩事件常見原因



人員

- 內部管理人員或委外廠商疏失
- 遭社交工程入侵電腦

系統

- 系統漏洞遭到利用
- 防火牆及其他雲端服務安全設定錯誤

流程

- 未妥善設置權限控管

如何降低個資外洩的危機?

個資保護落地措施

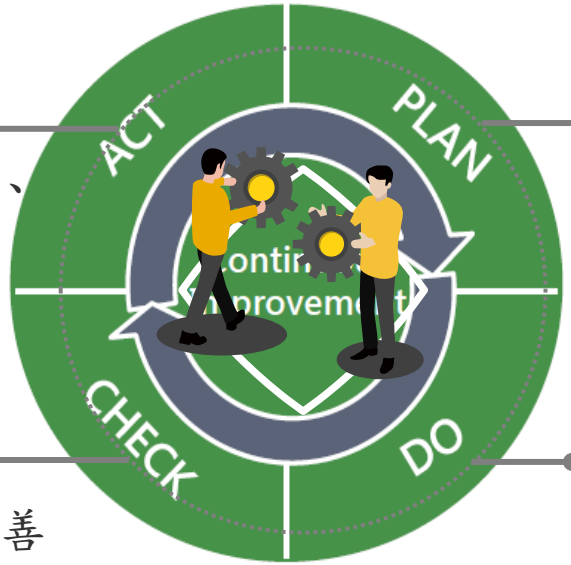
- 防毒防駭系統
- 導入資料盜失防護（DLP）等進階機制
- 確實監控資料庫活動
- 依據主管機關個人資料檔案安全維護計畫，並參考國際與國內資安標準，如ISO27001（資安管理制度）、ISO27701（隱私保護制度）等規範要求

資安意識提升

- 未經確認不任意提供資料
- 不開啟來路不明的電子郵件及附加檔案
- 不登入未經確認的陌生網站
- 避免社交工程的攻擊傷害

臺灣個人資料保護與管理制度規範 TPIPAS：2021

組織透過「PDCA方法論」，建立一套將個人資料保護與組織營運連結、符合我國個人資料保護相關法令與國際隱私保護趨勢之系統化管理制度。



檢查

依據個人資料保護管理政策、目標及要求，評估與監督流程及其產出，並將結果回報給最高管理階層加以審查。

計畫

建立個人資料保護管理政策、目標及相關程序。

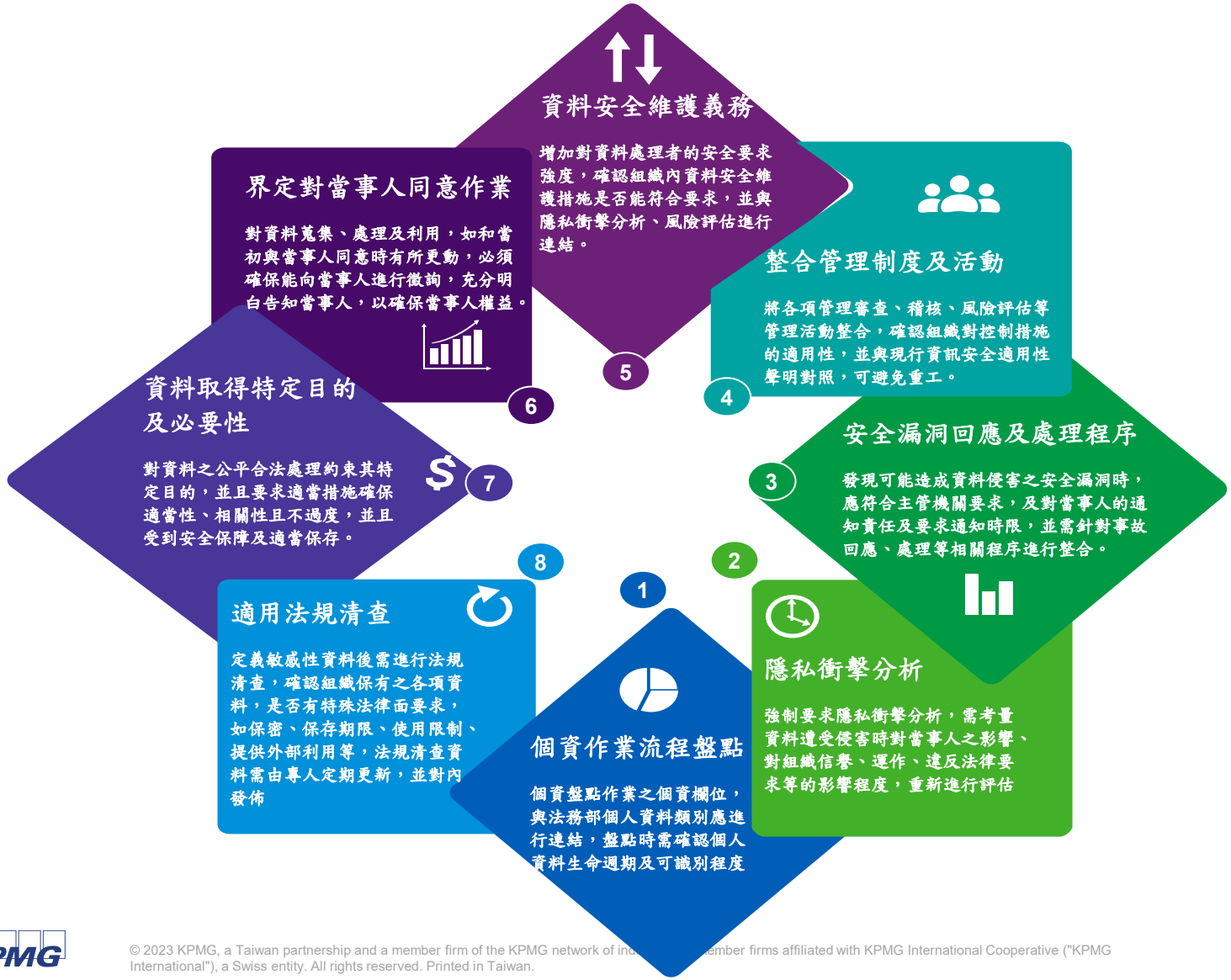
行動

採取措施，以持續改善個人資料管理制度之績效。

執行

實施個人資料管理制度。

個人資料保護管理制度之強化面向



資安宣導

資訊安全威脅

好奇人士

剛學會入侵電腦的方法，就應用書本上寫的方法當起駭客

內部員工

員工點開釣魚信件、下載病毒檔案、員工竊取內部資料

間諜

因商業上或政治上的因素，以各種滲透入侵技術取得企業、國家機密文件

組織型駭客

以竊取或破壞單位內部電腦機敏檔案資料為目的

資安事件

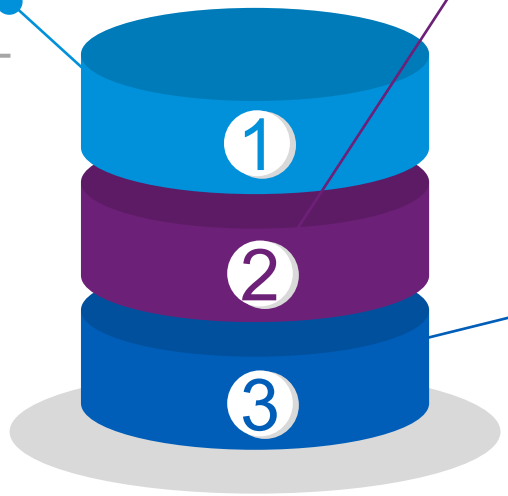
任何違反常軌的異常行為，其可能造成資訊系統及網路的安全威脅。

外部事件

- 電腦病毒感染事件
- 駭客攻擊
- 非法入侵

內部事件

- 設備故障
- 人員差錯
- 內部設備引起的火災、爆炸



自然事件

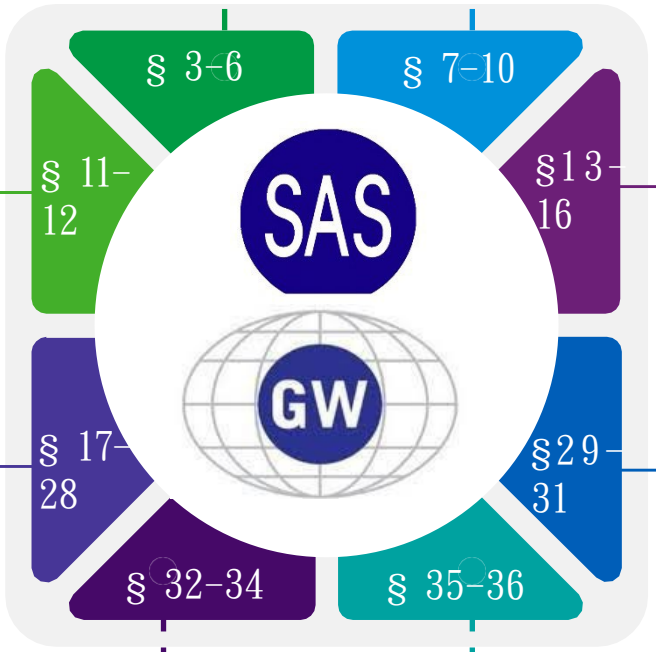
- 天然災害 (颱風、地震...)
- 重大突發事件 (爆炸、火災...)

資訊安全成為企業內部控制焦點

金管會為強化公開發行公司資訊安全管理機制，於2021年12月28日增訂發布「公開發行公司建立內部控制制度處理準則」第9條之1。依該條規定，公開發行公司應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。

資通安全管控指引 8大控制面向，34項資安要求

為協助上市櫃公司強化資通安全防護及管理機制，證交所於2021年12月23日發布「上市上櫃公司資通安全管控指引」。



政策及推動組織

資通安全治理

核心業務及其重要性

辨識公司核心業務

系統盤點及風險評估

辨識支持核心業務運作之系統

系統發展及維護安全

滲透測試、弱點掃描、源碼檢測

資安防護控制措施

主要資訊架構資安控管

委外辦理之管理措施

事件通報應變及情資評估因應

持續精進及績效管理

資安防護控制措施

以資安防護控制措施為例，資通安全管控指引第18條規定企業應具備以下措施：

上(興)櫃重大內部控制缺失及提醒事項-資安部分

財團法人中華民國證券櫃買賣中心於民國112年11月27日證櫃監字第1120203112號函知本所有關近期上(興)櫃公司發生重大內部控制缺失之情事，請會計師提醒公司右列事項：

近期資通安全事件頻傳，為應強化並落實資訊安全風險管理，提醒以下事項：

1. 參考主管機關發布之**上市上櫃公司資通安全管控指引**訂定並執行**資通安全防護及管理機制**。
2. 鼓勵公司可加入如**台灣電腦網路危機處理暨協調中心(TWCERT/CC)**等組織，以便免費取得資安預警情資及瞭解資安威脅與弱點資訊。

個人資料保護循環缺失

01

- 公司為連鎖零售通路業者，設有會員制度並蒐集會員個人資料，經惡意人士透過境外IP竊取並販售公司之會員資料，致消費者之姓名、電語、地址、消費時間及消費明細等個人資料外洩，並經主管機關依違反個人資料保護法處以罰鍰。

02

- 公司未落實資訊安全管理，致網站存在資訊安全弱點缺失，且未能察覺早已被植入之惡意程式，故未能及時執行適當安全維護措施，造成消費者個人資料外洩且無法回復。

KPMG

代理當事人線上申請
信用報告流程及資訊環境

- 作業流程及控制重點
- 資訊環境及控制重點

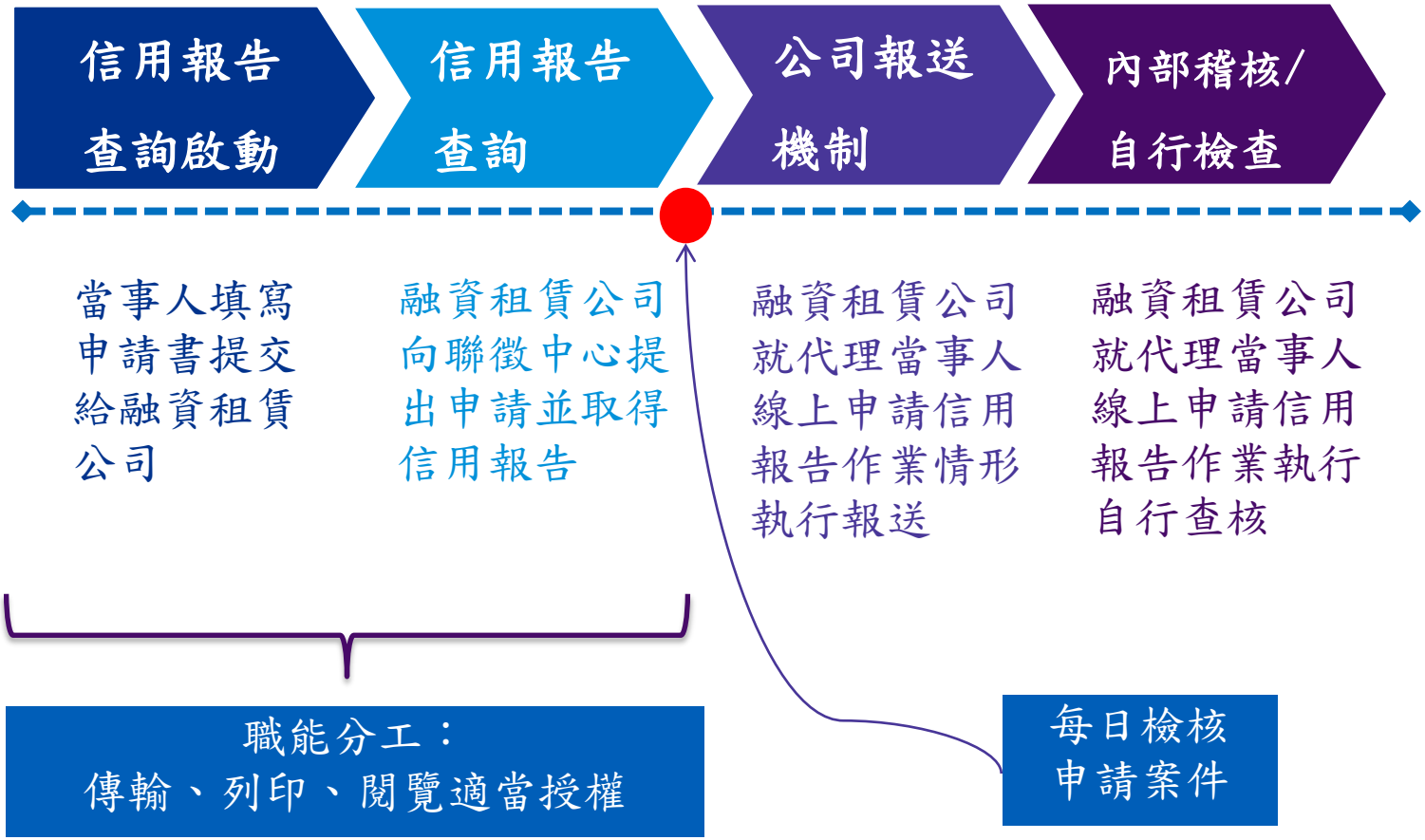
作業流程及控制重點

代理當事人線上申請信用報告作業依據

融資租賃公司代理當事人線上申請信用報告作業依據之規範：

- 融資租賃公司代理當事人線上申請信用報告作業控管要點
- 代理當事人線上申請信用報告作業辦法
- 融資租賃公司交易資訊報送作業要點

代理當事人線上申請信用報告作業流程



蒐集處理及利用個人資料告知與書面同意程序

流程控制點–信用報告查詢啟動

當事人填寫信用報告申請書及告知暨同意書並簽署，檢附相關身份證明文件，融資租賃公司業務人員確認上述文件係由當事人親自簽章且證件為當事人提供，並將相關文件傳輸予內部承辦人員。

控制重點

- ✓ 代理當事人線上申請信用報告是否取得當事人簽署同意。
- ✓ 融資租賃公司是否核實查驗當事人身分。

確認方式：
1.電話照會並留下照會紀錄
2.業務拍照證明由當事人親簽
3.由另一位業務人員於文件簽章，證明由當事人親簽

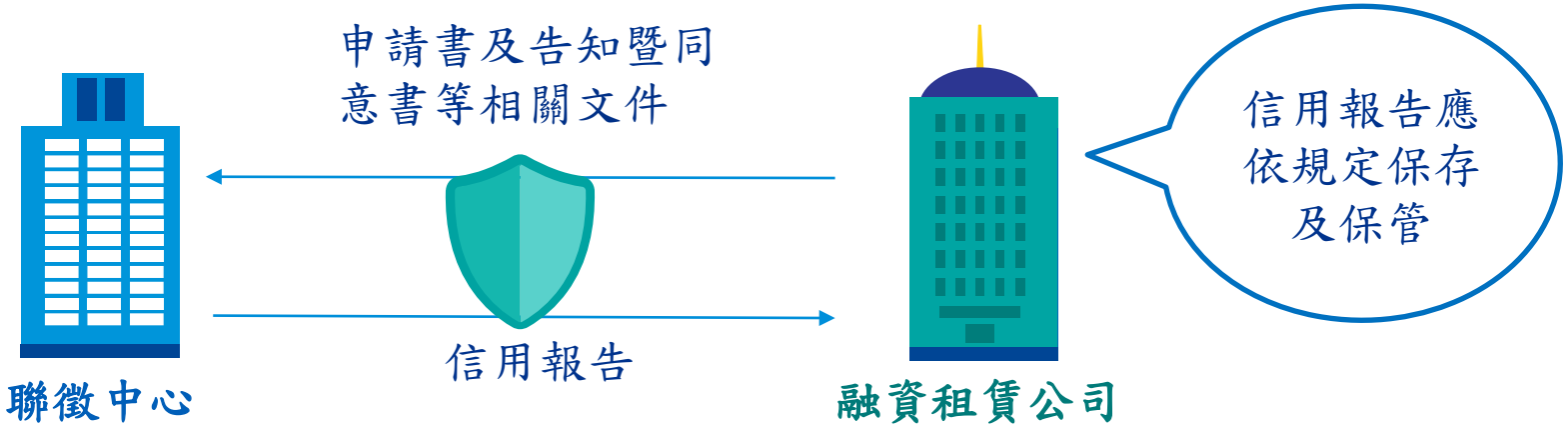
照會紀錄如使用書面紀錄，應包含以下資訊：
人：照會人及被照會人姓名
事：照會事項及內容摘要
時：照會日期
物：照會方式（電話、拍照、簡訊…）

流程控制點–信用報告查詢

融資租賃公司審查人員確認相關文件齊全，透過聯徵中心主機傳輸相關文件申請信用報告，聯徵中心受理申請後，確認文件齊全及核對內容無誤後，傳輸信用報告予融資租賃公司。

控制重點

- ✓ 信用報告是否有浮水印。
- ✓ 信用報告之存取及保管是否有妥善管理；資料銷毀是否有依照銷毀程序進行。



流程控制點–公司報送機制

報送規定：

報送資料	報送規定
企業交易契約資料(R01)	於新增、異動時，於交易完成後五個營業日內報送。
個人交易契約資料(R01)	於新增、異動時，於交易完成後二個營業日內報送。
繳款資料(R02)	於每月十日前，將截至上月底之繳款資料，報送至財團法人聯合徵信中心。
案件處理資料(R03)	於每筆代理案件決定承作或未承作時，於五個營業日內報送。

控制重點

- ✓ 資料報送時點是否及時。
- ✓ 資料報送是否完整及正確。

流程控制點-內部稽核/自行檢查

自行查核方式：

方式	重點項目
內部稽核	融資租賃公司對於代理當事人線上申請信用報告作業，由內部稽核人員執行查核，以確認執行上述作業之控管情形，是否符合相關規範。
自行檢查	融資租賃公司對於代理當事人線上申請信用報告作業，由具獨立性之人員執行自行檢查機制，以確認執行上述作業之控管情形，是否符合相關規範。

資訊環境發生變動時，依檢查表進行檢查

每年至少查核乙次，查核報告副本彙總送聯徵中心

控制重點

- ✓ 是否有定期執行內部稽核/自行檢查。
- ✓ 內部稽核/自行檢查人員是否具備獨立性。

流程控制點–職能分工

職能分工授權類別：

授權類別	授權項目
閱覽	閱覽信用報告之權限
列印	列印信用報告之權限
傳輸	1.線上傳輸申請信用報告之權限 2.線上傳輸報送交易資料之權限

控制重點

- ✓ 取得授權閱覽信用報告人員、線上傳輸執行人員及列印人員清單，檢視是否有設簿登記控管。
- ✓ 閱覽信用報告人員、線上傳輸執行人員及列印人員是否經適當授權。

流程控制點–每日檢核申請案件

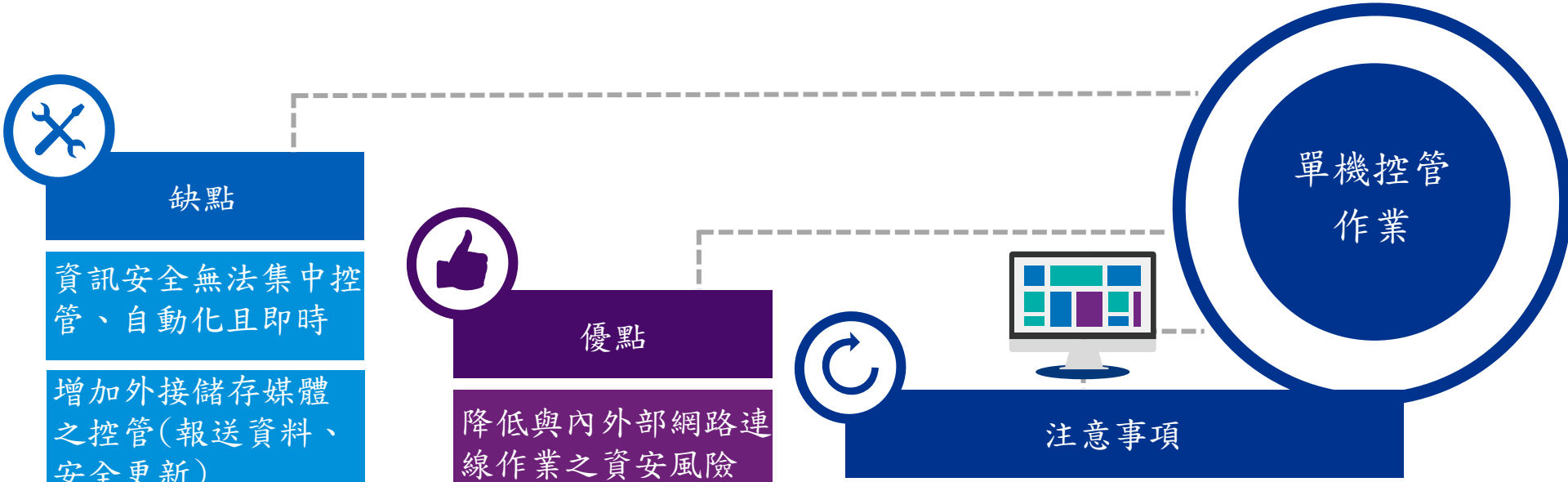
融資租賃公司應切實核對代理當事人線上申請信用報告清單與取具之信用報告，針對異常者追蹤原因，並由權責主管覆核。

控制重點

- ✓ 代理當事人線上申請信用報告清單是否切實核對，針對異常者追蹤原因，並由權責主管覆核。

資訊環境與控制重點

系統架構(單機作業)



缺點

資訊安全無法集中控管、自動化且即時

增加外接儲存媒體之控管(報送資料、安全更新)

聯徵專線主機設置於開放空間時，實體安全控管較不容易

優點

降低與內外部網路連線作業之資安風險

節省軟硬體設備維護成本

節省網路安全控管之成本

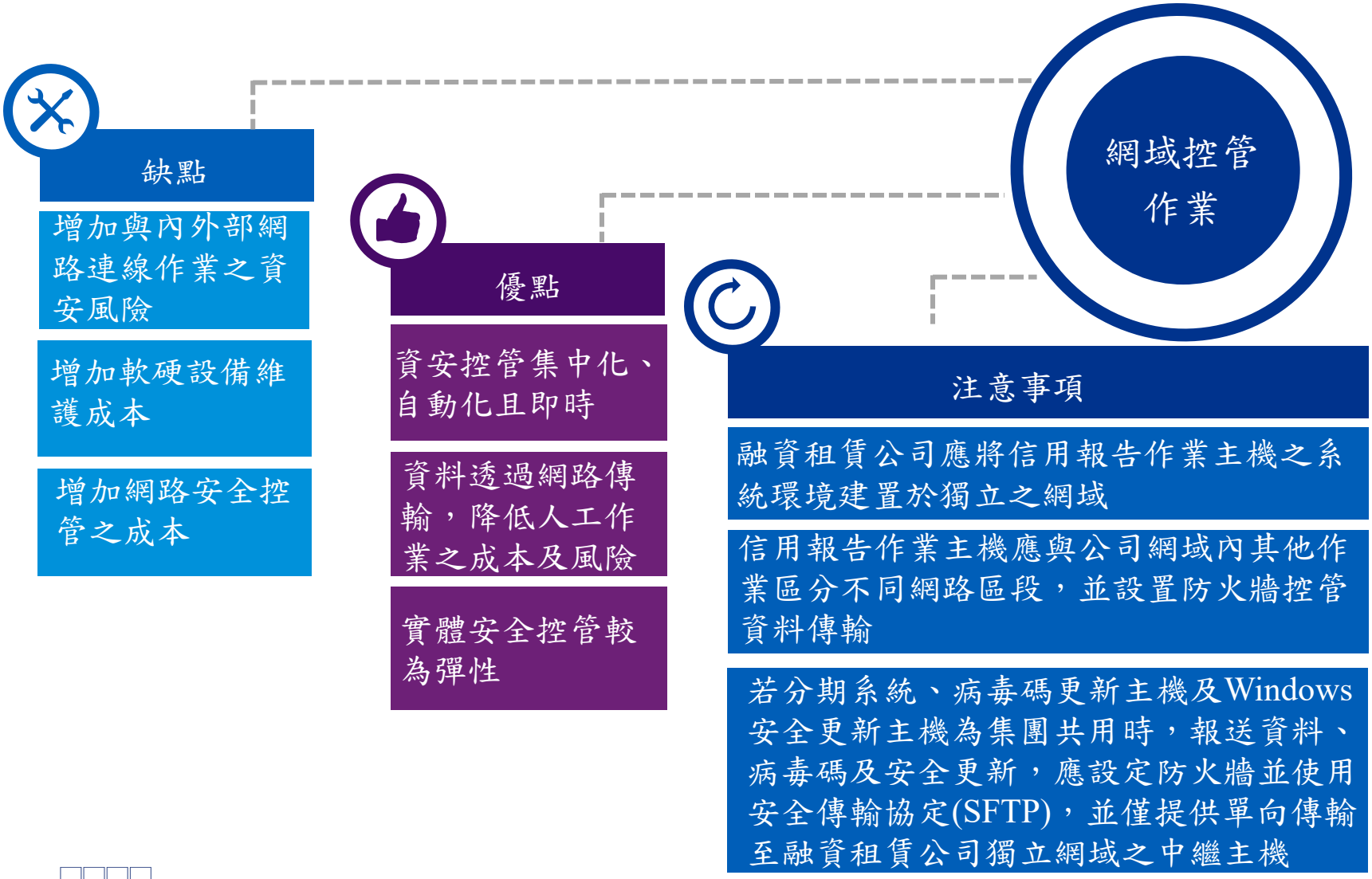
注意事項

Windows安全更新(至少半年更新一次)、病毒碼更新應注意時效性(至少每月更新)及定期執行掃毒作業(至少每週一次)

外接儲存媒體應加強控管其實體存取、讀寫及加密之控管機制

若聯徵專線主機設置於開放空間，應加強實體安全之控管

系統架構(網域作業)



資訊安全控制作業

資訊安全包含六大構面進行

1. 個人電腦與伺服器

① 帳號、權限與密碼之控管機制
② 作業系統與惡意程式之防護機制
③ 可安裝軟體控管機制
④ 螢幕保護裝置之控管
⑤ RCP、RDP 與FTP 等控管機制
⑥ 可攜式媒體控管機制

2. 網路安全

① 虛擬專屬網路(VPN)控管機制
② 禁止由外部VPN 連線到代理作業相關之主機及個人電腦
③ 個人電腦與伺服器防火牆設定
④ 僅限總公司及經本中心核可傳輸之分公司可閱覽或列印信用報告

3. 當事人信用報告電子檔案

① 存取控管機制
② 電子檔案備份機制
③ 電子檔案銷毀（含備份）機制

4. 應用系統

① 帳號、權限與密碼之控管機制
② 系統新開發、異動或刪除之控管機制，若委外開發或維護者，其資訊安全控管機制
③ 使用者檢視信用報告之控管機制（如浮水印、IP、時間…等）
④ 當事人信用報告列印控管機制
⑤ 當事人信用報告存取軌跡控管機制

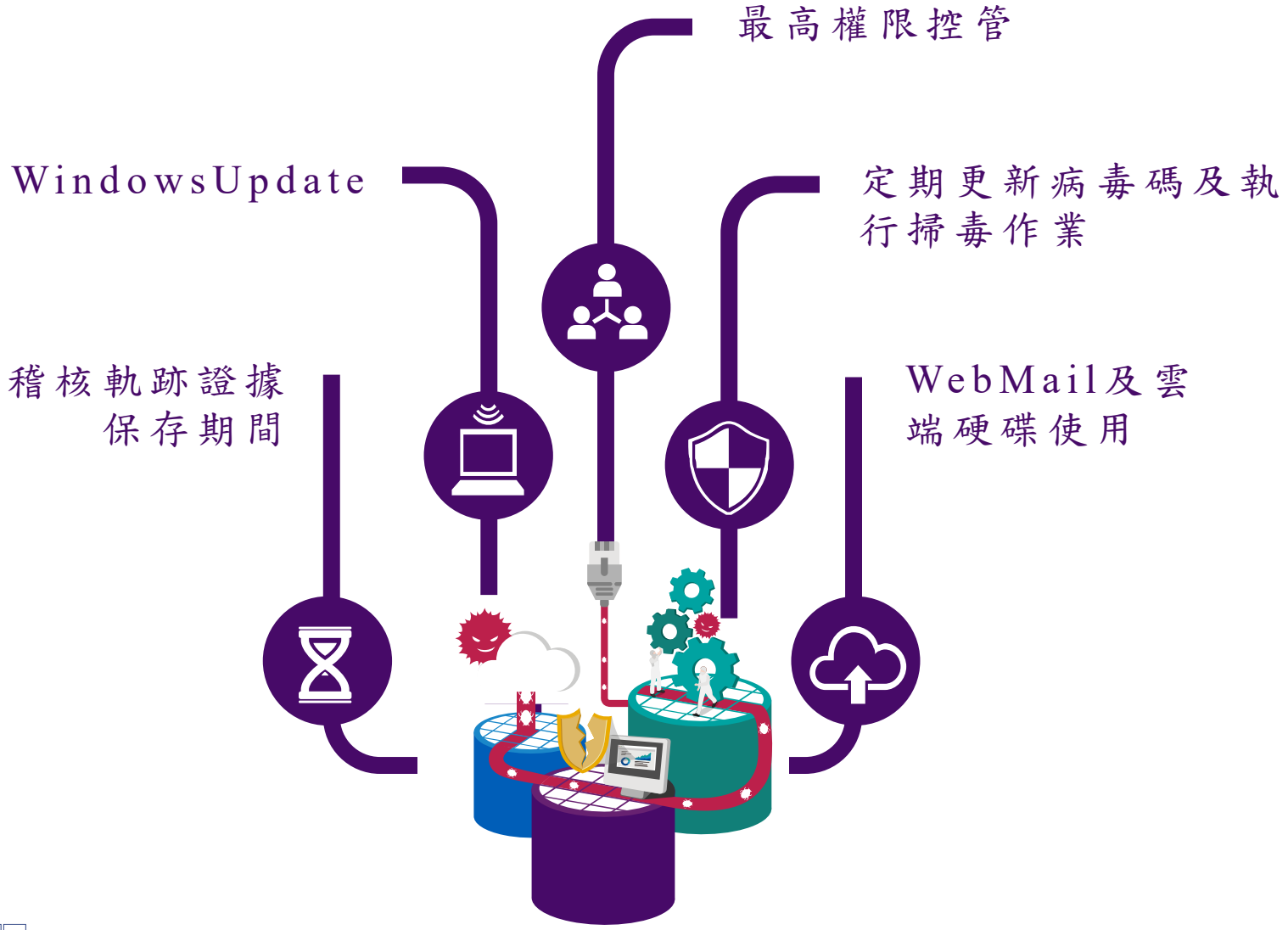
5. 資料庫

① 帳號、權限與密碼之控管機制
② 資料庫存取控管機制

6. 多功能事務機

① 帳號、權限與密碼之控管機制
② 當事人信用報告列印控管機制
③ 傳真控管機制
④ 可攜式媒體控管機制

資訊安全重點議題



最高權限帳號控管議題

密碼保管

- 密碼分持
- 密碼函封存

緊急取用程序

- 代理人機制
- 緊急密碼函

設簿登記

- 密碼變更機制
- 管理帳號使用紀錄

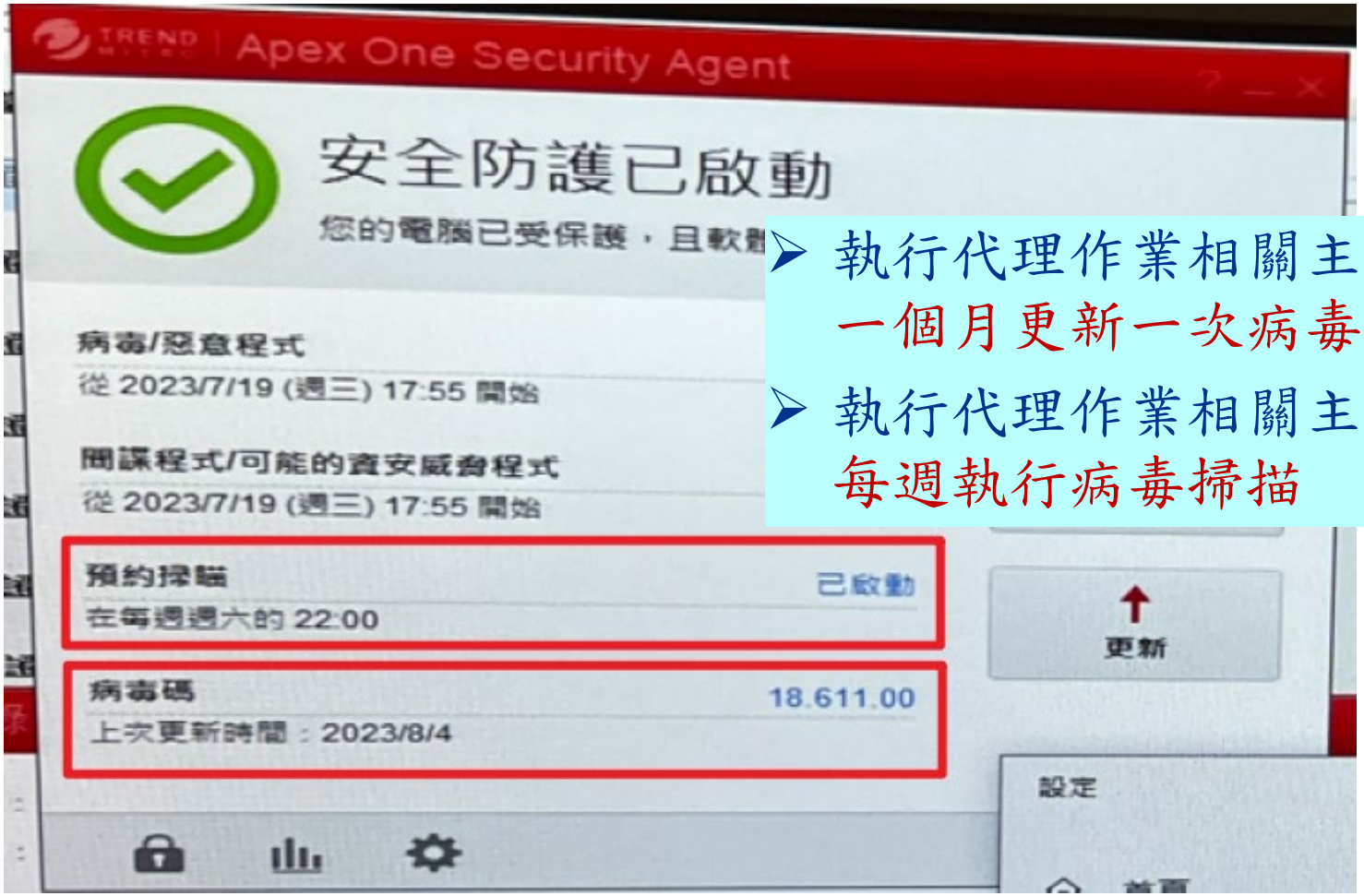
Part A　　Part B　　deputy

＊ 密碼如採分持控管，建議其中一半為主管分持

Windows更新頻率議題

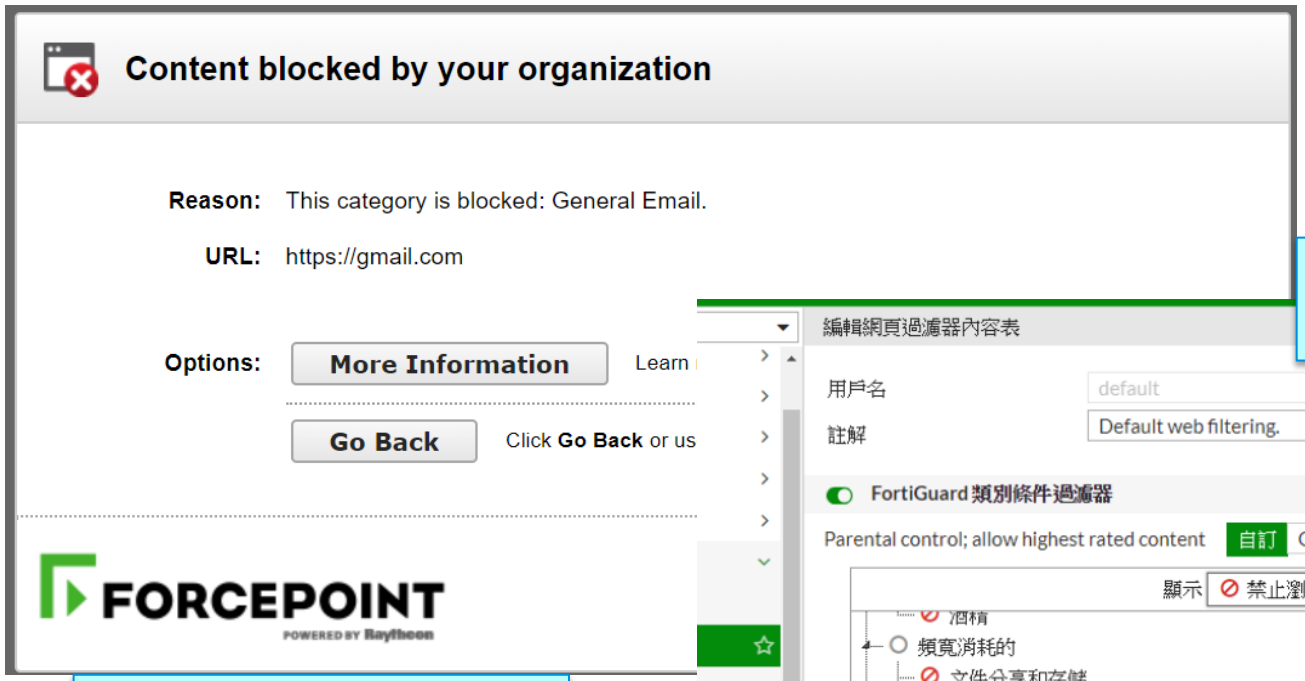
- Windows Update頻率至少半年更新一次。
- 人工更新需特別注意

病毒碼更新與掃描議題

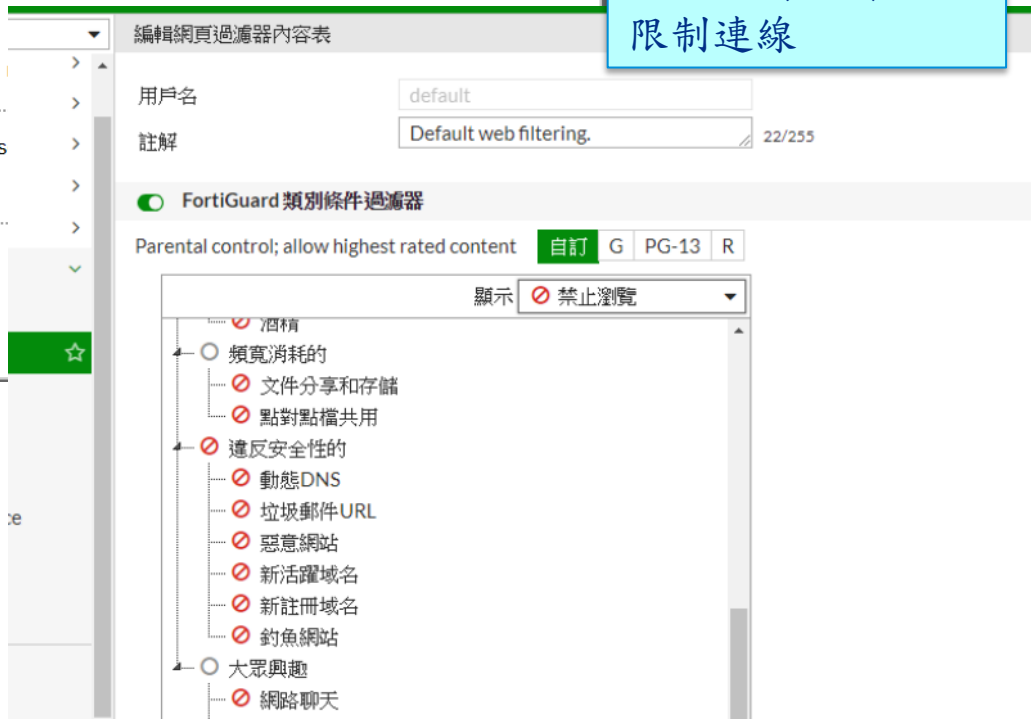


- 執行代理作業相關主機至少一個月更新一次病毒碼。
- 執行代理作業相關主機至少每週執行病毒掃描

WebMail及雲端硬碟使用議題



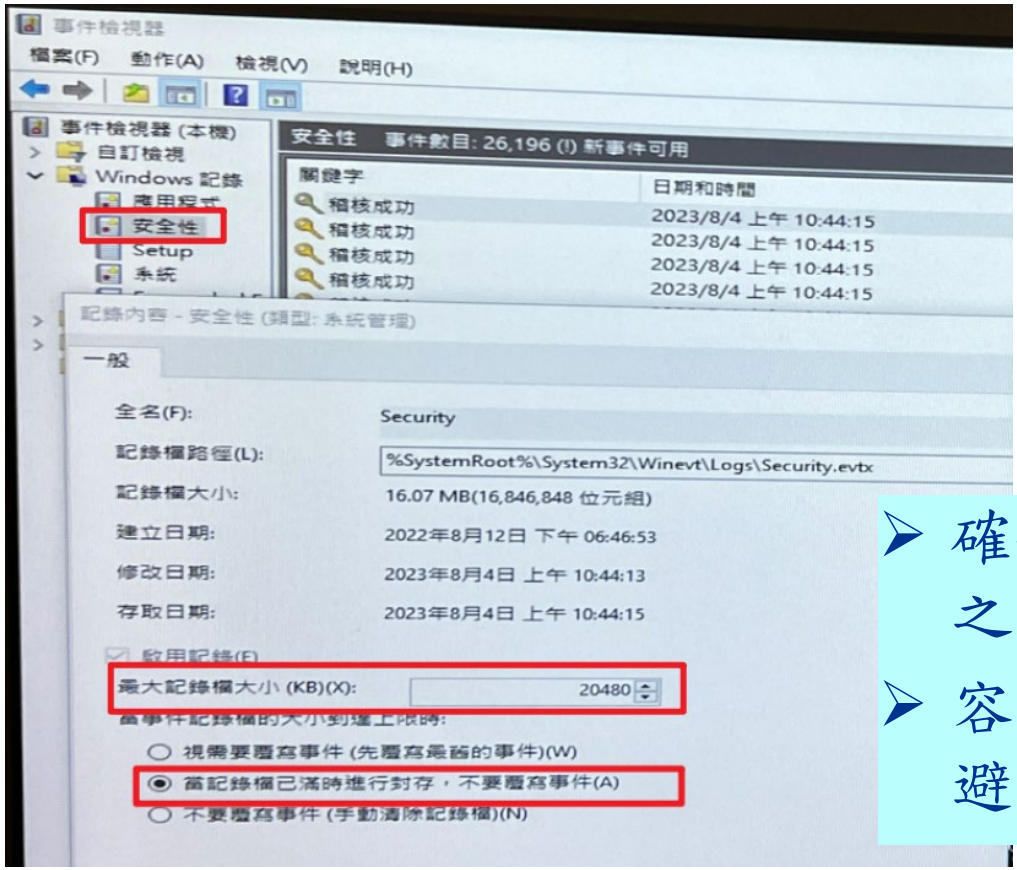
使用DLP軟體控管



於防火牆規則設定限制連線

稽核軌跡證據保存議題

執行代理作業相關主機或個人電腦之事件檢視器，應評估過去執行線上代理作業產生之稽核軌跡容量，以估算需設定最大稽核紀錄檔案之大小。



- 確保可留存至少一個月之稽核軌跡；或
- 容量屆滿時另行封存，避免覆蓋log紀錄。

KPMG

代理當事人線上申請信用報告常見缺失及改善建議事項

- 實地查核流程
- 常見缺失及改善建議事項-流程面
- 常見缺失及改善建議事項-資訊面
- 變更管理作業與Check List重點說明

實地查核流程

實地查核流程

啟動會議 → **資訊環境檢視 信用報告案件抽樣** → **結案會議** → **後續追蹤**

訪談融資租賃公司瞭解代理作業流程及架構

執行實地查核

- 資訊面：
  實地檢視資訊環境
- 流程面：
  信用報告案件抽樣

提出發現及建議事項與融資租賃公司及聯徵中心討論

後續追蹤發現及建議事項




實地查核作業-啟動會議議題

藉由訪談
了解流程及架構

討論議題：

1 代理作業分工、職掌及授權
1.1 簡明敘述代理作業組織架構、分工及職掌異動情形
1.2 代理作業組織架構、分工、職掌及相關作業規章異動情形
1.3 資訊部門人員配置、職掌及異動情形
1.4 案件承作情形

2 代理當事人線上申請信用報告之資訊系統架構及環境(存取權限、參數設定...等)及其異動情形

3 代理作業流程(從申請到報送)
3.1 申請：如何確認係由當事人親簽之相關機制
3.2 核對：每日核對申請案件紀錄相關機制
3.3 資料保存：申請相關文件之書面資料保存及信用報告之保存
3.4 報送：R01、R02及R03報送規則及流程
3.5 客訴：處理方式及實際情況

4 內部稽核及自行查核評估
4.1 查核計畫及執行情形
4.2 查核缺失之發現及其追蹤改善情形
4.3 查核報告副本彙總送聯徵中心之情形

5 分公司
5.1 分公司是否有代理當事人申請信用報告
5.2 企業及個人執行代理作業情形

控制測試

確認各項控制之設計是否有與程序不相符之處

確認各項控制執行落實度

常見缺失及改善建議事項-流程面

流程常見缺失及改善建議事項

職能分工與存取管理

針對代理當事人線上申請信用報告人員之線上傳輸、列印及閱覽之授權，並未確實登載於信用報告授權權限總表。

- 記錄之信用報告閱覽人員名單為可申請閱覽信用報告人員名單，非已授權之信用報告閱覽人員名單。
- 調/離職人員權限於職務調整或離職時，未即時調整帳號權限。

相關授權人員應記錄於授權明細表上，若有**異動**應確實登載於授權紀錄表，並經權責主管核准，帳號權限同步應即時調整。

流程常見缺失及改善建議事項

自行查核

- 未將實地查核發現事項列入自行查核之檢查項目

應確實將實地查核發現事項列入自行查核之檢查項目。

流程常見缺失及改善建議事項

公司報送機制

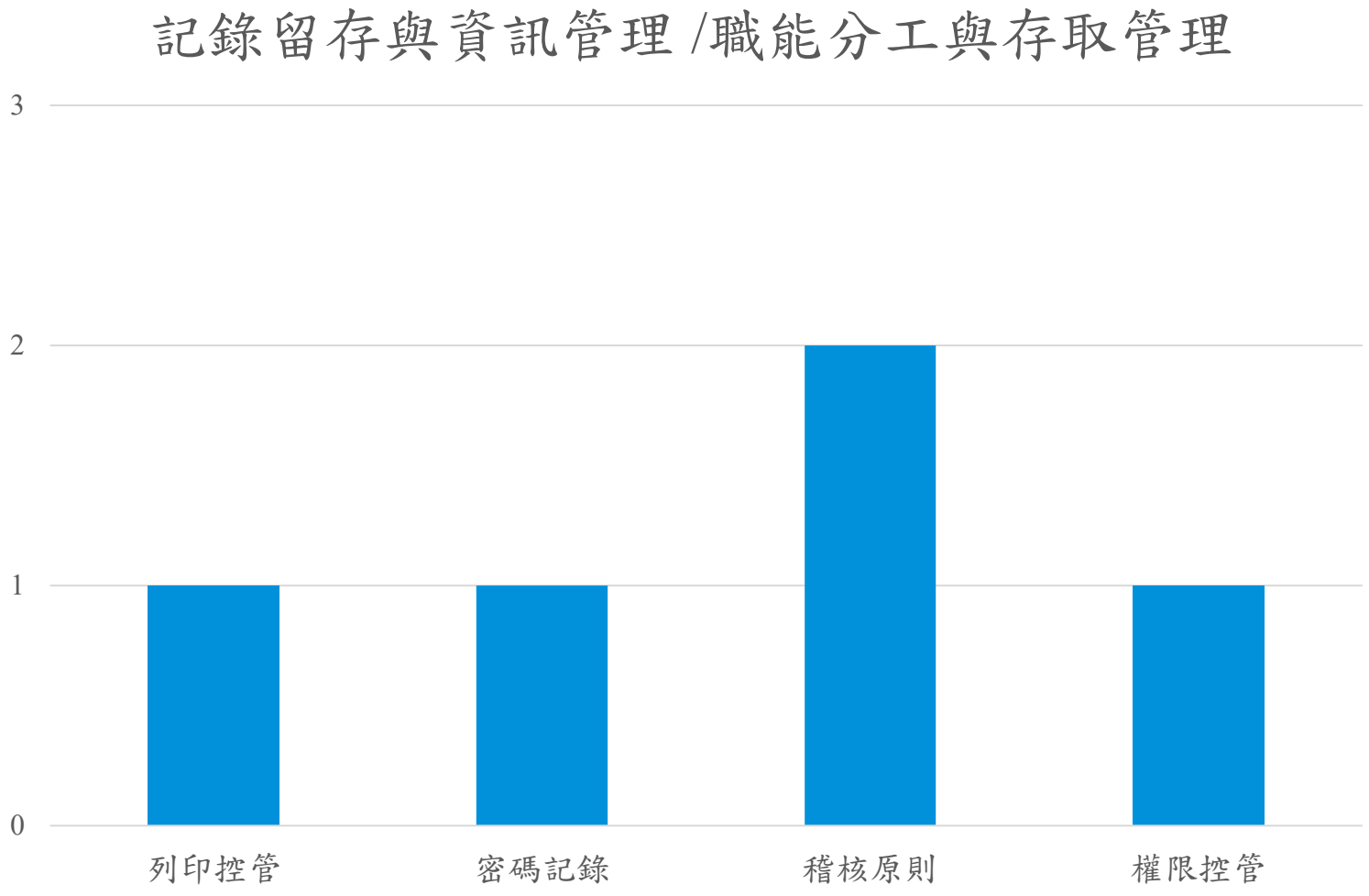
融資租賃公司資料報送時點不及時，報送資料不完整或不正確。

- 承作案件，有報送交易契約資料(R01)，漏報送繳款資料(R02)。
- 承作案件，交易契約資料(R01)及案件處理資料(R03)延遲報送。
- 承作案件，延遲報送繳款資料(R02)。
- 融資租賃公司未於確定承作或不承作日起，五個營業日內報送案件處理資料(R03)。

依循「融資租賃公司交易資訊報送作業要點」及時並正確報送資料。

常見缺失及改善建議事項-資訊面

112年實地查核常見建議事項



常見查核建議事項-職能分工與存取管理

最高權限帳號未分持密碼，使用帳號時未記錄登入的日期、時間、用途，並經帳號保管人簽名。

聯徵專用主機登入紀錄

No.	登入日期	主機/帳號	登入原因	密碼A	密碼B	處理人員
1						
2						
3						
4						
5						
6						
7						

管理者帳號密碼應以A、B Part 分持，且至少1Part須由主管持有

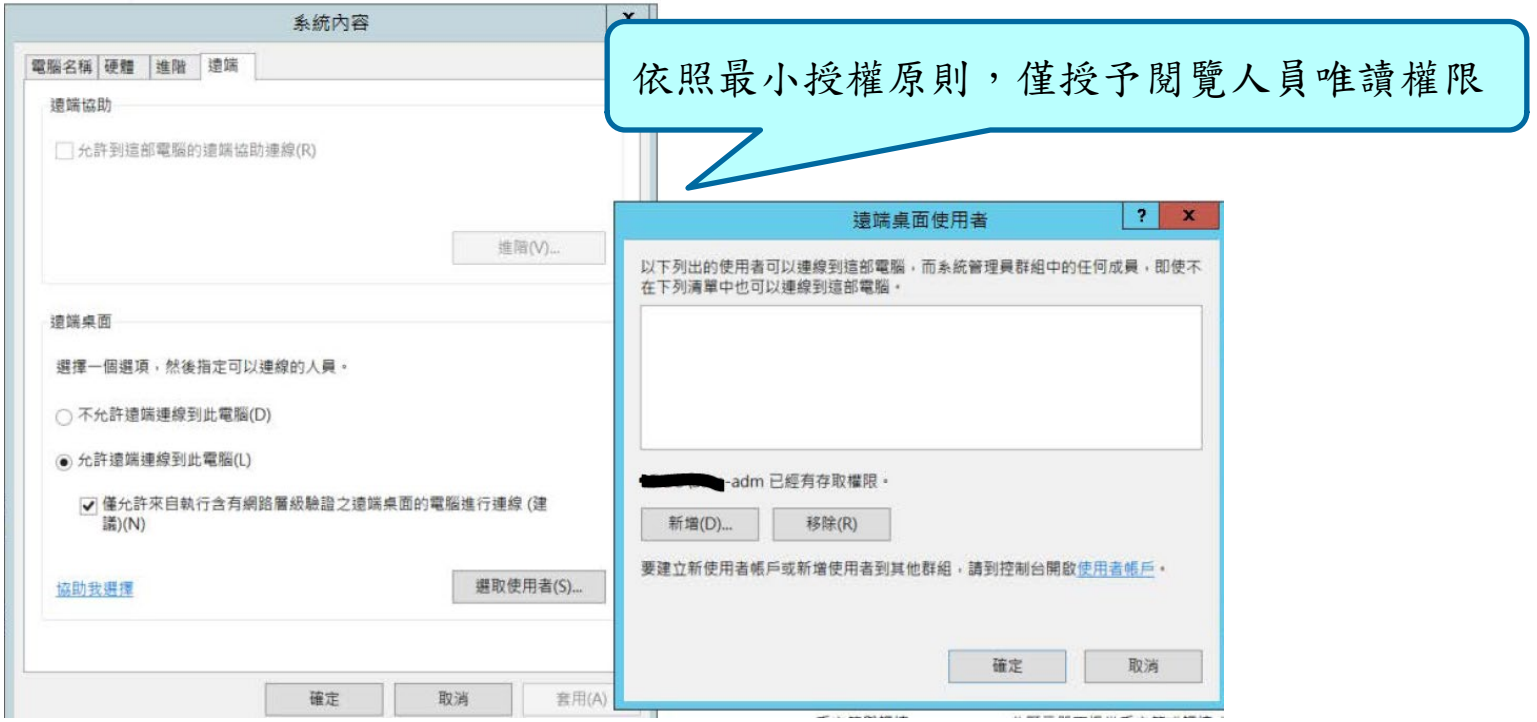
管理者帳號之使用情形需設簿登記，且密碼變更作業需紀錄。

管理者帳號彌封使用後需變更密碼，管理者帳號分持密碼需定期變更。

管理者帳號若長時間未使用，至少1年需變更1次密碼。

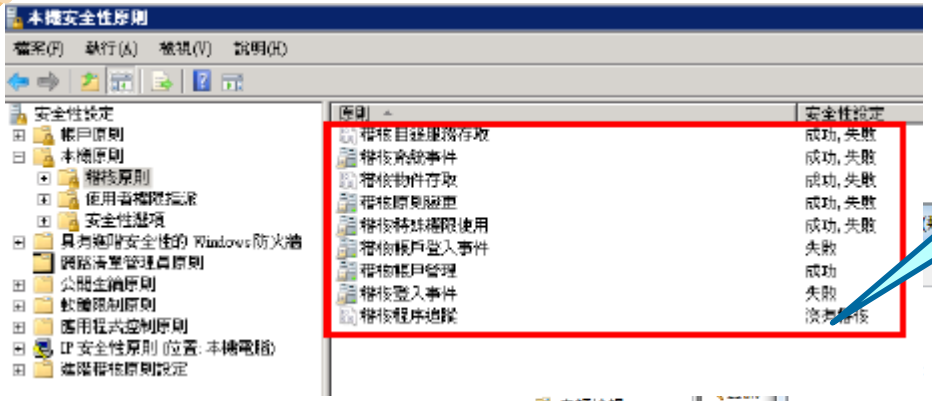
常見查核建議事項-職能分工與存取管理

閱覽人員登入JCIC信用報告主機檢視信用報告使用之帳號為系統管理員權限之帳號。



常見查核建議事項-記錄留存與資訊管理

未開啟本機稽核原則，或Windows稽核紀錄空間能保存的軌跡紀錄時間未滿1個月。

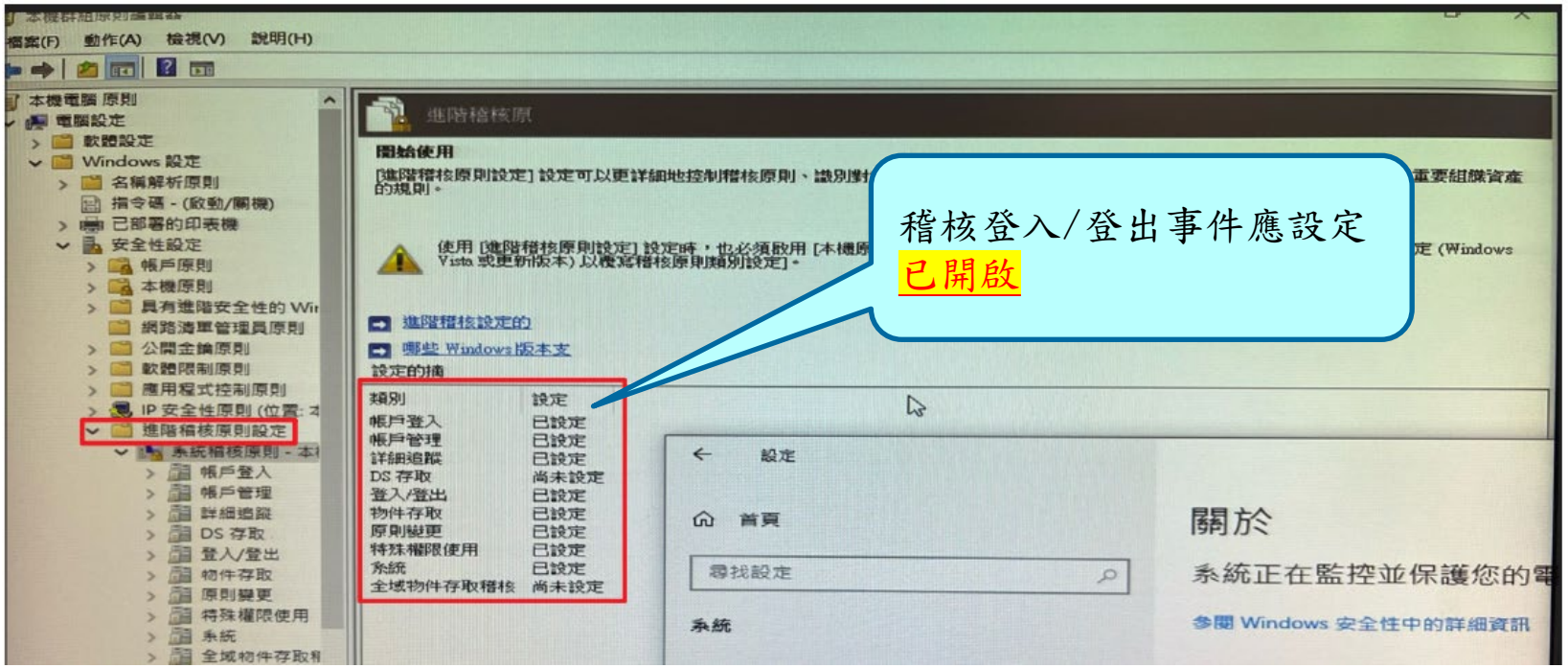


稽核紀錄應開啟，
稽核登入事件應設定
成功、失敗

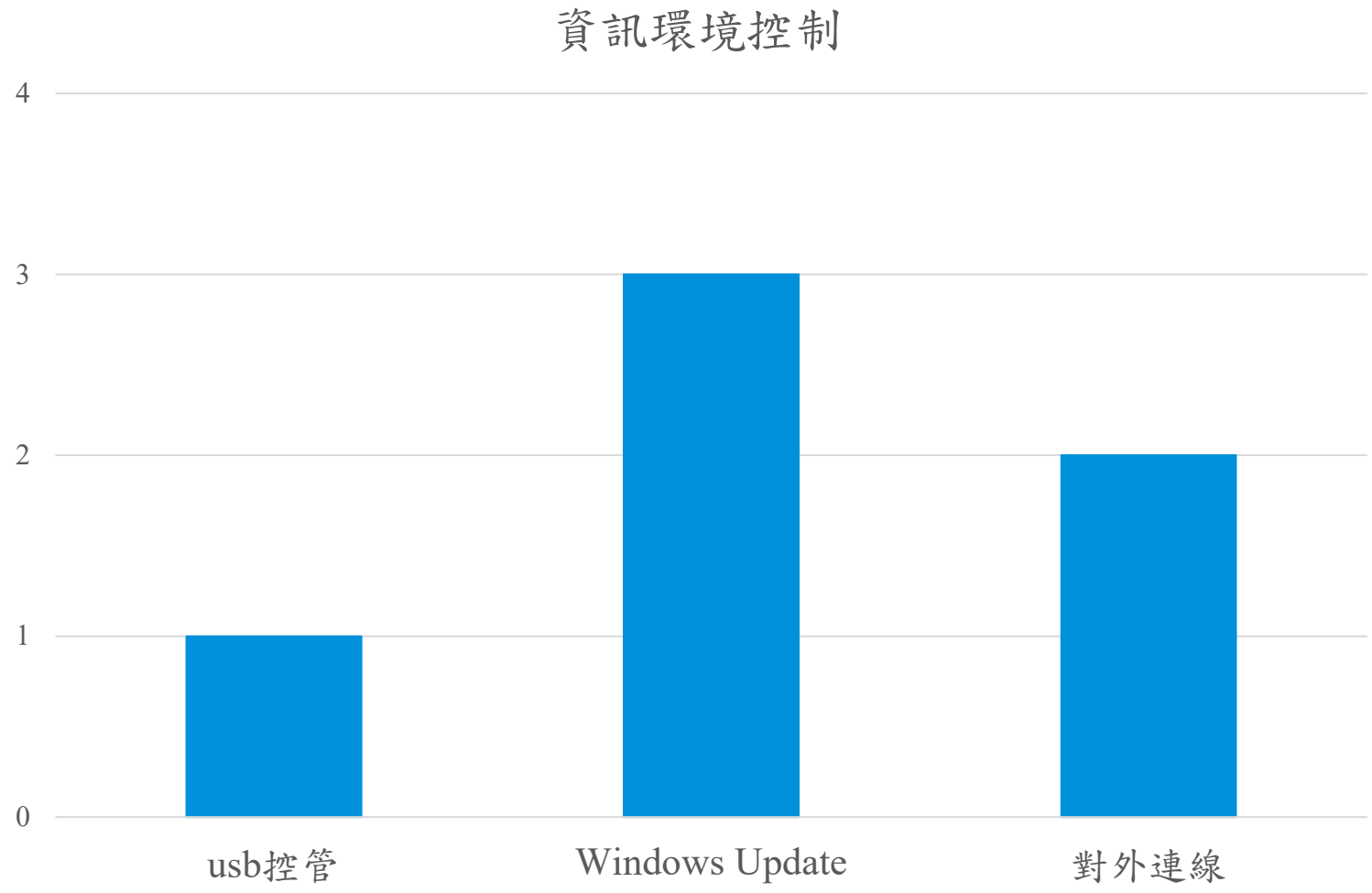
記錄檔大小設定，依實際能保存的天數進行評估

常見查核建議事項-記錄留存與資訊管理(續)

未開啟本機稽核原則，或Windows稽核紀錄空間能保存的軌跡紀錄時間未滿1個月。



112年實地查核常見建議事項



常見查核建議事項–資訊環境控制

防火牆規則或DLP設定不完善，導致可連線至雲端及WebMail，或可透過通訊軟體向外傳輸檔案。

常見查核建議事項-資訊環境控制

- JCIC信用報告主機仍維持舊版本之作業系統，該版本原廠已不支援作業系統之系統更新。

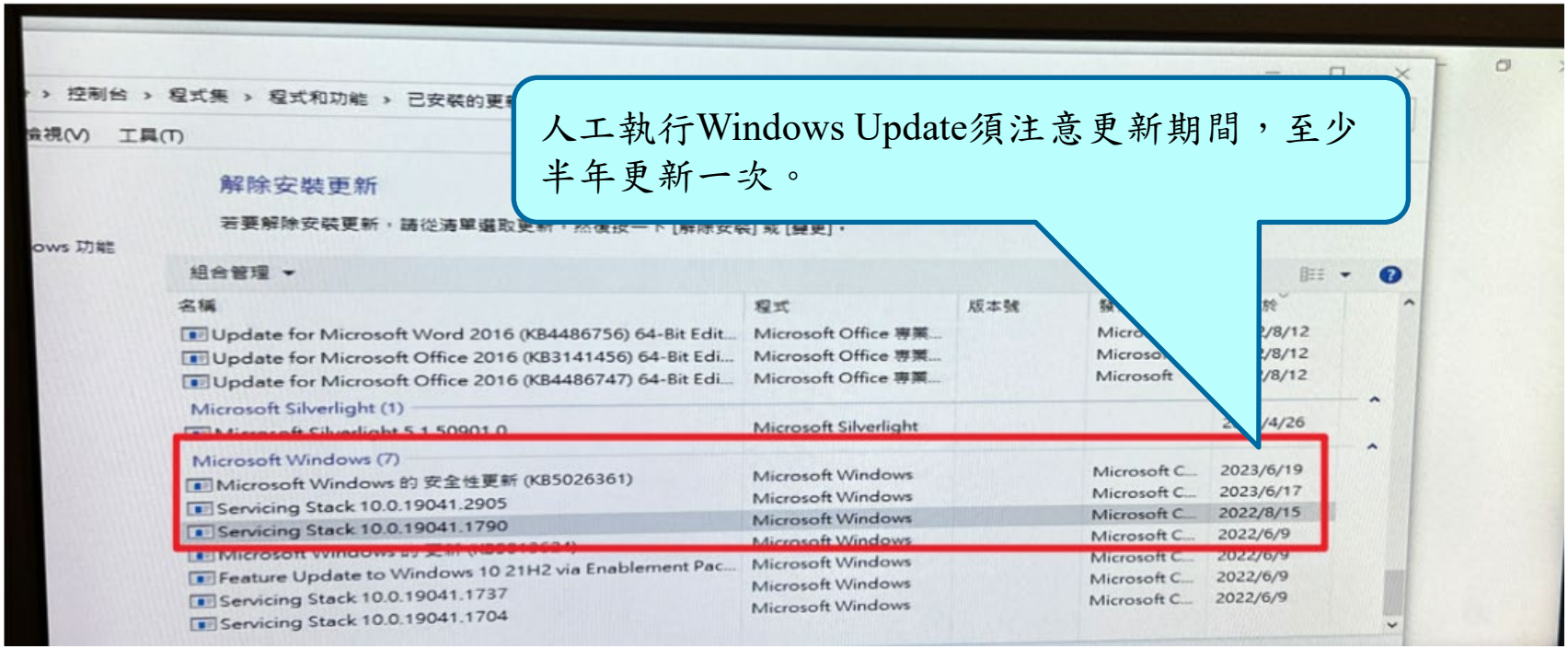
版本原廠已不支援系統更新，故若有系統安全漏洞無法及時進行修補。

項次	產品	停止支援日
1	Windows Server 2012 /2012 R2	2023 年 10 月 10 日

資訊來源：微軟官方網站公告

常見查核建議事項-資訊環境控制

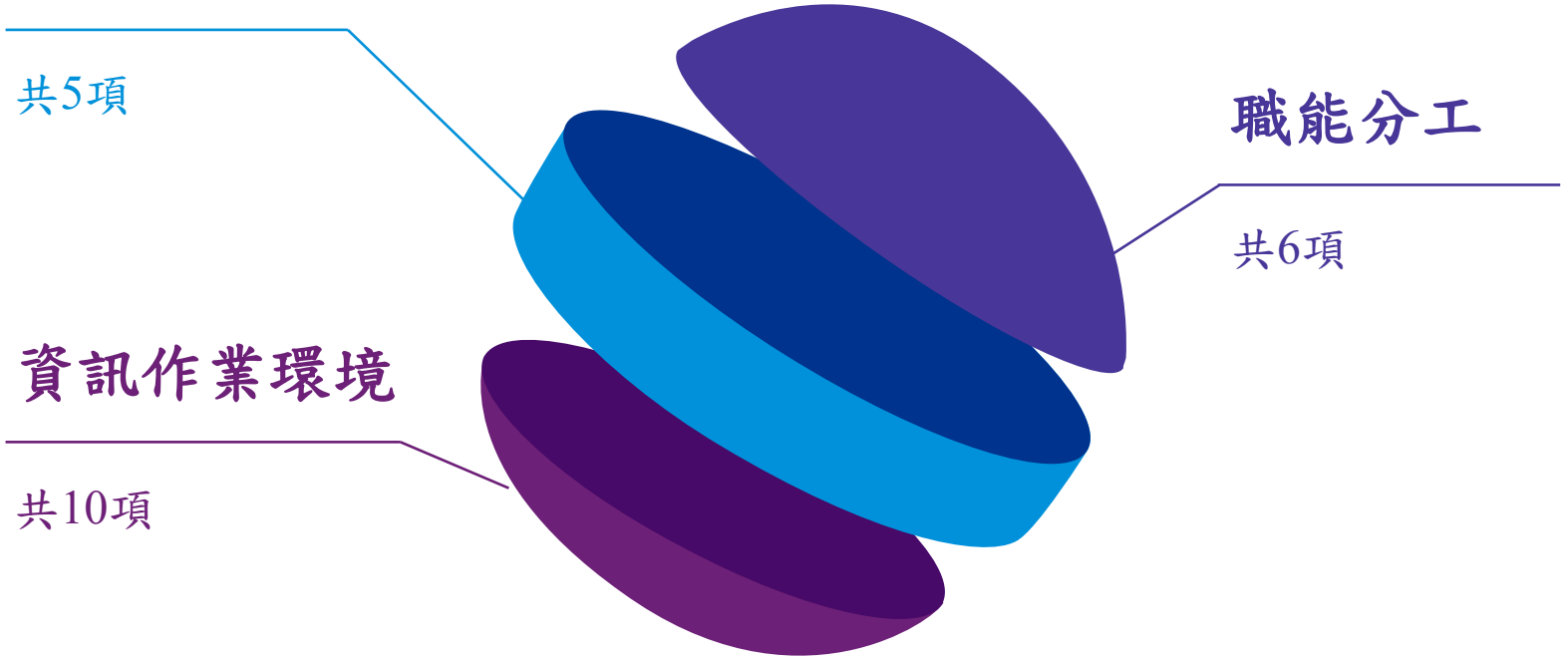
- 超過半年執行更新



KPMG

變更管理作業與Check List重點說明

資訊環境變更管理檢查表檢查項目



職能分工項目

	項次	檢核項目
	1	傳輸/報送相關資料夾之「共用」及「安全性」設定是否適當？
	2	信用報告回傳及保存相關資料夾之「共用」及「安全性」設定是否適當？
★	3	執行代理作業相關主機之管理者帳號設定是否適當？
★	4	執行代理作業相關主機之管理者帳號是否定期變更密碼？
	5	執行代理作業相關主機之使用者帳號設定是否適當？
	6	執行代理作業相關主機之本機密碼原則是否開啟？

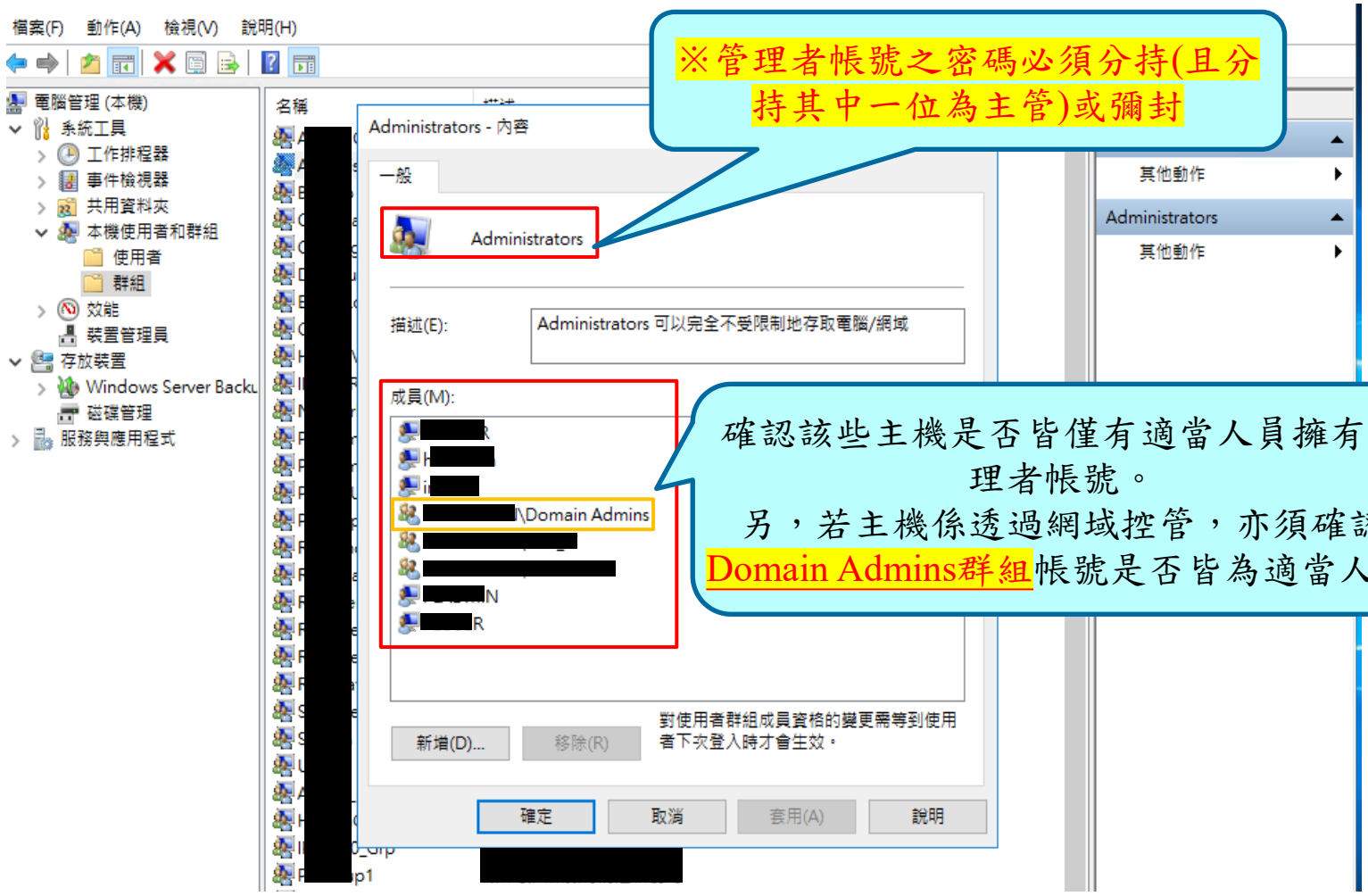
★ 重點說明檢核項目

★ 代理當事人線上申請信用報告作業資訊環境變更管理檢查表_v11202

職能分工
3

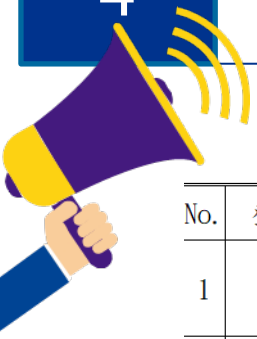
執行代理作業相關主機之管理者帳號設定是否適當？

v11202



職能分工
4

執行代理作業相關主機之管理者帳號使用後是否變更密碼？ v11202



聯徵專用主機登入紀錄

No.	登入日期	主機/帳號	登入原因	密碼A	密碼B	處理人員
1						
2						
3						
4						
5						
6						
7						

1. 管理者帳號密碼應以A、B Part 分持，且**至少1Part須由主管持有**
2. 管理者帳號之使用情形需設簿登記，且密碼變更作業需紀錄。
3. 管理者帳號彌封使用後需變更密碼，管理者帳號分持密碼需定期變更。
4. 管理者密碼若長時間未使用，至少1年需變更1次。
5. **啟用預設管理者帳號作為備援用途，須遵循上述規範。**

網路連線安全項目

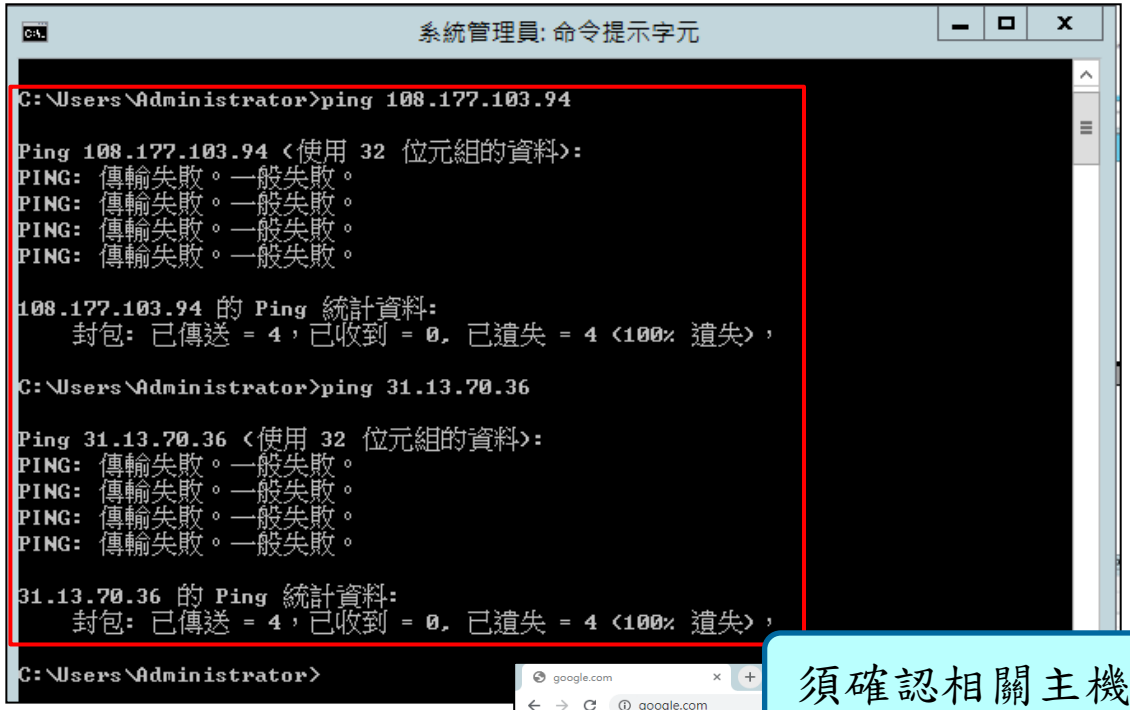
	項次	檢核項目
★	1	執行代理作業相關主機是否可連線至網際網路？
★	2	執行代理作業相關主機之防火牆設定是否適當？
★	3	執行代理作業相關主機之遠端桌面連線設定是否適當？
★	4	執行代理作業相關主機是否無法透過VPN方式自公司外部連線？
★	5	執行代理作業相關使用者/使用者電腦，是否無法透過VPN方式自公司外部連線並閱覽信用報告？

★ 重點說明檢核項目

★ 代理當事人線上申請信用報告作業資訊環境變更管理檢查表_v11202

網路安全
1

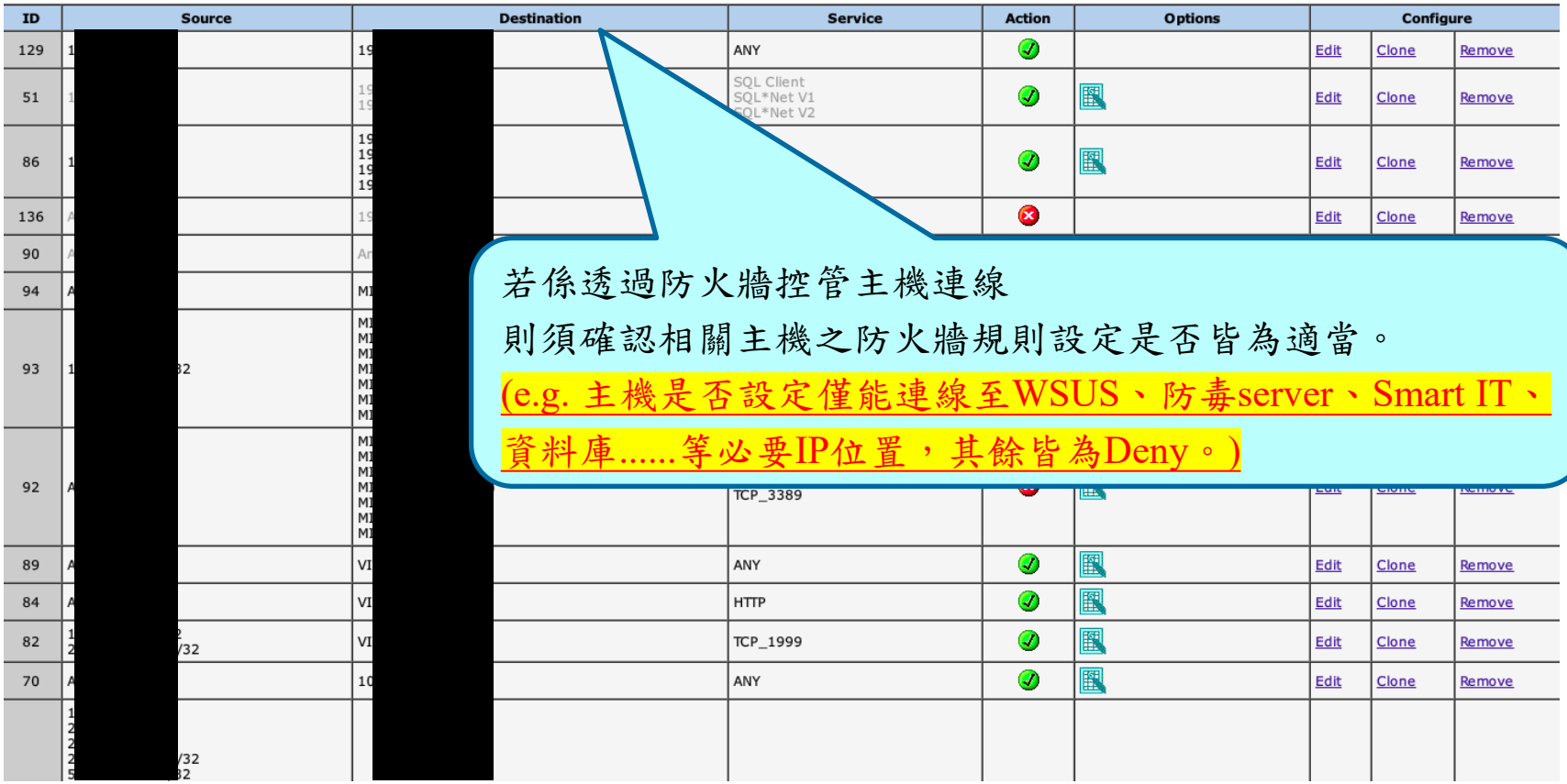
執行代理作業相關主機是否可連線至網際網路？



須確認相關主機是否皆無法連線至網際網路

網路安全
2

執行代理作業相關主機之防火牆設定是否適當？
(※視各融資租賃公司之作業情形而定)



ID	Source	Destination	Service	Action	Options	Configure
129	[redacted]	[redacted]	ANY	✓		Edit Clone Remove
51	[redacted]	[redacted]	SQL Client SQL*Net V1 SQL*Net V2	✓		Edit Clone Remove
86	[redacted]	[redacted]		✓		Edit Clone Remove
136	[redacted]	[redacted]		✗		Edit Clone Remove
90	[redacted]	[redacted]				
94	[redacted]	[redacted]				
93	[redacted]	[redacted]				
92	[redacted]	[redacted]	TCP_3389			
89	[redacted]	[redacted]	ANY	✓		Edit Clone Remove
84	[redacted]	[redacted]	HTTP	✓		Edit Clone Remove
82	[redacted]	[redacted]	TCP_1999	✓		Edit Clone Remove
70	[redacted]	[redacted]	ANY	✓		Edit Clone Remove
	[redacted]	[redacted]				

若係透過防火牆控管主機連線

則須確認相關主機之防火牆規則設定是否皆為適當。

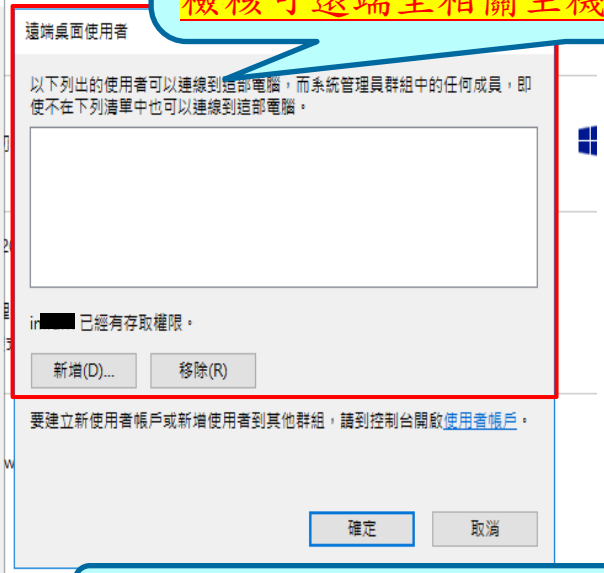
(e.g. 主機是否設定僅能連線至WSUS、防毒server、Smart IT、資料庫.....等必要IP位置，其餘皆為Deny。)

網路安全
3

執行代理作業相關主機之遠端桌面連線設定是否適當？

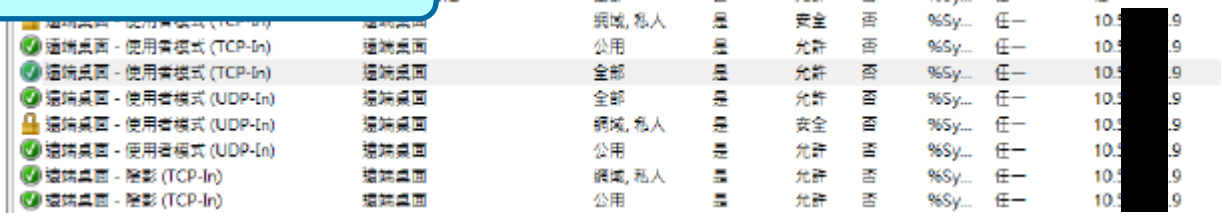
檢核是否僅適當人員可執行遠端連線。(若開啟則administrator預設有此權限)

檢核可遠端至相關主機之來源不能再被遠端連線。



確認該主機是否有遠端連線之作業需求

除授權使用者帳號外，亦需限制可遠端連線的來源IP。



網路安全
4

執行代理作業相關主機是否無法透過VPN方式自公司外部連線？

v11202

確認該些主機網路相關設定，是否無法以VPN自公司外部連線?（應同時考量VPN、遠端桌面連線及遠端連線軟體的控管）。

- ✓ 防火牆上設定VPN僅能使用特定服務、連線特定主機位置
- ✓ 代理作業相關主機設定不開放遠端桌面連線、不安裝其他遠端連線軟體
- ✓ 代理作業相關主機設定遠端桌面連線，但僅限於特定公司內部來源IP，且該來源的遠端連線關閉，不可再被其他人連線。

網路安全
5

執行代理作業相關使用者/使用者電腦，是否無法透過VPN方式自公司外部連線並閱覽信用報告？

v11202

確認該些使用者/使用者電腦，是否無法以VPN自公司外部連線後閱覽信用報告?（應同時考量VPN、遠端桌面連線使用、遠端連線軟體、線上閱覽信用功能的IP控管）。

- ✓ 防火牆上設定VPN僅能使用特定服務、連線特定主機位置
- ✓ 代理作業相關主機設定不開放遠端桌面連線、不安裝其他遠端連線軟體
- ✓ 代理作業相關主機設定遠端桌面連線，但僅限於特定公司內部來源IP，且該來源的遠端連線關閉，不可再被其他人連線。
- ✓ 線上閱覽信用報告功能禁止 VPN來源的IP存取。

資訊作業環境項目

	項次	檢核項目
★	1	執行代理作業相關主機之本機稽核原則是否開啟？
★	2	執行代理作業相關主機之事件檢視器留存之時間及容量設定是否適當？
★	3	執行代理作業相關主機及使用者電腦是否已執行病毒碼更新及掃毒作業？
★	4	執行代理作業相關主機及使用者電腦是否已更新Windows Update？
	5	執行代理作業相關主機之螢幕保護程式是否開啟？
	6	執行代理作業相關主機及使用者電腦之禁止列印設定是否適當？
	7	執行代理作業相關主機之印表機裝置設定是否適當？
	8	執行代理作業相關主機及使用者電腦之USB裝置控管是否適當？
★	9	執行代理作業相關使用者電腦是否可使用雲端空間及外部郵件網站？
	10	執行代理作業相關主機及使用者電腦之軟體安裝情形是否適當？

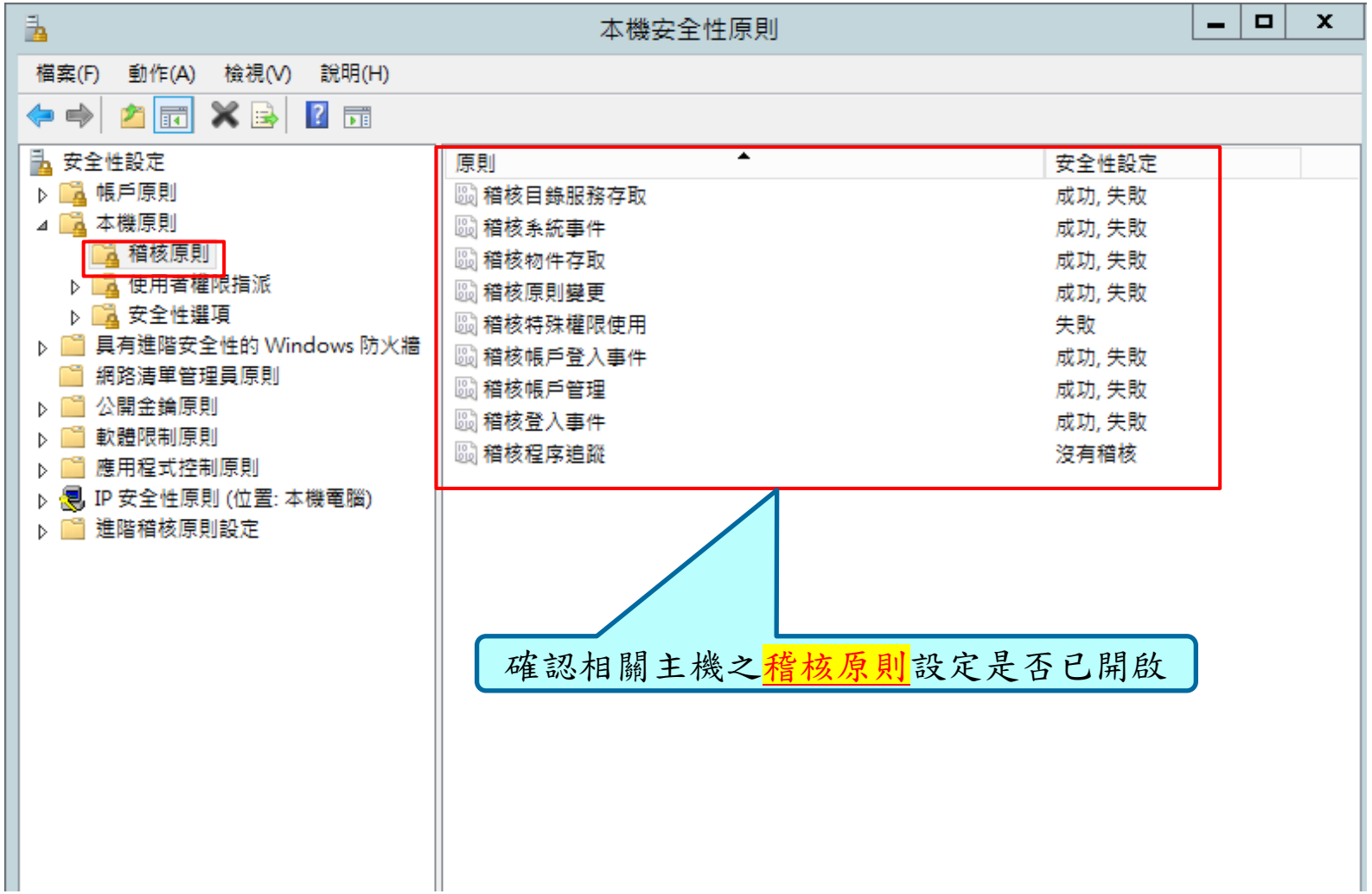
★ 重點說明檢核項目

★ 代理當事人線上申請信用報告作業資訊環境變更管理檢查表_v11202

資訊環境
1

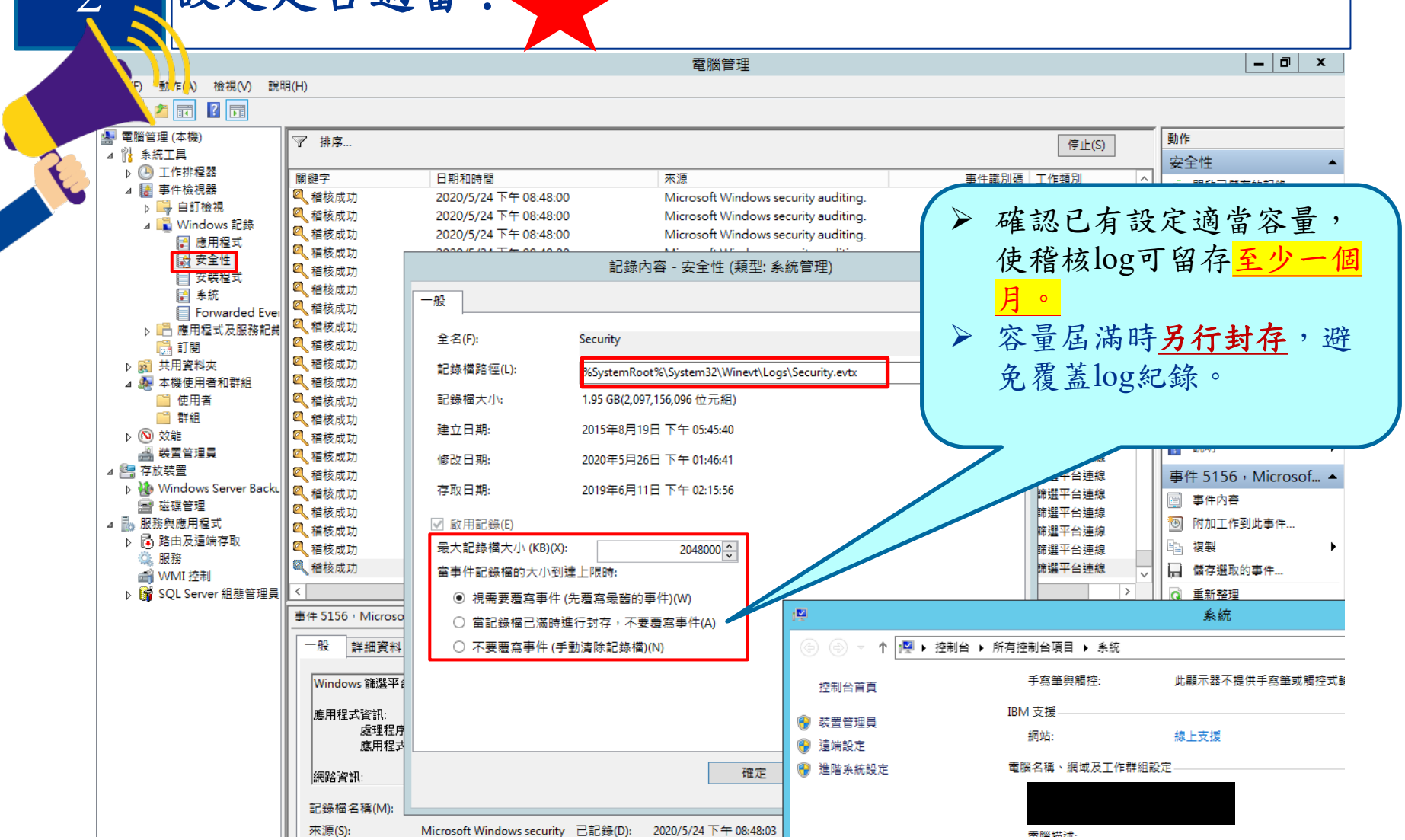
執行代理作業相關主機之本機稽核原則是否開啟？

v11202



資訊環境
2

執行代理作業相關主機之事件檢視器留存之時間及容量設定是否適當？

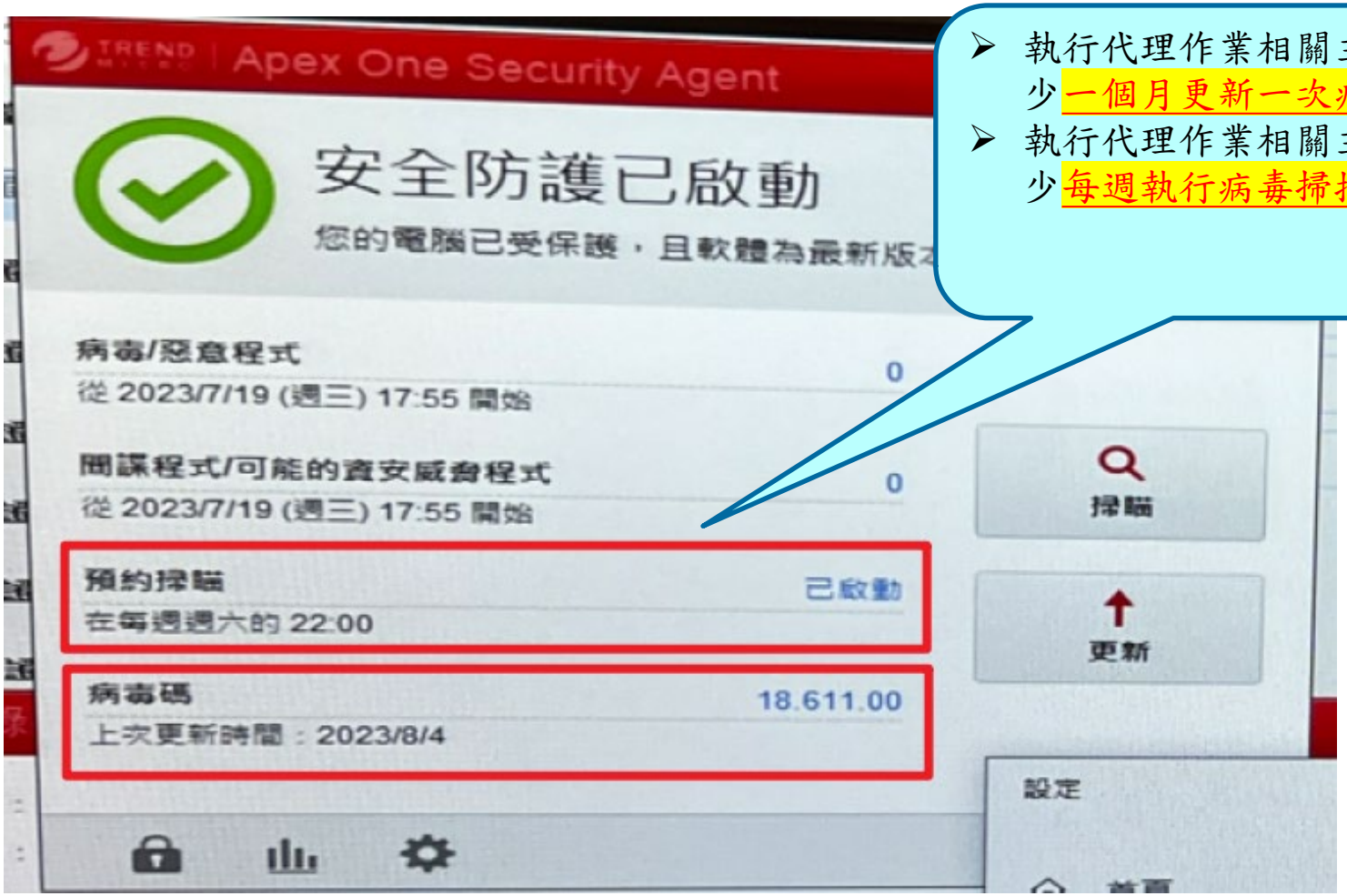


- 確認已有設定適當容量，使稽核log可留存<u>至少一個月</u>。
- 容量屆滿時<u>另行封存</u>，避免覆蓋log紀錄。

資訊環境
3

執行代理作業相關主機及使用者電腦是否已執行病毒碼更新及掃毒作業？

v11202



- 執行代理作業相關主機至少一個月更新一次病毒碼。
- 執行代理作業相關主機至少每週執行病毒掃描

資訊環境 4

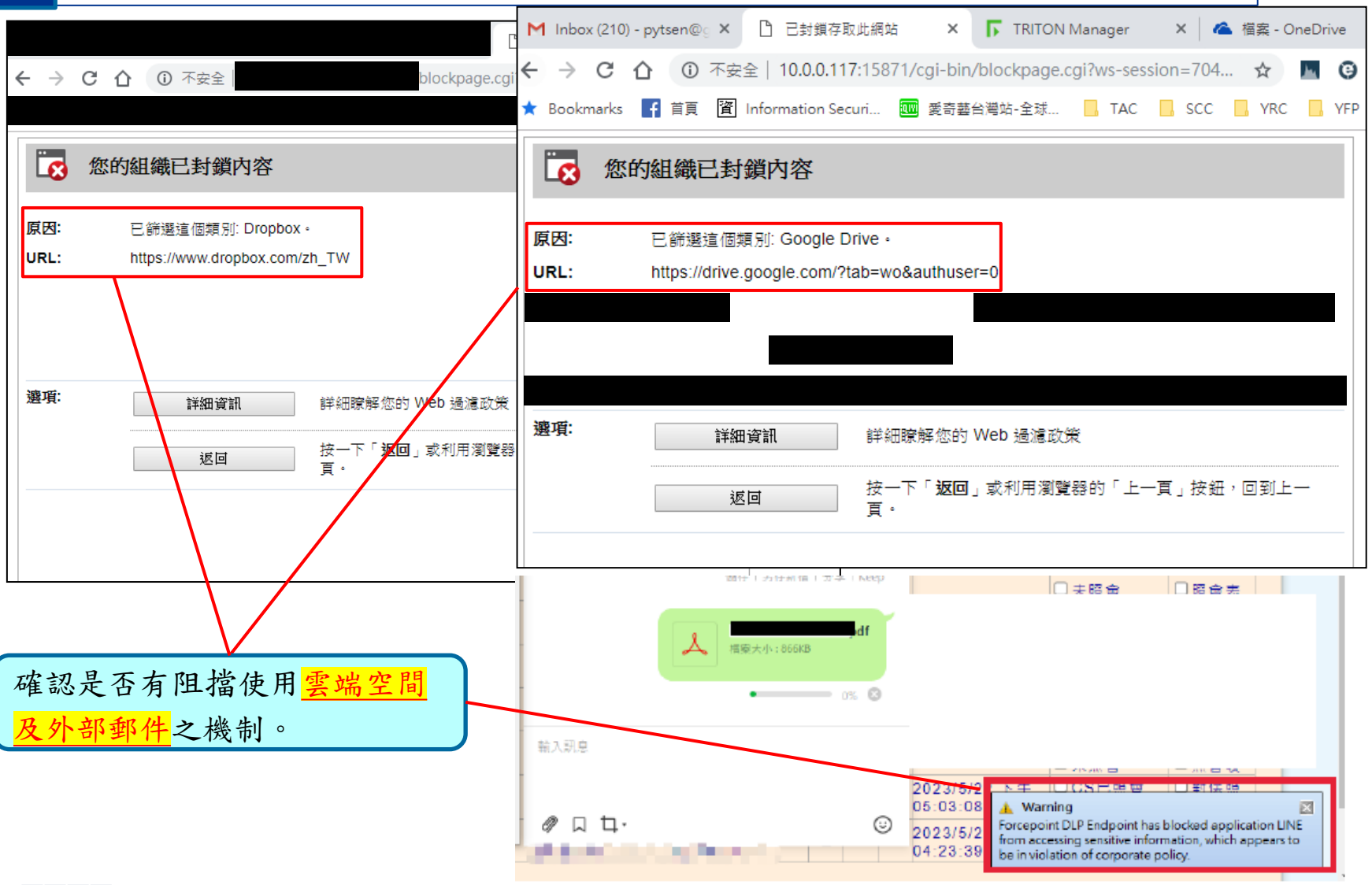
執行代理作業相關主機及使用者電腦是否於半年內更新Windows Update？

v11202

- 確認Windows Update定期更新，至少每半年進行更新，並保留相關紀錄。

資訊環境
9

執行代理作業相關使用者電腦是否可使用雲端空間、通訊軟體及外部郵件網站？



確認是否有阻擋使用雲端空間及外部郵件之機制。

KPMG

代理當事人線上申請信用報告
-重要事項提醒

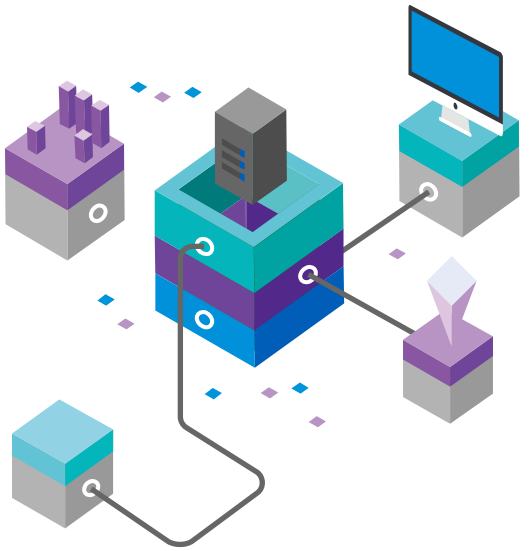
防毒軟體更新及病毒掃瞄

此項本年度為宣導，113年開始納入查核建議項目。

- 至少一個月更新病毒碼一次
- 至少一週執行掃瞄作業一次

實體防護及隔離宣導

- 執行代理作業相關主機盡量建立實體防護及隔離。



代理作業應包含主借款戶申請

依據110年度實地查核作業，發現有僅查詢債務關係人(負責人或連保人)資料，而主借款戶未委託查詢，致使案件即便有承作，而資料亦無法報送之情事。為健全融資租賃交易資訊的完整性並避免當事人對資料報送不實之爭議，謹重申代理作業限定須有主借款戶之委任申請，方能併同申請債務關係人之信用報告。

111年2月7日 金徵(信)字第1110100203號 函

分公司或異地備援申請/異動

針對融資租賃公司代理作業「信用報告有對分公司傳輸時」之控管機制：

- 總公司內所設分公司若遷址，需來函申請分公司輔導審查。
- 總公司內新設分公司，應來函說明並納入總公司查核範圍。
- 已申請審查通過之總公司或分公司遷址，應來函說明並依「代理當事人線上申請信用報告作業資訊環境變更管理檢查表」自行檢查，由本中心優先辦理實地查核。

若融資租賃公司因應疫情須設置異地備援或第二辦公室者，如有涉及當事人信用報告之利用，需向本中心申請並經輔導與審查通過後，方得使用。

111年2月7日金徵(信)字第1110100203號 函

重複發生相同缺失之違規處置

一.「融資租賃公司代理當事人線上申請信用報告作業」實地查核作業，針對查核發現之重複發生之相同缺失事項，將經本中心專案會議討論是否處以違約金，如需處以停止代理處分，將提請本中心違規事項查處委員會討論。

二. 重複發生之相同缺失處置措施自110年起實施，例如110年之缺失，如於111年重複發生，將適用此處置措施。

109年7月20日 金徵(輔)字第1090101862號函

自行查核項目增列實地查核發現之缺失

融資租賃公司應將當年度實地查核所發現的缺失，列入隔年自行查核項目中，以避免相同缺失重複發生。

108年11月18日 金徵(輔)字第108101938號 函

代理當事人線上申請信用報告作業安全控管查核報告彙總單

附件一

_____(融資租賃公司名稱)

_____年度 代理當事人線上申請信用報告作業安全控管查核報告彙總單

一、查核報告

(一)作業環境：

1.代理當事人線上申請信用報告作業之總公司單位名稱：_____。

2.使用當事人信用報告之單位共 ____家，其中分公司____家。

(二)查核方式：1.總公司執行

□內部稽核，共___家___次；□是□否為公司全面性。

□自行查核，共___家___次；□是□否為公司全面性。

2.□分公司自行查核共____家___次；□是□否為公司全面性。

(三)查核範圍：

□一年(含)以上； □半年(含)以上，一年以下； □半年以下

(四)查核項目內容：

□是□否涵蓋「融資租賃公司代理當事人線上申請信用報告作業辦法」

□是□否涵括本機構「代理當事人線上申請信用報告作業控管要點」要項

(五)本年度(112)查核結果彙總：

1、彙總說明本年度查核情形(內部稽核、自行查核)：

2、聯徵中心本年度實地查核發現之缺失及改善情形：

二、前一年度(111)缺失改善辦理情形(各發現及建議事項之追蹤結果請詳列)：

(一)內部稽核：

(二)自行查核：

(三)聯徵中心實地查核：

三、代理申請紀錄核對情形(請敘明核對情形)：

(一)核對頻率(每日、每週或不定期核對)：_____

(二)核對項目：_____

(例如：是否符合「代理申請要件」及「當事人信用報告之使用及保密」之規定)

四、其他

五、本案經辦單位(惠請提供，俾供必要時聯繫之用)

經辦人員：

聯絡電話：

當年度(112)內部稽核、自行查核及聯徵中心實地查核發現，於當年(112)年底之改善追蹤情形

前一年度(111)內部稽核、自行查核及聯徵中心實地查核發現，於當年(112)年再次執行內部稽核/自行查核之結果說明

變更管理程序

重大變更類別

- 組織分工
- 作業流程
- 資訊環境

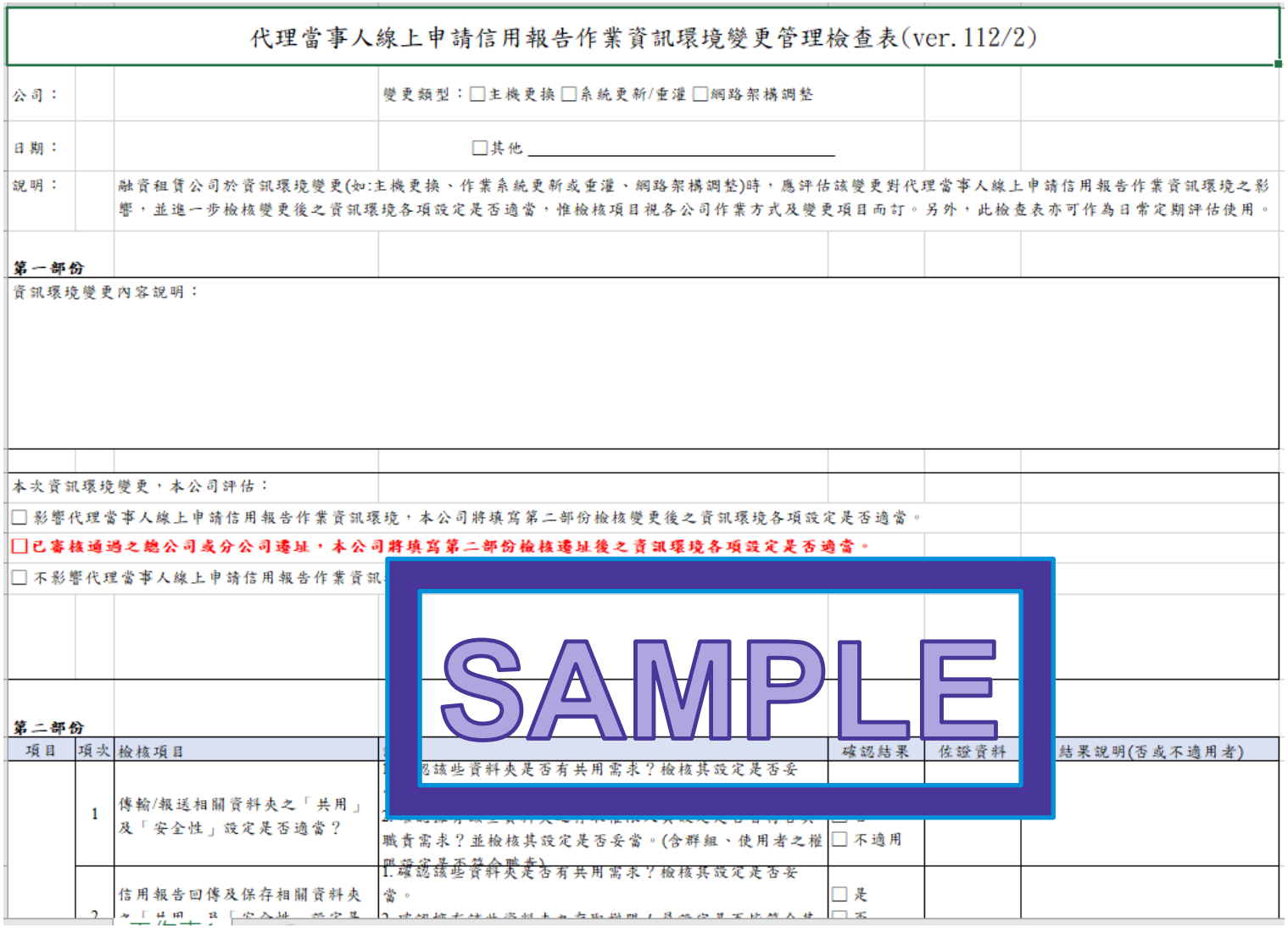
變更管理作業

- 風險評鑑
- 通報程序
- 變更核准

自行檢查/內部稽核

- 依檢查表自我檢查
- 追蹤改善

資訊環境變更管理檢查表更新



代理當事人線上申請信用報告作業資訊環境變更管理檢查表(ver. 112/2)

公司：　　變更類型：☐主機更換 ☐系統更新/重灌 ☐網路架構調整

日期：　　☐其他 _____

說明：　融資租賃公司於資訊環境變更(如:主機更換、作業系統更新或重灌、網路架構調整)時，應評估該變更對代理當事人線上申請信用報告作業資訊環境之影響，並進一步檢核變更後之資訊環境各項設定是否適當，惟檢核項目視各公司作業方式及變更項目而訂。另外，此檢查表亦可作為日常定期評估使用。

第一部份

資訊環境變更內容說明：

本次資訊環境變更，本公司評估：

☐ 影響代理當事人線上申請信用報告作業資訊環境，本公司將填寫第二部份檢核變更後之資訊環境各項設定是否適當。

☐已審核通過之總公司或分公司遷址，本公司將填寫第二部份檢核遷址後之資訊環境各項設定是否適當。

☐ 不影響代理當事人線上申請信用報告作業資訊

第二部份

項目	項次	檢核項目		確認結果	佐證資料	結果說明(否或不適用者)
	1	傳輸/報送相關資料夾之「共用」及「安全性」設定是否適當？	該些資料夾是否有共用需求？檢核其設定是否妥 職責需求？並檢核其設定是否妥當。(含群組、使用者之權限設定是否符合職責)	☐ 不適用		
	2	信用報告回傳及保存相關資料夾	1.確認該些資料夾是否有共用需求？檢核其設定是否妥當。	☐ 是		

SAMPLE

資訊環境變更管理檢查表使用時機

主機更換

- 硬體設備汰換

網路架構調整

- 防火牆規則調整
- 網域政策更新

系統升級重灌

- 作業系統升級
- 系統重灌

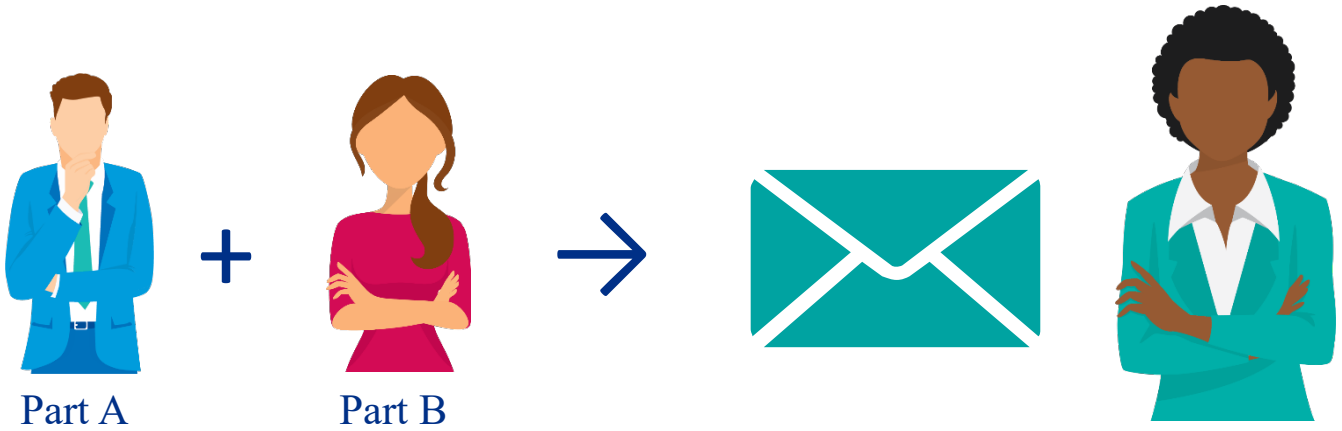
辦公室搬遷

- 實體環境改變
- 線路調整

與代理作業相關之資訊環境變更皆需評估檢核

執行代理作業相關主機之管理者帳號控管

1. 管理者帳號之使用情形(含變更密碼)需設簿登記
2. 管理者帳號之密碼需彌封或採密碼分持
3. 管理者帳號密碼如採分持控管，其中一半應為主管職分持(非同部門/職級人員)
4. 開啟管理者帳號作為備援使用，須符合前述規定



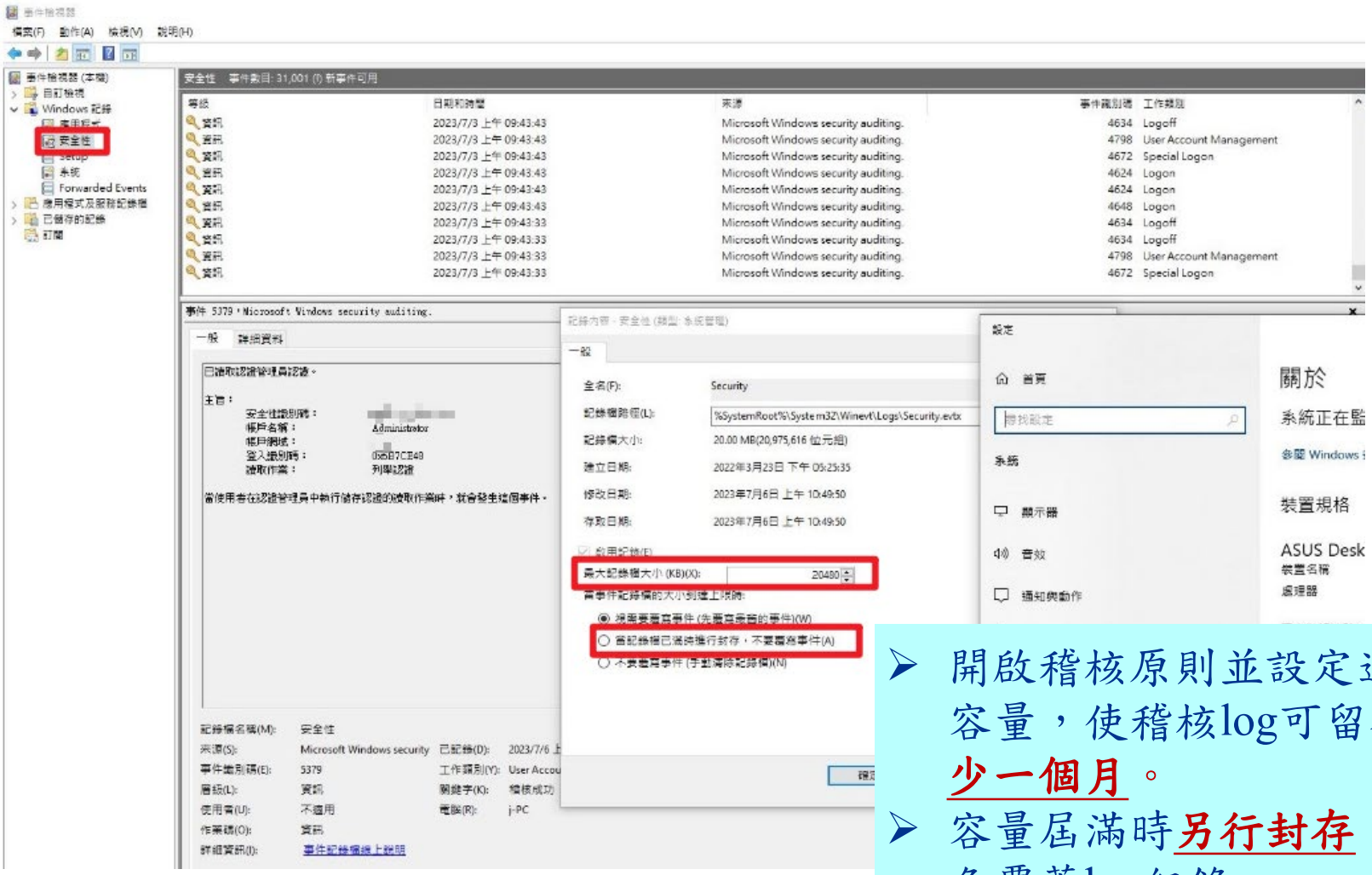
執行代理作業相關主機之管理者帳號密碼變更

聯徵專用主機登入紀錄

No.	登入日期	主機/帳號	登入原因	密碼A	密碼B	處理人員
1						
2						
3						
4						
5						
6						
7						

1. 管理者帳號密碼如採密碼函封存，每次拆封使用後須變更密碼，密碼變更需紀錄
2. 管理者帳號若長時間未使用，密碼至少1年需變更1次，密碼變更需紀錄

執行代理作業相關主機之事件檢視器留存之時間



- 開啟稽核原則並設定適當容量，使稽核log可留存<u>至少一個月</u>。
- 容量屆滿時<u>另行封存</u>，避免覆蓋log紀錄。

執行代理作業相關主機之Windows更新頻率

- Windows Update頻率至少半年更新一次。。

KPMG

Thank you

KPMG 安侯建業

Contact

謝秋華執業會計師
(02) 81016666 ext. 06477

kpmg.com.tw

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.