鼎新電腦

解密上市櫃資通安全管控指引

賴裕文

上市櫃資安專責單位要求

公開發行公司建立內部控制制度處理準則-2021年更新增加9-1條

自2020年起國內上市櫃公司爆發多起重大資安事件。
為避免網路攻擊造成市場重大影響，及配合金融監督管理委員會
強化上市公司資通安全管理政策，要求上市櫃公司應配置適當人力資源及設備，
進行資通安全制度之規劃、監控及執行資通安全管理作業。

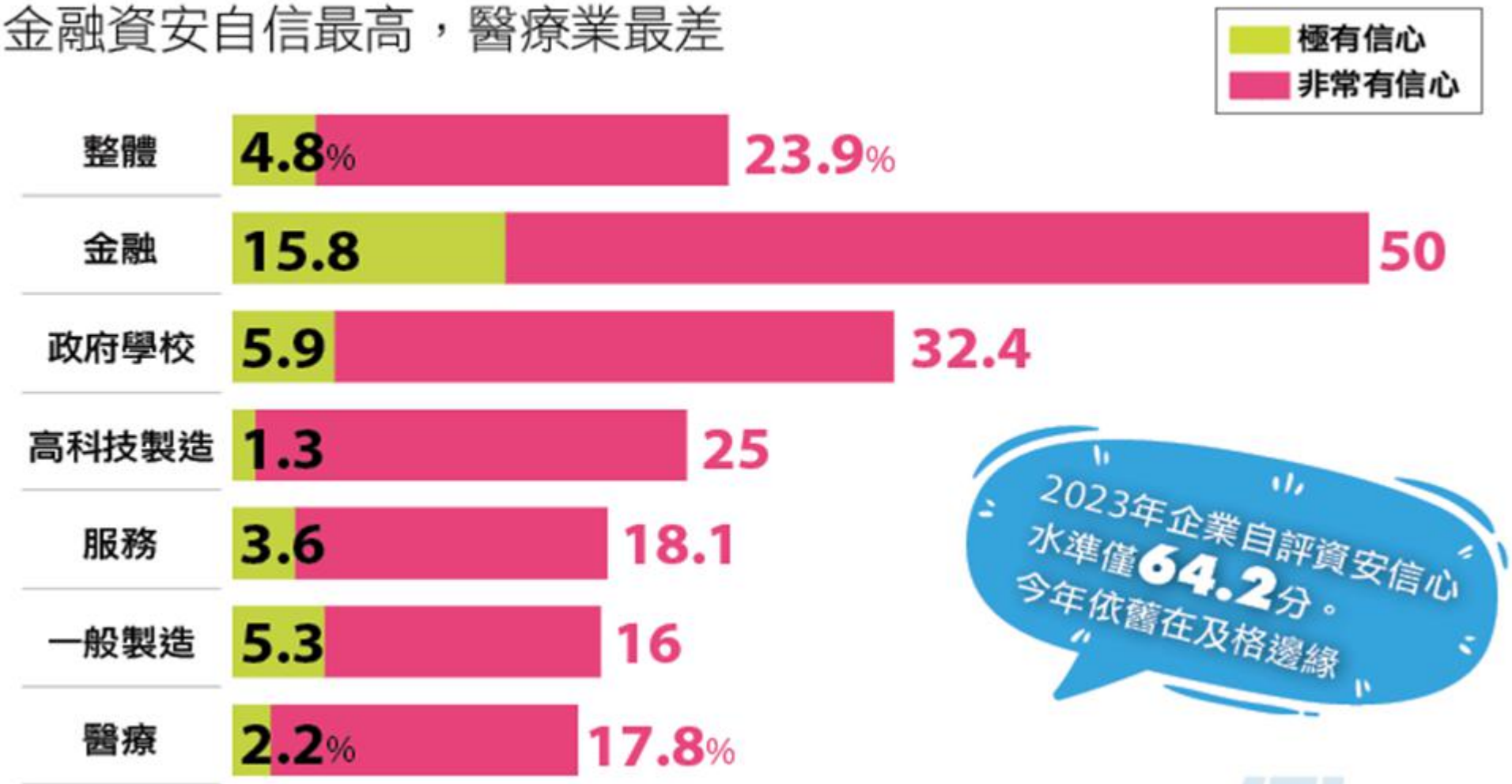
第9-1條

1.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。符合一定條件者，本會得命令**指派綜理資訊安全政策推動**及**資源調度事務之人**兼任**資訊安全長**，及設置**資訊安全專責單位、主管及人員**。

2.前項一定條件，由本會定之

多少企業對自家資安能力很有信心？

金融資安自信最高，醫療業最差



資料來源：2023 iThome CIO大調查，2023年7月

公開發行公司建立內部控制制度處理準則
分級標準、實施範圍與時程(2021/12/28)

等級	分級標準	資安單位暨人力編制	實施時程
第一級	符合下列條件之一者： ● 資本額100億元以上 ● 前一年底屬臺灣50指數成分公司 ● 藉電子方式媒介商品所有權移轉或提供服務（如電子銷售平台、人力銀行等）收入占最近年度營業收入達80%以上，或占最近二年度營業收入達50%以上者	應設資安長 及設置資安專責單位（含資安專責主管及至少2名資安專責人員）	2022年底設置完成
第二級	第一級以外之上市（櫃）公司，最近三年度之稅前純益未有連續虧損，且最近年度財務報告每股淨值未低於面額者。	資安專責主管 及至少1名資安專責人員	2023年底設置完成
第三級	第一級以外上市（櫃）公司，最近3年度稅前純益有連續虧損，或最近年度每股淨值低於面額。	至少1名資安專責人員	鼓勵設置

上市櫃資訊循環要求

第 9 條

公開發行公司使用電腦化資訊系統處理者，其內部控制制度除資訊部門與使用者部門應明確劃分權責外，至少應包括下列控制作業：

一、資訊處理部門之功能及職責劃分。
二、系統開發及程式修改之控制。
三、編製系統文書之控制。
四、程式及資料之存取控制。
五、資料輸出入之控制。
六、資料處理之控制。
七、檔案及設備之安全控制。
八、硬體及系統軟體之購置、使用及維護之控制。
九、系統復原計畫制度及測試程序之控制。
十、資通安全檢查之控制。
十一、向本會指定網站進行公開資訊申報相關作業之控制。

公開發行公司年報 應行記載事項準則(2021/11/30)

第18條 營運概況

六、資通安全管理：
（一）敘明**資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源**等。
（二）列明最近年度及截至年報刊印日止，因**重大資通安全事件所遭受之損失、可能影響及因應措施**，如無法合理估計者，應說明其無法合理估計之事實。

第20條 財務狀況及財務績效檢討分析

六、風險事項應分析評估
（四）國內外重要政策及法律變動對公司財務業務之影響及因應措施。
（五）**科技改變（包括資通安全風險）**及產業變化**對公司財務業務之影響及因應措施。**

1 上市櫃資通安全管控指引

2 資安推動組織&資安政策擬訂

3 資安事件應變程序擬定

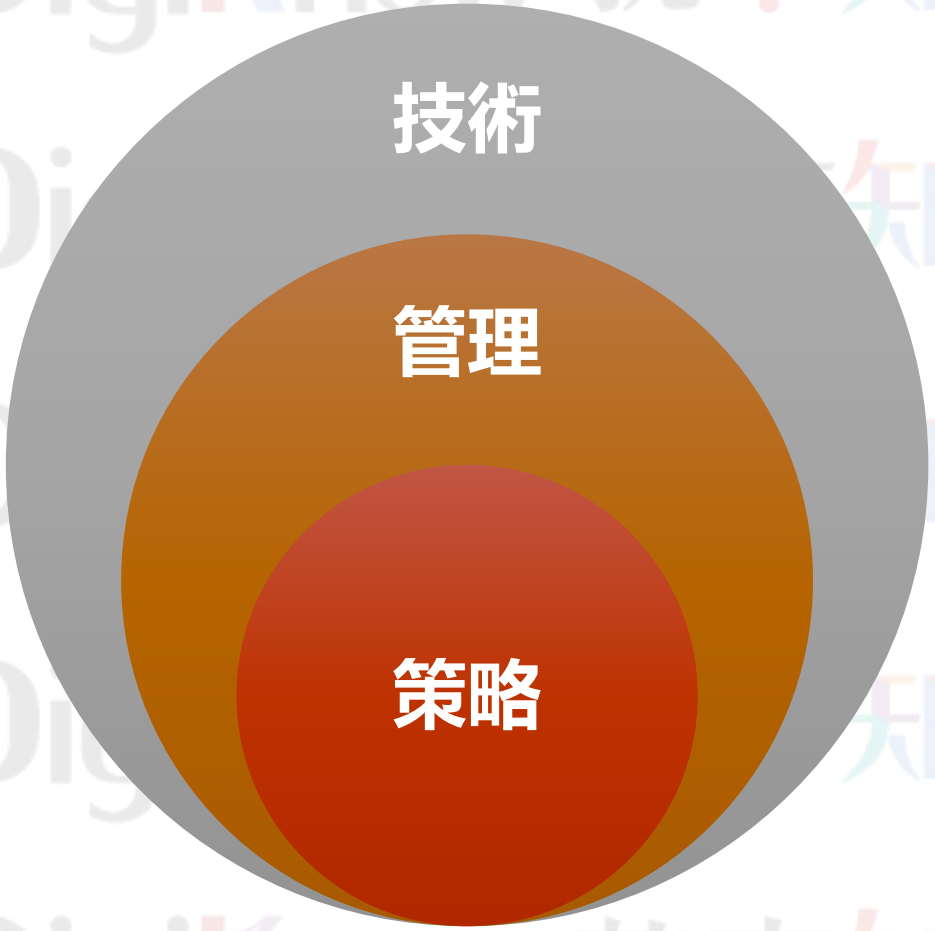
4 上市櫃風險評估計畫

5 企業運維平台-資安風險評估 體驗

• 上市櫃資通安全管控指引

2021年12月23日由證交所發佈,為協助上市、上櫃公司強化資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業。

上市櫃企業資安架構



利用各項系統或設備，

執行 資產盤點、防禦控制、入侵偵測、緊急回應、異常復原

等機制，及收集相關資安稽核、各項評量指標所需要之數據

成立管理團隊，制定各項管理辦法及機制，

有效佈達至全體員工，及定期資安訓練

並定期呈報結果及改善提案

經營核心支持，投入資源，制定目標及政策

進行發佈，指定專責人員及成立推動組織

第一章>>總則

項次	條文內容
第一條	為協助上市、上櫃公司(以下簡稱公司)強化資通安全防護及管理機制， 並符合「公開發行公司建立內部控制制度處理準則」第九條 使用電腦化資訊系統處理者相關控制作業，特擬定本資通安全管控指引。
第二條	一、 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。 三、 核心業務：公司維持營運與發展必要之業務。 四、 核心資通系統：支持核心業務持續運作必要之資通系統。 五、 機敏性資料：依公司業務考量，評估需保密或具敏感性之重要資料，如涉及營業秘密資料或個人資料等。

第二章>>資通安全政策及推動組織

管理及技術面向

項次	條文內容
第三條	成立資通安全推動組織，組織配置適當之人力、物力與財力資源， 並指派適當人員擔任資安專責主管及資安專責人員， 以負責推動、協調監督及審查資通安全管理事項。
第四條	訂定資通安全政策及目標，由副總經理以上主管核定， 並定期檢視政策及目標且有效傳達員工其重要性。

第二章>>資通安全政策及推動組織

管理及技術面向

項次	條文內容
第五條	訂定資通安全作業程序，包含核心業務及其重要性、 資通系統盤點及風險評估、 資通系統發展及維護安全、 資通安全防護及控制措施、 資通系統或資通服務委外辦理之管理措施、 資通安全事件通報應變及情資評估因應、 資通安全之持續精進及績效管理機制等。
第六條	所有使用資訊系統之人員，每年接受資訊安全宣導課程， 另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。

第三章>>資通安全政策及推動組織

管理及技術面向

項次	條文內容
第七條	鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
第八條	鑑別應遵守之法令及契約要求。
第九條	鑑別可能造成營運中斷事件之發生機率及影響程度， 並明確訂定核心業務之復原時間目標(RTO)及資料復原時間點目標(RPO)， 設置適當之備份機制及備援計畫。
第十條	制定核心業務持續運作計畫，定期辦理核心業務持續運作演練，演練內容包含 核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善。

第四章>>資通系統盤點及風險評估

管理及技術面向

項次	條文內容
第十一條	定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。
第十二條	定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等。

第五章>>資通系統發展及維護安全

管理及技術面向

項次	條文內容
第十三條	將資安要求納入資通系統開發及維護需求規格， 包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。
第十四條	定期執行資通系統安全性要求測試， 包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾測試等。
第十五條	妥善儲存及管理資通系統開發及維護相關文件。
第十六條	對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。 一、 定期辦理弱點掃描。 二、 定期辦理滲透測試。 三、 系統上線前執行源碼掃描安全檢測。

第六章>>資通安全防護及控制措施

管理及技術面向

項次	條文內容
第十七條	依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。
第十八條	具備下列資安防護控制措施： 一、 防毒軟體。 二、 網路防火牆。 三、 如有郵件伺服器者，具備電子郵件過濾機制。 四、 入侵偵測及防禦機制。 五、 如有對外服務之核心資通系統者，具備應用程式防火牆。 六、 進階持續性威脅攻擊防禦措施。 七、 資通安全威脅偵測管理機制(SOC)。

第六章>>資通安全防護及控制措施

管理及技術面向

項次	條文內容
第十九條	針對機敏性資料之處理及儲存建立適當之防護措施， 如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。
第二十條	訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。
第二十一條	建立使用者通行碼管理之作業規定， 如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術
第二十二條	定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。

第六章>>資通安全防護及控制措施

管理及技術面向

項次	條文內容
第二十三條	建立資通系統及相關設備適當之監控措施， 如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。
第二十四條	針對電腦機房及重要區域之安全控制、人員進出管控、環境維護 (如 溫溼度控制)等項目建立適當之管理措施。
第二十五條	留意安全漏洞通告，即時修補高風險漏洞， 定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。
第二十六條	訂定資通設備回收再使用及汰除之安全控制作業程序，以確保機敏性資料確實刪除。

第六章>>資通安全防護及控制措施

管理及技術面向

項次	條文內容
第二十七條	訂定人員裝置使用管理規範， 如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。
第二十八條	每年定期辦理電子郵件社交工程演練， 並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

第七章>>資通系統或資通服務委外辦理之管理措施

管理及技術面向

項次	條文內容
第二十九條	訂定資訊作業委外安全管理程序， 包含委外選商、監督管理 (如：對供應商與合作夥伴進行稽核)及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。
第三十條	訂定委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協議(SLA)、資安要求及對委外廠商資安稽核權。
第三十一條	公司於委外關係終止或解除時， 確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

第八章>>資通安全事件通報應變及情資評估因應

管理及技術面向

項次	條文內容
第三十二條	訂定資安事件應變處置及通報作業程序， 包含判定事件影響及損害評估、內外部通報流程、通知其他受影響機關之方式、 通報窗口及聯繫方式。
第三十三條	加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊， 如：所屬產業資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。
第三十四條	發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」或「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

第九章>>資通安全之持續精進及績效管理機制

管理及技術面向

項次	條文內容
第三十五條	資通安全推動組織定期向董事會或管理階層報告資通安全執行情形，確保運作之適切性及有效性。
第三十六條	定期辦理內部及委外廠商之資安稽核，並就發現事項擬訂改善措施，且定期追蹤改善情形。

第九章>>資通安全之持續精進及績效管理機制

管理及技術面向

項次	條文內容
第三十七條	除法令、臺灣證券交易所股份有限公司 及財團法人中華民國證券櫃檯買賣中心相關章則另有規定外， 本指引條文，上市、上櫃公司可衡諸產業特性、規模大小及資安風險適度採行之。

美NSA、DHS、CISA聯手揭露，帶來資安破口的10大配置錯誤問題

1. 軟體與應用程式的預設配置
2. 使用者與管理員權限的分離不當
3. 內部網路的監控不足
4. 網路分段的缺乏
5. 修補程式的管理不良
6. 系統存取控制可被略過
7. 多因素身分驗證的薄弱或設定錯誤
8. 網路共享與服務的存取控制名單設置不夠全面
9. 帳密資安衛生不佳
10 .程式碼執行未受到管制

資料來源：美國CISA，iThome整理，2023年10月

National Security Agency | Cybersecurity and Infrastructure Security Agency | Joint Cybersecurity Advisory

TLP:CLEAR

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

A plea for network defenders and software manufacturers to fix common problems.

Executive summary

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

1 上市櫃資通安全管控指引

2 資安推動組織&資安政策擬訂

3 資安事件應變程序擬定

4 上市櫃風險評估計畫

5 企業運維平台-資安風險評估 體驗

資安推動組織

資安推動組織

第三條、

成立資通安全推動組織，

組織配置適當之人力、物力與財力資源，

並指派適當人員擔任資安專責主管及資安專責人員，

以負責推動、協調監督及審查資通安全管理事項。

第三十五條、

資通安全推動組織定期向董事會或管理階層

報告資通安全執行情形，確保運作之適切性及有效性。

資安推動組織

第三條、

成立資通安全推動組織，

組織配置適當之人力、物力與財力資源，

並指派適當人員擔任資安專責主管及資安專責人員，

以負責推動、協調監督及審查資通安全管理事項。

第三十五條、

資通安全推動組織定期向董事會或管理階層

報告資通安全執行情形，確保運作之適切性及有效性。

資通安全管理推動委員會
(功能性委員會)

資通安全推動組織 (範例)

召集人：
資安專責主管：

資安稽核單位
稽核：

資安推動單位
各部門主管：

資安文件管制單位
文管：

資安管理單位
主管：
資安技術人員：

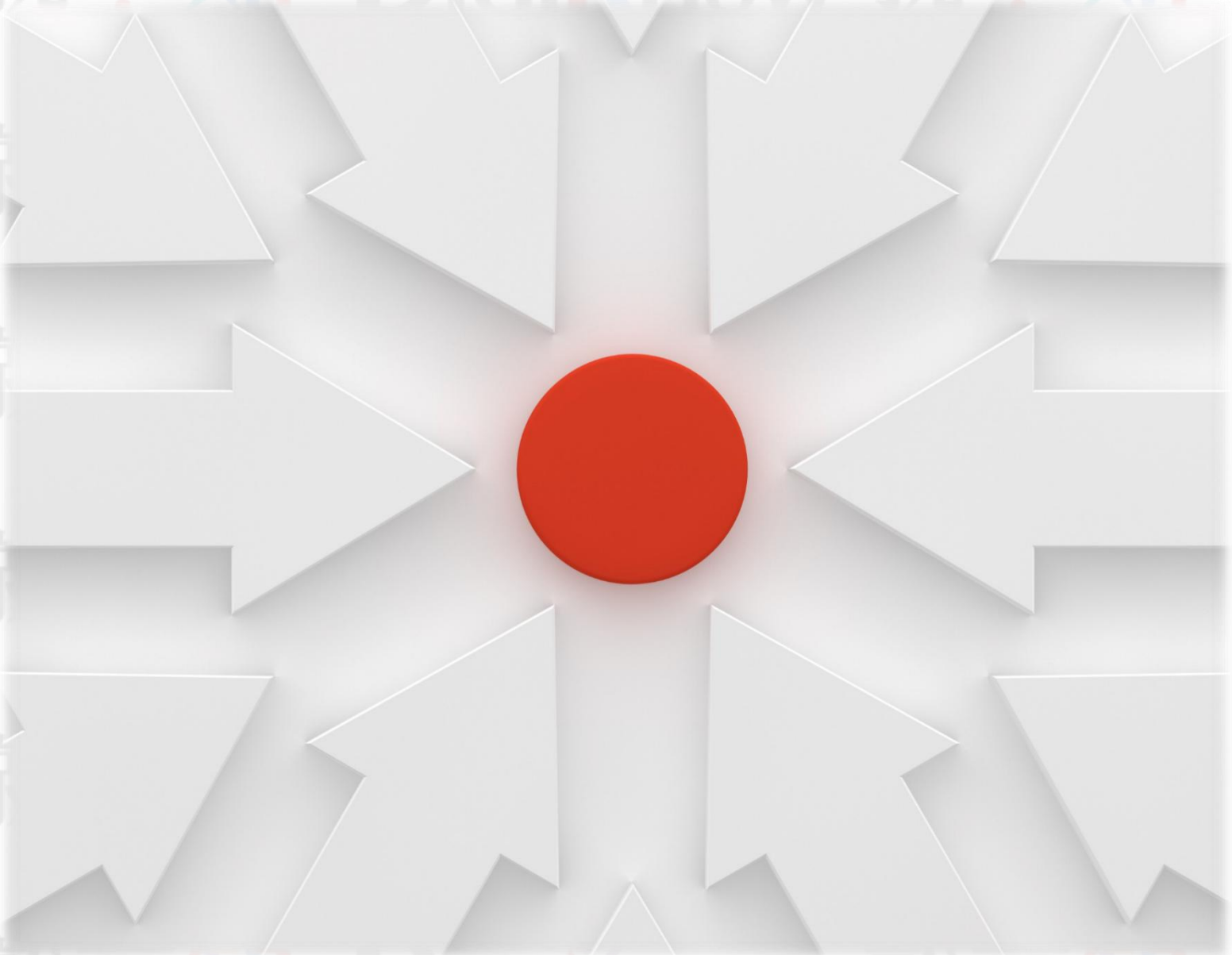
事件通報及應變單位
指揮官：
副指揮官：
發言人：
情資及計畫組：
應變執行組：
後勤調度組：
財務行政組：

資通安全推動組織權責 (範例)

委員會責任	權責說明
召集人	由本企業召集人，負責部門間問題協調與資通安全政策、資通安全目標及相關管理作業辦法之核定、公告、發布、宣導，並於內部管理階會議/董事會中提報資通安全事項執行情形說明。
資通安全專責主管	由召集人指定專人擔任，為負責本企業資通安全管理主管。 負責委員會執行狀態確認與回報之角色，若接獲內外部資通安全管控要求或資通安全管理相關事件，應聯繫相關處理單位進行控管與處理。
資通安全稽核單位	為稽核室指派專人擔任，除參與「資通安全管理推動委員會」審查外， 並評估將資通安全相關作業納入稽核項目，以利相關企業內部及委外廠商之資通安全稽核執行。
資通安全推動單位	責任委員為相關部門主管，除協同「資通安全管理推動委員會」審查外，負責於部門內推動資通安全相關作業並督導執行，使同仁理解企業於資通安全管理之決心與目標共同遵守。
資通安全文件管制單位	由企業ISO文件管理部門擔任，主要為直執行文件保存相關規定、為相關管理作業辦法之版本控制與管理發佈單位，提供最新版本給予內部相關同仁使用。
資通安全管理單位	為企業內資通安全負責部門及資訊部門全體成員， 主要為日常維護、管理、紀錄、因應、回報執行單位。

事件通報及應變單位權責 (範例)

成員責任	權責說明
事件指揮官	為通報應變小組總召集人（同推動委員會召集人），綜理全般業務，直接督導各單位聯絡人員及企業發言人。
副指揮官	為事件指揮官幕僚，負責督辦通報應變小組各項業務。
發言人	為為企業對外發言人擔任，主要任務為企業對外發布新聞或說明負責窗口， 負責事件綜整與定期更新訊息及擬定媒體溝通計畫。
情資及計畫組	成員為資通安全專責主管或資通安全專責人員（視情況納入委外廠商或外部專家），主要任務為 資通安全事件通報及情資分享：釐清事件影響與清查影響單位範圍。 應變策略及計畫研擬：研擬損害控制、復原作業及跡證保存計畫。
應變執行組	成員為資通安全專責主管或資通安全專責人員（視情況納入委外廠商），主要任務為 執行損害控制：依上組研擬之應變策略及計畫，調度人員執行搶救及損害管制防止攻擊擴散。 復原作業：依上組研擬之應變策略及計畫，完成系統重建、弱點掃描或漏洞修補等事宜。
後勤調度組	成員為資通安全專責主管或資通安全專責人員（視情況納入委外廠商或外部專家），主要任務為 跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。 事件根因查找：依系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。 提出改善建議：依事件調查根因，提出短(立即)、中(3至6月)、長期(二年內)改善建議。
財務行政組	成員為企業財務主管或秘書單位主管組成，主要任務為視事件需求辦理預算調撥及提供行政支援事宜。



資安政策擬訂

資通安全政策及目標

第四條、

訂定資通安全政策及目標，由副總經理以上主管核定，

並定期檢視政策及目標且有效傳達員工其重要性。

資通安全政策 (範例)

1、目的:

為強化資訊安全管理，確保所屬資訊資產之機密性、完整性與可用性，及提高相關人員資訊安全意識，以提供資訊服務持續運作之環境，並符合相關法規要求，特訂定本政策

2、適用範圍:

本公司所有同仁均應遵循之。

資通安全政策 (範例)

3、政策內容:

- 強化人員資安意識，企業同仁應參與資通安全相關教育訓練，以提高全公司資通安全意識。
- 恪遵資訊安全措施，各項資通安全管理作業與辦法，應確實遵守，並定期依實際狀況評估及調整
- 避免機敏資料外洩，保護企業機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
- 落實內部資安稽核，定期執行內部資通安全各項稽核措施，確保各項作業落實執行。

資通安全政策 (範例)

4、發佈實施：

本公司之資通安全政策及資通安全目標，由資通安全管理推動委員會擬訂，並呈 總經理/副總經理 審核後公告實施。

本公司資通安全政策應對利害關係人宣導與公佈，遇有事項變更時，亦同。

總經理/副總經理 ： OOO

2023年 00 月 00 日

資通安全目標 (範例)

1、資通系統操作人員，需接受資通安全教育訓練，
每年執行 O小時，本年度預計於第O季完成。

2、資訊安全主管及負責人員，需接受資通安全專業教育訓練，
每年執行 O小時 ，本年度預計於第O季完成。

3、核心資通系統，需執行弱點掃描，每年執行乙次，並於執行後一個月內
將高風險弱點100%完成控制。本年預計於第O季完成。

4、核心資通系統，需執行滲透測試，每年執行乙次，並於執行後一個月內
將高風險弱點100%完成控制，預計於第O季完成。

資安目標(範例)

5、本公司郵件服務之使用人員，需接受社交工程演練，
每年執行乙次，並對誤點、誤下載、誤點擊人員實施教育訓練。
本年度預計於第O季完成。

6、本公司若發生資安事件，應於規定的時間完成通報、應變及復原作業。
(每年度重大事件發生頻率應 ≤ 2次)。

7、本公司落實資通安全與管理之持續改善，於前次內部稽核發現事項，
未完成改善之件數應 ≦ 2件。

1 上市櫃資通安全管控指引

2 資安推動組織&資安政策擬訂

3 資安事件應變程序擬定

4 上市櫃風險評估計畫

5 企業運維平台-資安風險評估 體驗

資安事件應變程序

重訊要求法規

第三十四條、

發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」或「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

第二章　重大訊息 。第四條

二十六、發生災難、集體抗議、罷工、環境污染、資通安全事件或其他重大情事，致有下列情事之一者：

（一）造成公司重大損害或影響者；
（二）經有關機關命令停工、停業、歇業、廢止或撤銷污染相關許可證者；
（三）單一事件罰鍰金額累計達新台幣壹佰萬元以上者。

第三章　重大訊息說明記者會。

九、發生災難、集體抗議、罷工、環境污染、資通安全事件、遭主管機關處分或其他重大情事致造成公司重大損害或影響，且扣除其依保險契約設算獲賠金額後之預估損失超過該公司實收資本額百分之二十或新台幣三億元以上者。

無面額或每股面額非屬新台幣十元之公司，前開有關股本百分之二十之計算應以淨值百分之十替代之。

資安事件應變處置及通報作業程序(範例)

1、目的:

為使公司資安事件之處理有明確的相關規範，當事件發生，能迅速依通報程序進行通報，並採取必要之應變措施，降低事件可能帶來之衝擊，並建立事件學習機制，降低事件造成的損害。

2、適用範圍:

公司各項資訊資產之管理，均適用之。

3、名詞定義:

- 資訊安全事件：凡於作業環境中，資訊或資通系統之機密性、完整性、可用性，遭受破壞之事件。
- 發現人員：指企業所有人，含正式或非正式人員（臨時員工或派駐人員），發現疑似資安事件時，皆負有即時通報之責任。

資安事件通報及應變作業程序(範例)

4、資安事件通報及處理程序：

資安事件通報及應變作業程序(範例)

4.1 資安事件發現

- 若發現或疑似資訊安全事件時，

  由發現人員依事件狀況，迅速通報相關資安管理單位，並告知直屬單位主管。

- 資安管理單位，

  依「資安事件通報單」發現人員通報之資料，進行記錄及分類。

- 資安管理單位於收到通知後，研判是否為資訊安全事件。
  - 若判斷為非資訊安全事件時，將判斷結果回覆發現人員。
  - 若判斷為資安事件時，則依資安事件之影響程度通知權責單位主管。

資安事件通報及應變作業程序(範例)

- 資訊安全事件之分類 1/2

類別	事件狀況
天然災害	如：火災、地震、水災、颱風…等
機房設施失效	如：不斷電系統、電力或冷氣空調失效…
系統異常	硬體設備故障，如主機故障，硬體障….等 系統、軟體異常，如資料庫服務、ERP系統異常…等
網路異常	網路中斷，如網路無法連接、對外網路無法連接…等
駭客入侵	駭客攻擊致系統損壞或中斷，如 加密勒索、挖礦病毒、DDoS攻擊…

資安事件通報及應變作業程序(範例)

- 資訊安全事件之分類 2/2

類別	事件狀況
人員操作失當	執行人員未遵守相關作業程序 廠商維修及維護人員未依規定執行評估及風險控管作業。 人為蓄意破壞、無意疏失、洩漏機敏資料或違反資安規範之行為
電腦或週邊失效	個人電腦設備、硬體、軟體、作業系統、電力、網路失效，或週邊設備故障。
設備失竊	設備遭竊
一般中毒	中毒，但未造成服務異常或中斷。
其他	無法歸於分類項目之事件

資安事件通報及應變作業程序(範例)

4.2 資安事件記錄

- 資安管理單位，於發生資安事件時，記錄相關資訊並將資安事件發現之狀況、評估可能影響之範圍、損失評估、支援申請、採取之應變措施等事項，詳細記錄於「資安事件通報單」中。
- 提供 [應變執行組] 於評估事件等級影響及損害評估判定

一、通報單位聯絡資料：			
通報單位名稱：		通報人：	電話：
通報時間： 年 月 日 時 分		事件發生時間： 年 月 日 時 分	
設備資料	IP 位址：	外部 IP/Web URL：	
	名稱：	安全防護機制：	
	作業系統及版本：		
二、事件通報及處理事項：			
事件分類	☐天然災害 ☐機房設施失效 ☐系統異常 ☐網路異常 ☐駭客入侵 ☐人員操作失當 ☐電腦或週邊失效 ☐設備失竊 ☐中毒 ☐其他_____		
事件狀況說明：			
可能影響及範圍評估：			
資安管理單位人員：		通報單編號：	
三、事件分級及應變措施：			
資安事件等級： ☐非資訊安全事件；☐一般資訊安全事件；☐1級；☐2級；☐3級；☐4級			
應變/處置措施說明：			
事件追蹤調查：			

資安事件通報及應變作業程序(範例)

4.3 事件記錄分級

- [應變執行組] 接獲資安事件通報單發生時，應先研判資安事件等級之對應。
- 資安事件等級，共分為4級，如下說明

事件衝擊 / 等級	評估內容
4級	機密等級資料洩漏。 核心業務系統或資料遭受嚴重竄改或毀損。 嚴重衝擊多個業務、系統運作，影響企業聲譽，無法於時效復原
3級	內部限閱等級資料洩漏。 影響核心業務運作或相關系統中斷服務。影響之重要業務、系統運作，可於時效內復原
2級	一般等級，非核心業務系統。 只是資料遭輕微竄改，業務運作遭影響或系統效率降低。不影響重要業務、系統運作。
1級	非核心業務之資產。 受到衝擊的損失程度很低，不影響業務、系統運作。

資安事件通報及應變作業程序(範例)

4.4 資安事件通報

- 資訊安全事件發現後，發現人員應以電話通知資安管理單位，並由資安管理單位填寫「資安事件通報單」提交[應變執行組]。
- [應變執行組]，應視情況尋求維護廠商或公司相關人員協助判斷，並填入「資安事件通報單」中。
- 需持續向權責主管報告事件處理狀況，待事件處置完成並一切回復正常運作後，須將處置之結果，記錄於「資安事件通報單」中，再依資安事件等級逐級報告。
- 資安事件若 涉及利害關係人（或主管機關/情資共享機關）
  - 應依與各利害關系人，制定或要求之通報機制執行通報。
  - 通知利害關係人接獲本公司通報過程，應予留存軌跡記錄。
  - 應依據與利害關係人之合約/契約進行事件等級評估。
  - 應視利害關係人要求或依情況召開雙方資安防護會議

資安事件通報及應變作業程序(範例)

4.5 資安事件應變處理

- 4至3級事件，指揮官由指揮官（召集人）擔任；2至1級事件，指揮官由副指揮官擔任。

  (指揮官應視狀況完成緊急應變小組配置，進行異常事件排除及控制。)

- 4至3級資安事件須於**36小時**內；2至1級資安事件須於**72小時**內。 (完成復原或損害管制)

- 資訊安全事件通報對象、通報方式及處置期限如下表所示。

資訊安全事件等級	指揮統籌	通報方式	處置期限
第4級(嚴重)	指揮官	電話 (或任何可通訊手段)	接獲通報後36小時以內
第3級(重大)	指揮官		接獲通報後36小時以內
第2級(注意)	副指揮官		接獲通報後72小時以內
第1級(輕微)	副指揮官		接獲通報後72小時以內

資安事件通報及應變作業程序(範例)

4.5 資安事件應變處理

- 資安事件無法於評估修復完成之時間內修復
  - 通知資通安全管理單位 (資訊單位)，
    並需於一小時內釐清，發生事實、可能影響，並重新核定等級。
  - 重新核定之範圍、損失評估與事件等級、事故分類、判斷資源申請、
    採取之緊急應變措施與利害關係人，補充於【資通安全事故通報單】，
    並評估是否聯繫相關維護廠商協助事件處理。

- 視事故類型採取應變程序因應，
  必要時得經權責主管同意後，進行備援或緊急應變作業
- 資安事件等級為4級，指揮官應成立 重大資安事件緊急應變小組，應符合上市上櫃公司資通安全管控指引「第三十四條」，啟動 重大資安事件通報，並依相關規定辦理重訊通報。

資安事件通報及應變作業程序(範例)

4.6 事件追蹤調查

- 檢討分析相關資訊以釐清事件發生的原因與責任，
  並分析是否會重複發生，審視現有資訊環境的漏洞，加以修補。

- 資訊安全事件應保留事件發生之線索。

- 為有效追蹤，檢討事件原因，
  應審視現有環境的漏洞，細節記錄於「資安事件通報單」。

資安事件通報及應變作業程序(範例)

4.7 檢討改善會議

- 若為重大等級以上之資訊安全事件，於處理完畢且獲得控制後，為預防資安事件不再重複發生，須由事件指揮官召集相關單位，或委由副指揮官，召開資安事件檢討會議，研析問題發生之原因。

- 依據資安事件檢討會議之結果，由系統負責人執行矯正措施，進行問題矯正的作業，以降低事件再發生的可能性。

- 資安事件應列入[資安事件管制表]進行案件管制連同資安事件通報單及事件軌跡資料，應定期呈主管覆核。

資安事件通報及應變作業程序(範例)

5.本作業程序經董事會通過後實施，修正時亦同。

6.稽核控制重點

- 是否依【資安事件通報及應變作業程序】通知相關單位。
- 相關紀錄表單資料是否適當填寫。
- 相關紀錄表單資料是否經適當核准。
- 相關通報軌跡資料是否歸檔保存。
- 相關事件檢討會議及矯正的作業是否追蹤與改善。

7.表單

7.1 資通安全事故通報單

7.2 資通安全事故通報管制表

1 上市櫃資通安全管控指引

2 資安推動組織&資安政策擬訂

3 資安事件應變程序擬定

4 上市櫃風險評估計畫

5 企業運維平台-資安風險評估 體驗

- 資安風險評估計畫

風險評估目的

- 通過此辦法識別及盤點公司資通系統，鑑別資訊資產價值
- 評估可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊
- 依目前公司既有之資通安全管理及技術面的控制機制進行強化及改善
- 應對可能面對的資安風險衝擊

組織與職責

- 負責制定『風險評估及改善作業程序』，
- 依風險評估執行時企業面臨的狀況，進行適度增刪，且經權責主管同意後進行實施。
- 負責定期或不定期，執行核心資通系統之風險評估，並產出『風險評估報告』
- 及依據評估結果之風險衝擊程度，制定『風險改善計畫』。
- 向經營決策單位提報
  『風險評估報告』及『風險改善計畫』。
- 依決議之改善計畫項目，
  依排程進行改善並定期回報進度，直至完成。

風險評估執行時機

- 定期執行
- 相關法規有所增刪或修改
- 核心業務出現變動或核心資通系統發生較大變動時
- 出現嚴重的資安事故時
- 資安政策或目標發生變動時

風險評估暨改善執行做法

1.資產價值識別

2.風險識別

3.風險分析

4.風險評估

5.風險改善計畫

6.殘餘風險審核

7.風險改善計畫執行及控制

階段1：資產價值識別

1.資產價值識別
2.風險識別
3.風險分析
4.風險評估
5.風險改善計畫
6.殘餘風險審核
7.風險改善計畫執行及控制

- 評估資通系統並建立核心資通系統資產清冊，
- 並通過確認資通系統之業務影響程度，
- 透過機密性、完整性、可用性、適法性的評估，
- 進行資產價值識別，資產價值(取最大值)
- 識別標準及計量方式(BIA營運衝擊分析)

  如: 資產價值識別標準及計量表

資產價值識別標準及計量表(BIA營運衝擊分析)

計量分數	資產價值(重要性)	機密性	完整性	可用性	適法性
4	極高	未經授權之機敏資訊揭露，造成可預期非常嚴重影響。 如：聲譽/權益/安全/形象之重大損失	未經授權之極重要資訊修改或破壞，造成可預期之嚴重影響。 如：聲譽/權益/安全/形象 之重大損失	資訊、資通系統之存取或使用上的中斷在營運、信譽造成可預期非常嚴重或災難性負面影響， 容許<4hr 不使用	國家法律要求
3	高	未經授權之限制資訊揭露，造成可預期重大影響。 如：聲譽/權益/安全/形象之明顯損失	未經授權之重要資訊修改或破壞，造成可預期之嚴重影響。 如：聲譽/權益/安全/形象 之明顯損失	資訊、資通系統之存取或使用上的中斷在營運、或信譽等方面，造成可預期之嚴重負面影響。 容許4hr-1Day不使用	外部合約規範要求
2	中	未經授權之內部資訊揭露，造成可預期影響。 如：可承受損失	未經授權之一般資訊修改或破壞，造成可預期之影響。 如： 可承受損失	資訊、資通系統之存取或使用上的中斷在營運、或信譽等方面，造成可預期之負面影響。 容許1Day-3Days不使用	內部政策要求
1	低	公開資訊揭露， 可預期不會造成影響。	未經授權之一般資訊被修改或破壞，不造成損失	資訊、資通系統之存取或使用上的中斷在營運、或信譽等方面不受響。 容許>3Days不使用	無此特性

階段2：風險識別

1.資產價值識別

2.風險識別

網路線與老鼠的糾葛

明日大理想 聰明管理

ektrontek 2013-03-24 17:59:44 · 11451 瀏覽

老鼠咬斷網路事件頻傳，實在是困擾許久
我希望公司的網路線及電源線，不要再被老鼠咬了。
因為只要一咬斷，使用者就會開始哇哇叫，這樣MIS就要去分公司修電腦也順便去抓老鼠，我們就會忙到天昏地暗地，換電源線、網路線是還好，最怕要與老鼠PK一回，重點是還未必可以抓到老鼠。

當使用環境電壓不穩時，會造成電腦的電源供應器容易故障

2013年11月5日 — 藤小二電腦知識-當使用環境電壓不穩時，會造成電腦的電源供應器容易故障，或是在使用電腦時會很頓頓頓..... 藤之前在某家公司的電腦上有遇到一個問題 ...

電磁干擾（英文：Electromagnetic Interference，或 Electromagnetic Disturbance，簡稱EMI）是指任何在傳導或電磁場伴隨著電壓、電流的作用而產生會降低某個裝置、設備或系統的性能，或可能對生物或物質產生不良影響之電磁現象。

或說電子設備都會產生傳導性電磁雜訊干擾，就像傳染病般地透過電源線傳導（一般稱作Power Line Noise）。

電磁干擾也是變頻器驅動系統的一個主要問題。在許多國家，尤其在歐洲，對任何系統可能散發的電磁干擾有嚴格的限制。

- 提列已知或曾經發生的資產之風險威脅，
  評估對核心資通系統可能造成的風險威脅及風險弱點

硬體威脅	• 因硬體故障、老化等 造成的威脅。 如：硬碟損毀，POWER故障等
系統、軟體威脅	• 因系統或軟體問題，造成的威脅。 如：當機、服務中斷等
使用者威脅	• 內部使用者，因程序、習慣、忽疏，造成的威脅
外部環境威脅	• 外部環境造成的威脅， 如：溫溼度異常、粉塵、漏水、失火等
	• 自然災害造成的威脅， 如：雷擊、地震、水災等
	險，
駭客攻擊	如：社交攻擊、漏洞攻擊、暴力破解..等

階段3：風險分析(威脅可能性等級

1.資產價值識別
2.風險識別
3.風險分析
4.風險評估
5.風險改善計畫
6.殘餘風險審核
7.風險改善計畫執行及控制

威脅可能性等級：威脅等級、說明及發生頻率			
等級	辨識	說明(取最高值)	發生頻率
3	高	◦防護脆弱性被利用的安全對策無效 ◦威脅來源有強烈的動機與足夠能力 ◦時常發生	◦平均 每年可能發生 4 次(含)以上
2	中	◦防護脆弱性被利用的安全對策有效 ◦威脅來源有動機也有能力 ◦有可能發生	◦平均 每年可能發生 1 次以上， 低於 4 次
1	低	◦防護脆弱性被利用的安全對策有效 ◦威脅來源缺乏動機或能力不足 ◦發生頻率低	◦事件或威脅雖然沒發生過， 但有可能發生 ◦平均每年發生不到 1 次

階段3： 風險分析(脆弱性利用等級

1.資產價值識別

2.風險識別

3.風險分析

4.風險評估

5.風險改善計畫

6.殘餘風險審核

7.風險改善計畫執行及控制

脆弱性利用等級：脆弱等級、說明及發生頻率		
等級	辨識	說明
3	高	◦不需具備任何能力均能有意或無意的利用脆弱性 ◦資訊、資通系統資產，受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊及資通系統資產遺失或損壞，無法復原 ◦無保護或防護機制或機制無效，威脅來源於短期(1週內)即可攻擊成功 ◦未建立控制措施
2	中	◦具備一定的專業技術知識，才能利用脆弱性 ◦資訊、資通系統資產受到損害，或是受到損害後72小時內可回復 ◦已實施保護或防護機制，威脅來源必須花費一段時間(可能是數週以上)進行資料蒐集始能接觸到重要資訊、資產，攻擊成功 ◦已執行現有控制措施, 但仍有缺項，無法有效避免
1	低	◦需專精於脆弱性技術，並於特定條件或環境下方能利用脆弱性 ◦不會損害資訊、資通系統資產，或是受到損害後能於24小時回復 ◦威脅來源必須花費長時間(可能需一個月以上)的資料蒐集，突破各層防護，才能接觸到重要資訊、資產，攻擊成功 ◦已確實執行現有控制措施, 且能有效避免

階段4：風險評估(詳細風險評估-機率/影響矩陣)

1. 資產價值識別
2. 風險識別
3. 風險分析
4. 風險評估
5. 風險改善計畫
6. 殘餘風險審核
7. 風險改善計畫執行及控制

威脅可能性(F) X 弱點衝擊程度(I)		1	2	3	4	5	6	7	8	9
資產價值 (V)	4	4	8	12	16	20	24	28	32	36
	3	3	6	9	12	15	18	21	24	27
	2	2	4	6	8	10	12	14	16	18
	1	1	2	3	4	5	6	7	8	9

風險等級		風險值	處理原則
高風險	H	大於20	儘速處理，影響整體企業的營運， 需緊急處理改善
中風險	M	大於6 小於等於20	需處理，影響部份業務工作的運行， 需要訂立排程改善或接受
低風險	L	小於等於6	可接受，對業務運作極小， 可評估改善或接受

階段5：風險改善計畫

1.資產價值識別
2.風險識別
3.風險分析
4.風險評估
5.風險改善計畫
6.殘餘風險審核
7.風險改善計畫執行及控制

風險處理順序：
依風險等級不同，給予不同的改善優先順序，高風險威脅需優先處理，中風險 排程處理，低風險為可接受風險，可不處理

風險處理方式：
依據風險評估結果採取管控措施：接受、降低、轉移、規避等

管控措施	說明
接受	接受風險的威脅，如低、中風險的威脅， 對企業營運不造成危害或危害可控之情況下，可接受
降低	降低風險發生的機率及影響程度， 透過管理或技術面象，控制風險至可接受的程度
轉移	評估全部轉移或部份轉移風險發生的責任及影響， 轉嫁至其他外部組織，如資安險、或委外
規避	避免承擔風險之作為， 如結束、放棄某營運項目或服務。

階段6：殘餘風險審核

1.資產價值識別
2.風險識別
3.風險分析
4.風險評估
5.風險改善計畫
6.殘餘風險審核
7.風險改善計畫執行及控制

- 經過改善計畫提案之風險項，需執行殘餘風險審核，
- 確保經過改善計畫後之風險餘留之殘餘風險為可接受程度

資產價值(V)									
4	4	8	12	16	20	24	28	32	36
3	3	6	9	12	15	18	21	24	27
2	2	4	6	8	10	12	14	16	18
1	1	2	3	4	5	6	7	8	9

改善前風險值 = 資產價值(V)（4） x 威脅/風險可能性(F)（3） x 弱點衝擊程度(I)（3） = **36**

改善後風險值 = 資產價值(V)（4） x 威脅/風險可能性(F)（1）↓ x 弱點衝擊程度(I)（1）↓ = **4**↓

階段7：風險改善計畫執行及控制

1.資產價值識別
2.風險識別
3.風險分析
4.風險評估
5.風險改善計畫
6.殘餘風險審核
7.風險改善計畫執行及控制

- 專案執行過程，需確保改善進度及預期效果如預期。
- 且需定期向決策單位進行提報進度及效果，
- 直至改善計畫項目全數完成

風險評估類別\控制措施	管理面控制措施	技術面控制措施
服務	購買委外服務（含維護合約）/調整SLA服務水準	增建備援服務/取得原廠受訓證書
硬體	重新規劃建置新硬體/購買維護合約	良品替換/備援設備替代
軟體	購買正式版本軟體/購買維護合約	系統復原/重新安裝建置

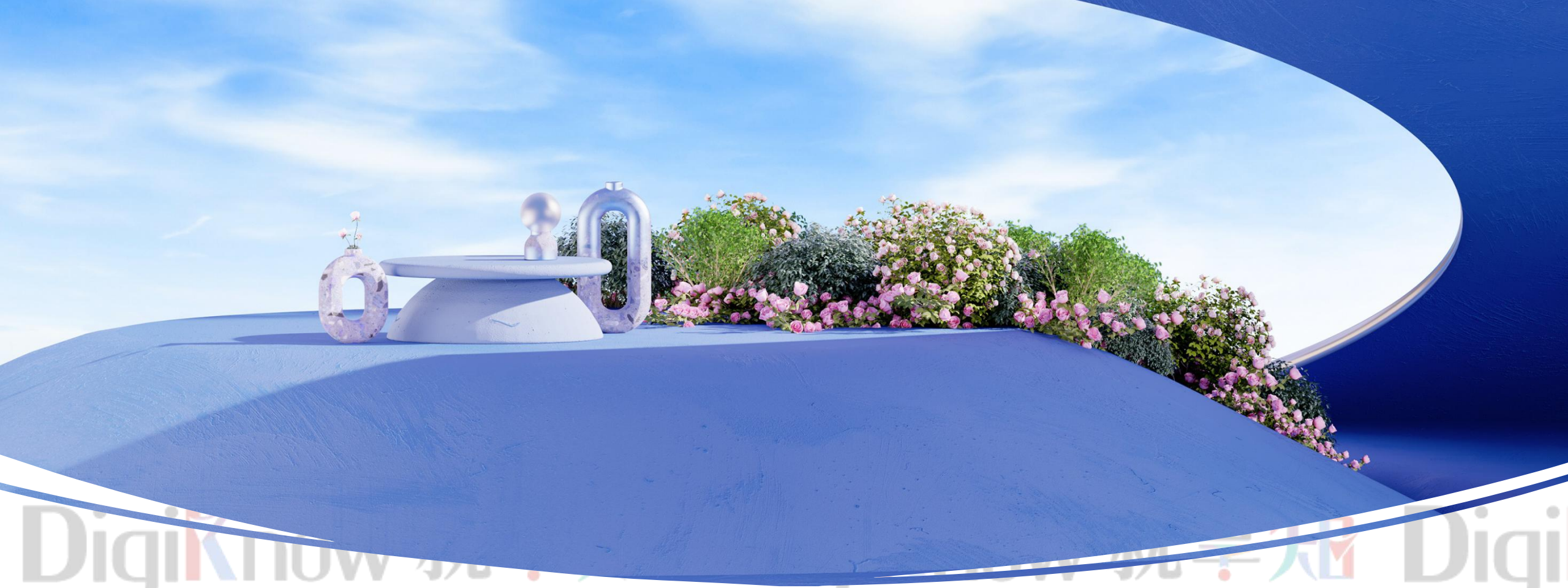
1 上市櫃資通安全管控指引

2 資安推動組織&資安政策擬訂

3 資安事件應變程序擬定

4 上市櫃風險評估計畫

5 企業運維平台-資安風險評估 體驗

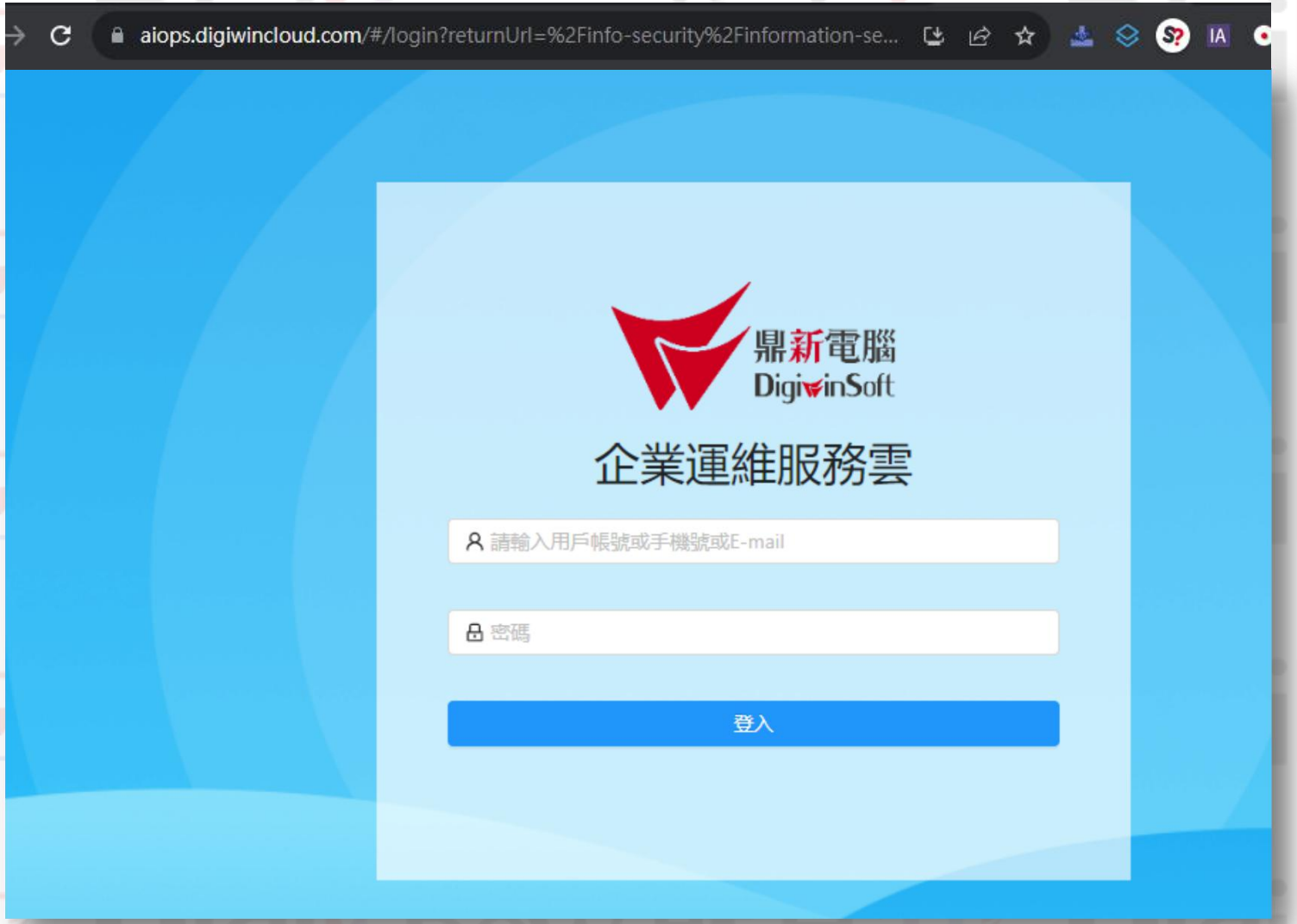


企業運維平台-資安風險評估 體驗

企業運維服務雲平台（資安風險評估模組體驗）

請於瀏覽器輸入
鼎新電腦電腦企業運維服務雲網址:
https://aieom.digiwincloud.com

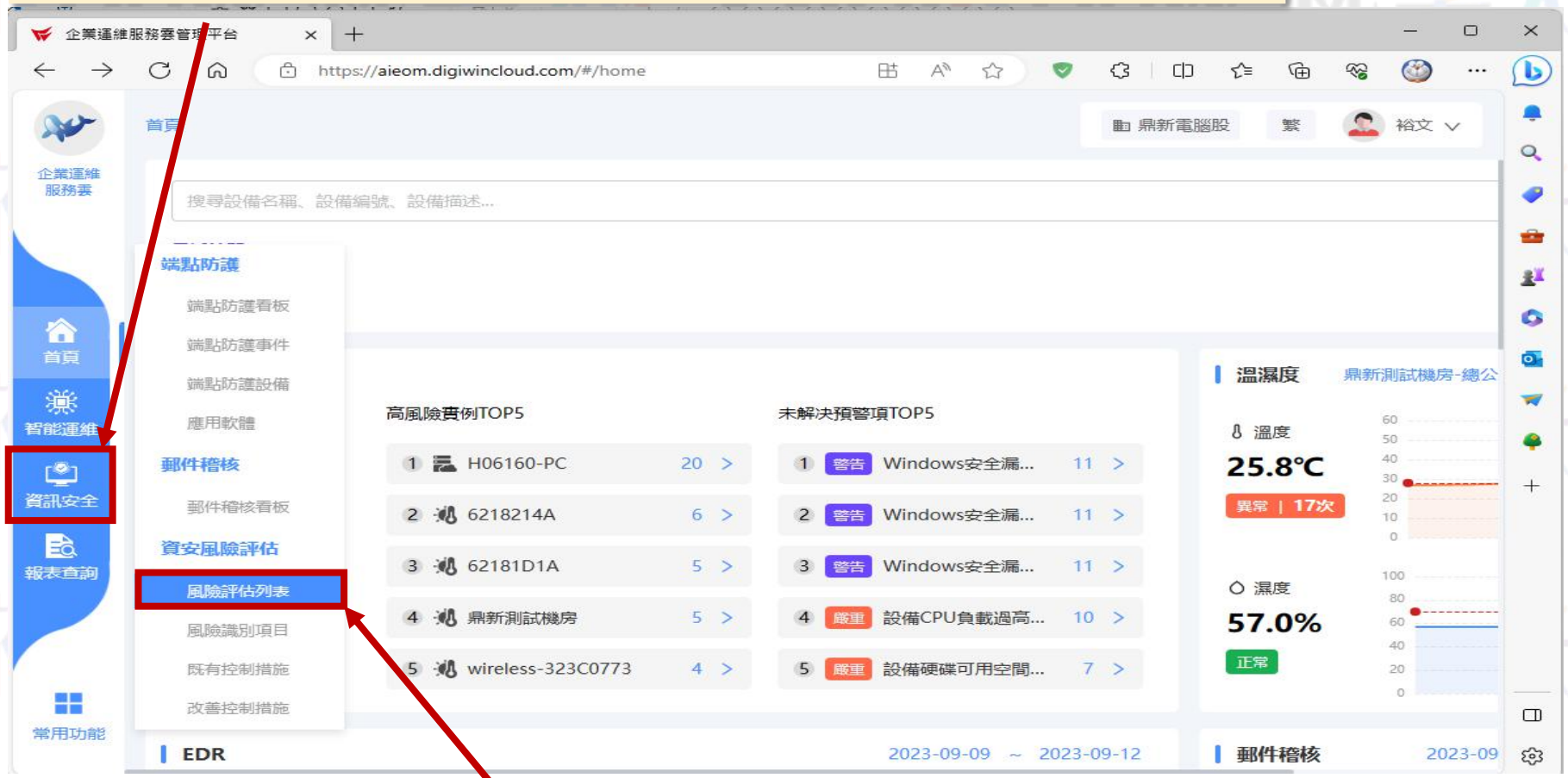
輸入您報名課程時預先申請
「帳號」「密碼」點選登入後
即可登入



建立新評估

企業運維服務雲平台（介面環境認識）

登錄後我們於頁面左方，切換至 「**資訊安全**」頁簽



選擇頁面右方，「資安風險評估」模組中的風險評估列表

企業運維服務雲平台（新建風險評估）

於工作區中 點選「**新建風險評估**」

選擇客戶：輸入貴公司名稱帶入

標題：輸入給予的風險評估名稱

評估人：為課程報名帳號人員

上傳資產清單：（本步驟先跳過）

□同意勾選Ai智管家聲明:要勾選

點選「**確定**」即建立

企業運維服務雲平台（風險評估4步驟）

接下來呢我們就跟著「評估進度 1、2、3、4步驟」，逐步建立企業資通系統風險評估

建立資產清單

企業運維服務雲平台（進入資產清單）

評估進度 >> 點選「1資產清單」下方「**查看資產清單**」

企業運維服務雲平台（建立資產清單-平台輸入1/2）

上傳公司的資產清單，有兩個方法進行資訊的輸入或上傳

方法一：直接在平臺點選「+ 新增數據」做輸入。

企業運維服務雲平台（建立資產清單-平台輸入2/2）

同左方欄位輸入

欲風險評鑑之資產資訊

輸入完成後點選「**確定**」

(請注意 紅色*為必填欄位)

企業運維服務雲平台（建立資產清單-清單下載1/4 ）

方法二：點選「↓下載資產清單」下載xlsx檔 (請至個人電腦下載資料夾取得)

企業運維服務雲平台（建立資產清單-清單下載2/4 ）

依表格欄位格式填寫(請注意 所有欄位皆為必填欄位) 存檔

資產編號	資產評估類別	資產分類	資產名稱	資通系統/用途描述	數量	存放位置/安裝設備	權責單位	保管人	維護廠商	維護狀態
1	硬體	網路防護	Forti防火牆	Forti防火牆	1	台北機房/防火牆	資訊室	Andy	鼎新電腦	無合約
2	軟體	虛擬平台	VMWare	VMWare	1	台北機房/ST550主機	資訊室	Andy	鼎新電腦	無合約
3	服務	上網線路	中華電信網路服務	中華電信網路服務	1	台北機房/數據機	資訊室	Andy	中華電信	合約內
4	軟體	ERP系統	TIPTOP_ERP	TIPTOP_ERP	1	台北機房/ST550主機	資訊室	Andy	鼎新電腦	合約內
5	軟體	ERP系統	Oracle資料庫	Oracle資料庫	1	台北機房/ST550主機	資訊室	Andy	鼎新電腦	合約內
6	軟體	ERP系統	Linux作業系統	Linux作業系統	1	台北機房/ST550主機	資訊室	Andy	鼎新電腦	合約內

企業運維服務雲平台（建立資產清單-清單下載3/4 ）

點選「↑重新上傳資產清單」，選擇檔案位置後點選「**確定**」，將清單上傳至平台

企業運維服務雲平台（建立資產清單-清單下載4/4 ）

上傳至平台，確認上傳資訊與狀態都為「正常」（若重新上傳發生減少項次 狀態將為「刪除」）

資產鑑值與整合

資安風險評估模組 操作體驗

企業運維服務雲平台（資產鑑值與整合）

評估進度 >> 點選「2.資產鑑值與整合」下方「**查看詳情**」

企業運維服務雲平台（資產鑑值與整合-新增資通系統1/8）

點選下方「＋新增資通系統」協助公司建立資訊資產整合分類標籤，

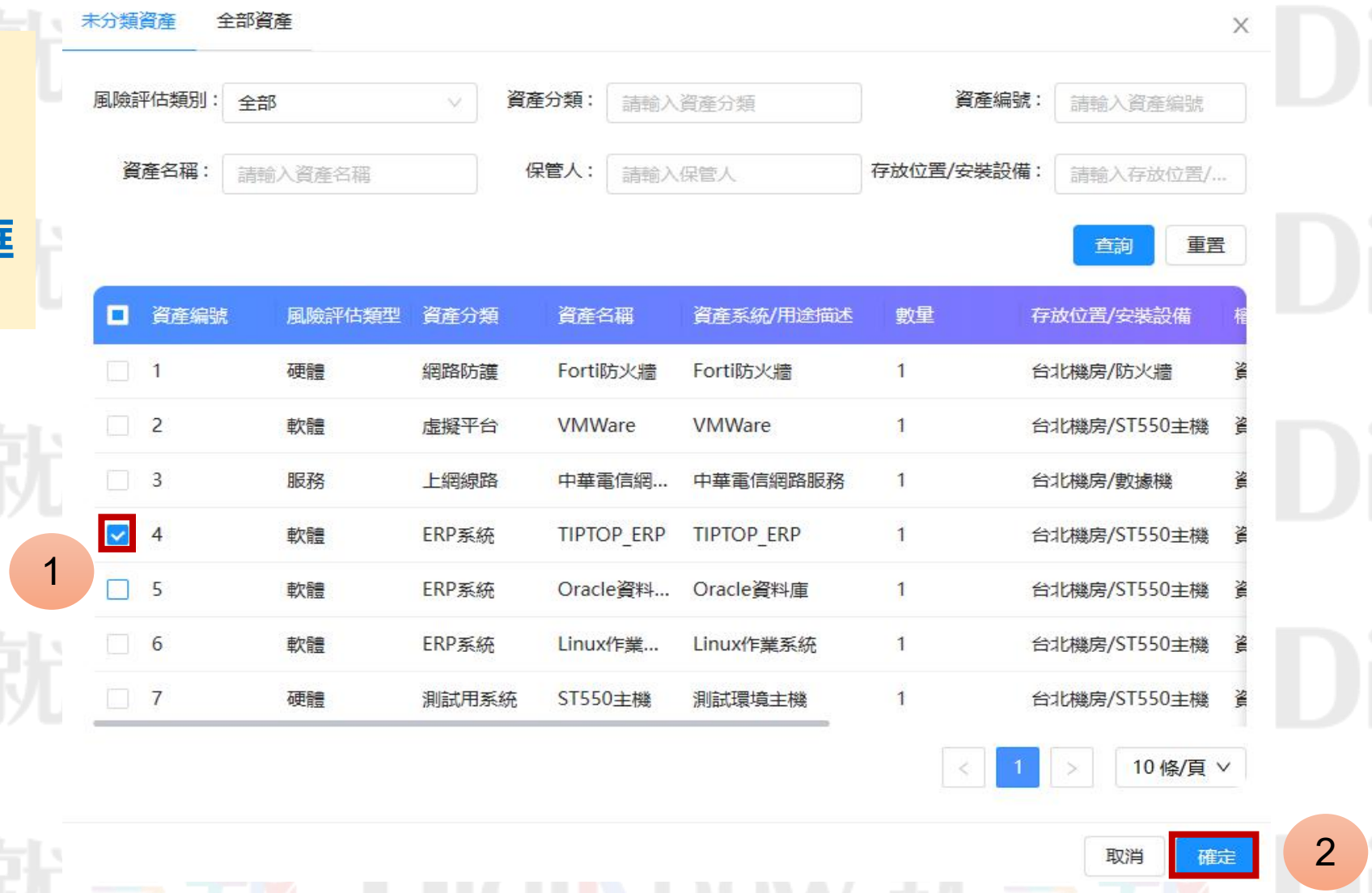
輸入 資產需要之整合類別名稱（如一般資通系統設備/核心營運系統…等）
點選「下一步」

企業運維服務雲平台（資產鑑值與整合-新增資通系統2/8）

點選「**下一步**」後，

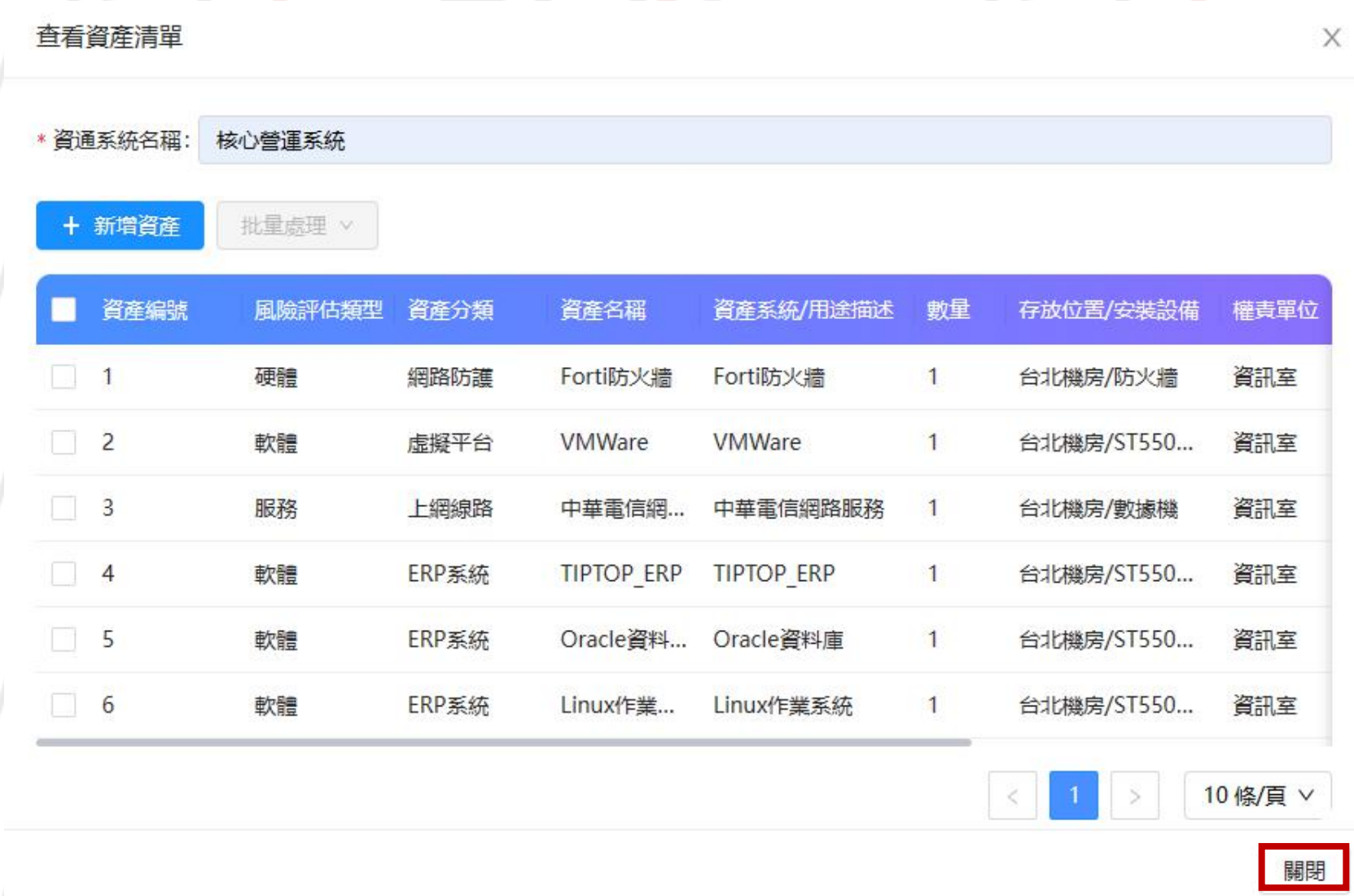
請勾選

1.欲加入設備前方 □ **方框**
2.再點選「**確定**」儲存



企業運維服務雲平台（資產鑑值與整合-新增資通系統3/8）

3.點選「關閉」



3

企業運維服務雲平台（資產鑑值與整合-新增資通系統4/8）

企業運維服務雲平台（資產鑑值與整合-新增資通系統5/8）

確定新增正確後

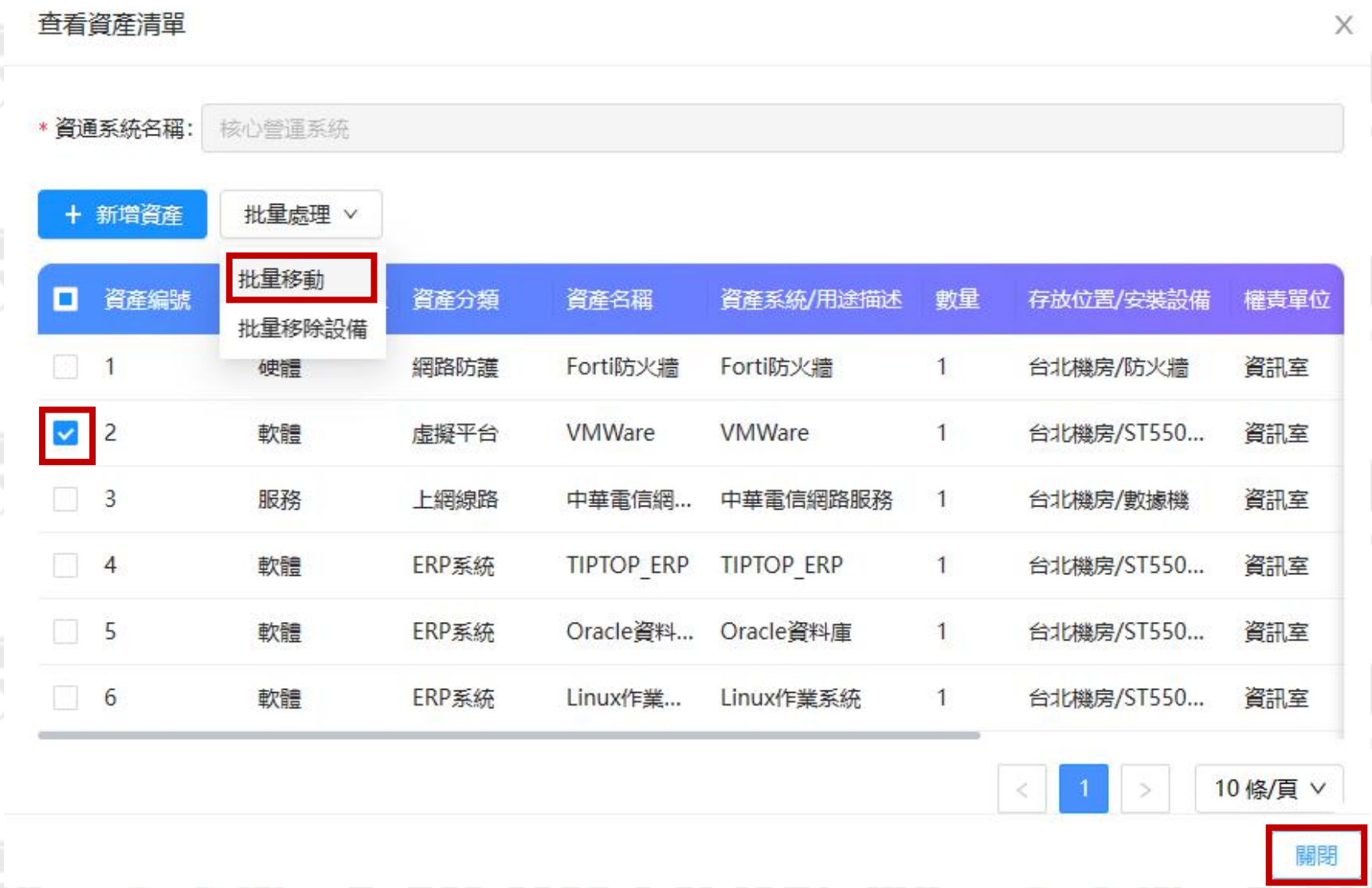
可**點選 [:]** 為整合分類標籤 **「添加」**、**「查看」**或**「刪除」**設備

企業運維服務雲平台（資產鑑值與整合-新增資通系統6/8）

添加設備
資通系統分項後方
點選 [:]「添加設備」
勾選□**項目**後按**「確定」**

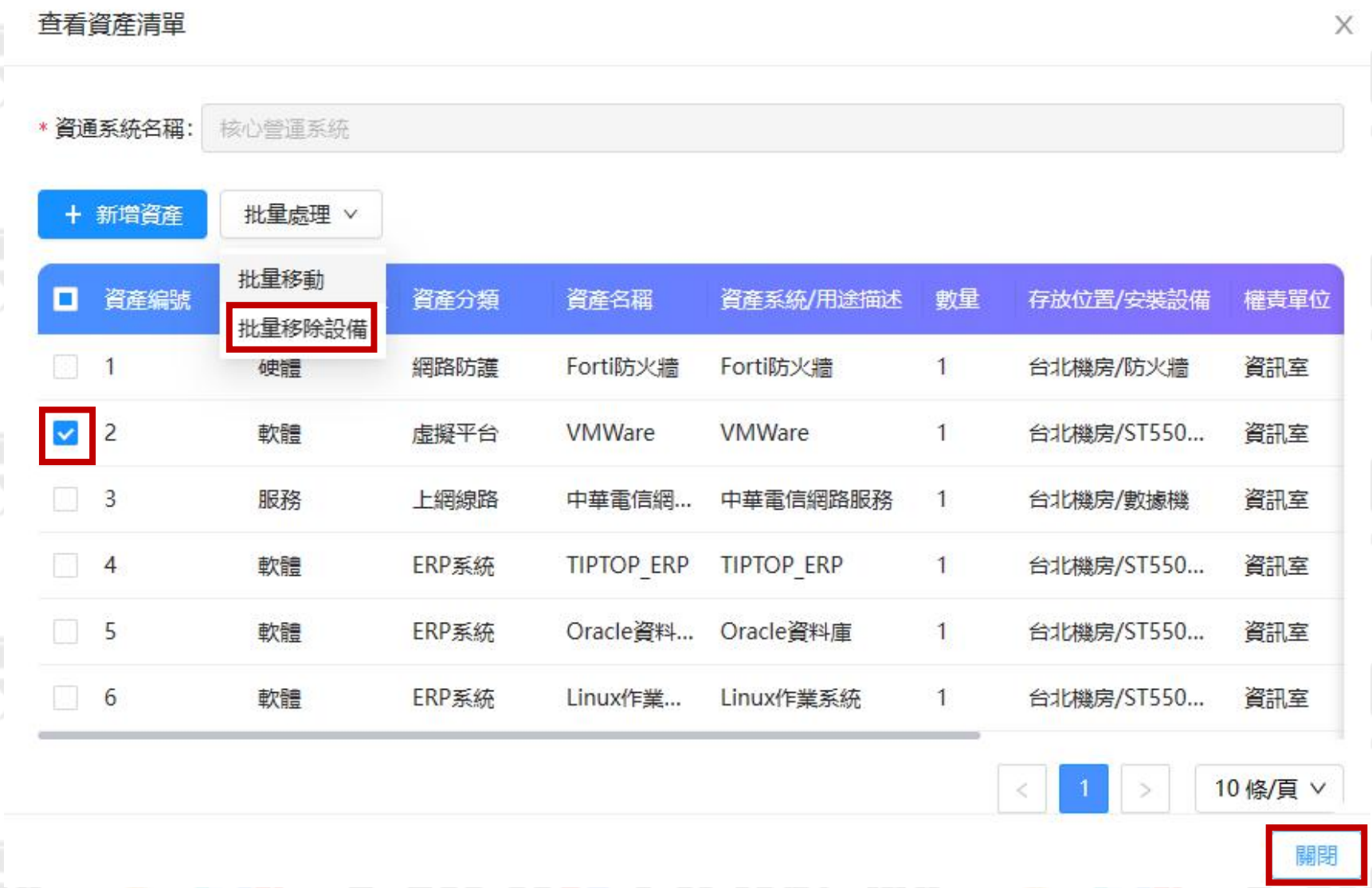
企業運維服務雲平台（資產鑑值與整合-新增資通系統7/8）

移動設備
資通系統分項後方
點選 [:]「查看資產清單」
勾選□項目後
下拉選「批量移動」



企業運維服務雲平台（資產鑑值與整合-新增資通系統8/8）

移除設備
資通系統分項後方
點選 [:]「查看資產清單」
勾選□項目後
下拉選「批量移除設備」



企業運維服務雲平台（資產鑑值與整合-風評基礎設定1/3）

先確認目前的「資產鑑值評估準則」 是否符合公司的風險鑑值標準

企業運維服務雲平台（資產鑑值與整合-風評基礎設定2/3）

可選擇 **編輯**，重新調整公司資產價值參數（預設為4級分數計量）

風險評估基礎設定 ∨ | 資產鑑值評估準則 | 風險分析準則 | 維護既有控制措施 | 編輯

資產鑑值等級劃分：4級 ∨

計量分數	資產價值(重要性)	機密性	完整性	可用性	適法性
4	極高	未經授權之機敏資訊揭露，...	未經授權之極重要資訊修改...	資訊、資通系統之存取或使...	國家法律要求
3	高	未經授權之限制資訊揭露，...	未經授權之重要資訊修改或...	資訊、資通系統之存取或使...	外部合約規範要求
2	中	未經授權之內部資訊揭露，...	未經授權之一般資訊修改或...	資訊、資通系統之存取或使...	內部政策要求
1	低	公開資訊揭露，可預期不會...	未經授權之一訊修改或破壞...	資訊、資通系統之存取或使...	無此特性

企業運維服務雲平台（資產鑑值與整合-風評基礎設定3/3）

請確認參數描述 符合公司認知與定義,若須變更請於變更後點選「**確定**」儲存變更
* 請注意*
1.**可用性** 欄位時間描述是否需調整（如：<4HR)
2.是否須全部調整一致性（如：其他記量分數）

企業運維服務雲平台（資產鑑值與整合-BIA分數變更）

完成風評基礎設定後，回「資產鑑值與整合」頁面點選 「編輯」

企業運維服務雲平台（資產鑑值與整合-BIA變更完成）

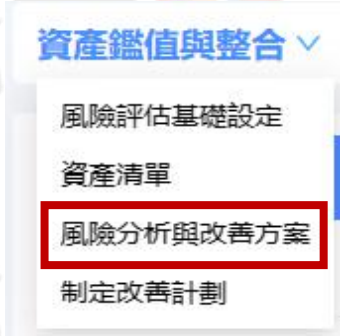
「風險評估類別」可再作調整
填入各項資產價值評定，（直接於欄位上輸入數值即可）
輸入完成後點選**「確定」**，再點選**「確定」**儲存

風險分析

資產鑑值與整合

- 風險評估基礎設定
- 資產清單
- 風險分析與改善方案
- 制定改善計劃

企業運維服務雲平台（風險分析）



評估進度 >> 點選「3.風險分析」下方「**查看詳情**」

企業運維服務雲平台（風險分析-風險對應新增）

選擇設備分類 （如 選擇 核心營運系統）

點選「新增」依據**公司現況與先前經歷**選擇欲增加之風險分析項目

選定之資產類別會對應可能之風險威脅。

目前硬體、軟體、服務 已有預設的風險評估項目
若不足，之後可新增所需之風險評估類別

企業運維服務雲平台（風險分析-風險選用）

檢視風險/威脅/脆弱性 描述

選用**公司現況與先前經歷**

可能發生/關連之風險分析項目

請勾選設備前方 □ **方框**

（若不足可再點各分頁勾選）

再點選「**確定**」儲存

企業運維服務雲平台（風險分析準則-參數檢視）

請點選「風險評估基礎設定」後選「風險分析準則」檢視/編輯目前系統定義之風險評估之參數定義

風險分析準則中，律定我們此次用的評估矩陣及每個分數，代表的含義才能在評估時，給予分數，並且在矩陣圖中，可定義 風險值分數 改善的處理原則，何種數值的風險，應該特別優先改善，那些數值是排程改善

1 → 2 → 3

風險分析準則
矩陣參數調整

參數檢視 上半部 檢視

風險評估基礎設定 ∨ | 資產鑑值評估準則 | 風險分析準則 | 維護既有控制措施 | 取消 | 保存

風險分析及處理原則

等級	風險值	威脅可能性
高風險	20 ≤ x	儘速處理，影響整體企業的營運，需緊急處理改善
中風險	6 ≤ x <20	需處理，影響部份業務工作的運行，需要訂立排程改善，或於可控前提下 接受風險
低風險	x<6	可接受，對業務運作極小，可評估改善或接受

風險可能性(F) X 威脅性利用程度(I)		1	2	3	4	5	6	7	8	9
資產價值(V)	4	4	8	12	16	20	24	28	32	36
	3	3	6	9	12	15	18	21	24	27
	2	2	4	6	8	10	12	14	16	18
	1	1	2	3	4	5	6	7	8	9

高風險 應快速處理改善

中風險 須排程改善或接受

低風險 評估改善或接受

資安風險評估模組 操作體驗

參數檢視 下半部 檢視

檢視目前設定3x3矩陣，
可自行調整(如4x4矩陣)
若「修改」點選「保存」儲存

風險評估基礎設定 ∨ | 資產鑑值評估準則 | 風險分析準則 | 維護既有控制措施

取消 保存

風險評估定義 風險等級劃分: 3級 ∨

等級	辨識	威脅可能性	脆弱性利用
3	高	說明 .防護脆弱性被利用的安全對策無效 .威脅來源有強烈的動機與足夠的能力 .時常發生 發生頻率 .平均每年可能發生 4 次(含)以上	說明 不需具備任何能力均能有意或無意的利用脆弱性;資訊、資通系統資產，受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊及資通系統資產遺失或損壞，無法復原;利用簡易的方法就能利用脆弱性進行攻擊、破壞;無保護或防護機制或機制無效，威脅來源於短期(1~3天內)即可攻擊成功;尚未建立控制措施。
2	中	說明 .防護脆弱性被利用的安全對策有效 .威脅來源有動機也有能力 .有可能發生 發生頻率 .平均每年可能發生 1 次以上，低於 4 次	說明 具備一定的技術知識，才能利用脆弱性;資訊、資通系統資產受到損害，或是受到損害後24小時內可回復;不需用特殊的方法就能利用脆弱性進行攻擊;已實施保護或防護機制，威脅來源必須花費一段時間(可能是3天以上)進行資料蒐集始能接觸到重要資訊、資產，攻擊成功;已執行現有控制措施，但仍有缺項，無法有效避免。
1	低	說明 .防護脆弱性被利用的安全對策有效 .威脅來源缺乏動機或能力不足 .發生頻率低 發生頻率 .事件或威脅雖然沒發生過，但有可能發生 .平均每年發生不到 1 次	說明 需專精於脆弱性技術，並於特定條件或環境下方能利用脆弱性;不會損害資訊、資通系統資產，或是受到損害後能於4小時回復;必須運用特殊的方法才能利用脆弱性進行攻擊;威脅來源必須花費長時間(可能需一個月以上)的資料蒐集，突破各層防護，才能接觸到重要資訊、資產，攻擊成功;已確實執行現有控制措施，且能有效避免。。

企業運維服務雲平台（風險分析-確認與分析）

由「風險評估基礎設定」回「風險分析與改善方案」頁面
選擇設備分類（如 選擇 核心營運系統
確認選用之風險描述，點選「編輯」輸入「現有控制措施/風險分析」

企業運維服務雲平台（風險分析-確認與分析）

現有控制措施：**輸入**目前公司建置控制措施，若沒有請輸入「無」（如：管理面/技術面 有哪些因應）

風險分析：請依據**控制錯施之有效性**輸入 **F(威脅可能) 與 I (脆弱性利用)**（三級分為 低1 - 中2 - 高3)

填寫完畢後，將自動計算出風險等級（高/中/低），點選「**保存**」存檔

請記得所有分類都要設定

企業運維服務雲平台（風險分析-下載）

資訊安全 / 資安風險評估 / 風險評估列表 / 風險分析

下載

02400000_鼎新電腦股_風險評估記錄表_20230912154...

開啟檔案

下載風險分析

裕文

風險分析與改善方案

風險分析 | 改善方案

資通系統

查詢資通系統

核心營運系統 3/3

一般資通系統/設備 1/1

核心營運系統 資產：Forti防火牆、VMWare、中華電信網路服務、TIPTOP ERP、Oracle資料庫、Linux作業系統

+新增 | 編輯 | 查看資產

風險描述	威脅	脆弱性	現有控制措施	風險分析	操作
設備使用多年/設備零件故障	設備/零組件故障	系統或服務無法使用，資料毀損 / 無異常偵測機制，無備援機制，無資料備...	無	高(24) V(4) x F(3) x I(2)	
未評估設定風險	組態設定錯誤	可用性、效能降低，甚至被駭客入侵 / 無設定人員能力評估、套用設定前確...	無	中(8) V(4) x F(2) x I(1)	
未評估更新風險	韌體更新失敗	更新失敗，可用性喪失 / 無事前風險評估，非作業時間更新，無備援設備	無	低(4) V(4) x F(1) x I(1)	

風險編號	資產		威脅與脆弱性識別			現有控制措施識別	風險分析					風險可接受評估		新建置控制措施
	資通系統	資產	風險描述	威脅	脆弱性	現有控制措施	資產價值(V)(CIA面象)	風險可能性(F)	弱點衝擊程度(I)	風險值=(V)x(F)x(I)	風險等級	處置優先順序	風險接受選項(降低、轉移、避免、接受)	
1	一般資通系統/設備	ST550主機	設備使用多年/設備零件故障	設備/零組件故障	未使用，資料毀損 / 無異常偵測機制，無備援機制，		4	1	1	1	低		接受	
2	核心營運系統	IPTOP_ERP,中華電信	未評估更新風險	韌體更新失敗	可用性喪失 / 無事前風險評估，非作業時間更新，	無	4	1	1	4	低	排程	接受	
3	核心營運系統	IPTOP_ERP,中華電信	設備使用多年/設備零件故障	設備/零組件故障	未使用，資料毀損 / 無異常偵測機制，無備援機制，	無	4	3	2	24	高	優先	降低	A備援架構
4	核心營運系統	IPTOP_ERP,中華電信	未評估設定風險	組態設定錯誤	客入侵 / 無設定人員能力評估、套用設定前確認、非	無	4	2	1	8	中	排程	降低	E檔備份首

增列風險

企業運維服務雲平台（風險分析-增列風險）

若須增加**風險分類**（目前為服務/數據/軟體/硬體）或**風險分類項目**
請點選**「風險評估列表」**中的 **「風險識別項目」**

企業運維服務雲平台（風險分析-增列風險）

風險識別項目

風險評估類別

請輸入風險評估類別

- 服務
- 數據
- 軟體
- 硬體

服務

搜尋 | + 新增

威脅來源	風險描述	威脅(發生的威脅)	脆弱性(影響狀態、分析發生威脅原因)	操作
供應商威脅	更新管道被駭客入侵，產生供應鏈攻擊	網路被駭		
供應商威脅	ISP供應商網路服務中斷	網際網路中		
使用者威脅	因使用者自行外接裝置、自帶設備、網...	網路衝突		
使用者威脅	無線訊號過度覆蓋	網路被入侵		
駭客攻擊	駭客攻擊(透過暴力破解攻擊)	設備遭入侵		
駭客攻擊	駭客攻擊(透過漏洞攻擊)	設備遭入侵		

新增風險項目(來源/描述/威脅/脆弱性)

添加新欄位

服務

威脅來源 *

請輸入威脅來源

風險描述 *

請輸入風險描述

威脅(發生的威脅) *

請輸入威脅(發生的威脅)

脆弱性(影響狀態、分析發生威脅原因) *

請輸入脆弱性(影響狀態、分析發生威脅原因)

取消 | 確定

改善方案

企業運維服務雲平台（改善方案-建置改善）

「風險分析」完成後，接下來點選右側**「改善方案」**建立分類標籤
為風險分析後，評估新建置控制措施，已降低風險發生之可能性與影響

點選**「編輯」**調整

企業運維服務雲平台（改善方案-建置改善）

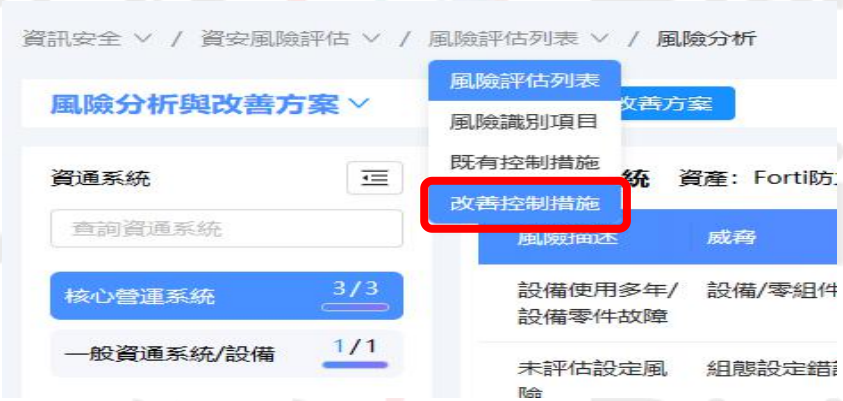
勾選風險可接受評估， 優先順序及新建控制措施
新建置控制措施：**輸入新建置**控制措施，若不足請新增（控制措施可一項或多項）
殘餘風險審核：依據**控制錯施有效性**輸入 **F(威脅可能) 與 I (脆弱性利用)**（三級分為 低1 - 中2 - 高3)
點選「保存」儲存參數

企業運維服務雲平台（改善方案-改善再評鑑）

評估 新建置的改善控制措施，完成後，剩餘的風險，**須為可接受**
輸入風險可能性及弱點衝擊程度可顯示 降低之風險值
（若風險值不足以降低，則應該調整控制措施）

請記得所有分類都要**設定改善與再評鑑**

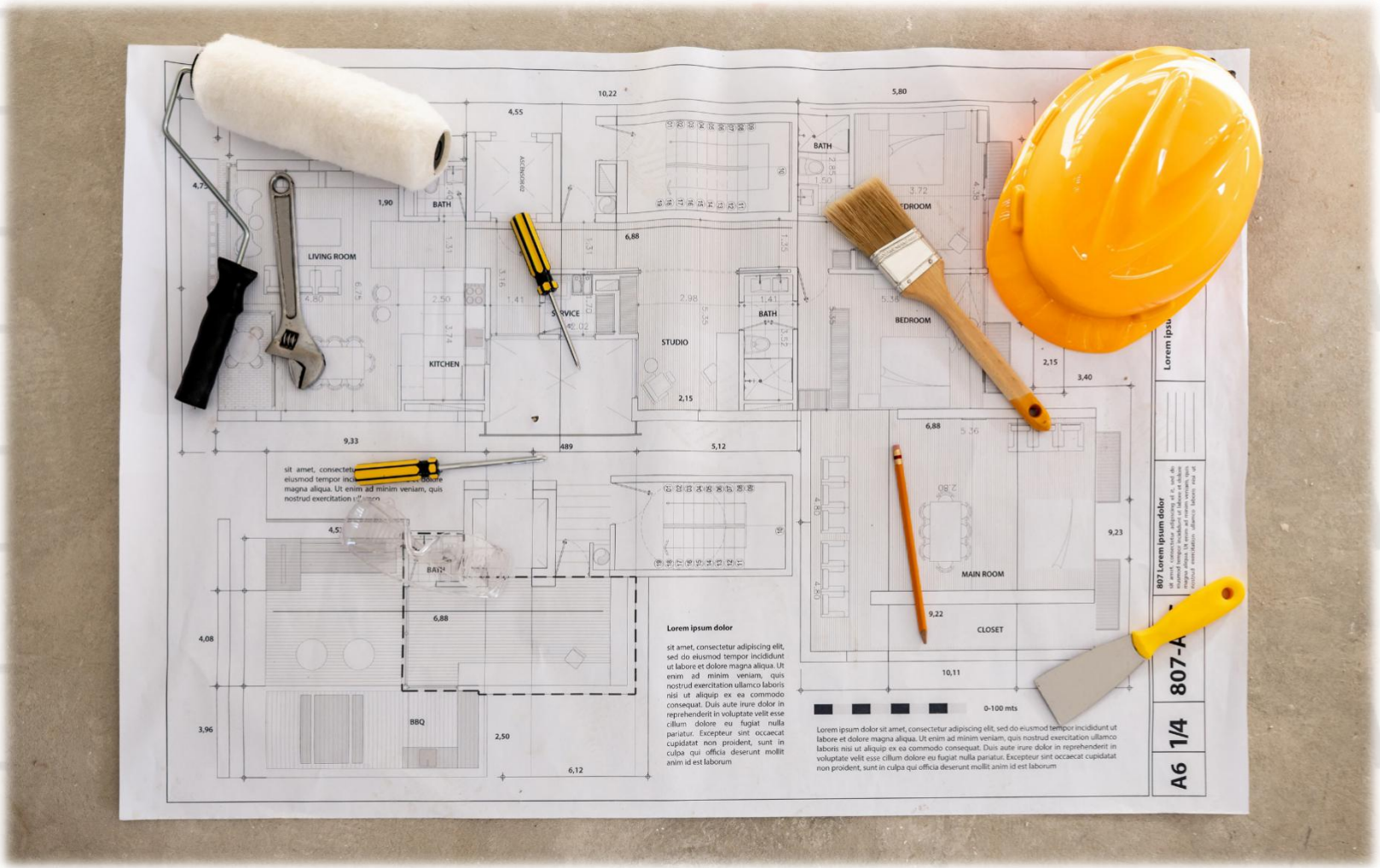
增加控制措施


資訊安全 / 資安風險評估 / 風險評估列表 / 風險分析
風險分析與改善方案
風險評估列表
風險識別項目
既有控制措施
改善控制措施
改善方案
資通系統
查詢資通系統
資產：Forti防
威脅
核心營運系統 3/3
一般資通系統/設備 1/1
設備使用多年/設備零件故障
設備/零組件
未評估設定風險
組態設定錯

企業運維服務雲平台（改善控制措施 - 新增分類）

「改善控制措施」頁面
點選「新增」
增加分類標籤

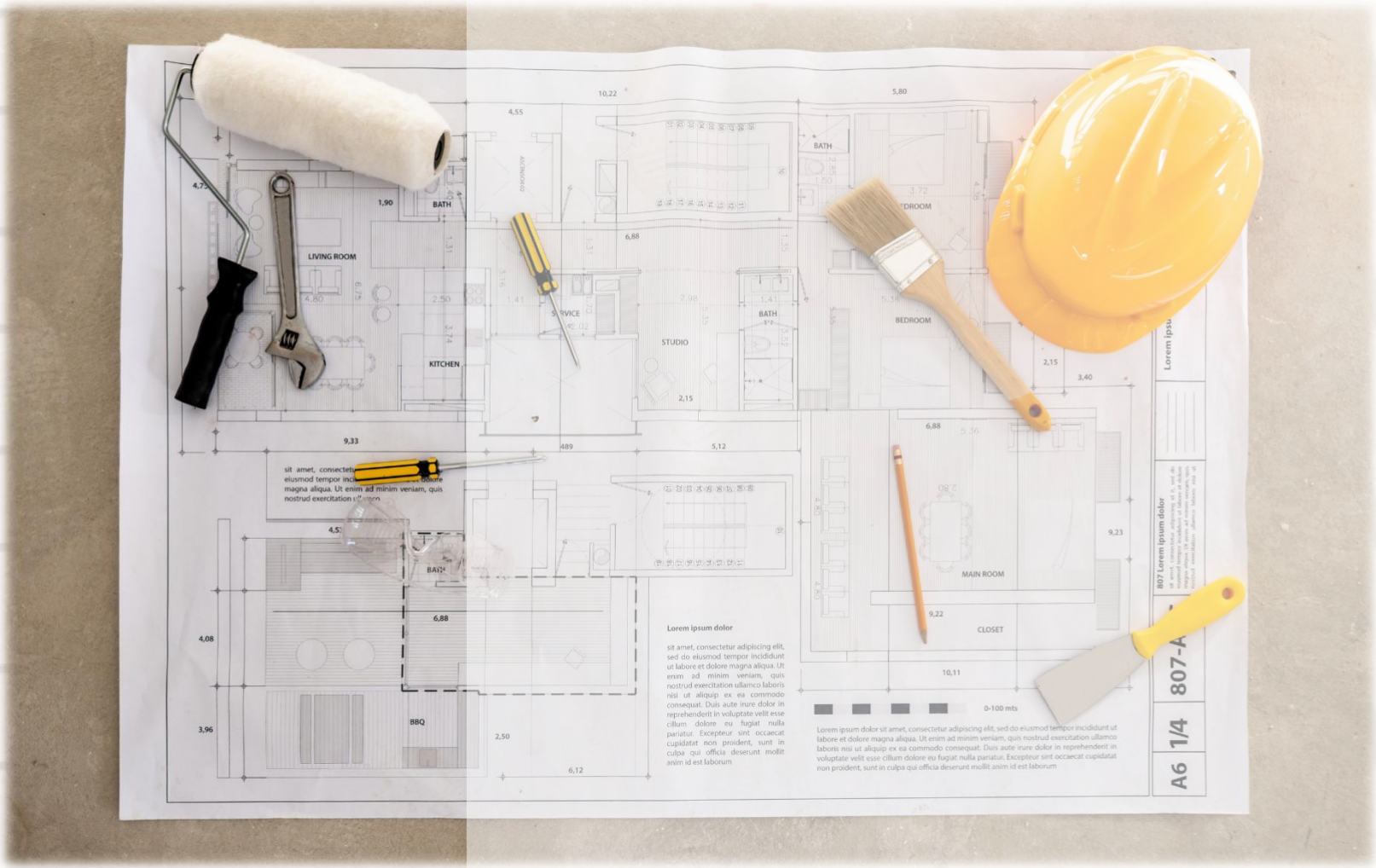
企業運維服務雲平台（改善控制措施 - 新增項目）



制訂改善計畫

企業運維服務雲平台（制訂改善計畫）

評估進度 >> 點選「4.制訂改善計畫」下方「**查看詳情**」



制訂改善計畫

企業運維服務雲平台（制訂改善計畫-計劃編輯）

於**單項**改善控制措施後**點選 [:] 為「制定計劃」**

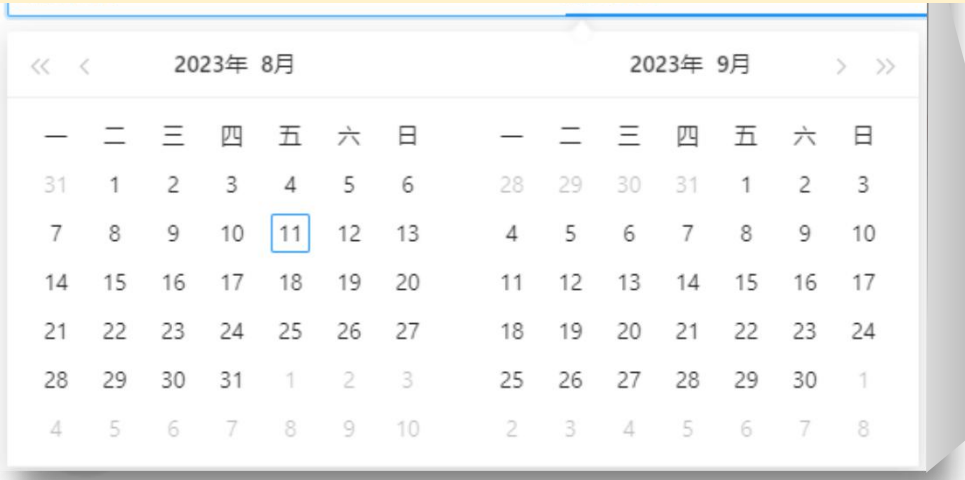
制定改善計劃

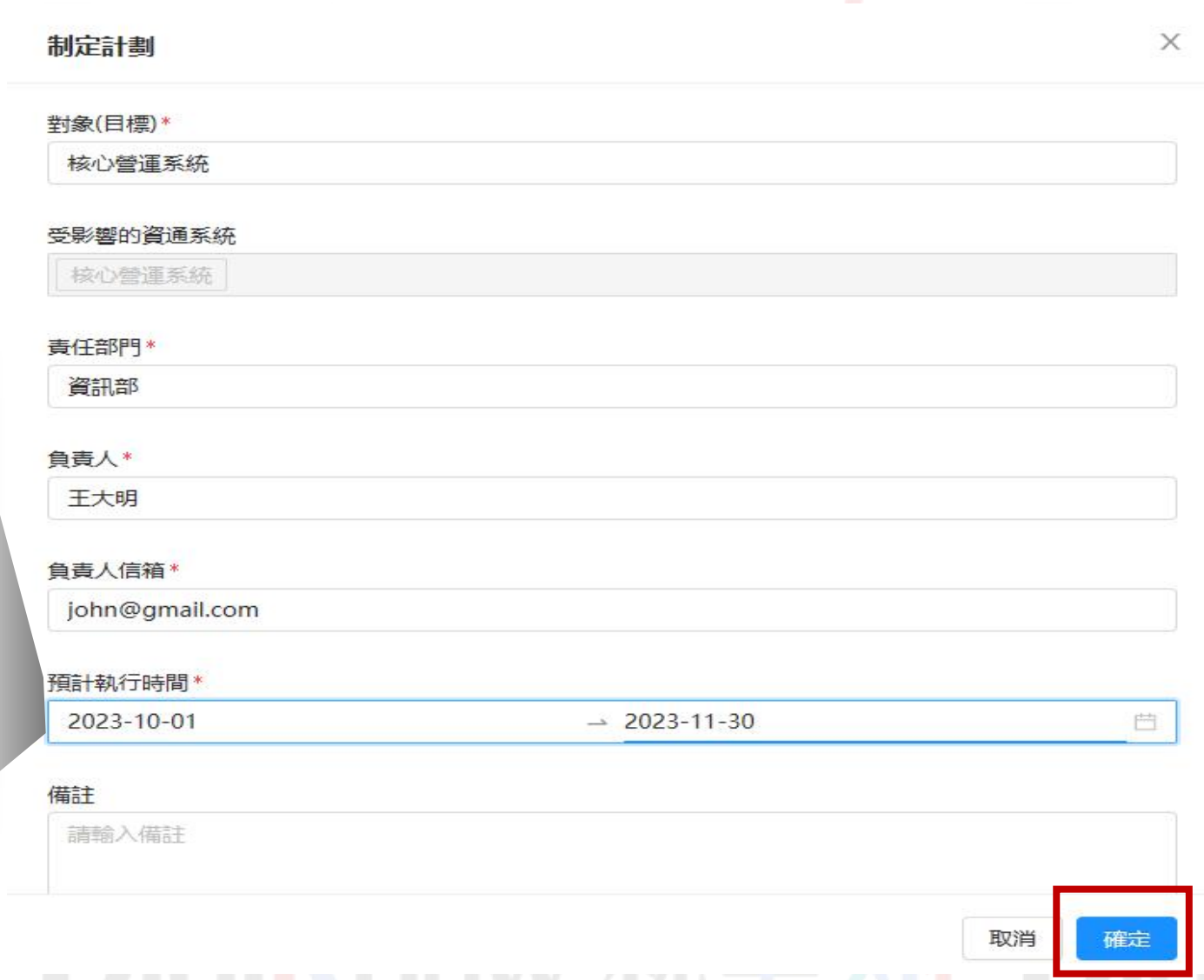
搜尋 | 下載制定改善計劃 | 提交審核

編號	控制措施	對象(目標)	受影響的資通系統	效益	計劃狀態	責任部門	負責人	負責人信箱	預計執行時間	操作
378	優先 HA備援架構	核心營運系統	核心營運系統	避免單點故障	未計劃				-	⋮
379	排程 設定檔備份管理	核心營運系統	核心營運系統	設定錯誤快速回復	未計劃				-	制定計劃

企業運維服務雲平台（制訂計畫-計畫編輯）

輸入單項風險之
對象(目標)
受影響的資通系統（不可調整）
責任部門
負責人及其信箱
預計執行日期 (開始日期 結束日期)
點選「**確定**」儲存





企業運維服務雲平台（制訂計畫-察看執行狀況）

單項改善控制措施後**點選 [:] 中「查看執行狀況」**

制定改善計劃 ∨

搜尋 | 下載制定改善計劃 | 提交審核

編號	控制措施	對象(目標)	受影響的資通系統	效益	計劃狀態	責任部門	負責人	負責人信箱	預計執行時間	操作
378	優先 HA備援架構	核心營運系統	核心營運系統	避免單點故障	已計劃	資訊部	王大明	john@gmail.com	2023-10-01-2023-11-30	⋮
379	排程 設定檔備份管理	核心營運系統	核心營運系統	設定錯誤快速回復	已計劃	資訊部	林小偉	tom@gmail.com	2023-10-01	

制定計劃

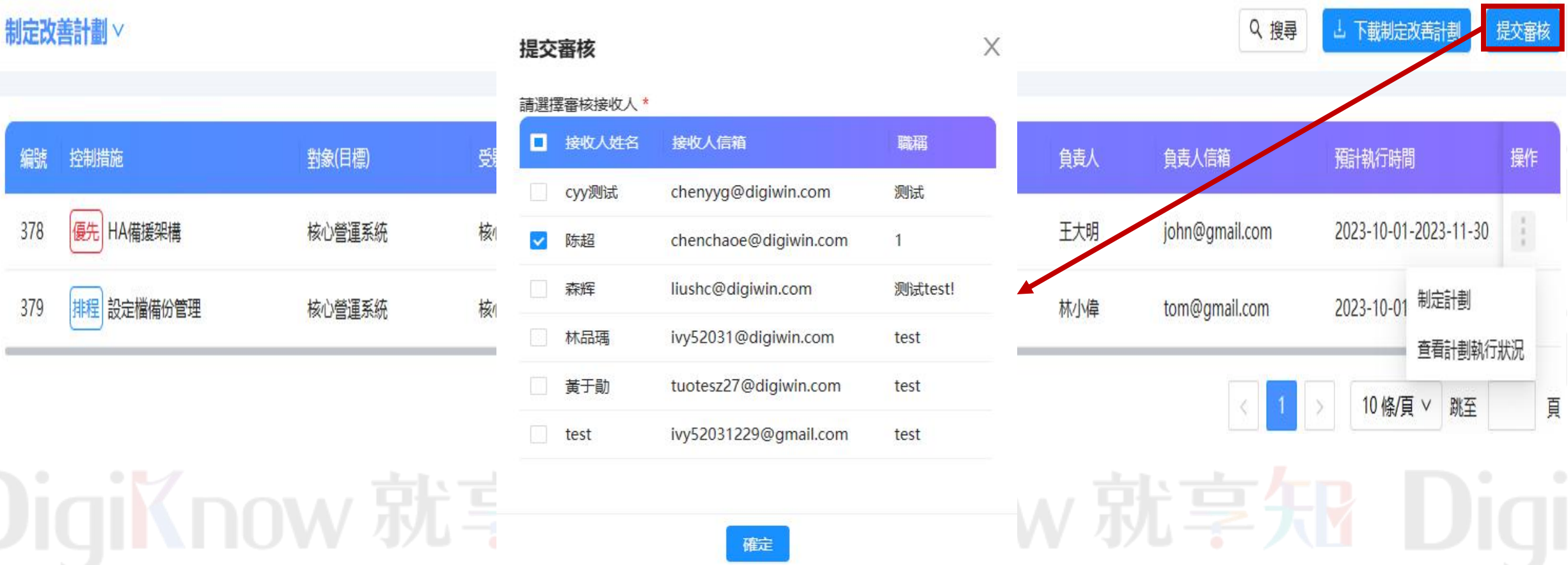
查看計劃執行狀況

1 | 10 條/頁 ∨ | 跳至 | 頁

查看計劃執行狀況 ×

操作時間	操作人	操作	備註	註記
2023-09-12 15:22	裕文	已計劃		制定計劃

企業運維服務雲平台（制訂改善計畫-提交審核）



企業運維服務雲平台（制訂改善計畫-下載）

改善編號	優先級	改善措施	對象目標	受影響的資通系統	效益	計劃狀態	責任部門	負責人	負責人郵箱	預計執行開始時間	預計執行完成時間	實際執行開始時間	實際執行完成時間
378	優先	HA備援架構	核心營運系統	核心營運系統	避免單點故障	已計劃	資訊部	王大明	john@gmail.com	2023-10-01	2023-11-30		
379	排程	設定檔備份管理	核心營運系統	核心營運系統	設定錯誤快速回復	已計劃	資訊部	林小偉	tom@gmail.com	2023-10-01	2023-11-30		

鼎新電腦

匯報完畢 敬請指教