資通安全查核重點及缺失案例分享

114年度

大綱

一、缺失態樣分析

二、重點案例分享

三、近期宣導事項

證券商資安查核之法源依據

臺灣證券交易所股份有限公司查核證券商作業辦法

第1~11條說明辦理查核依據及方式

建立證券商資通安全檢查機制

91.2.21台證（九一）稽字第003551號，修訂「建立證券商資通安全檢查機制」檢查項目，並自91.4.1日起實施。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核簡介

年度資安例查

- 檢視證券商資安防護辦理情形

選案查核

- 投資人檢舉、資通安全事件、主機共置服務

專案查核

- 特定議題對 證券市場之影響 或 檢視 整體辦理情形

TAIWAN STOCK EXCHANGE
臺灣證券交易所

資安查核簡介

資通安全檢查機制

- 辨識資安風險
- 訂定資安政策
- 配置組織資源
- 清查資訊資產
- 強化人員管理
- 監控環境設備
- 管理通訊作業
- 落實存取控制
- 控管開發維運
- 提升營運韌性
- 實作規範相符
- 納管新興科技

TAIWAN STOCK EXCHANGE
臺灣證券交易所

近三年資安查核作業

111年－113年

14個 資安 控制領域

依嚴重程度扣分

(每年查核約50間)

☑未制定 規範
嚴 重 缺 失（扣 10 分）

☑未依規定 執行
中 等 缺 失（扣 5 分）

☑未留下 操作記錄
輕 微 缺 失（扣 2 分）

追蹤改善

最近3年
150份查核報告
(736項缺失)

資料治理
缺失態樣分類共 65 類

TAIWAN STOCK EXCHANGE
臺灣證券交易所

114年資安查核作業

01/01 – 09/30

14個 資安 控制領域

依嚴重程度扣分

☑未制定 規範
嚴 重 缺 失（扣 10 分）

☑未依規定 執行
中 等 缺 失（扣 5 分）

☑未留下 操作記錄
輕 微 缺 失（扣 2 分）

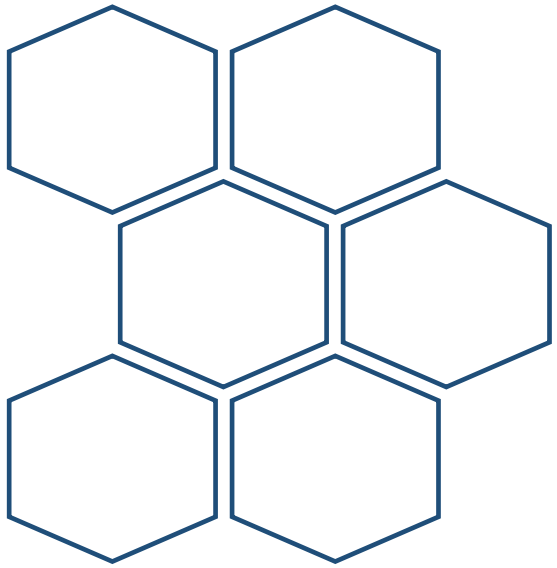
目前已結案件
共 32 件

目前缺失數量
共 86 項

缺失態樣分類
65 類增加至 94 類

TAIWAN STOCK EXCHANGE
臺灣證券交易所

缺失態樣分析



TAIWAN STOCK EXCHANGE
臺灣證券交易所

控制領域分布狀況

近三年缺失態樣分析

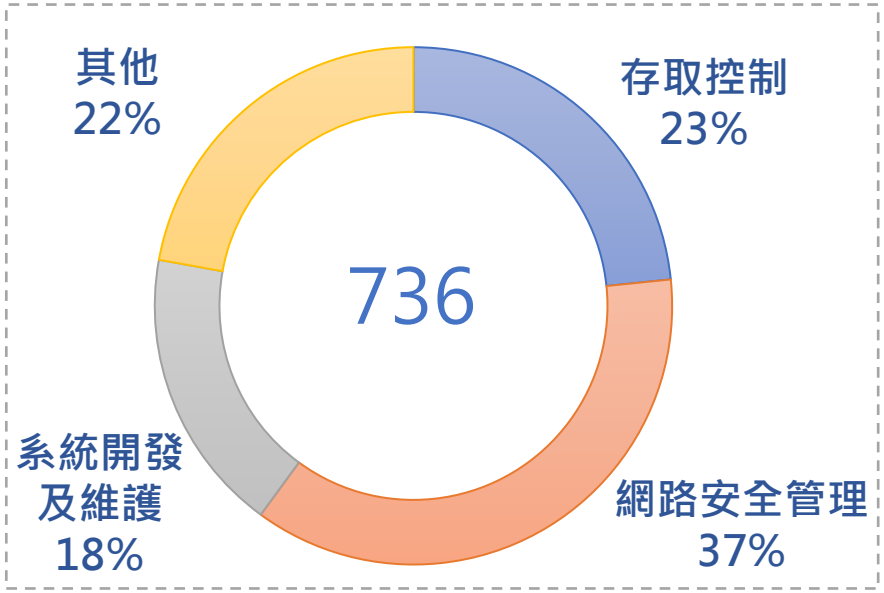
111年 – 113年

● 控制領域缺失數量

控制領域	113年	112年	111年
存取控制	56	42	74
網路安全管理	54	95	121
系統開發及維護	31	48	52
電腦系統及作業安全管理	12	24	15
營運持續管理	11	12	9
新興科技應用	5	8	7
實體與環境安全	4	2	6
資產分類與控制	2	6	7
資訊安全政策	2	1	12
符合性	2		1
風險評鑑與管理	2	7	3
主機共置服務管理	1	1	
安全組織			1

缺失主要集中在
TOP3控制領域

合計占比 達到78%



TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失增減趨勢

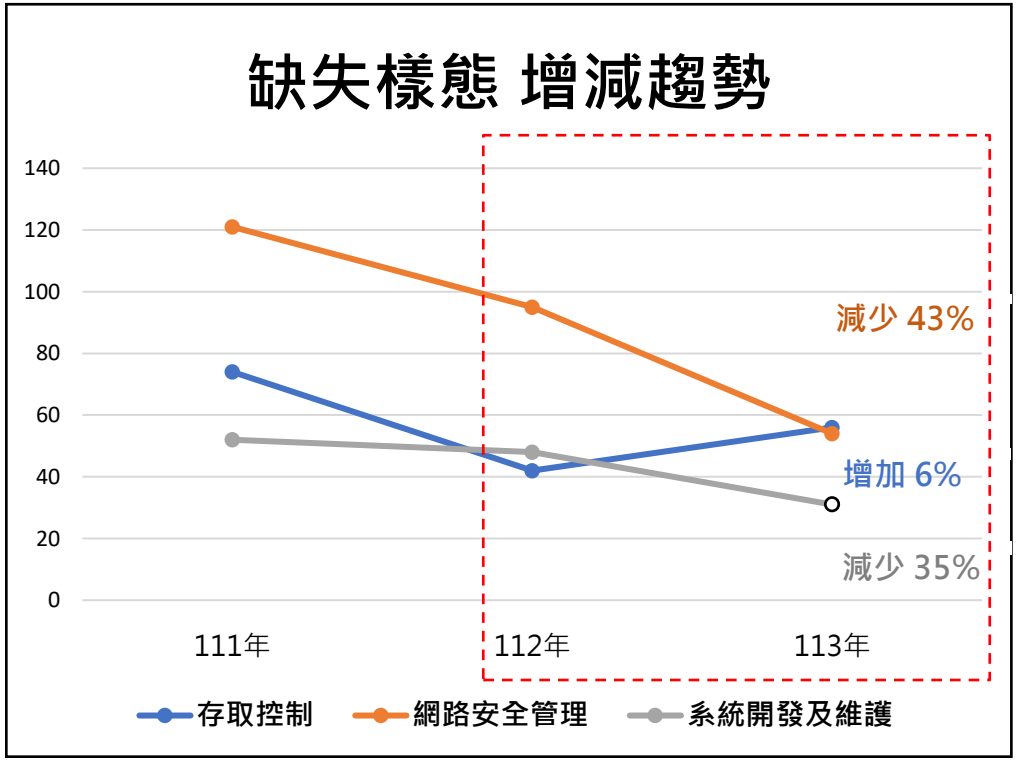
近三年缺失態樣分析

111年－113年

● 控制領域缺失數量

控制領域	113年	112年	111年
存取控制	56	42	74
網路安全管理	54	95	121
系統開發及維護	31	48	52
電腦系統及作業安全管理	12	24	15
營運持續管理	11	12	9
新興科技應用	5	8	7
實體與環境安全	4	2	
資產分類與控制	2	6	7
資訊安全政策	2	1	12
符合性	2		1
風險評鑑與管理	2	7	3
主機共置服務管理	1	1	
安全組織			1

主要缺失數量近年呈下降趨勢

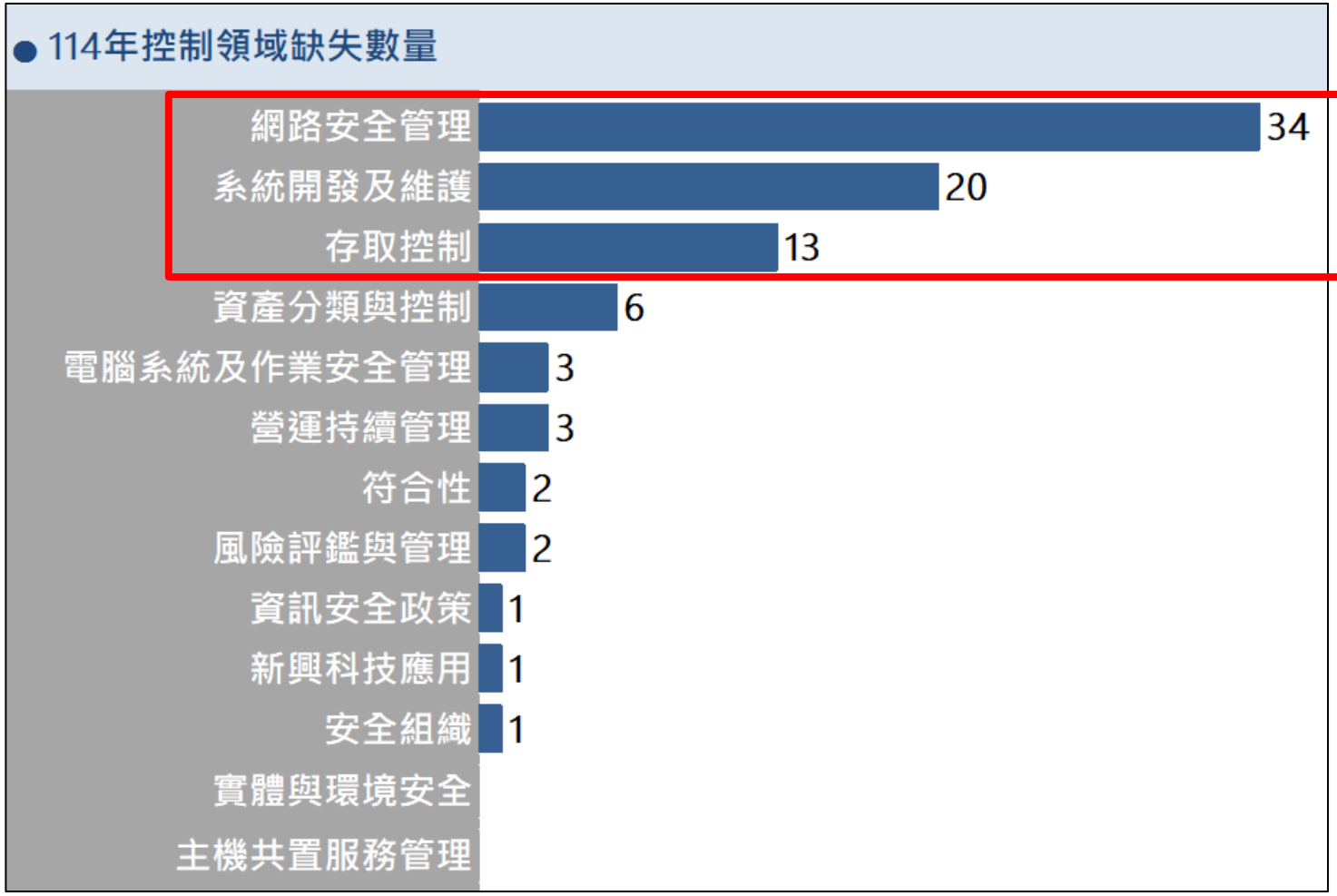


TAIWAN STOCK EXCHANGE
臺灣證券交易所

控制領域分布狀況

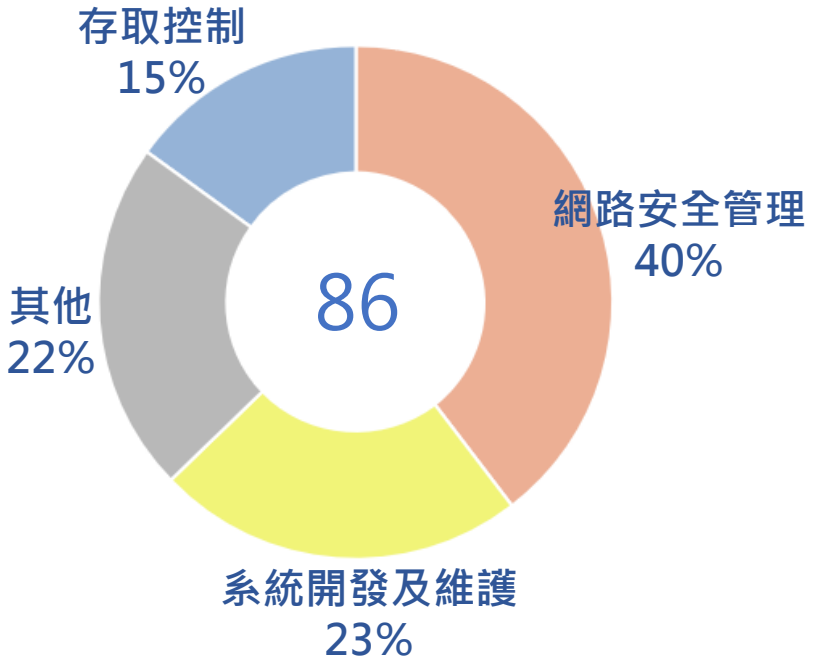
114年缺失態樣分析

114/01/01 – 114/09/30



缺失主要集中在
TOP3控制領域

合計占比 達到78%



TAIWAN STOCK EXCHANGE
臺灣證券交易所

缺失分類

114年缺失態樣分析

114/01/01 – 114/09/30

風險評鑑與管理	
1	未識別適用範圍
2	未確定可接受風險
3	**未進行定期評鑑**
4	**未評估可容忍中斷時間**
資訊安全政策	
5	未訂定資訊安全政策
6	資訊安全政策未臻完善
7	政策未經核准或無轉知
8	**政策未每年評估**
9	政策評估未臻完善
10	資安整體執行情形未完善
11	未辦理資安防護分級表
12	未持續驗證系統有效性
安全組織	
13	未依規定適當配置
14	未依規定指定資安長
15	未依分級進行資安宣導課程
16	資安能力配置不足
17	權責未明確劃分
18	**未依規定取得資安證照**
資產分類與控制	
19	**資訊資產未列清冊**
20	未訂定資訊分級規範
21	**未定期檢視分級妥適性**
22	未依規定規範保存期限
人員安全	
23	未填具保密切結書
24	離職未取消識別資料
25	未定期對員工辦理宣導
26	未適當進行教育訓練
27	未設置電腦稽核人員
實體與環境安全	
28	機房未設置門禁管制
29	未有防火設施並定期檢驗
30	天然災害未列入考量
31	未含UPS及發電機
32	未訂報廢程序及留存紀錄
33	未定期審查門禁管制權限
網路安全管理	
34	**網路系統安全評估未完善**
35	**網路設備之安全管理未完善**
36	**網路傳輸及連線安全管理未完善**
37	多因子驗證未完善
38	身分認證與憑證管理未完善
39	**電腦病毒及惡意軟體之防範未完善**
40	網路系統功能檢查未完善
41	**公司未提供API服務規範**
42	**網際網路下單服務品質未完善**
43	網路攻擊防護機制導入及安全性檢測未完善
44	帳號登入或異常態樣通知未完善
45	**異常 IP 登入之監控與預警未完善**
電腦系統及作業安全管理	
46	電腦設備之管理未完善
47	**電腦作業系統環境設定及使用權限設定未完善**
48	**電腦媒體之安全管理未完善**
49	電腦操作管理未完善
50	未配置適足容量之電腦系統
51	未定期進行評估及壓力測試
存取控制	
52	未訂定資訊系統存取控制相關規定
53	**權限管理未執行完善**
54	**密碼管理不當**
55	**電腦稽核紀錄管理不適切**
56	**資料輸入管理不當**
57	資料輸出未妥善管理
系統開發及維護	
58	**應用系統規畫時未納入資安需求**
59	**輸入資料未確認正確性**
60	未使用合法軟體
61	**委外廠商管理不當**
62	**程式維護未依據辦理**
63	文件與手冊未適當維護
64	應用系統未指派專人負責
65	應用系統異動管理不當
66	**未定期辦理弱點掃描**
67	程式原始碼安全規範未確實執行
68	**行動應用程式安全管理不當**
69	核心系統頁面顯示不當
70	**未進行源碼掃描**
71	異業合作問題
營運持續管理	
72	**未明確訂定復原程序、執行及記錄**
73	故障程序未定期測試
74	未建立備援措施
75	未擬訂營運持續計畫
76	**未訂定資訊安全訊息通報機制**
77	未函報資安事故
78	未明訂DDoS相關程序
79	未辦理相關資安防護事宜
80	未辨識風險情境
81	服務中斷未於容忍時間恢復
82	委外作業未定期提供回復計畫
符合性	
83	**未定期辦理資安查核作業**
84	追蹤改善情形未完全改善
新興科技應用	
85	雲端服務未妥善管控
86	社群媒體管理不當
87	**行動裝置程序未明確制定**
88	未明訂物聯網規範與管理辦法
89	遠距辦公規範不當
90	深度偽造未完善
其他	
91	資訊提供作業缺失
主機共置服務管理	
92	主機共置用戶服務系統未清點及留存紀錄
93	未定期盤點設備
94	未依規定建立及落實檢查機制

現行資安查核缺失態樣分類共 94 類。

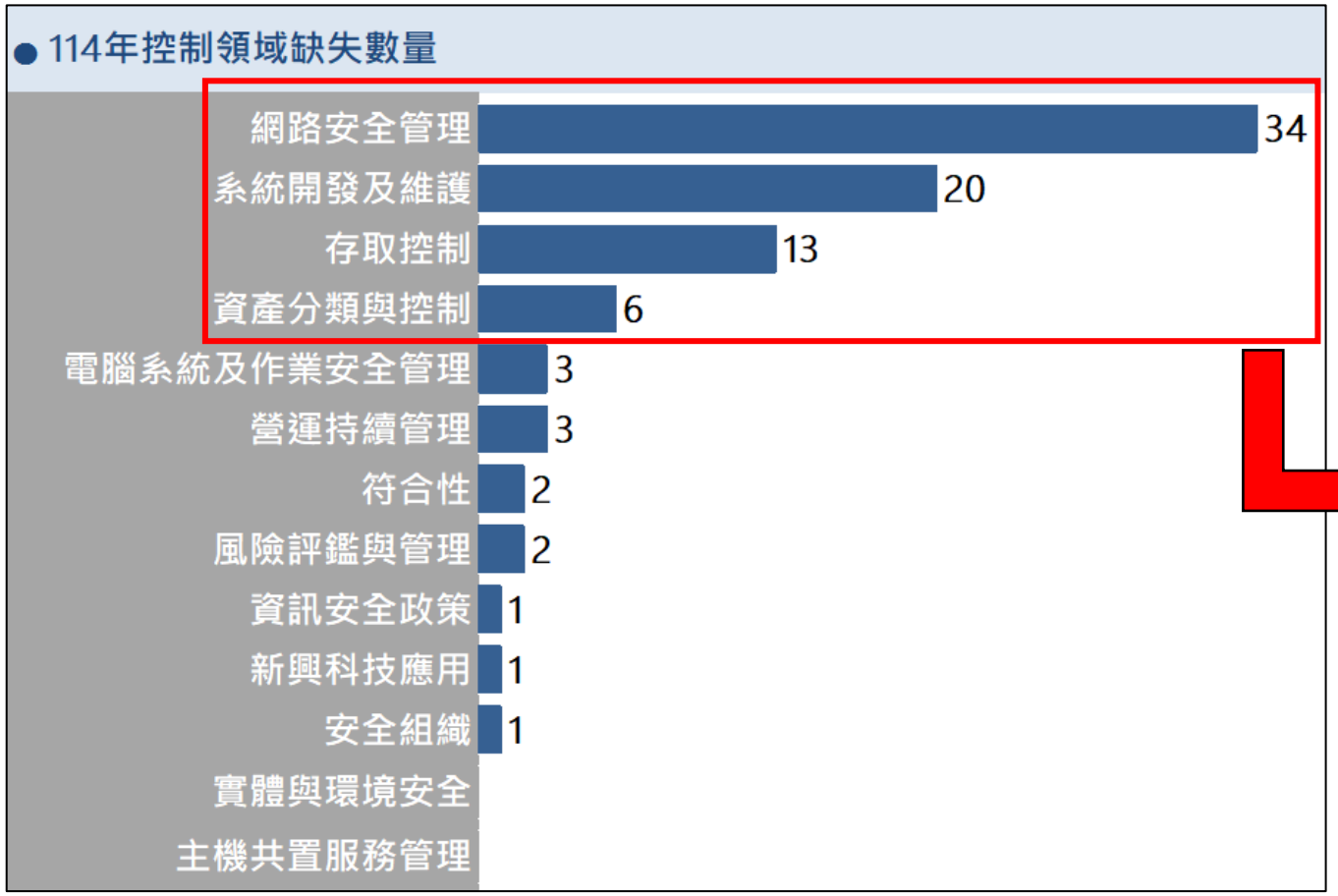
114 年目前已結案件之 86 項缺失種類共 30 類。(如黃底標示)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

114年 缺失種類 TOP10

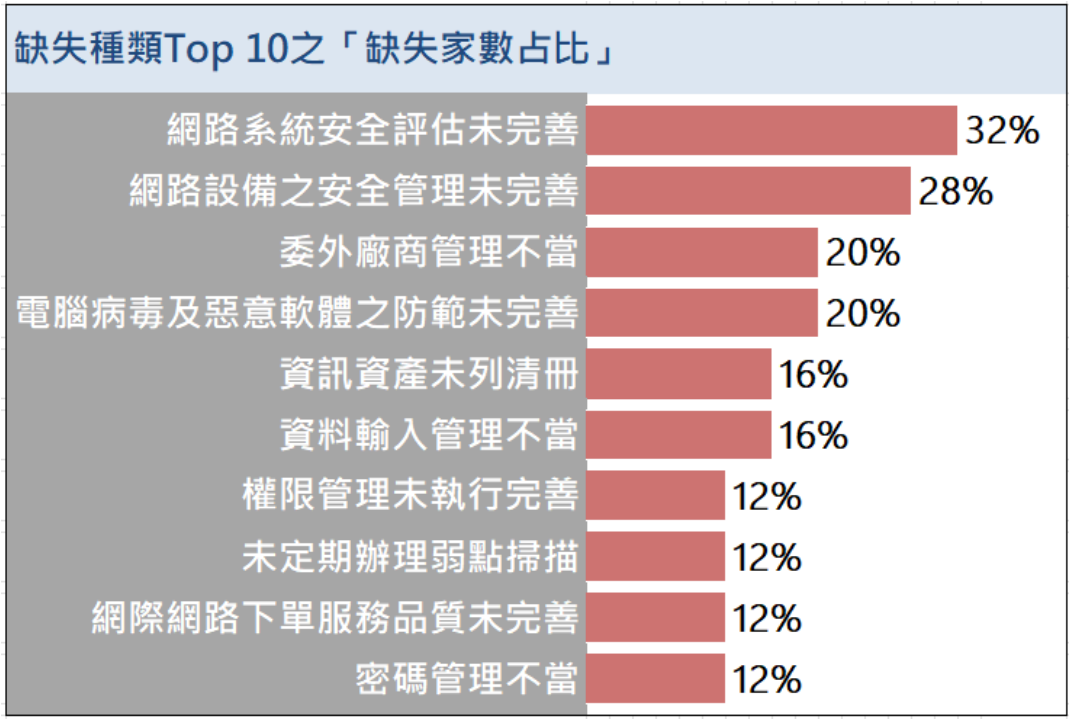
114年缺失態樣分析

114/01/01 – 114/09/30



114年已查核券商之缺失種類Top 10

(114年已查核券商家數共 25 家)



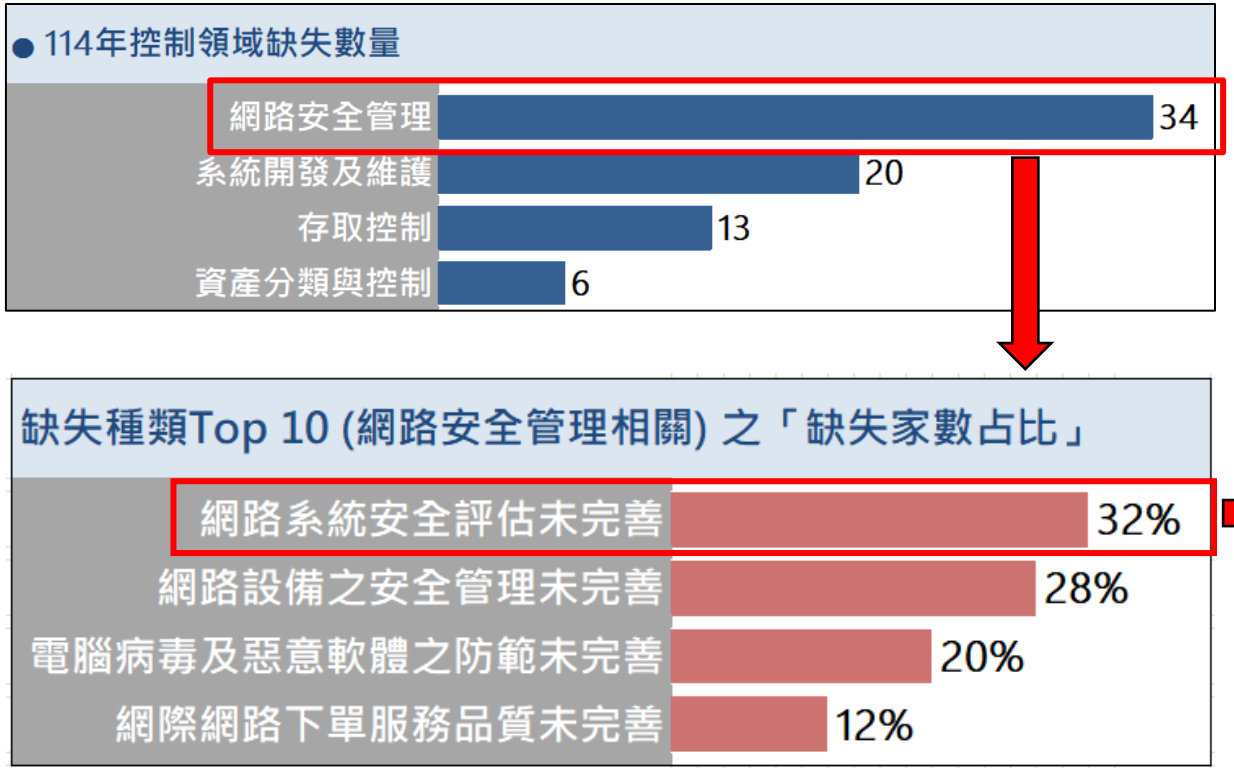
「缺失家數占比」=有該類缺失的家數 / 114年已查核家數

TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30



1. 部分原廠終止支援服務之網路設備無適當管理作業，包含風險評估紀錄及處理措施、汰換計畫及定期追蹤。
2. 遠端連線維護未進行適當之控管(如：留存連線紀錄或重設其登入之密碼等)。
3. 公司網路未有適當區隔機制
4. 未依規定期評估網路系統安全(如伺服器、防火牆等)並留存相關紀錄。
5. 未定期或適時修補網路運作環境之安全漏洞（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等），並留存相關文件。

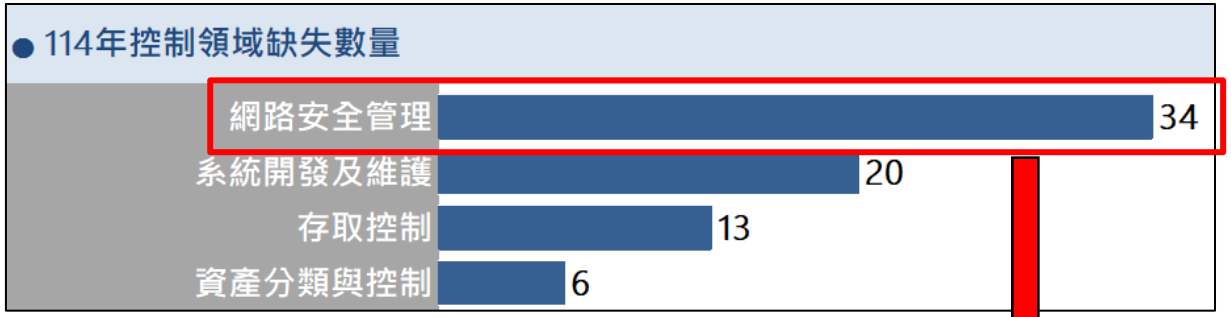
網路設備與系統之安全性更新狀態應確實定期執行評估或進行更新，整體網路環境之連線存取限制亦應妥適管控。

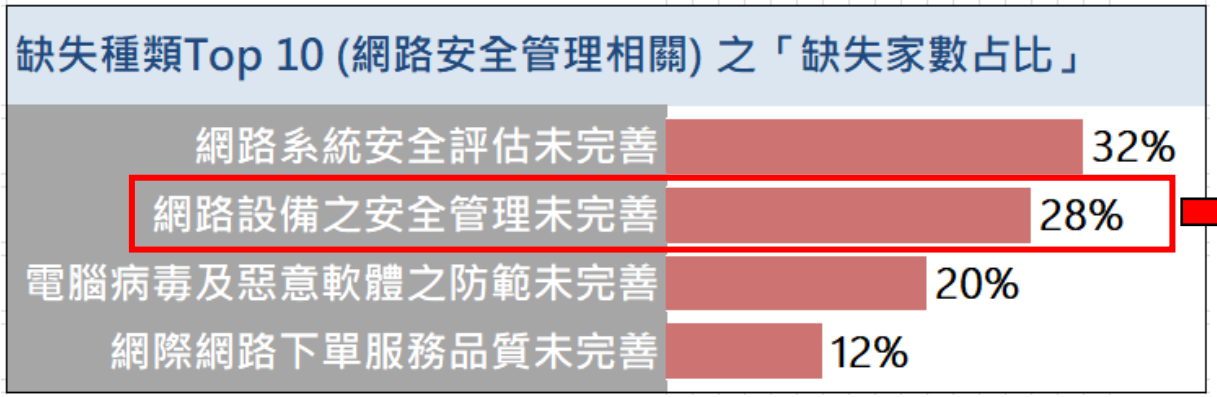
TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30





1. 公司建立網路設備規則未以最小授權及正面表列為原則。
2. 未每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。
3. 系統未依最小原則開啟必要之服務及程式。
4. 防火牆系統之設定未經權責主管之核准。

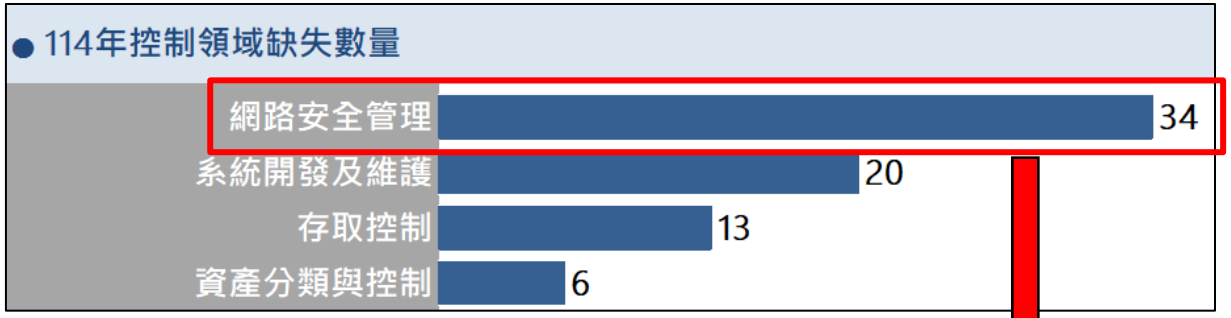
防火牆及主機系統應僅限開啟必要之連線存取設定或服務，並定期檢視調整。

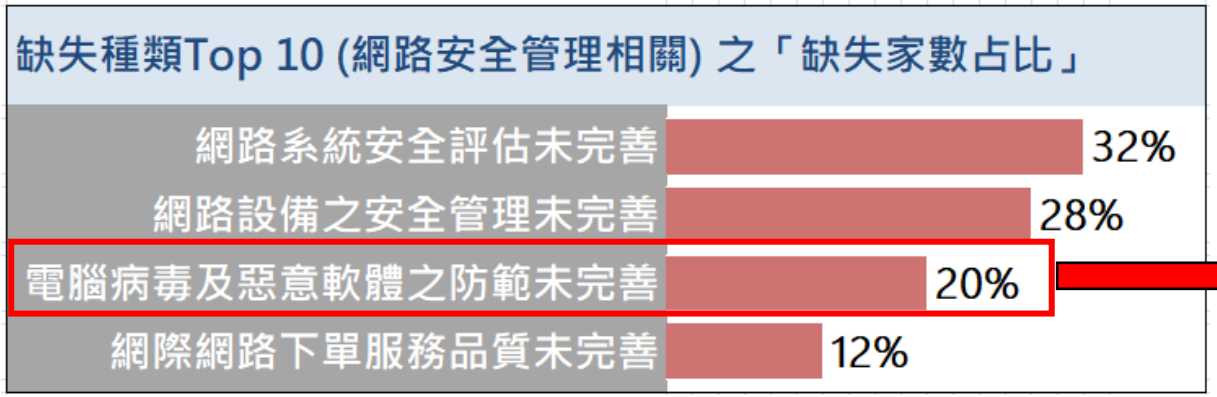
TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30





1. 社交工程未執行或未落實追蹤輔導。
2. 個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦未安裝防毒軟體並及時更新程式及病毒碼。
3. 未訂定軟體安裝白名單或未臻完善。

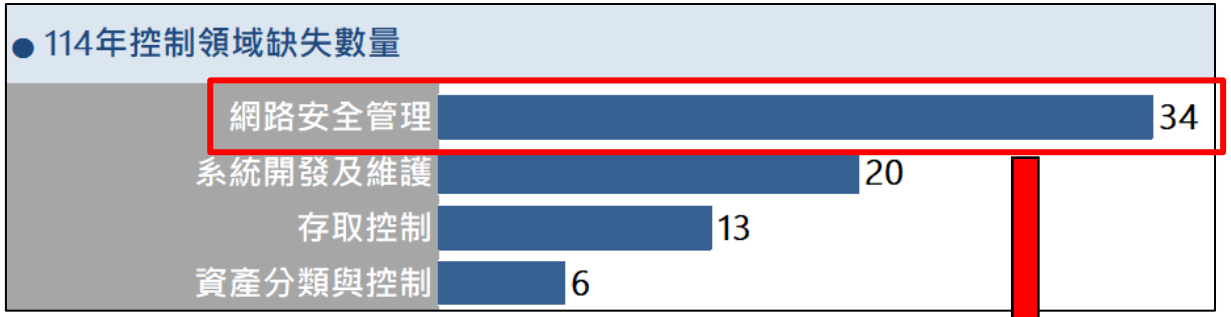
應定期強化使用者端之設備安全防護及個人網路安全意識。

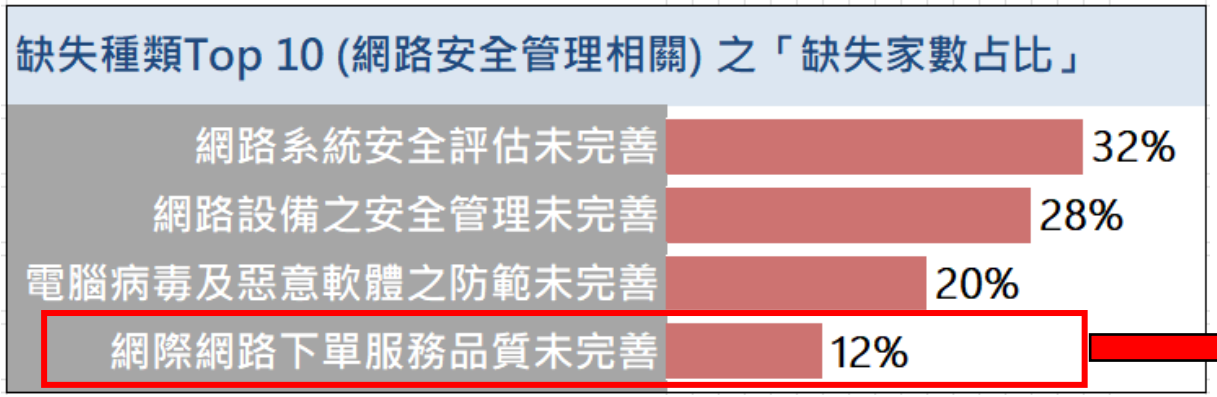
TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30





1. 網際網路下單服務品質標準未依規訂定或未臻完善(如缺少系統正常營運時數、硬體效能使用情形等可用性指標)。

2. 網路下單系統交易穩定性或系統可用性不足，或提供客戶服務(如:報價資訊、委託下單、帳務查詢、技術分析、即時庫存、資券配額及整戶維持率等)之資訊錯誤，致未符合服務品質相關標準。

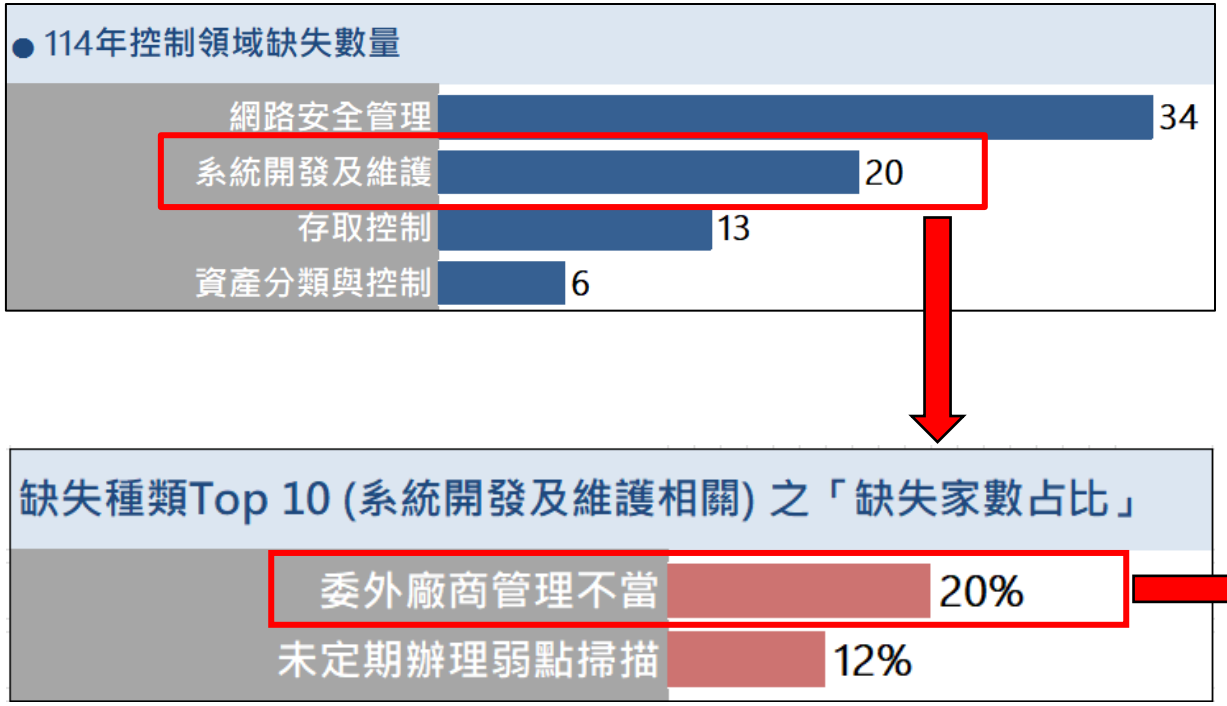
網路下單服務品質水準應訂定妥適之標準，並確實定期檢視達成情形。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30



1. 未於資訊委外期間每年至少一次對該委外資訊廠商進行查核。
2. 未依規定與委外廠商簽署保密切結書。
3. 評選資訊服務供應商未留存相關文件紀錄。
4. 委外資訊服務供應商未定期提交服務水準報告。
5. 規劃委外作業未進行相關風險評估。

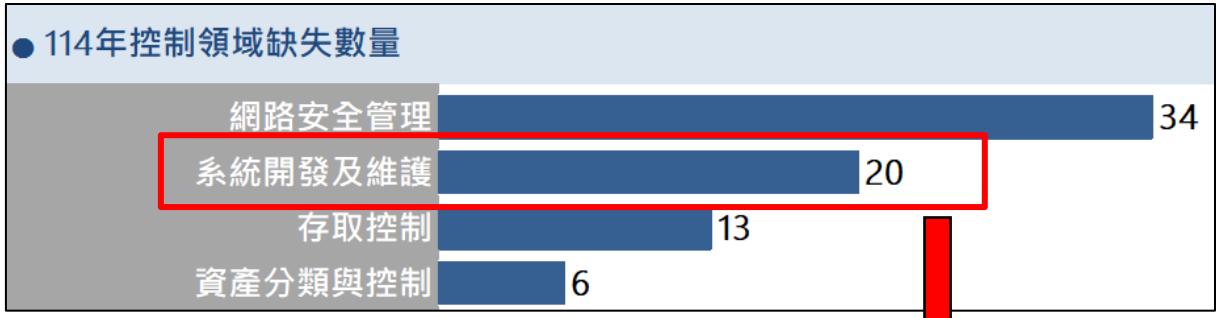
委外資訊作業應於簽約前妥善規劃與評估，於合約期間內定期監督，於合約終止後確實回收權限。

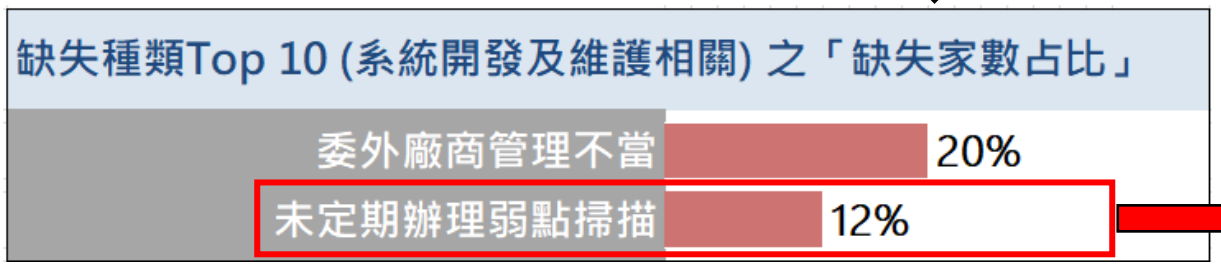
TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30





1. 未依規辦理定期系統弱點掃描作業。
2. 未對弱點掃描所辨識出之潛在系統弱點，評估其風險或安裝修補程式、執行複測，並留存紀錄。

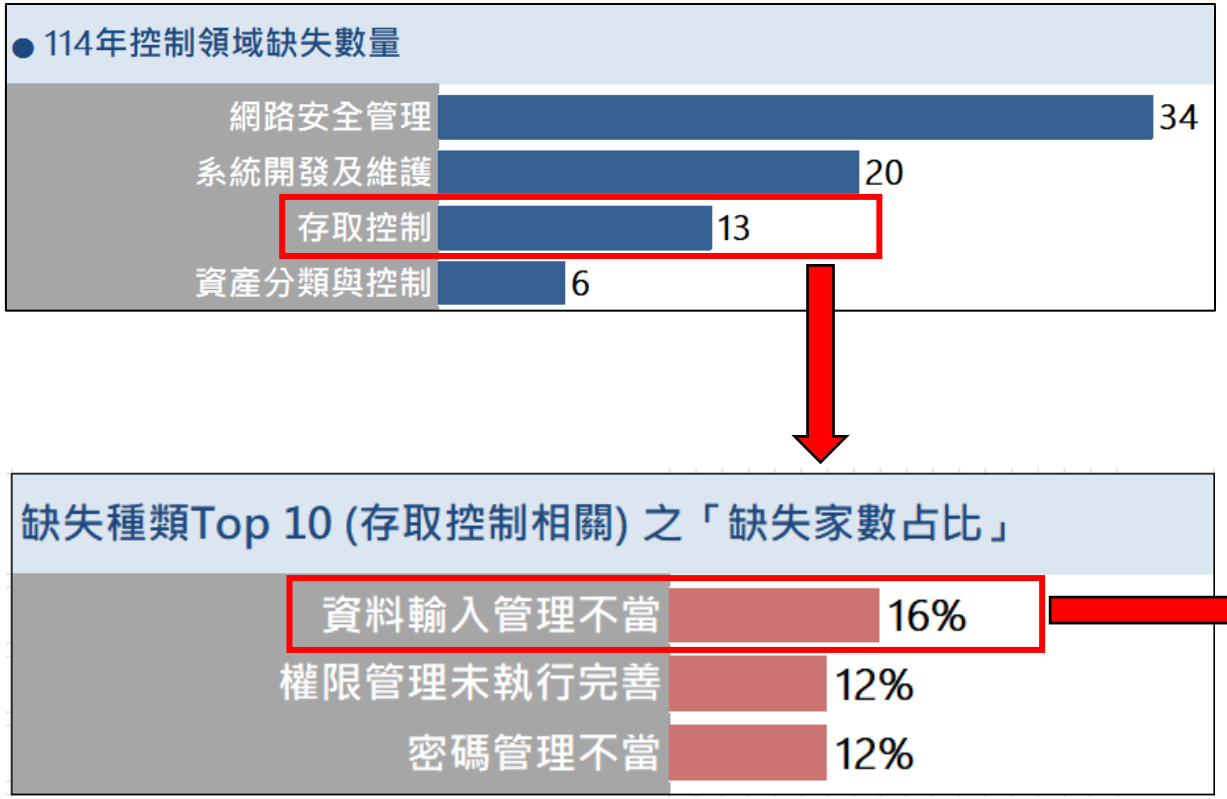
資訊服務系統應定期辦理弱點掃描，並依資訊資產風險評鑑等結果評估進行弱點修補、規劃升級汰換，或採取其他補償性風險控制措施。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30



1. 未定期盤點確認所保有之個人資料現況。
2. 未依「個人資料保護法」對客戶及公司內部人之個人資料進行妥善之蒐集、處理或利用。
3. 於系統測試環境使用含個資之正式資料進行測試時，未進行去識別化處理，或未於測試完畢後確實清除相關資料。

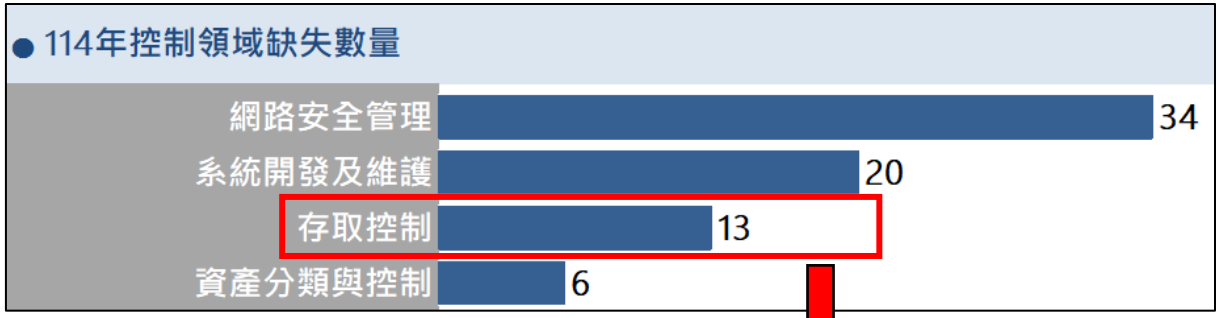
機敏資料之取得、使用、儲存、刪除皆應妥適管控操作權限及流程，並完整留存相關紀錄。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30



1. 應定期（至少每半年一次）審查資通系統帳號及權限之適切性，並視審查結果停用資通系統內久未使用之閒置帳號。

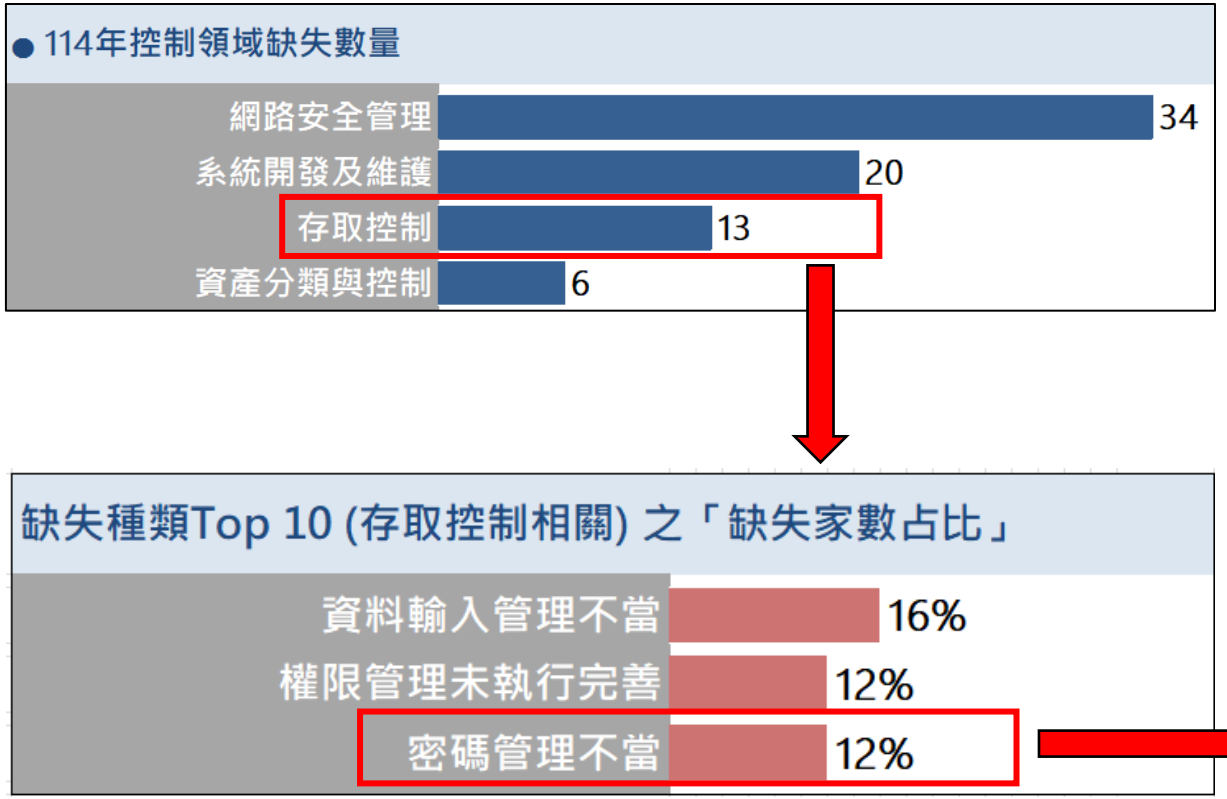
作業系統及應用系統之帳號權限皆應定期進行盤點，僅保留必要之帳號與權限，針對核心系統高權限帳號另應搭配多因子登入驗證等存取管控措施。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30



1. 資訊系統未定期更改密碼。
2. 密碼輸入錯誤次數達5次者，未中斷連線及鎖定該帳號至少15分鐘不允許該帳號繼續嘗試登入，並留存紀錄。
3. 資訊系統未依規設定密碼複雜度 (長度至少6個字元、包含文數字或符號、至少每三個月變更一次)，或未於系統設計受限而無法符合複雜度要求時，採取補償性風險控制措施。

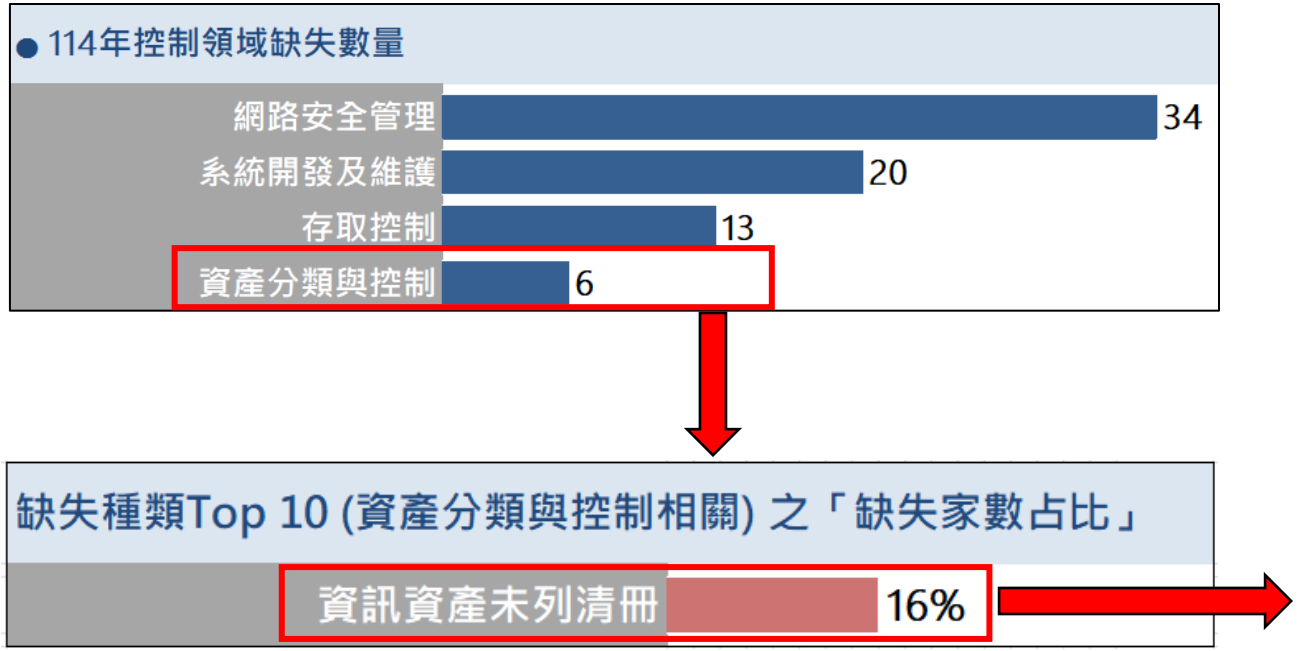
資訊系統密碼管理包含複雜度設定、加密儲存方式、交付與變更流程、鎖定與解鎖機制等，應依規對各類資訊系統採取適當之管控。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

主要缺失領域分析

114年缺失態樣分析

114/01/01 – 114/09/30



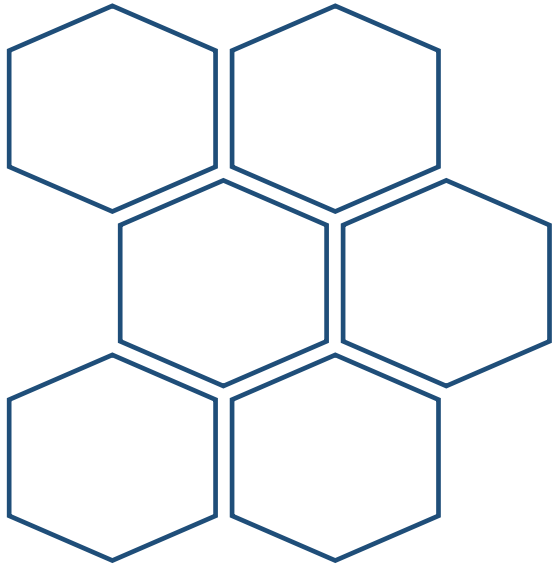
1. 未編列資訊資產清冊或盤點內容未臻完善。

1. 資訊資產清冊應包含軟體、硬體、場地及資料等類別，並應對資訊資產之資料或文件的保存期限進行規範，於保存期限到期後進行刪除與銷毀。

2. 資通系統應進行分級，至少區分核心與非核心系統，並定期檢視(每年至少一次)分級妥適性。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

重點案例分享



TAIWAN STOCK EXCHANGE
臺灣證券交易所

近期資安重大事件案例(1)

基礎設施服務商異常

事件原因：複委託之上手證券商網路異常，致無法進行交易

影響範圍：造成相關證券商投資人之複委託無法正常下單

處理措施：要求上手證券商強化持續營運作業

TAIWAN STOCK EXCHANGE
臺灣證券交易所

近期資安重大事件案例(2)

接收回報資訊異常

事件原因：經紀業務下單主機交易訊息格式錯誤，導致證券交易中台系統接收回報資訊異常，造成接收回報程式無法提供服務，無法進行交易

影響範圍：造成相關電子交易系統交易回報資料異常

處理措施：要求資料修改須進行必要驗證以確認變更作業之正確性
優化程式(避免因程式錯誤影響系統運作)

TAIWAN STOCK EXCHANGE
臺灣證券交易所

近期資安裁罰事件案例(1)

電子下單平台無法登入

事件原因：期貨行情劇烈震盪，大量投資人登入下單平台，
欲確認持有部位，並進行委託，人數達平日之2倍，
造成系統服務異常

影響範圍：查詢帳務資料回應緩慢、投資人登入異常

強化措施：評估整體資源配置（前、中、後台、憑證系統、資料庫）
優化程式效能（放寬可允許連線數、調整資料庫連線機制）
加強故障復原程序 與 壓力測試
提高警戒標準

TAIWAN STOCK EXCHANGE
臺灣證券交易所

近期資安裁罰事件案例(2)

委外廠商管理不當

事件原因：證券商對測試系統與正式系統未隔離，並提供廠商高權限帳號及遠端登入功能，廠商於盤中進行系統下單測試。

影響範圍：造成1.4億元鉅額錯帳，回補後虧損113萬

處理措施：落實網段區隔
加強上線管控作業

TAIWAN STOCK EXCHANGE
臺灣證券交易所

近期資安裁罰事件案例(3)

未落實資安防護致惡意程式攻擊

事件原因：證券商對外系統遭受攻擊。

影響範圍：部分內網主機遭植入惡意程式。

處理措施：停用多部內部主機上特定高權限帳號
落實網段區隔
加強異常連線監控
弱點程式修補

TAIWAN STOCK EXCHANGE
臺灣證券交易所

近期宣導事項

TAIWAN STOCK EXCHANGE
臺灣證券交易所

推動證券商導入零信任架構相關規劃

先行機構導入分享研討會	挑選之導入零信任**先行示範單位**，將零信任架構導入經驗與其他證券商分享。
參考指引解析說明會	依金管會發布「金融業導入零信任架構參考指引」，對**框架概念、導入策略、建議實作參考原則分級**進行說明。
零信任系列說明會	根據五大支柱共36個參考原則，分享**導入實務**及**案例**，並提供導入零信任架構相關諮詢**常見問題**及**解決方向**。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

證券期貨市場資通安全事件通報應變作業注意事項

初步通報	應於知悉事件 30 分鐘內進行初步通報。
正式通報	查明事實後，應於24小時內轉為正式通報。
解除通報	事件處理完成後，應於3日內解除通報。

TAIWAN STOCK EXCHANGE
臺灣證券交易所

簡報結束
敬請指導