

CYBERSEC 2024
臺灣資安大會

5/14_{Tue} — 5/16_{Thu}
臺北南港展覽二館

**Generative
Future**

上市櫃資安標竿論壇

在內部控制制度導入 『上市上櫃公司資通安全管控指引』

主講人：彭偉鎧

新聞稿



金管會持續推動相關措施精進上市（櫃）公司資通安全管理

2024-03-05

為強化上市（櫃）公司資訊安全管理機制，金管會已要求上市（櫃）公司於發生重大資安事件時，應即時發布重大訊息及損失達一定金額應召開重大訊息記者會；自111年起應於年報敘明資安政策、具體管理方案、投入資安管理之資源、重大資安事件之損失與可能影響及因應措施等資訊；依資本額規模等分階段完成設置資安長、專責主管及人員；訂定資通安全管控指引供公司參考；推動依風險等級分期加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)共享資安情資，以達資安聯合防禦之效能。

鑒於資訊化時代資通安全管理已成為公司營運之重要議題，並攸關投資大眾權益，為進一步強化上市（櫃）公司資通安全，金管會近期督導證交所及櫃買中心(下稱二單位)從「強化監理」及「協助與輔導」二大面向推動資安治理相關精進措施，包括檢視修正「上市上櫃公司資通安全管控指引」、提高資訊安全內部控制查核比例及追蹤缺失改善情形、修訂重大訊息問答集明確規範資安事件之「重大性」標準、落實企業對子公司資訊安全之監督與管理、強化資訊安全人員教育訓練、分享資訊安全事件案例、持續推動加入TWCERT/CC分享資安事件之情資、取得資安標準國際認證及取得外部驗證等，以協助企業提升資安自身防禦能力。

金管會亦將持續督導二單位，蒐集國內外資安風險重大議題及案例、技術發展及規範等資訊，以完善上市（櫃）公司資通安全強化措施。

聯絡單位：證券期貨局證券發行組

聯絡電話：2774-7129

金管會資安治理兩大面向

強化監理

檢視修正
「上市上
櫃公司資
通安全管
控指引」

提高資訊
安全內部
控制查核
比例及追
蹤缺失改
善情形

修訂重大
訊息問答
集明確資
安事件之
「重大性」
標準

落實企
業對子
公司資
訊安全
之監督
與管理

協助與輔導

強化資
訊安全
人員教
育訓練

分享資
訊安全
事件案
例

持續推
動加入
TWCE
RT/CC
分享資
安事件
之情資

取得資
安標準
國際認
證及取
得外部
驗證

何謂『指引』？

- 指引是「**引導方向**」，所以『指引』**並非是辦法或法規**。
- 因此這份指引只是一個參考用的規定，**並非具有強制性**。
- 所以一般的公發公司在了解之後，在制訂內部控制制度時，就應該要思考一下指引內的要求，應該怎麼訂入內控制度之內。

上市上櫃公司資通安全管控指引：

- 共分九個章節，36條資通安全管控指引

《第一章 總則》

《第二章 資通安全政策及推動組織》

《第三章 核心業務及其重要性》

《第四章 資通系統盤點及風險評估》

《第五章 資通系統發展及維護安全》

《第六章 資通安全防護及控制措施》

《第七章 資通系統或資通服務委外辦理之管理措施》

《第八章 資通安全事件通報應變及情資評估因應》

《第九章 資通安全之持續精進及績效管理機制》

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。

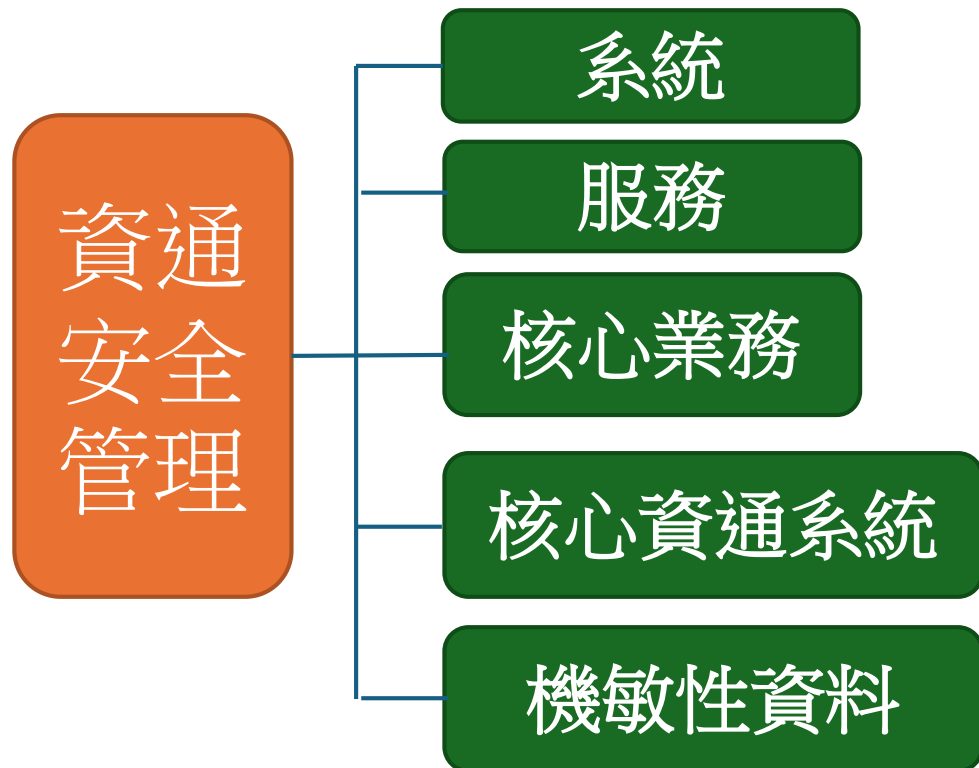
第9-1條

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。

前項一定條件，由本會定之。

第二條、名詞定義

- 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。



廣義的去解釋，其實是涵蓋整個內部控制的八大循環、電腦化資訊系統作業以及18個管理辦法之內的。尤其是對於敏感性較高的產業，都有其制定及查核的要求。

《第二章 資通安全政策及推動組織》的部分



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**。

- 一、資訊處理部門之功能及職責劃分。
- 十、資通安全檢查之控制。

- 有關第三、四、六條，除股東會年報要揭露之外，一般發行公司應訂在「資訊處理部門之功能及職責劃分」這個作業項目。
- 一般發行公司至少都要由副總職位的主管來控管組織的資安單位，因此，如果是外部人或等級不夠高的內部經理人，自然就不符合指引所希望的目標了。
- 第五條所規定的「資通安全作業程序」至少要訂定以下七個項目：
 - (1) 核心業務及其重要性
 - (2) 資通系統盤點及風險評估
 - (3) 資通系統發展及維護安全
 - (4) 資通安全防護及控制措施
 - (5) 資通系統或資通服務委外辦理之管理措施
 - (6) 資通安全事件通報應變及情資評估因應
 - (7) 資通安全之持續精進及績效管理機制



會訂定在『資通安全
檢查之控制』作業內
但是，其他循環是否
也該考量呢？

《第三章 核心業務及其重要性》的部分

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。

「鑑別」與「檢視」是應該由誰來鑑別？

通常公司自己對於核心業務一定都是最重要的部分，也是business model裡面能夠獲利之處，這其中也包括專利、技術、服務等等都算是高度核心業務，即使要請第三方或外部來評鑑，這部分也是很高度的機密，不可能做外部評鑑的，更何況這也涉及營業秘密法，所以，這個鑑別的方式的定義，是應該要更明確。

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**。

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。

《第四章 資通系統盤點及風險評估》的部分

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。

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。

分析機密性、完整性及可用性

可以去參酌『不動產、廠房及設備循環』裡的『不動產及設備保管及記錄作業』的內容。

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。

六、資料處理之控制。

參考資安署，提供以下幾個盤點的重點方向：

- (1) 確認資訊資產盤點及相關管理程序。
- (2) 資訊資產處置規範與異動汰除管控作業。
- (3) 風險評估。
- (4) 風險處理及後續追蹤情形。
- (5) 管理與限制使用中國大陸廠牌資通訊產品。

如果有資訊委外的情形之下，在資安盤點時，可參考以下的重點進行盤點：

- (1) 確認資訊作業委外安全管理程序。
- (2) 資訊委外資安要求及服務等協議。
- (3) 委外人員管理。
- (4) 委外供應商之管理、監督及稽核。

《第五章 資通系統發展及維護安全》的部分



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。

二、系統開發及程式修改之控制。

四、程式及資料之存取控制。

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

五、資料輸出入之控制。

第十五條、妥善儲存及管理資通系統開發及維護相關文件。

三、編製系統文書之控制。

可以廣義的去定義到『研發循環』所包含的：基礎研究、產品設計、技術研發、產品試作與測試、研發記錄與文件保管、智慧財產權之取得、維護及運用等之政策及程序裡面。除了上述這兩個內控制度的部份之外，發行公司也必須再配合公司管理性作業當中的『財務及非財務資訊之管理』，也就是文件管理的程序之內，做適當的內控制度修訂。

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。

- 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。

《第六章 資通安全防護及控制措施》的部分



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)。

七、檔案及設備之安全控制。

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。

四、程式及資料之存取控制。

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。

- 一、資訊處理部門之功能及職責劃分。
- 三、編製系統文書之控制。
- 四、程式及資料之存取控制。

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。

- 四、程式及資料之存取控制。

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**。

- 二、系統開發及程式修改之控制。
- 四、程式及資料之存取控制。
- 五、資料輸出入之控制。

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**。

- 六、資料處理之控制。
- 七、檔案及設備之安全控制。

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。

- 二、系統開發及程式修改之控制。
- 四、程式及資料之存取控制。
- 六、資料處理之控制。
- 七、檔案及設備之安全控制。

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。

- 七、檔案及設備之安全控制。

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。

七、檔案及設備之安全控制。

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。

一、資訊處理部門之功能及職責劃分。

《第七章 資通系統或資通服務委外辦理之管理措施》的部分

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。

- 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。
- 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。

《第八章 資通安全事件通報應變及情資評估因應》的部分

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)。

一、資訊處理部門之功能及職責劃分。

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。

十一、向本會指定網站進行公開資訊申報相關作業之控制。

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。

十、資通安全檢查之控制。

公開發行公司建立內部控制制度處理準則第 4 條

公開發行公司應以書面訂定內部控制制度，含內部稽核實施細則，並經董事會通過，如有董事表示異議且有紀錄或書面聲明者，公司應將異議意見連同經董事會通過之內部控制制度送各監察人；**修正**時，亦同。

公開發行公司設置獨立董事者，依前項規定將內部控制制度提報董事會討論時，應充分考量各獨立董事之意見，並將其**同意或反對之明確意見及反對之理由列入董事會紀錄**。

公開發行公司設置審計委員會者，訂定或修正內部控制制度，**應經審計委員會同意，並提董事會決議**。

前項如**未經審計委員會同意者，得由全體董事三分之二以上同意行之**，並應於董事會議事錄載明審計委員會之決議。

CYBERSEC 2024
臺灣資安大會

5/14_{Tue} — 5/16_{Thu}
臺北南港展覽二館

**Generative
Future**

上市櫃資安標竿論壇

簡報結束
謝謝大家