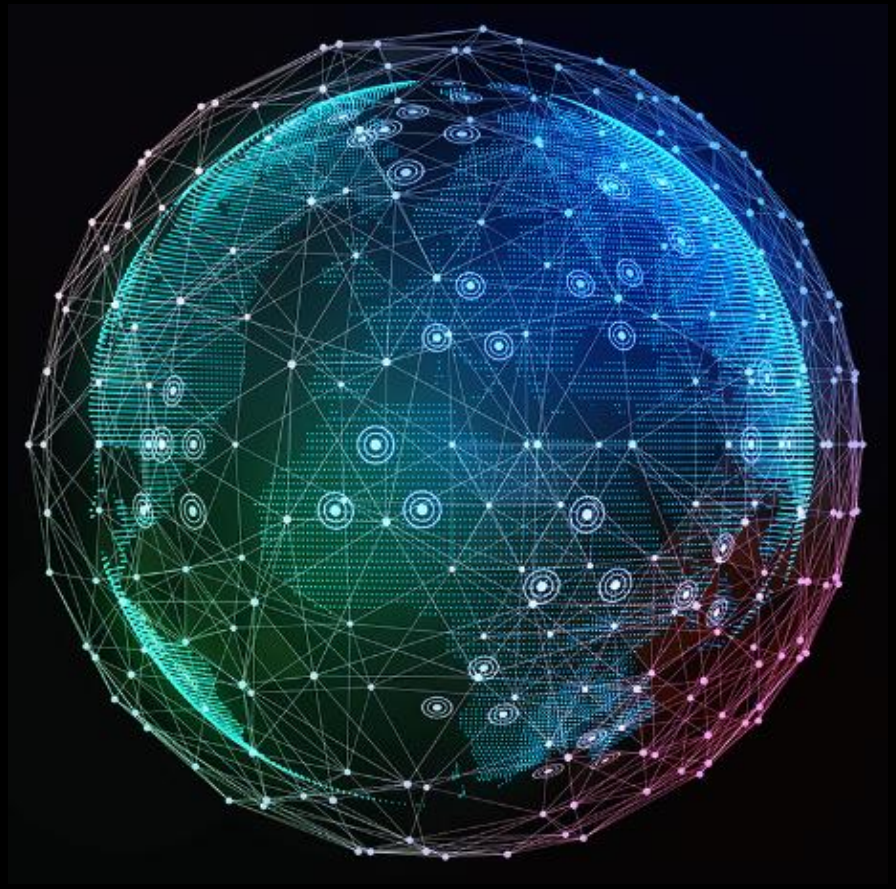
Deloitte.

勤業眾信



證券櫃檯買賣中心

上市上櫃資通安全管控指引

勤業眾信聯合會計師事務所 風險諮詢部門 2022/10

講師簡介

- 臺北市信義區松仁路100號20樓
- Tel : 2725- 9988 分機7807
- Fax: 4051- 6888 分機7807
- ikewchen@deloitte.com.tw

陳威棋

Ike W. Chen

執行副總經理

學歷：

國立中央大學
資訊管理學系碩士

專業資格：

- 國際資訊系統資安專家(CISSP)
- 國際認證資訊安全經理人(CISM)
- 認證隱私解決方案工程師(CDPSE)
- 國際認證道德駭客(CEH)
- 國際認證舞弊偵防師(CFE)
- 國際認證電腦稽核師(CISA)
- 國際資安鑑識調查專家(CHFI)
- ISO 27001 主導稽核員
- BS 10012 主導稽核員

陳威棋擁有十六年資訊安全、滲透測試、資安事件數位鑑識調查經驗，他曾協助許多客戶進行資訊安全檢測服務並針對許多不同產業有豐富資安機制導入經驗，包含科技製造產業、金融產業及政府產業等，目前主要帶領資安技術團隊執行資安檢測服務、資安危機因應、資安策略規劃、外部威脅情資管理、行動應用APP資安檢測、IOT安全檢測服務、工控系統(ICS/SCADA)資安檢測、資安事件應變調查及數位鑑識服務。

經歷：

- 勤業眾信聯合會計師事務所　副總經理
- 勤業眾信資安科技與鑑識分析中心實驗室主管

參與專業組織：

- 台灣金融研訓院課程菁英講座
- 中華民國電腦稽核協會課程講師
- 敏捷專家學會理事
- 台灣舞弊防治與鑑識協會會員
- 國際資訊系統安全核準聯盟((ISC)2)會員
- 國際電腦稽核協會(ISACA)會員
- 國際舞弊稽核師協會(ACFE)會員

Agenda

- 資安發展趨勢調查
- 上市櫃公司相關資通安全法令法規與要求
- 上市櫃公司資通安全管控指引解析
- 上市櫃公司資安管理組織建議
- 上市櫃公司資通安全治理實施策略

資安發展趨勢調查

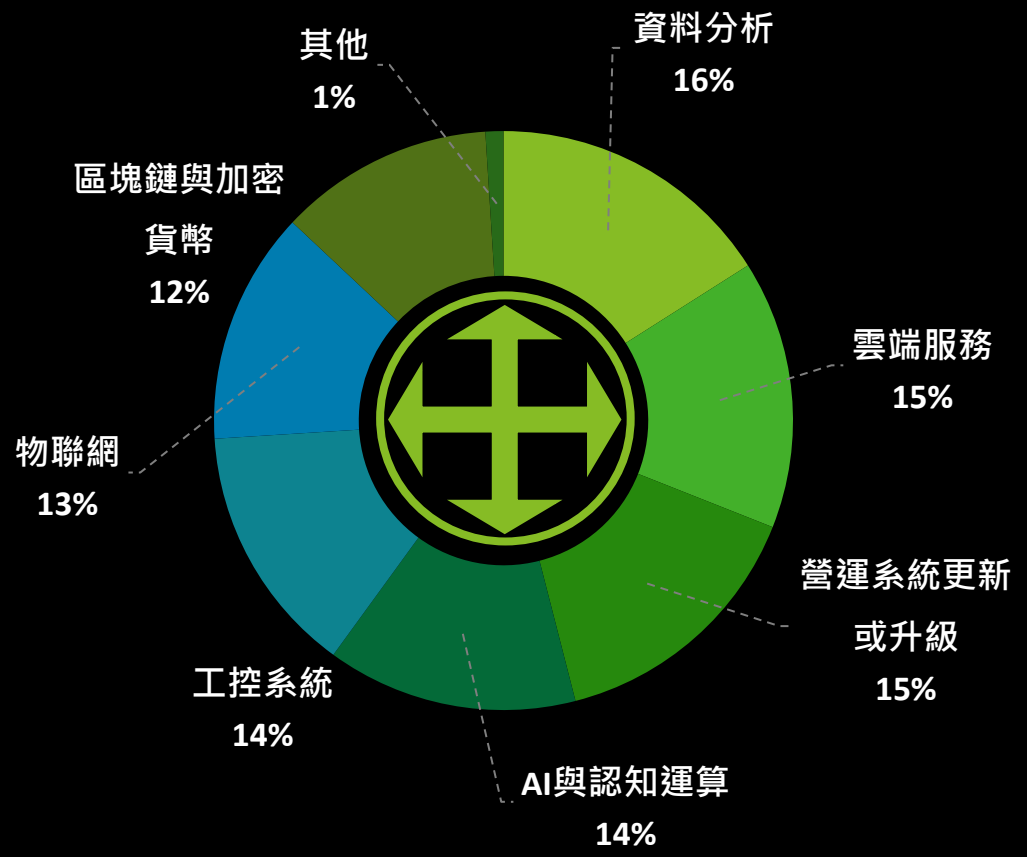
Deloitte 調查：企業優先考量的數位轉型重點

在每個行業中，為了保持競爭力需要快速開發新服務和產品並將其推向市場。

創新的商業模式不僅僅是簡單地數位化現有流程，而是圍繞供應鏈並創造新的客戶體驗領域。這種轉變也使企業面臨新形式的網路風險，需要新的網路安全策略來保護不斷發展的商業模式。成功取決於高級管理層的承諾、他們了解網路風險的能力以及對安全的有效投資。

"我們正處於轉型和快速發展的時期。企業面臨的兩個最大挑戰是混合 IT 和轉型。這創造了一個更加多樣化的環境並提高了複雜性。更高的可見性，尤其是對雲部署的可見性，是組織正在尋找的第一件事。"

— EMILY MOSSBURG, DELOITTE GLOBAL CYBER LEADER



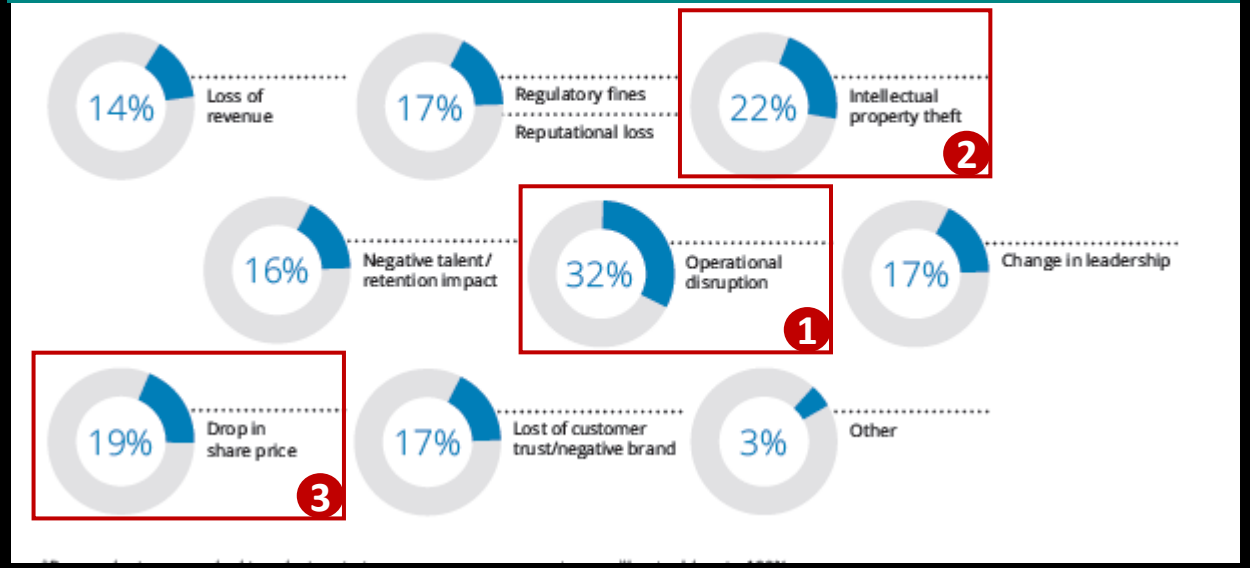
Deloitte 調查：企業遭受到的網路安全攻擊顯著增加

在數位轉型加速發展下，近七成（69%）受訪企業表示，今年遭受的網路攻擊較往年有顯著增加之趨勢。

網路風險的增加，影響之層面不只限於資安和資訊，亦涵蓋了企業營運之風險

科技的融合和網路風險增加，刻正改寫資安長的角色。勤業眾信報告發現，在美國資安長直接向企業CEO報告之情形，已從2019年的32%提升至 2022年的42%；全球平均統計結果則約為33%。此現象亦反映了資安投入之透明度，將有助提高業務計劃並增進各階主管之的參與度。更重要的是，可有效提升資安長與財務長、行銷長等CXO之關係，將有助於降低營運風險和共創更安全的客戶體驗。

網路風險帶來的重大損失，以營運中斷之影響最大，其次是智慧財產 (IP) 盜竊和股價下跌



Deloitte 觀點：安全是資產也是競爭力，企業應從風險全景建立對安全責任的可視性

隨著網路安全的影響日益顯著，建立具備安全性的服務與產品，將使企業在市場上佔有優勢，在日益互聯的世界中更具吸引力。

董事會與高階管理層參與

資安長直接向企業CEO報告，將有助提高業務計劃並增進各階主管之的參與度，並有助於降低營運風險和共創更安全的客戶體驗。

掌握風險與效益

為有效運用資源，應掌握科技可帶來的效益、體驗混合式工作模式所帶來的敏捷度、以充分利用並為客戶帶來全新的體驗

跨越孤島

打破機構內部的界線，促使業務、產品開發、合規、資訊等單位在網路上可共同協作，以在產品及服務設計之初，即考量資安和隱私之需求，避免孤島產生。

知識共享

網路攻擊的普及與頻繁，是各行業或地域都無法倖免的，因此互相學習如何在事件發生時有效地處理事件，與同業分享經驗和知識是全面改善安全環境的基本要素。

推動零信任意識

在組織內以零信任之精神為核心，以來弭平業務、資訊和網路領域之間的差距，從而降低營運複雜度並強化安全

將安全視為資產

以安全的資料治理能力，為企業打造強大之競爭力，以贏得客戶和業務合作夥伴的信任，並提昇品牌形象及價值

上市櫃公司相關資通安全法令法規與要求

上市櫃公司相關資通安全法令法規與要求總覽

行政院

- 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法-105/11/9
- 資通安全管理法-107/6/6
- 資通安全管理法施行細則-110/8/3

金融監督管理委員會

- 公開發行公司年報應行記載事項準則-110/11/30
  (一) 強化環境、社會及治理（下稱「ESG」）之資訊揭露（準則第10條）
  (二) 強化資通安全管理之資訊揭露（準則第18、20條）
  (三) 提升股東會年報資訊揭露時效（準則第23條）
- 公開發行公司年報應行記載事項準則-110/11/30
- 上市上櫃公司資通安全管控指引-110/12/23
- 公開發行公司建立內部控制制度處理準則-110/12/28

行政院法務部

- 個人資料保護法 – 104/12/30
- 個人資料保護法施行細則-105/3/2

行政院經濟部/衛福部

- 營業秘密法-109/1/15
- 醫療法-109/1/15
- 食品業個人資料檔案安全維護計畫實施辦法-111/1/19

財團法人中華民國證券暨期貨市場發展基金會

- 公司治理評鑑指標(二、強化董事會結構與運作 與 四、推動永續發展)-110年第八屆
- 公司治理評鑑指標((二、強化董事會結構與運作 與 四、推動永續發展)-111年第九屆

臺灣資通安全管理法架構

資通安全管理法

資通安全推動組織

- 行政院、委託或委任單位、各公務機關
- 中央目的事業主管機關權責
- 權限委託(6)

公務機關資通安全管理

- **資安責任等級分級(7I)**
- 資安維護計畫之制定與實施(10)
- 資安長之設置(11)
- 年度資安維護計畫實施情形之提出(12)
- 資安稽核(13I)
- 改善報告(13II)
- **資安事件通報應變(14IV)**
- **獎勵辦法(15II)**
- **懲處辦法(19II)**

特定非公務機關資通安全管理

- **資安責任等級分級(7I)**
- 資安維護計畫之制定與實施(16III、17I)
- 年度資安維護計畫實施情形提出 (16IV、17II)
- **資安稽核(7II)**
- **資安事件通報應變(14IV、18IV)**
- 改善報告(7III 、16VI、17III)
- 公告(18V)
- 罰則(20~21)

資安整體環境與產業發展

- 資安專業人才之培育(4)
- 資安科技之研發、整合、應用、產學合作及國際交流合作(4)
- 資安產業發展(4)
- 資安軟硬體、設備技術規範、資安相關服務及審驗機制之發展(4)
- 定期公布國家資安情勢、對公務關稽核概況之報告及資安發展案(5)
- **資安情資分享(8 II)**

資通服務之委外管理

- 委託機關應監督受託者資安之維護(9)

註：1. 粗體藍字部分，係以個別子法規範。
2. 其頭規範事項，由施行細則補充(22)。

強化上市櫃公司資訊安全管理四大面向

- 「公開發行公司內部控制制度處理準則」

上市櫃公司應建立適當內部控制以降低資通安全風險，除應建立適當資通安全作業，並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。

- 「公司治理評鑑指標」

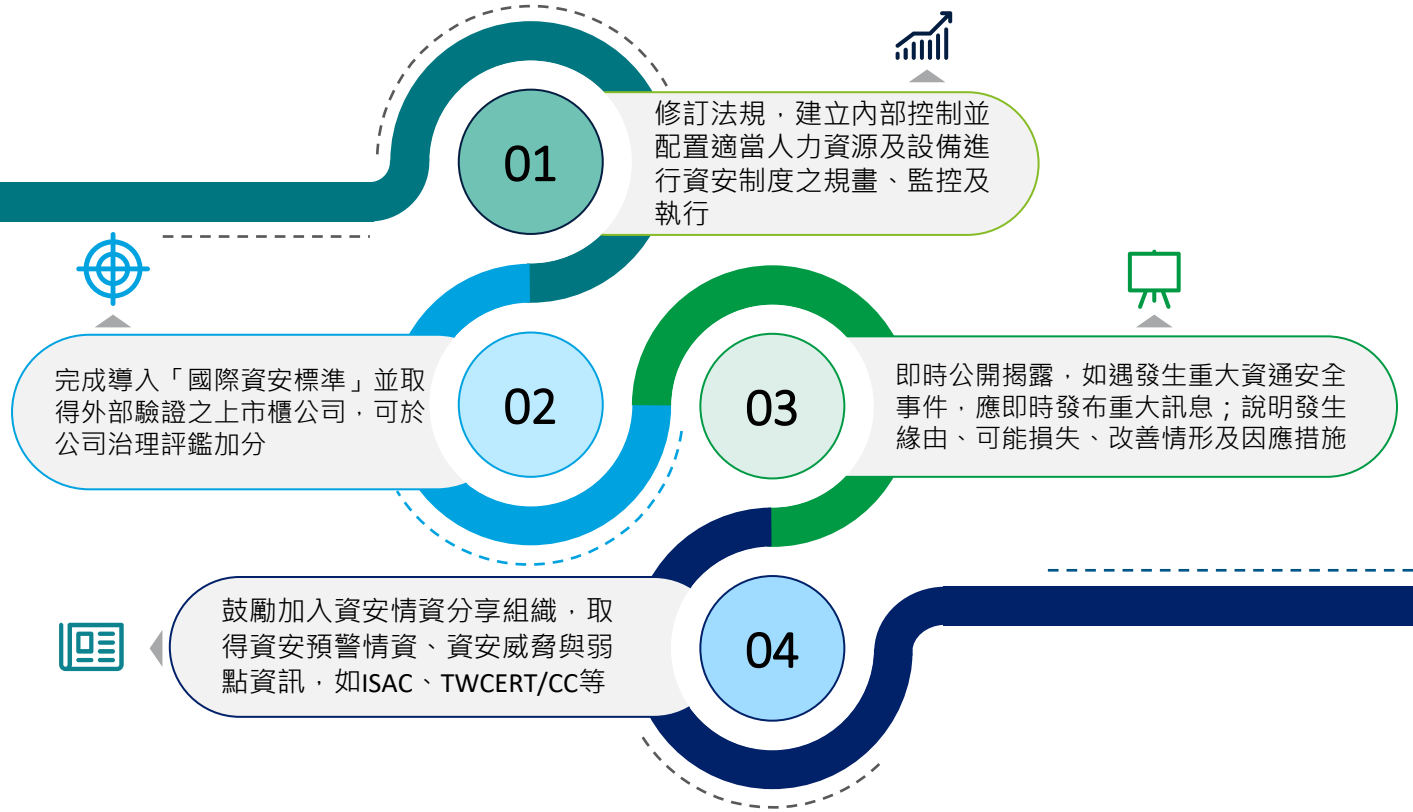
修正公司治理評鑑指標，完成導入「國際資安標準」並取得外部驗證之上市櫃公司，將於公司治理評鑑時加分，並發布上市上櫃公司資通安全管控指引，提供上市櫃公司執行內部控制措施時之參考。

- 「上市櫃公司重大訊息之查證暨公開處理程序」

為強化上市櫃公司資通安全資訊公開，除了應於股東會年報中敘明資通安全政策、具體管理方案及投入資通安全管理之資源等資訊外，如遇發生重大資通安全事件，應即時發布重大訊息；說明發生緣由、可能損失、改善情形及因應措施，並於損失達一定金額以上時，召開重大訊息記者會對外說明。

- 「資安訊息分享」

鼓勵上市櫃公司透過資安資訊之情資分享，以達資通安全聯合防禦之效能



公開發行公司建立內部控制制度處理準則

110年中華民國110年12月28日金融監督管理委員會金管證審字第1100365654號令修正發布第47條；增訂第9條之1條文，自發布日施行。

目的：提升公開發行公司對資訊安全之重視

一、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，並要求公開發行公司符合一定條件者

二、應指派資訊安全長統籌資訊安全政策推動與資源調度事務，並設置資訊安全專責單位、主管及資訊安全人員，專門負責資訊安全事務。

三、資訊安全長及設置資訊安全專責單位、主管及人員之一定條件，授權主管機關另定之。

第九條之一

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。

第四十七條

1.本準則自中華民國一百零四年一月一日施行。

2.本準則修正條文自發布日施行。

公開發行公司建立內部控制制度處理準則

公開發行公司建立內部控制制度處理準則第9條之1規定之令 - 金管證審字第11003656544號

	上市(櫃)公司分級標準	資安單位人力編制要求	實施時程
第一級	• 實收資本額達新台幣100億元以上 • 前一年底屬臺灣50指數成分公司 • 最近一年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	• 指派人員兼任資安長 • 設置資安專責單位（包含資安專責主管及至少2名資安專責人員）	• 111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 • 至少1名資安專責人員	• 112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

※依據資通安全管理法座談會會議紀錄(1070802)說明，「專責」可兼辦其它非資通安全相關業務。

公開發行公司建立內部控制制度處理準則

110年中華民國110年12月28日金融監督管理委員會金管證審字第1100365654號令修正發布第47條；增訂第9條之1條文，自發布日施行。

主旨：為強化上市公司資安防護及管理，請貴公司自即日起申報資安人員基本資料，請查照。

說明：

一、依據「公開發行公司建立內部控制制度處理準則」第9條之1及金融監督管理委員會(下稱金管會)110年12月28日金管證審字第11003656544號令辦理。

二、金管會已於110年12月28日公告將上市公司分為三級，上市公司應按所屬分級分別於111年及112年底前完成資安人力資源及設備配置，相關執行細節可參考金管會證券期貨局111年1月12日修正之「公開發行公司建立內部控制制度處理準則問答集」第21題至第25題（如附件）。請貴公司依規於時限內完成設置資安人員，已完成設置者，自即日起請至公開資訊觀測站電子認證申報系統「資安長、資安主管及資安人員資料申報作業」項下申報資安人員基本資料，後續人員若有異動，亦請於2日內完成申報。

三、另為強化上市公司資安情資共享，提升資安事件通報應變能量，本公司鼓勵上市公司免費申請成為台灣電腦網路危機處理暨協調中心(TWCERT/CC)會員，該中心可提供資安事件諮詢及協調協處服務，使上市公司有效接收及傳遞資安情資，會員申請表請參閱TWCERT/CC官網（https://www.twcert.org.tw/tw/cp-114-2919-b483d-1.html），填寫後請逕以電子郵件向TWCERT/CC申請加入會員。

正本：各上市公司
副本：財團法人中華民國證券櫃檯買賣中心(含附件)、本公司上市二部(含附件)

電子文章交換章

公開發行公司建立內部控制制度處理準則常見Q&A(Cont'd)

110年中華民國110年12月28日金融監督管理委員會金管證審字第1100365654號令修正發布第47條；增訂第9條之1條文，自發布日施行。

使用電腦化資訊系統處理之公司應包括對資通安全檢查之控制。
何謂「資通安全」？
公司應如何訂定相關控制作業？
（111.01.11 修正）

- （一）「資通安全」一詞已於資通安全管理法明文定義，詳細內容可逕自上網查詢或下載(行政院國家資通安全會報/資安法專區 https://nicst.ey.gov.tw/Page/EB237763A1535D65)。
- （二）公司於設計關於資通安全管理之控制作業時，可參考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發布之**「上市上櫃公司資通安全管控指引」**（查詢網址：www.twse.com.tw/zh），以強化資通安全防護管理機制。

處理準則第 9 條之 1 規定公開發行公司符合一定條件者，應指派資訊安全長及設置資訊安全專責單位、主管及人員，該一定條件及設置時程為何？
（111.01.11 新增）

- 上市（櫃）公司符合下列條件之一者，應於**111 年底前**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**，並設置**資訊安全專責單位**，該單位應配置**專責主管及至少二名專責人員**，專門負責資訊安全相關工作或職務

  法令依據：處理準則第 9 條之 1 及 110 年 12 月 28 日金管證審字第 11003656544 號令。

公開發行公司建立內部控制制度處理準則常見Q&A(Cont'd)

110年中華民國110年12月28日金融監督管理委員會金管證審字第1100365654號令修正發布第47條；增訂第9條之1條文，自發布日施行。

處理準則第 9 條之 1 所指資訊安全單位及人力（含資訊安全長、資訊安全專責主管及人員）之設置程序及職責為何？資訊安全人力是否屬內部人？其任免是否需經董事會通過？（111.01.11 新增）

- （一）按處理準則第 5 條及第 9 條之 1 規定，公開發行公司之內部控制制度應訂定明確之內部組織架構、呈報體系及適當權限與責任，載明經理人之設置、職稱、委任與解任及職權範圍等事項，並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，故公開發行公司應依前揭規定於內部控制制度中**明確劃分各部門之權限、責任及職權範圍，並明定資訊安全專責單位之功能及職責**；若公司於設置資訊安全單位及人力時有調整內部組織架構之必要，應配合修訂相關內部控制制度並提報董事會通過後實施。
- （二）依 92 年 3 月 27 日台財證三字第 0920001301 號令規定，證券交易法第 22 條之 2 及第 25 條等規定之經理人適用範圍包括：
  (1)總經理及相當等級者。(2)副總經理及相當等級者。(3)協理及相當等級者。(4)財務部門主管。(5)會計部門主管。(6)其他有為公司管理事務及簽名權利之人，故公司應視所指派予資訊安全人力之職務層級及職權範圍，依前揭令釋原則予以認定，若符合前揭令釋或相關法令所訂經理人範疇，則相關委任、解任及報酬程序應依公司法第 29 條有關經理人規定辦理，並按證券交易法第 22 條之 2 及第 25 條等規定辦理內部人申報事宜。
  法令依據：證券交易法第 22 條之 2 及第 25 條、處理準則第 9 條之 1、92 年 3 月 27 日台財證三字第 0920001301 號令及本會 110 年 12 月 28 日金管證審字第 11003656544 號令。

公開發行公司建立內部控制制度處理準則常見Q&A

110年中華民國110年12月28日金融監督管理委員會金管證審字第1100365654號令修正發布第47條；增訂第9條之1條文，自發布日施行。

資訊安全長是否指定由一定層級以上人員擔任？（111.01.11 新增）

- 依處理準則第 9 條之 1 規定，應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，通常具備前開資訊安全長職能之人為一定層級以上之高階主管（如副總等），爰公司於指派資訊安全長時，應**考量其職級權責是否足以勝任資訊安全長職務**。

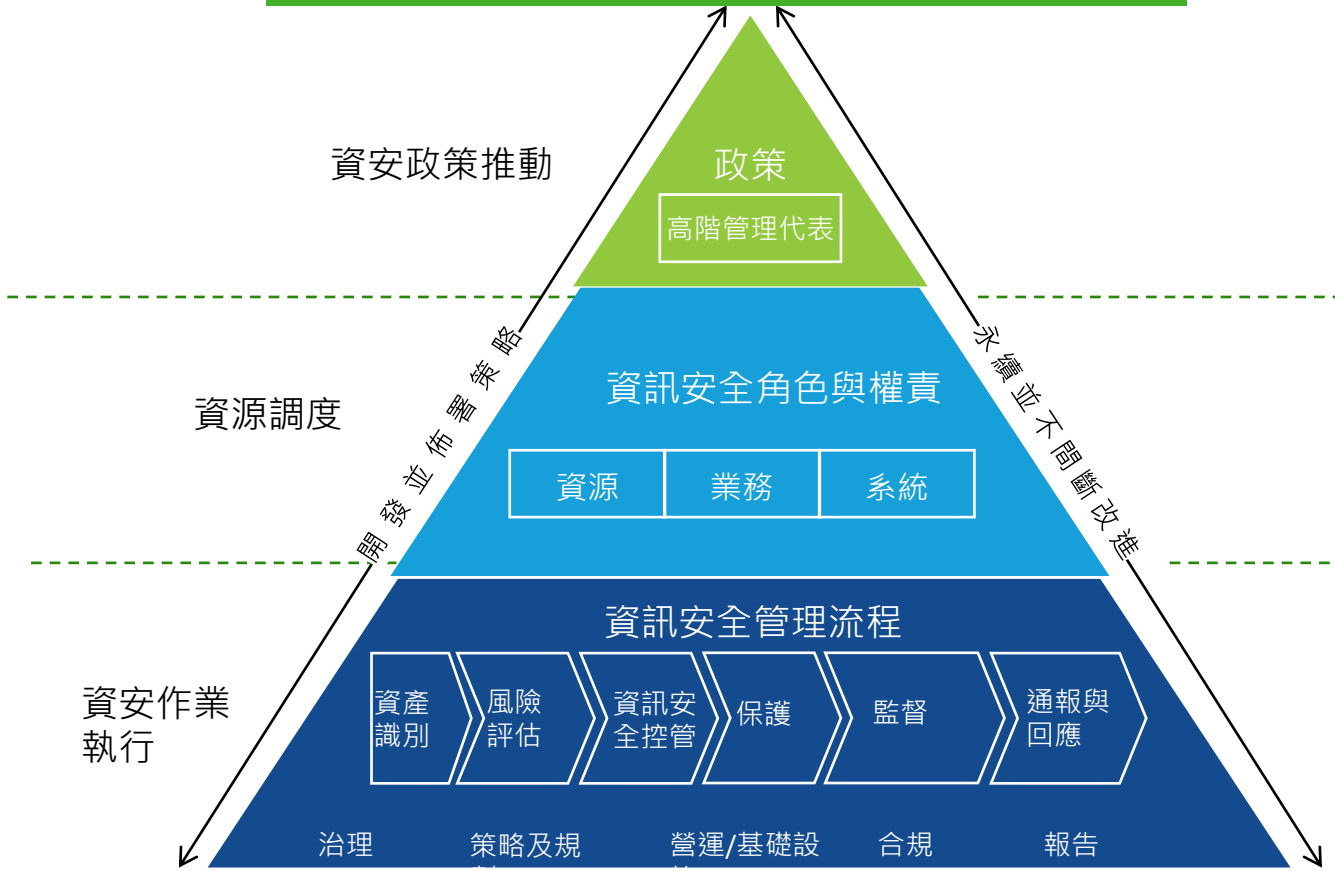
資訊安全專責主管及人員之資格條件及是否應為專任？（111.01.11 新增）

- （一）依處理準則第 9 條之 1 規定，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，故公司應於內部控制制度中明定資訊安全專責人力之功能及職責，且於安排資訊安全專責人力時考量其能力及適格性，並給予適當之教育訓練或要求取得相關之資通安全職能證照，以確保其勝任職務內容。
- （二）按負責資通安全事務之人即為資安專責人員，**並無強制公司投入專職人力之要求**，公司應視**實際面臨之資訊安全風險及需求，評估是否藉額外投入或職務劃分方式配置專職負責資訊安全之人力資源**，以強化資訊安全控制作業之有效性。

公開發行公司建立內部控制制度處理準則

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

資訊安全制度規劃



上市上櫃公司資通安全管控指引

第二章 資通安全政策及推動組織		
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

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，特擬定資通安全管控指引。

證交所及櫃買中心對有價證券上市公司重大訊息之查證暨公開處理程序

證交所於2021年4月27日發布第4條第26項修訂，櫃買中心於2021年4月29日發布第4條第26項修訂，將資通安全事件明確訂於法規之中，屬於重大訊息，應發布即時重大訊息。

因應「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」第2章第4條第26項之規定，重大訊息包含：

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。

「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」第4條第26項之規定，重大訊息包含：

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。

如上市(櫃)公司發生資通安全事件，符合上述情事者，應比照重大訊息做即時發布與通報。

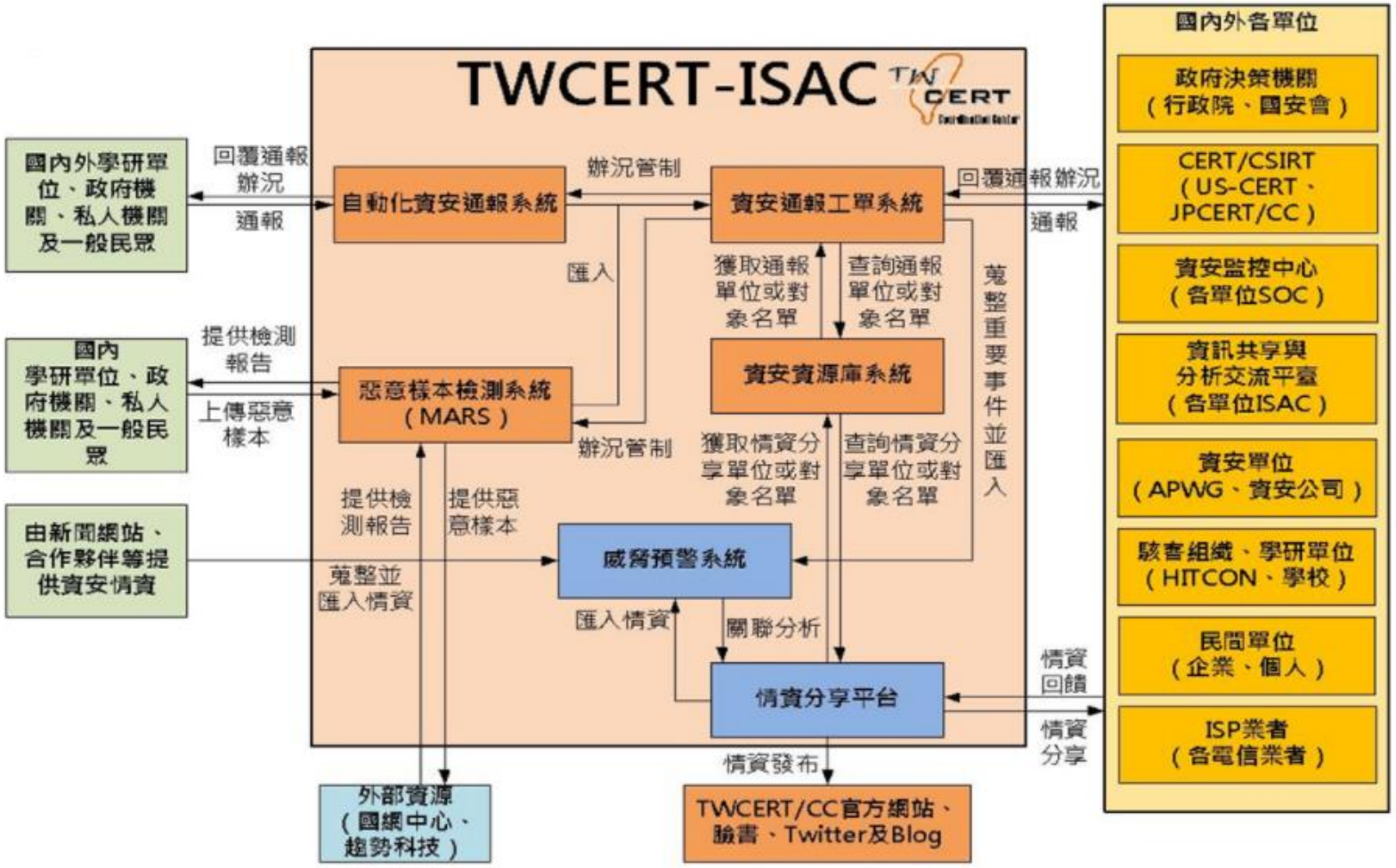
二十六、發生災難、集體抗議、罷工、環境污染、資通安全事件或其他重大情事，致有下列情事之一者：

（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。

鼓勵上市櫃公司加入ISAC、TWCERT等資安情資分享平台

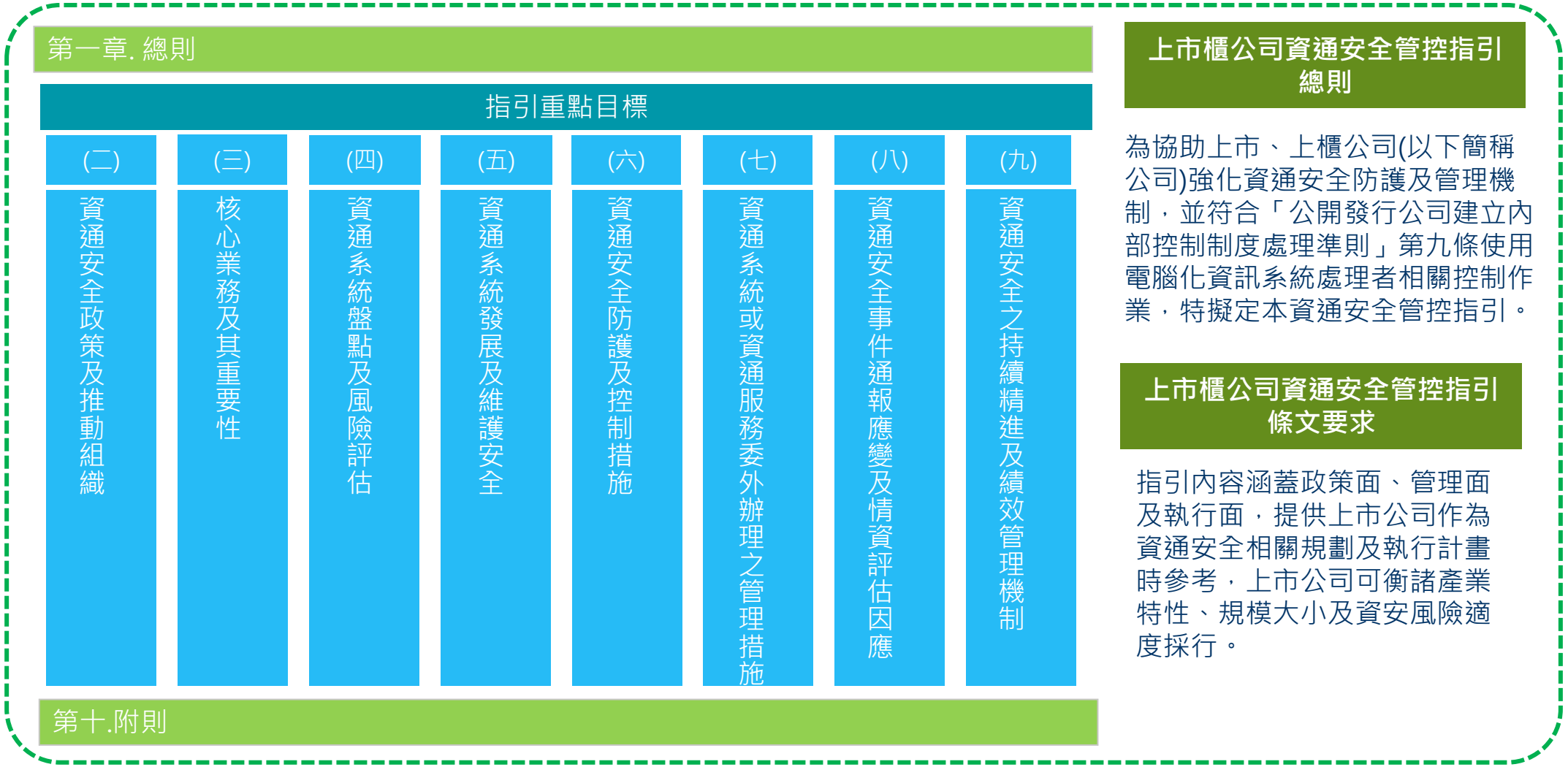


資料來源：TWCERT/CC

上市櫃公司資通安全管控指引解析

上市櫃公司資通安全管控指引

上市櫃公司及證券商應建立適當內控，以降低資通安全風險，除應建立適當資安作業，並應配置適當人力資源及設備，進行資安制度規畫、監控及執行



上市櫃公司資通安全管控指引總則

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。

上市櫃公司資通安全管控指引條文要求

指引內容涵蓋政策面、管理面及執行面，提供上市公司作為資通安全相關規劃及執行計畫時參考，上市公司可衡諸產業特性、規模大小及資安風險適度採行。

上市櫃公司資通安全管控指引

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，特擬定資通安全管控指引。

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
強化上市、上櫃公司之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」第九條管控指引。	• 成立資通安全推動組織 • 訂定資通安全政策、程序規範及目標 • 所有資訊系統人員每年接受資訊安全宣導課程。	• 鑑別核心業務及機敏資料、應遵守之法令及契約要求， • 落實營運持續管理，設置適當備援機制及備援計劃 • 制定業務營運持續計畫及演練	• 定期盤點資通系統並建立清冊 • 定期執行資安風險評估及其對應管控措施。	• 定期辦理核心資通系統之資安檢測、弱點掃描、滲透測試及源碼檢測。 • 定期執行資通系統安全性測試(存取控制及身分驗證等)

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	第十章 附則
• 落實網路安全管理及資安防護措施 • 訂定離到職管理程序並簽屬NDA • 建立通行碼管理規則 • 定期執行權限審查 • 建立資通系統監控措施 • 建立機房實體安全管制 • 訂定設備汰除及回收安全控制作業程序 • 訂定裝置使用管理規範 • 定期辦理電子郵件社交工程。	• 訂定資訊作業委外安全管理程序、委外廠商資通安全責任及保密規定 • 委外關係終止或解除後應返還、移交、刪除或銷毀因履行契約而持有之資料。	• 訂定資安事件應變處置及通報作業程序 • 加入資安情資分享組織，如(ISAC/TWCERT) • 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。	• 資通安全推動組織定期向董事會或管理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。	• 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。

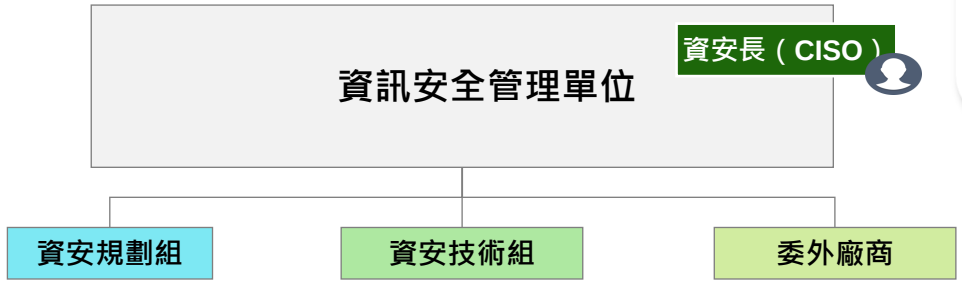
資通安全政策及推動組織(Cont.)

成立資通安全推動組織、訂定資通安全目標、資通安全作業程序，並要求所有資訊系統人員每年接受資訊安全宣導課程。

第二章 資通安全政策及推動組織

NIST CSF IDENTIFY (ID) PROTECT (PR) / ISO 27001:2013 5.領導作為、6.規劃、7.支援、A.5 資訊安全政策、A.6 資訊安全組織、A.12 運作安全

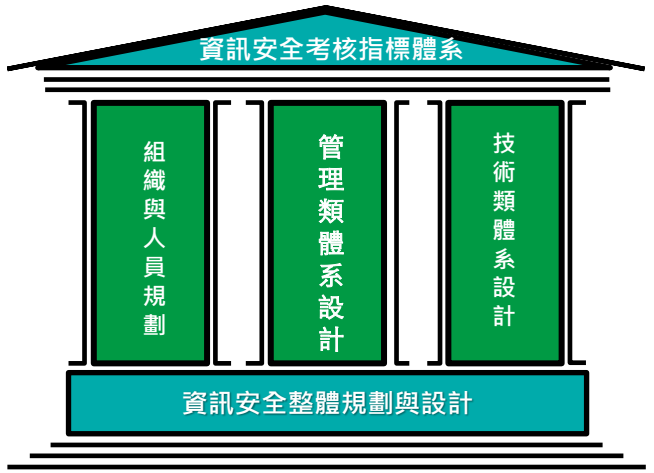
• 成立資通安全推動組織



- 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。

• 訂定資通安全目標與作業程序

- 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。



資通安全政策及推動組織

成立資通安全推動組織、訂定資通安全目標、資通安全作業程序，並要求所有資訊系統人員每年接受資訊安全宣導課程。

第二章 資通安全政策及推動組織

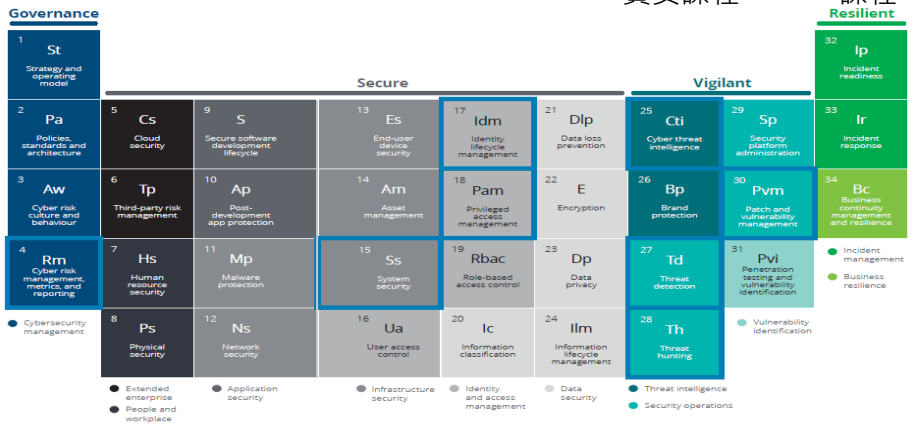
NIST CSF IDENTIFY (ID) PROTECT (PR) / ISO 27001:2013 5.領導作為、6.規劃、7.支援、A.5 資訊安全政策、A.6 資訊安全組織、A.12 運作安全

- **安排資訊安全宣導課程**

認知培養：資安通識教育	**專業提升：資安專業課程**
領域深耕：關鍵技能解析	**創新科技：新興科技資安控管**

- **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。**

資安通識課程　資安技術實作課程　跨域應用資安課程　資安治理課程



核心業務及其重要性

鑑別核心業務及機敏資料、應遵守之法令及契約要求，落實營運持續管理，含訂定RTO、RPO，設置適當備援機制及備援計劃，制定業務營運持續計畫及演練

第三章 核心業務及其重要性

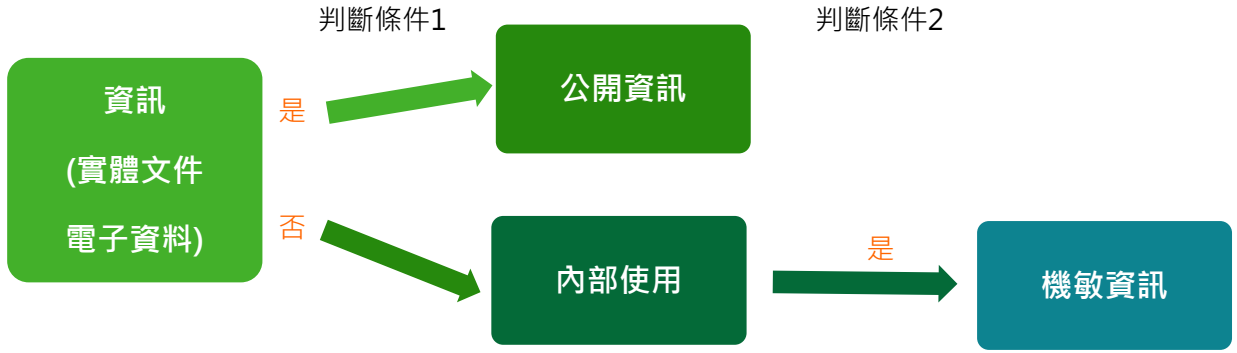
NIST CSF RESPOND (RS) RECOVER (RC) / ISO 27001:2013 A.8 資產管理、A.17 營訊持續管理之資訊安全層面、A.18 遵循性

- **識別核心業務及機敏資料，並盤點應遵守之法令及契約要求**

- **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。**

核心業務：	**公司維持營運與發展必要之業務。**
核心資通系統：	**支持核心業務持續運作必要之資通系統。**



- **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。

資通系統盤點及風險評估(Cont'd)

定期盤點資通系統，建立核心系統資訊資產清冊；定期執行資安風險評估並執行對應管控措施。

第四章 資通系統盤點及風險評估

NIST CSF IDENTIFY (ID) / ISO 27001:2013 8. 運作、A.8 資產管理

- **定期盤點資訊資產清冊**

- **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。**

資產識別 → 威脅定義 → 弱點定義 → 風險評估 → 剩餘風險評估

資產分級分類

人員類	軟體類	硬體類	資料類	文件類
• 內部員工	• 業務系統	• 虛擬伺服器	• 網頁公開資料	• 內部政策
• 委外廠商	• 支援軟體	• 虛擬網路	• 主機設定資料	• 申請表單
•	• 管理平臺	• 個人電腦	• 資料庫資料	• 對外文宣
		•	•	• .....

解決方案

- 利用現有的資產清單，有效收集完整之資訊資產清冊。
- 制訂資訊資產群組，做為管理資訊資產之基礎。透過採用群組管理之方式，係在不改變風險程度之情況下，所採取為適度簡化風險評估作業，所作之設計。

資通系統盤點及風險評估

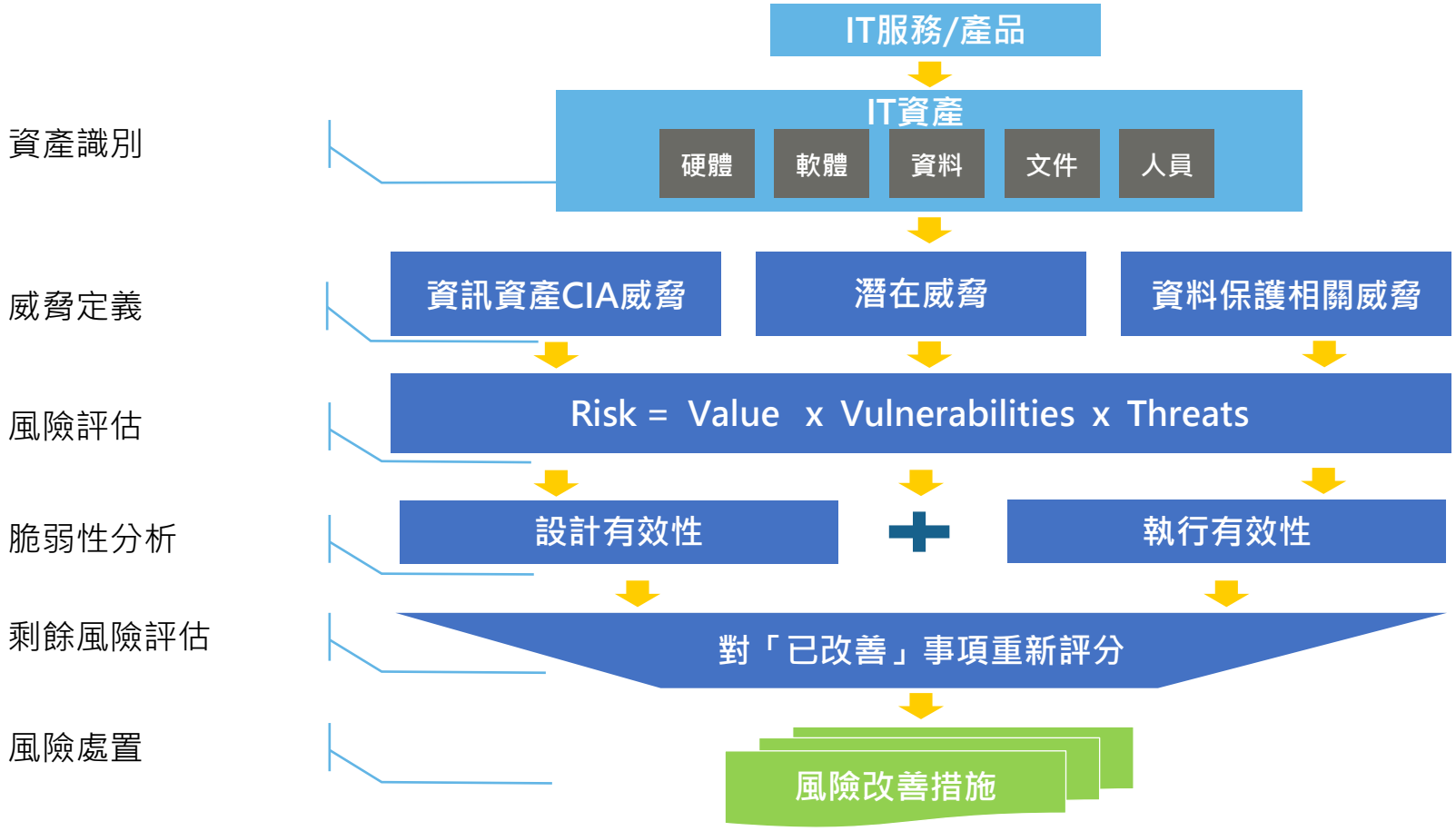
定期盤點資通系統，建立核心系統資訊資產清冊；定期執行資安風險評估並執行對應管控措施。

第四章 資通系統盤點及風險評估

NIST CSF IDENTIFY (ID) / ISO 27001:2013 8. 運作、A.8 資產管理

- **定期執行風險評估並進行改善**

- **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。**



資通系統發展及維護安全(Cont'd)

落實資通系統開發及維護管理，含存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等，妥善管理資通系統開發及維護相關文件；定期對核心資通系統辦理資安檢測，含(弱點掃描、滲透測試、上線前原碼掃描)。

第五章 資通系統發展及維護安全

NIST CSF PROTECT (PR) / ISO 27001:2013 A.9 存取控制、A.12 運作安全、A.14 系統獲取、開發及維護

- **制定資通系統開發及維護文件**

- **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。**

系統安全開發

- 原始碼管理
- 安全性檢測
- 測試環境與資料保護
- 輸入輸出檢查過濾…

系統安全維護

- 存取控制
- 使用者身分驗證機制
- 系統變更管理
- 系統事件軌跡留存…

資通系統發展及維護安全

落實資通系統開發及維護管理，含存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等，妥善管理資通系統開發及維護相關文件；定期對核心資通系統辦理資安檢測，含(弱點掃描、滲透測試、上線前原碼掃描)。

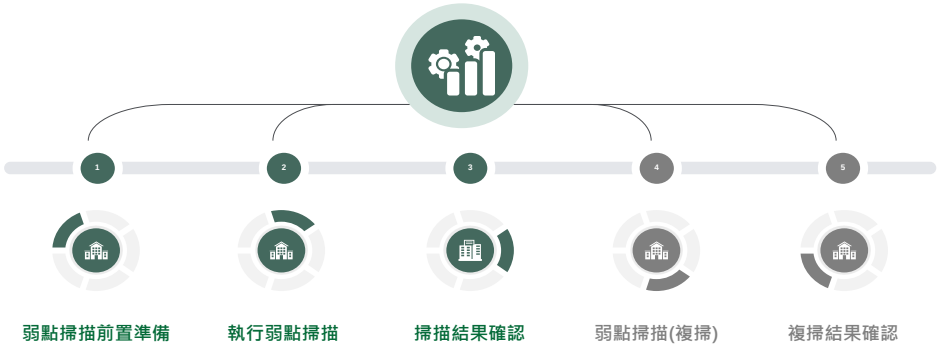
第五章 資通系統發展及維護安全

NIST CSF PROTECT (PR) / ISO 27001:2013 A.9 存取控制、A.12 運作安全、A.14 系統獲取、開發及維護

- **定期執行核心系統資安檢測(含弱點掃描、滲透測試、上線前原碼掃描)**

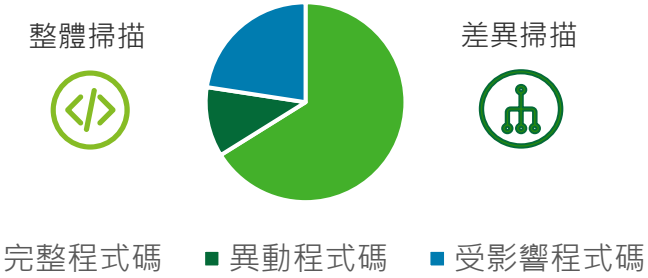
- **第十六條、 對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。**
  - **一、定期辦理弱點掃描。**
  - **二、定期辦理滲透測試。**
  - **三、系統上線前執行源碼掃描安全檢測。**

- 弱點掃描



- 滲透測試

- 原碼掃描



資通安全防護及控制措施(Cont'd)

落實網路安全管理，如(網路架構安全設計、防火牆、郵件過濾機制、資安威脅偵測管理機制SOC等...)，針對機敏資料處理及儲存建立適當防護，訂定離到職管理程序，建立通行碼管理規則，定期執行權限審查，建立資通系統監控措施，機房實體安全管制，訂定設備汰除及回收安全控制作業程序，訂定裝置使用管理規範，定期辦理電子郵件社交工程。

第六章 資通安全防護及控制措施

NIST CSF PROTECT (PR) DETECT (DE)/ ISO 27001:2013 A.7 人力資源安全、A.8 資產管理、A.9 存取控制、A.10 密碼學、A.11實體及環境安全、A.13 通訊安全

- **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)。**

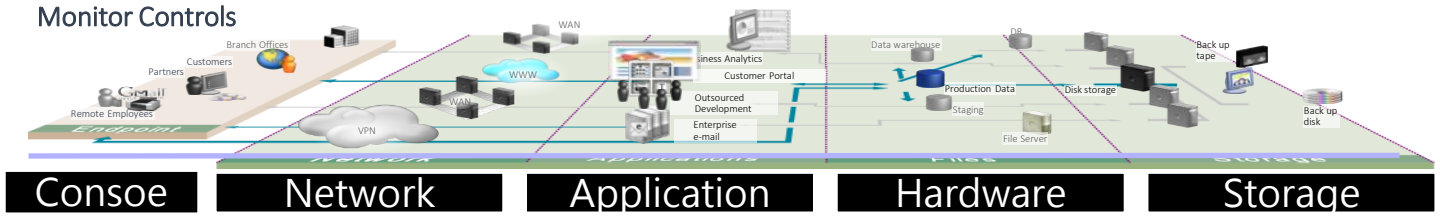
- **制定網路安全管理程序，並建立適當資安防護**

網路安全管理

設備配置	網路拓樸
資訊作業安全	節點安全

設備安全管理

安控機制	設備管理	存取控管
作業程序	日誌資料保護	事件存錄



資通安全防護及控制措施(Cont'd)

落實網路安全管理，如(網路架構安全設計、防火牆、郵件過濾機制、資安威脅偵測管理機制SOC等...)，針對機敏資料處理及儲存建立適當防護，訂定離到職管理程序，建立通行碼管理規則，定期執行權限審查，建立資通系統監控措施，機房實體安全管制，訂定設備汰除及回收安全控制作業程序，訂定裝置使用管理規範，定期辦理電子郵件社交工程。

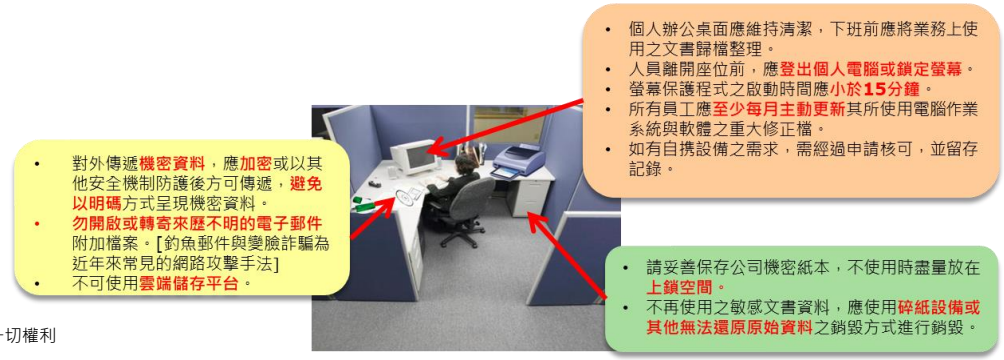
第六章 資通安全防護及控制措施

NIST CSF PROTECT (PR) DETECT (DE) / ISO 27001:2013 A.7 人力資源安全、A.8 資產管理、A.9 存取控制、A.10 密碼學、A.11實體及環境安全、A.13 通訊安全

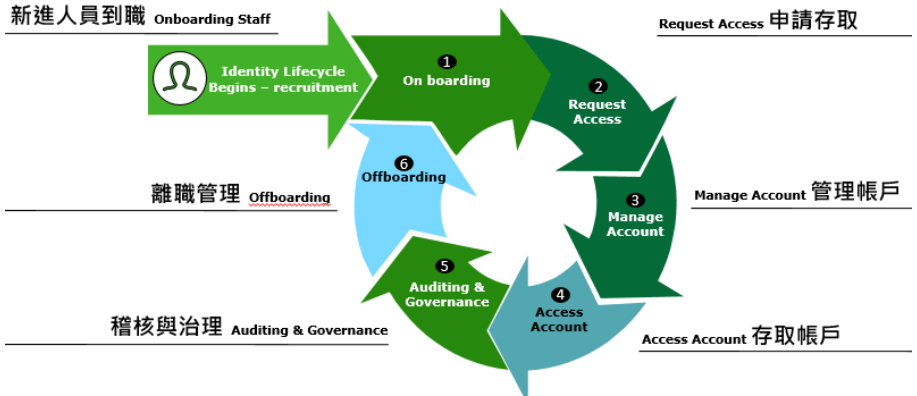
- **建立資料保護措施、人員離到職管理、存取控管、權限審查、適當監控機制等資安防護**

- **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，**
- **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。**
- **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。**
- **第二十三條、建立資通系統及相關設備適當之監控措施。**

- 機敏資料保護



- 人員生命週期及存取權限管理



資通安全防護及控制措施

落實網路安全管理，如(網路架構安全設計、防火牆、郵件過濾機制、資安威脅偵測管理機制SOC等...)，針對機敏資料處理及儲存建立適當防護，訂定離到職管理程序，建立通行碼管理規則，定期執行權限審查，建立資通系統監控措施，機房實體安全管制，訂定設備汰除及回收安全控制作業程序，訂定裝置使用管理規範，定期辦理電子郵件社交工程。

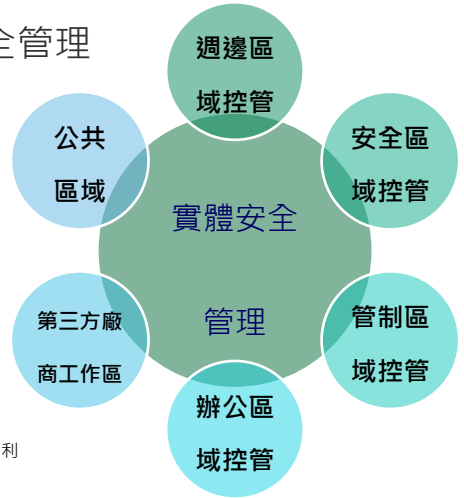
第六章 資通安全防護及控制措施

NIST CSF PROTECT (PR) DETECT (DE) / ISO 27001:2013 A.7 人力資源安全、A.8 資產管理、A.9 存取控制、A.10 密碼學、A.11實體及環境安全、A.13 通訊安全

- **建立實體安全保護、脆弱性管理、設備汰除、個人設備管控、社交工程演練管控等資安防護**

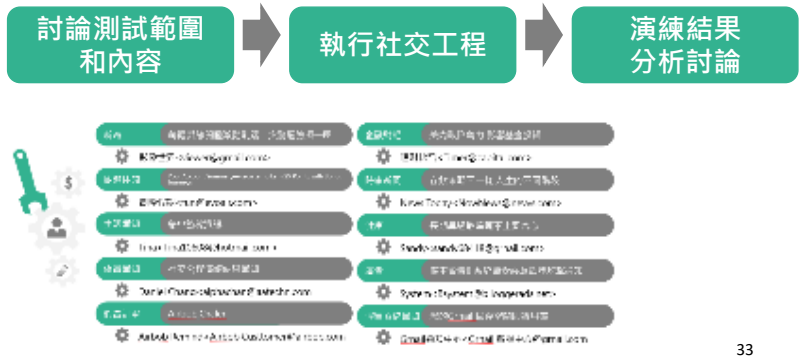
- **第二十四條、針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。**
- **第二十五條、留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。**
- **第二十六條、訂定資通設備回收再使用及汰除之安全控制作業程序，以確保機敏性資料確實刪除。**
- **第二十七條、訂定人員裝置使用管理規範。**
- **第二十八條、每年定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。**

- 實體安全管理



- 脆弱性管理

- 社交工程演練



資通系統或資通服務委外辦理之管理措施

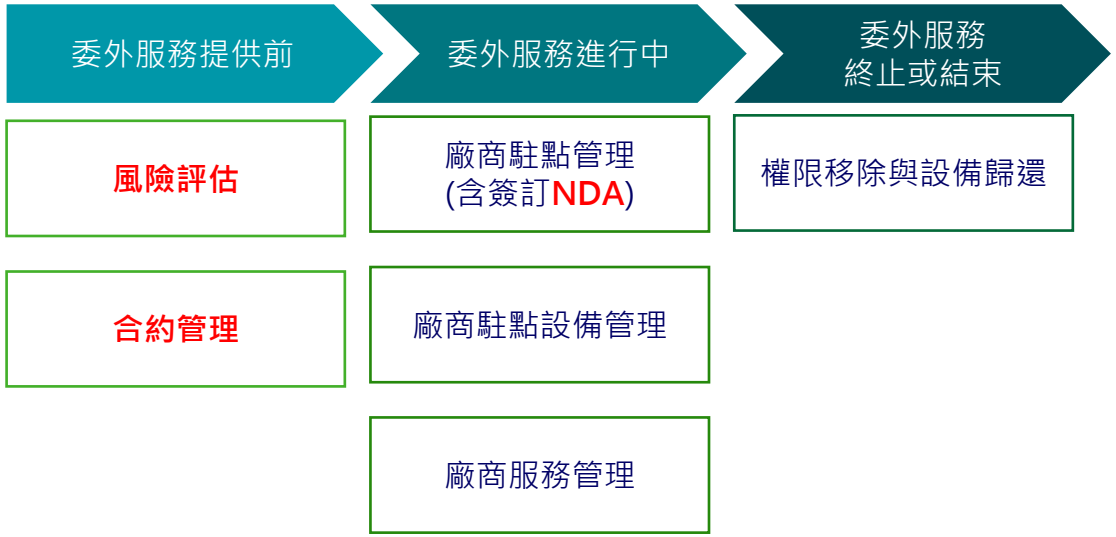
訂定資訊作業委外安全管理程序、委外廠商資通安全責任及保密規定，並要求委外關係終止或解除後應返還、移交、刪除或銷毀因履行契約而持有之資料。

第七章 資通系統或資通服務委外辦理之管理措施

NIST CSF IDENTIFY (ID) PROTECT (PR) / ISO 27001:2013 A.15 供應者關係

- **制定第三方委外安全管理程序，並建立適當管理流程**

- **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。**



資通安全事件通報應變及情資評估因應

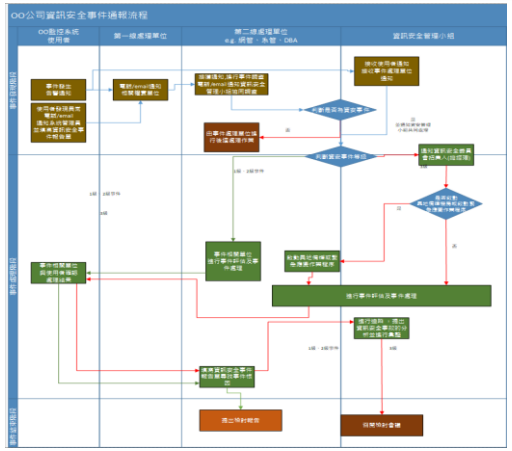
訂定資安事件應變處置及通報作業程序，加入資安情資分享組織，如(ISAC/TWCERT)。發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」或「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

第八章 資通安全事件通報應變及情資評估因應

NIST CSF RESPOND (RS) / ISO 27001:2013 A.16 資訊安全事故管理

• 設計資安事件應變處置與通報作業程序及流程

- 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。



• 加入資安情資分享組織

- 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)。

• 如上市(櫃)公司發生資通安全事件，符合情事者，應比照重大訊息做即時發布與通報。

- 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。

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。

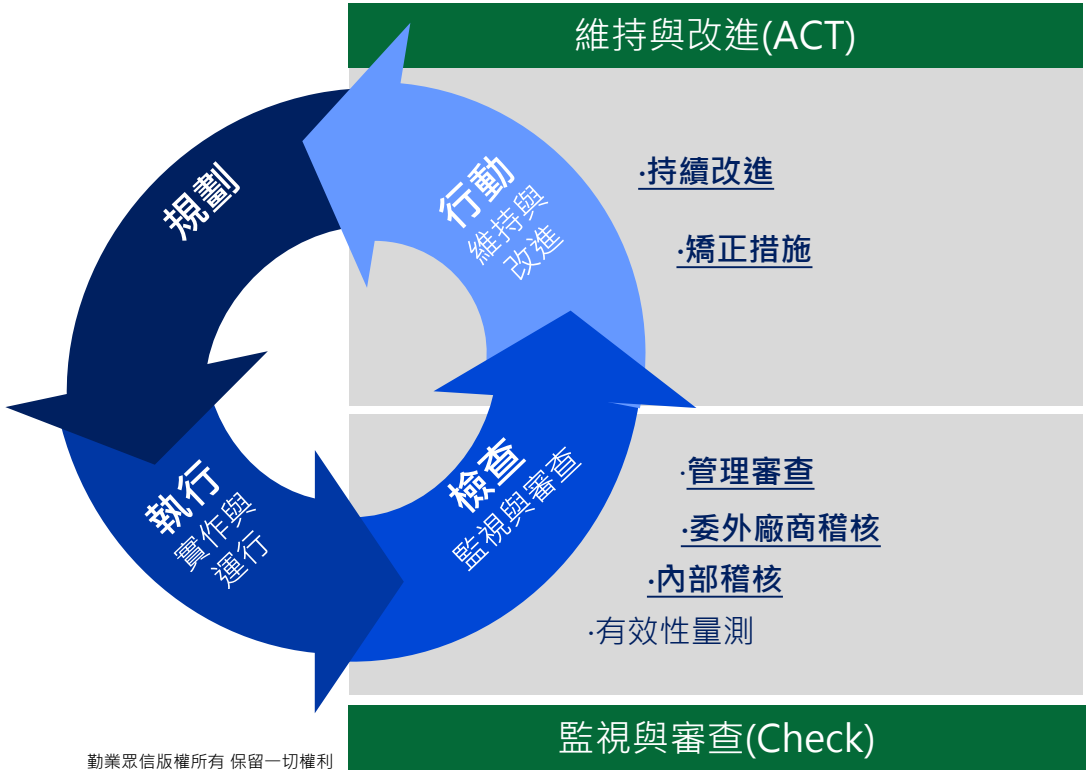
資通安全之持續精進及績效管理機制

資通安全推動組織定期向董事會或管理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。

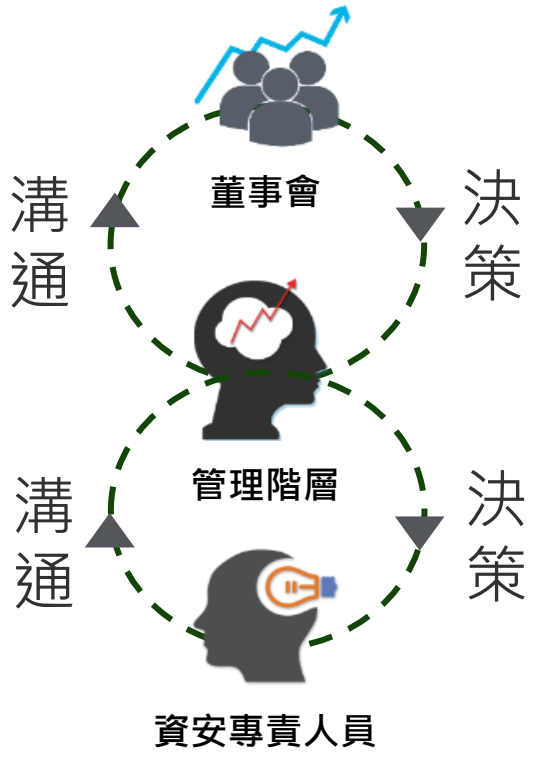
第九章 資通安全之持續精進及績效管理機制

NIST CSF IDENTIFY (ID) / ISO 27001:2013 9. 績效評估、10.改善

- **組織應規劃內部與外部稽核計畫並改善，並向董事會呈報，不斷提升資訊安全管理的適切性、適用性及有效性**



- 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。



上市櫃公司資安管理組織建議

國內資安相關法令法規及國際標準對資安組織設置之要求

資通安全管理法&施行細則	第10、16之2、17條：公務機關、關鍵基礎設施提供者與以外之特定非公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施**資通安全維護計畫**。 施行細則第6條：本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：一、核心業務及其重要性。二、資通安全政策及目標。**三、資通安全推動組織**。四、專責人力及經費之配置。五、公務機關**資通安全長之配置**。
公開發行公司建立內部控制制度處理準則	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**。
上市上櫃公司資通安全管控指引	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
DJSI 問卷問項	問卷問項：1.9.1 Information Security/Cybersecurity Governance 資訊安全治理 Are the board of directors and executive management engaged in the information security /cybersecurity strategy and review process? 董事會和執行管理階層是否參與了資訊安全策略和審查流程？
ISO/IEC 27001/27002	27001 本文5-3 組織角色、責任及權限：最高管理階層應確保**資訊安全相關角色之責任及權限已指派並傳達**。 27002 6.1 內部組織：目標：建立管理框架，以於組織內啟動及控制資訊安全之實作及運作。

風險管理的三道防線

三道防線架構是通過釐清角色和職責來強化對風險管理和控制的理解。其基本前提，從風險管理和控制有效程度而言，在董事會及高階管理層的監督和指導下，在組織內建立相互分離的群體（或防線）是必需的。

- **第一道防線**

  承擔及管理風險，並採取改正行動，以持續執行風險及控制程序。

  （一線單位負責執行資訊化日常作業及資訊資產管理及維護）

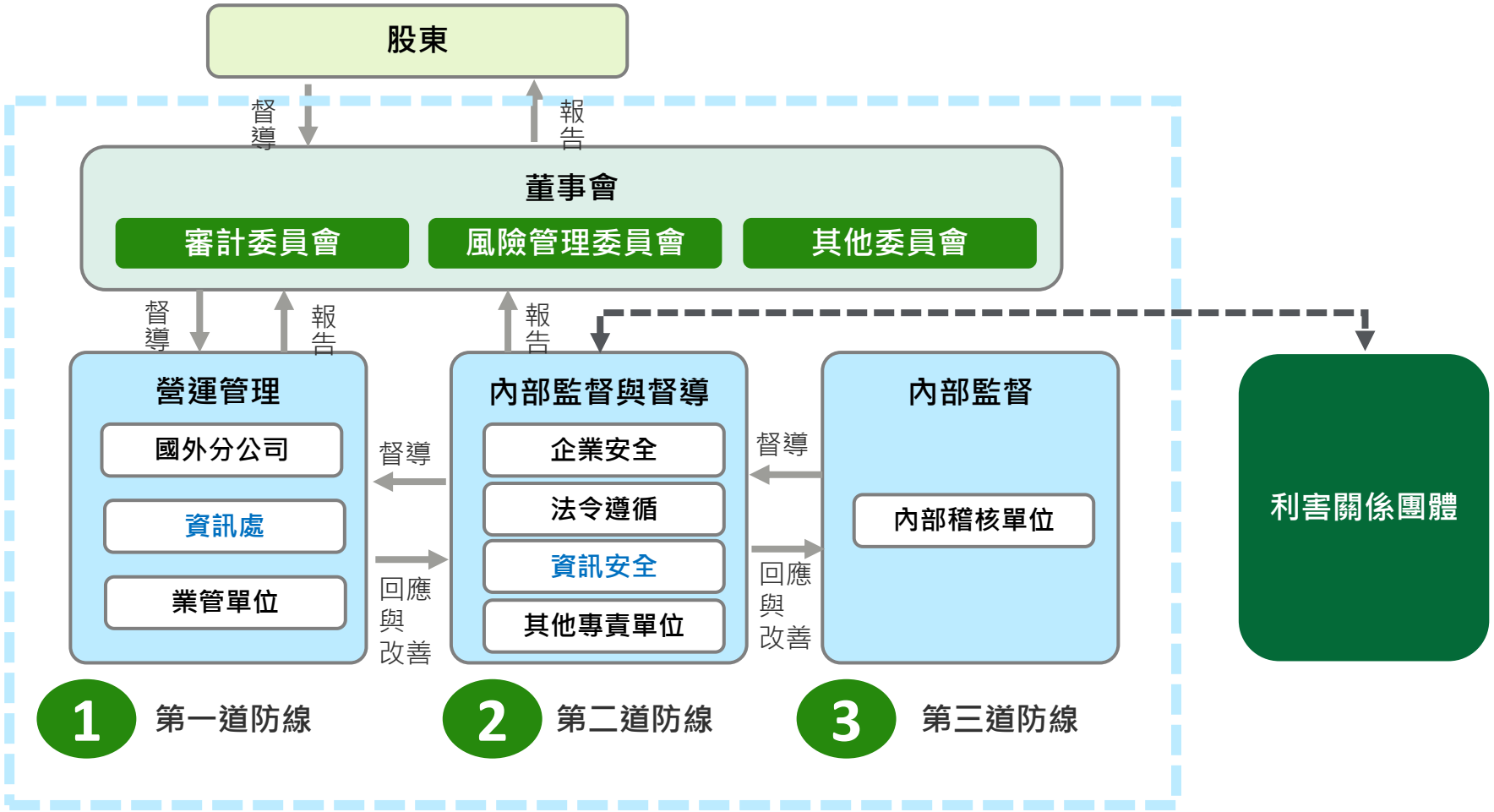
- **第二道防線**

  協助管理層並負責監控管理資訊安全政策之執行情形及其衍生之資安風險。

  （主要任務包括資安治理、資安監控與應變、風險評估與改善等）

- **第三道防線**

  對董事會和高階管理層所關心的風險和控制的有效性，進行獨立稽核並報告。（內部稽核）



資安長(CISO)與其他高階主管之分工與溝通方式

A：Accountable / R：Responsible / C：Consult / I：Inform

權責	CEO/ CFO	CCO	CISO	CIO
資訊安全控管	I	C	A	R
營運持續管理	I	C	A	R
資訊治理	I	I	C	A/R
責任保險	A/R	I	C	C
委外管理	A	C	R	R
法規監管要求	I	A	R	R

資安長(CISO) vs 資訊長(CIO)

角色	定義	職掌
資安長 (CISO)	**資安長為資訊安全風險主管。** 資安長應考量組織發展策略與願景，檢視組織環境所面臨之資訊安全風險議題後，建立和維持組織資訊安全政策，透過評估與監督資訊安全策略與計畫之實施情形，確保組織資訊安全風險管理之有效性。	• 資訊安全政策與目標建立，統籌資訊安全方針之發展與監控 • 資訊安全風險之管理及監督，發掘潛在資安風險及需求，並協助與內外部利害關係團體進行溝通與回饋 • 組織內部資訊安全責任之定義與宣導，以明確宣達資訊安全責任與要求 • 資訊安全控管標準之建立與整合，並統籌資訊安全解決方案之推動與核准，以保護資訊資產機密性、完整性和可用性 • 跨部門資訊安全事務之協調，資訊安全執行績效之評估 • 資訊安全事件之應變與協調，監督數位證據保全、數位鑑識之執行
資訊長 (CIO)	**資訊長為資訊政策與資訊治理主管。** 資訊長應考量組織發展策略與願景，定義資訊治理，負責資訊資源之分配，以確保組織之資訊技術和資訊資源規劃和整合有效性。	• 負責資訊政策與資訊發展方針之建立 • 統籌資訊資源與資訊架構發展之規劃 • 推動資訊技術與資訊業務之發展 • 督導資訊技術部門之運作，與評估資訊部門與資訊業務運作績效

資安專責單位職能規畫

資安專責單位設立目的：以全組織營運管理之角度規劃與管理資訊安全風險，以提昇整體資安維護能量

經營策略

營運管理

基礎設施管理

董事會

策略發展部門

風管法遵部門

人資部門

法務

財務

業務部門

資訊安全部門

開發中心

測試中心

維運中心

稽核組

稽核人員

制度稽核
供應商稽核
第三方稽核

治理組

合規與法令遵循人員

智財與營業秘密管理
科技法律風險評估
合規分析、遵法風險評估

技術組

資安管理人員

企業資安治理
策略規劃
制度設計
企業架構安全
流程風險管理
第三方管理
制度溝通與宣導

資安威脅分析人員

系統安全監控
弱點研究
技術檢測
資料分析
外部威脅情資蒐集
資安威脅警訊

數位鑑識人員

緊急應變
數位證據保全
數位證據分析

產品/服務設計人員

職能權限設計
智財與營業秘密管理
商業邏輯安全設計

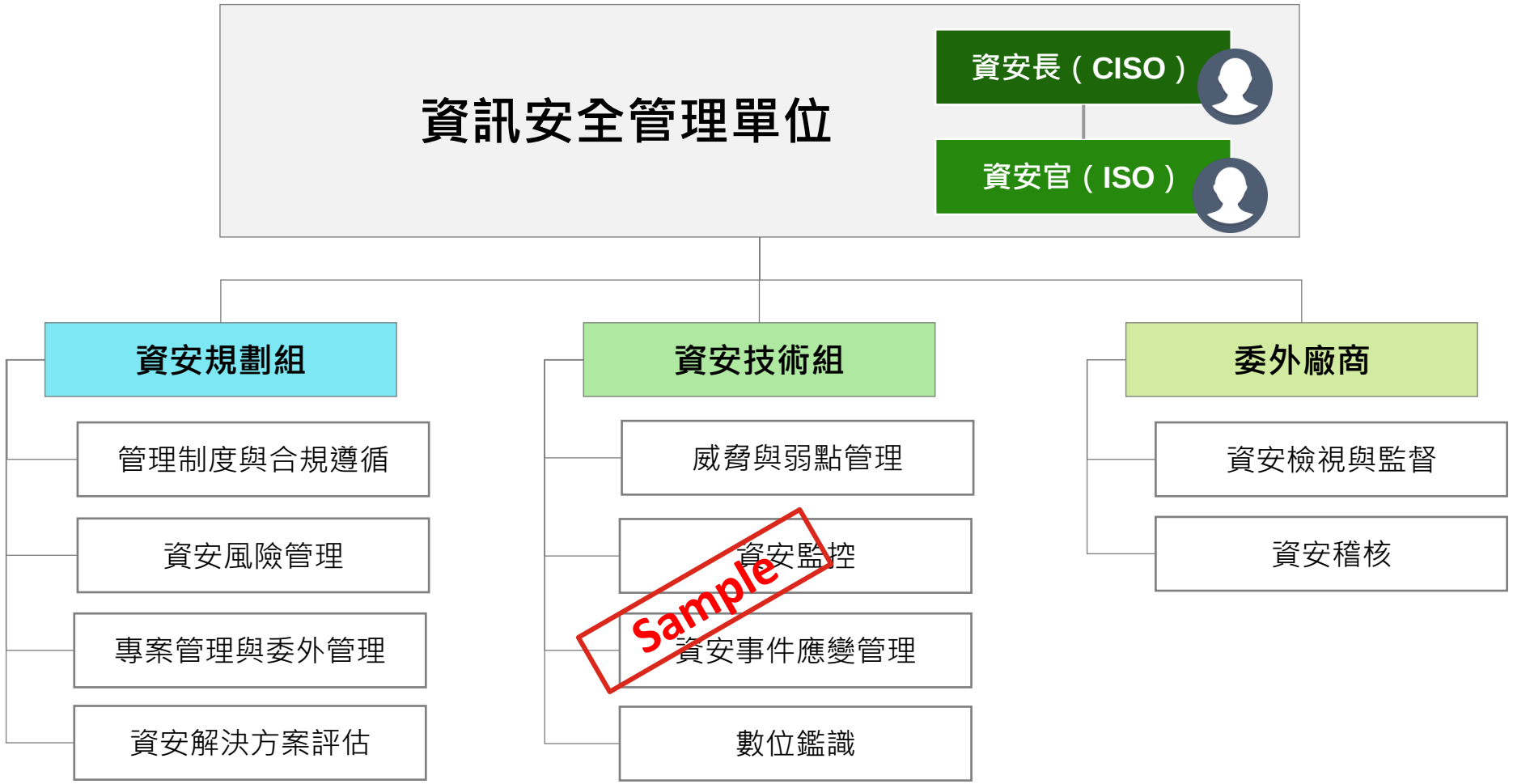
系統開發人員

資料安全
AP開發安全
產品漏洞修補

系統維運人員

網路安全
系統安全
實體安全

資安管理組織建議配置

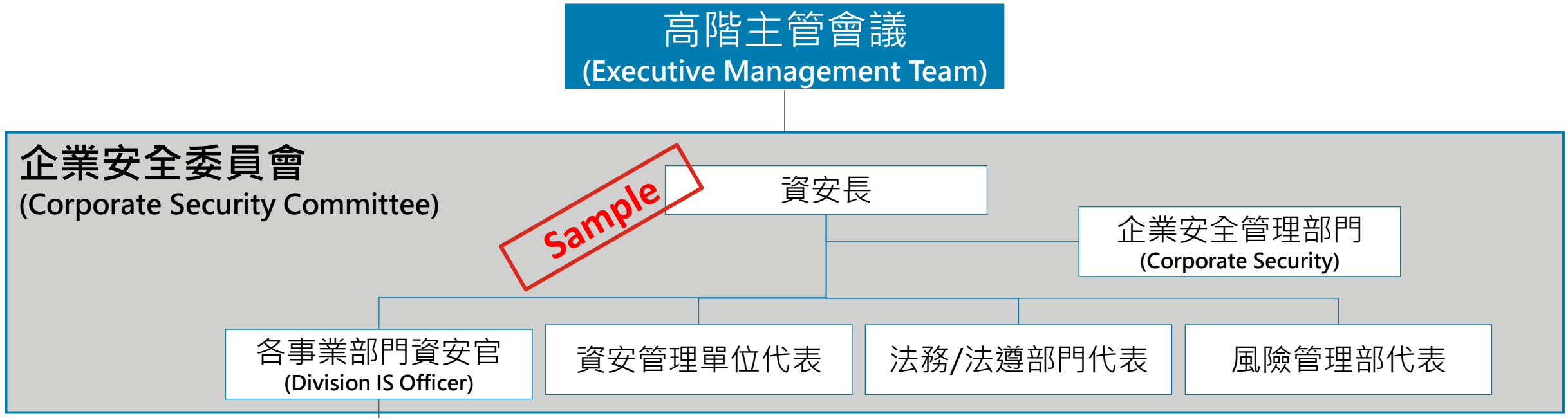


資安單位組織角色與職能定義

資安單位的功能

管理制度與資安合規遵循	- 建立符合稽核和資安合規要求之資訊安全策略、管理制度與資訊安全發展方針。 - 監控與確認資訊安全控管之有效性，確保資訊安全制度永續運作。 - 持續追蹤海內外資安合規要求，並更新管理制度。
專案管理與委外管理	- 配合業務單位之需求，建置資訊安全最佳實務。 - 配合電腦鑑識與法律遵循之活動。 - 跨部門資訊安全事務之協調，以及溝通與宣導資訊安全管理要求。
資安風險管理	- 發掘潛在資安風險及需求。 - 定義與管理風險管理程序。 - 提供業務單位相關風險諮詢服務，與提供風險管理解決方案。
資安解決方案評估	- 協助資訊安全產品之選擇。 - 提供資訊服務安全和相關解決方案之專業技術研究與諮詢服務。
資安檢視與監督	- 檢視、覆核資訊安全發展成效。 - 配合企業策略與法規要求，評估相應之資訊風險與可能之控管。
威脅與弱點管理	- 蒐集與管理外部網絡攻擊威脅與內部弱點之情報。 - 建立IT基礎架構和應用程序的弱點管理服程序。
資安監控	- 基礎架構和應用系統之稽核軌跡留存之定義、調整與等規劃管理。 - 監控及分析日誌，調查與處置疑似異常之行為。
事件應變管理	- 資訊安全事件監控與反饋，包含蒐集資訊安全事件相關資訊並反饋於監視作業中、彙整疑似資訊安全風險項目、主動通報資訊安全事件。 - 攻防演練規劃、執行結果追蹤與改善檢討。
數位鑑識	- 蒐集異常活動之紀錄，支援鑑識需要 - 鑑識資料之蒐集分析及保存 - 產製定期報告
資安稽核	- 辦理資訊安全內、外部稽核活動，與追蹤相關改善措施。

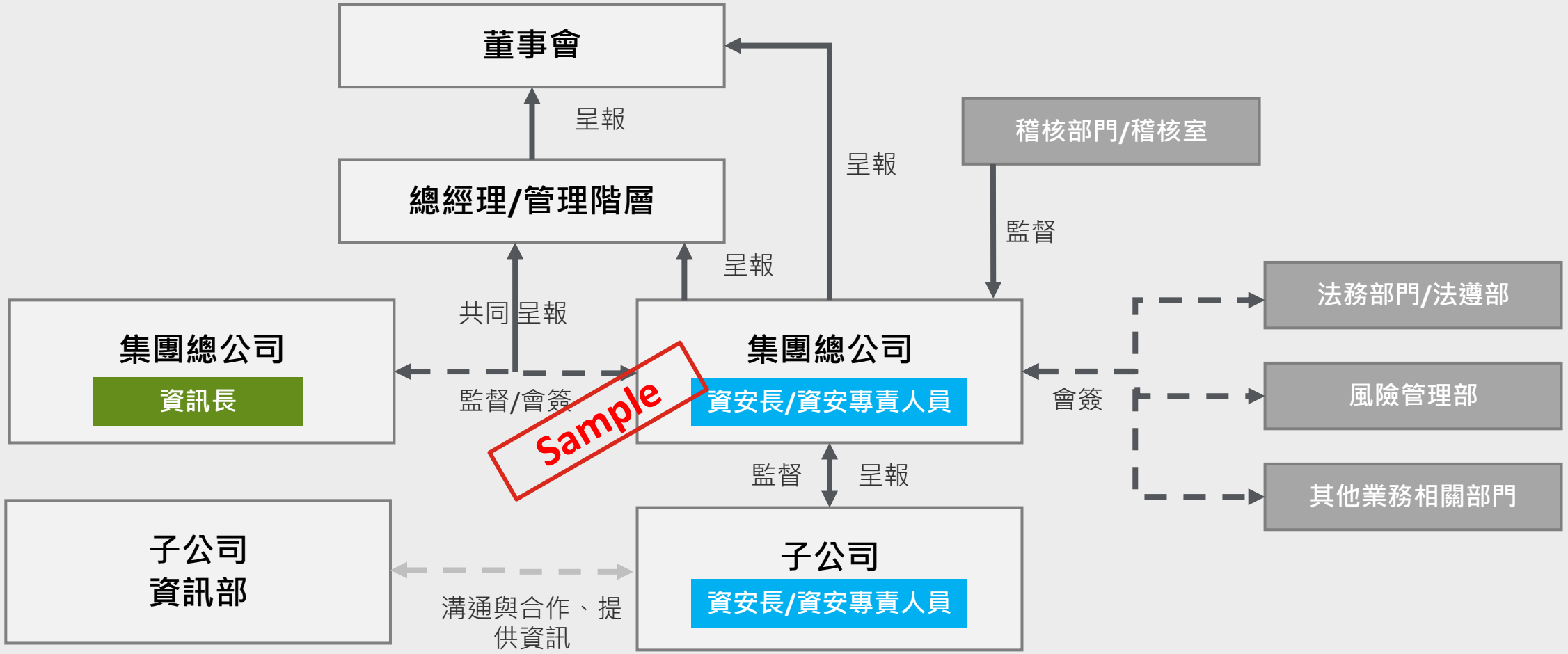
定期召開資安會議



協助企業安全委員會推動資訊安全各項事務，由各部門指派專責人員擔任成員。

- 討論與議定全公司資訊安全之重大事項。
- 督導各項管控措施之實施，評估可能面臨威脅與潛在風險。
- 覆核資訊安全風險評鑑報告，決定可接受之資訊安全風險水準。
- 考量公司之營運需求、法令異動、資訊安全需求、技術變遷及可接受風險水準等因素，審議及公布資訊安全政策、資訊安全組織、資訊安全目標及資訊安全相關規範，以確保資安制度持續有效地運作。
- 針對資訊安全議題進行意見議決、仲裁。
- 督導重大資訊安全事件之應變處理與改善措施。
- 檢討並改進現行資訊安全管理制度，以提高其運作效率及有效性。

董事會或管理階層報告路徑

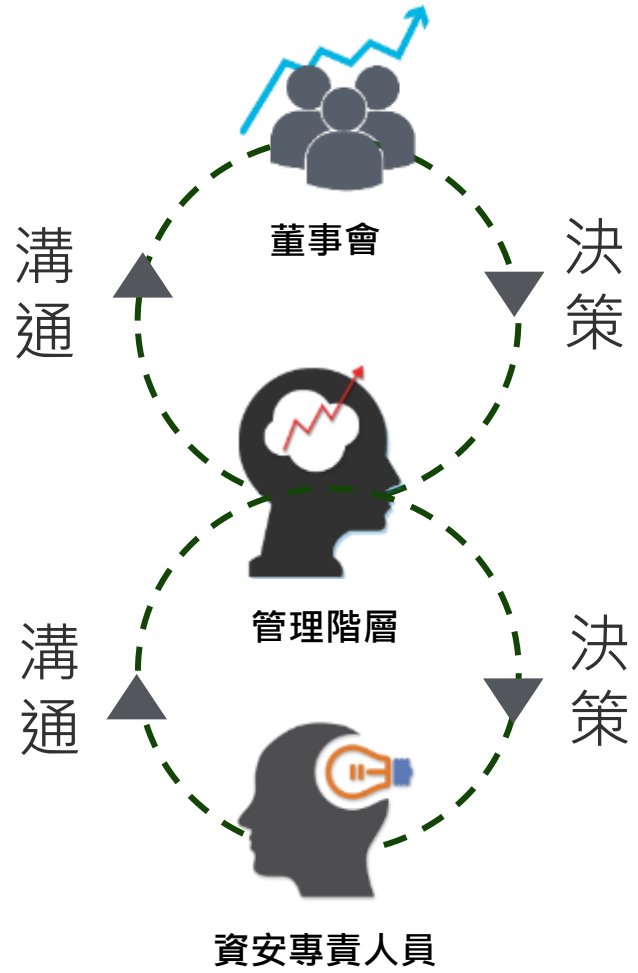


董事會或管理階層報告事項

依據董事會運作情形，提供專業人員參與董事會議方式之規畫方案，包含背景建議及專業人力清單等，並協助彙整資安相關計畫推動情形，以建立與董事會溝通機制。

風險評估過程的結果	安全監控和測試的結果	資訊安全稽核結果
• 風險評估方法、面向 • 評估所需資料蒐集來源(如內外部Cyber Security議題) • 風險評估結果	• 企業網路架構安全評估結果 • 網路與主機異常活動監控報告 • 實體安全評估與測試結果 • 系統安控測試結果(如系統、網路、APP檢測等黑白箱測試)	• 內外部查核結果 • 內外部查核發現事項改善結果
風險管理和控制決策	**安全違規事件與管理團隊回饋**	**營運持續與緊急應變**
• 風險可接受水準決策，包含固有風險、控制成熟度等 • 風險處理計畫 • 再次評估結果	• 任何可能提高風險的非法操作或安全事件分析報告 • 事件調查後的風險處理計畫 • 針對各安全違規事件的管理團隊回應(如績效考評等)	• 營運衝擊分析結果 • 營運持續計畫演練結果 • 事件通報演練結果
服務供應商的安排	**資訊安全意識提昇**	**Cyber Security 計畫更新**
• 重大服務供應商選擇與評估結果 • 重大服務供應商安全責任與要求 • 重大服務供應商定期安全評估結果 • 重大服務供應商安全事件通報應變處理結果	• 資訊安全宣導活動 • 人員資訊安全教育訓練	• 內外部Cyber Security相關議題(如生態系發展、法令法規變遷、客戶要求等) • 因應前述各項議題之Cyber Security計畫更新方案

重點議題



上市櫃公司資通安全治理實施策略

上市櫃公司資安治理要求彙整

落實內部控制制度處理準則及上市櫃資通安全指引

- 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
- 成立資通安全推動組織
- 指派適當人員擔任資安專責主管及資安專責人員
- 落實資通安全指引要求
- 與董事會及管理階層報告

遵循上櫃公司重大訊息之查證暨公開處理程序

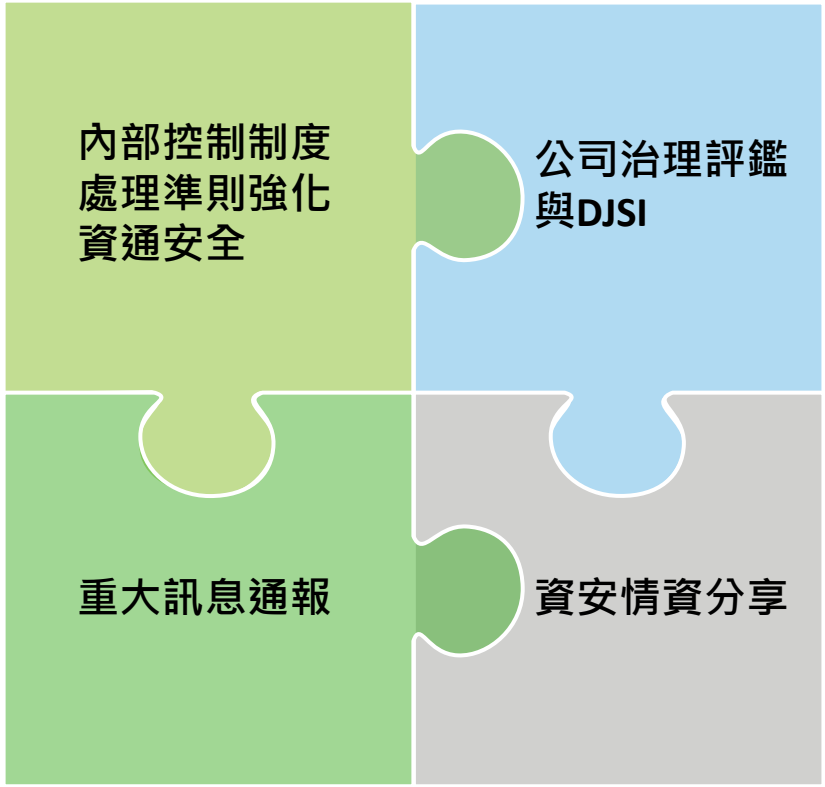
- 二十六、發生災難、集體抗議、罷工、環境污染、資通安全事件或其他重大情事，致有下列情事之一者：

  (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。

- 如上市(櫃)公司發生資通安全事件，符合上述情事者，應比照重大訊息做即時發布與通報



強化資通安全管理

- 建立資通安全管理架構及框架
- 訂定資訊安全政策
- 具體管理方案及投入資通安全管理之資源，揭露於公司網站或年報
- 邀請董事會成員或高階管理參與資訊安全策略之規劃
- 專責高階管理者統籌資訊安全策略之執行
- 取得資訊安全第三方證書或定期由專業第三方查核

資通安全事件應變與參與情資分享組織

- 訂定資安事件應變處置及通報作業程序
- 加入資安情資分享組織，如(ISAC/TWCERT)

TW CERT Coordination Center

上市櫃公司資訊安全發展藍圖

立足於2022年開始，打下組織內部資訊安全保護的根基，各階段的政策重點與關鍵工作項目說明

準備階段		機制建置階段			持續運作階段
指派專責人員	**盤點資源**	**規劃資安組織**	**建立資安機制**		**落實與維運**
指派資訊安全長	盤點核心業務及機敏資料	設計組織職掌	分析資安程序合規差異	建立委外管理機制	演練核心業務營運持續計畫
指派資安專責主管及人員	盤點資訊設備(軟體/硬體)	切分資訊與資安作業	評估技術安全控管有效性	加入資安情資分享ISAC/TWCERT	演練資安事件通報應變機制
	盤點委外服務與供應商	規劃人員編制	執行資安風險評估	建立核心業務營運持續計畫	執行委外服務供應商稽核
	盤點現有資安人力	設計資安組織與人員KPI	建立資安管理制度	建立年度資安運作計畫	執行內部稽核/外部稽核
	盤點現有資安技術控制	設計Reporting line	設計資安事件通報應變機制		發佈年度執行情形報告
	盤點現有資安程序				向董事會或管理階層報告

上市櫃公司資安治理發展策略 – 強化營運持續管理與資安韌性應有策略

謝謝聆聽

Deloitte.

勤業眾信