
CYBERSEC 2022 臺灣資安大會
CHANGE NOW
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

年報揭露資安管理作為的實務議題

報告人：陳志明

陳志明
資深總監
安永諮詢服務

Mobile +886 936 169 800
Tel +886 2 2757 8888 #67836
Email Jemmy.CM.Chen@tw.ey.com

背景介紹

學歷

- 中山大學 資訊管理研究所 碩士
- 中山大學 資訊管理學系 學士

專業資格:

- CISSP
- CISA
- ISO 27001 LA
- BS 10012 LA

相關工作經驗

- 具備金融、高科技、電信等產業商業及資訊流程的風險管理經驗，在資訊安全、機敏資料/個人資料/隱私權保護相關領域有超過15年的工作經驗
- 協助多家金控、銀行、保險及證券公司建構資訊安全風險管理架構，並取得資訊安全管理制度(ISO 27001)及個人資料保護管理制度(PIMS)國際認證
- 協助多家半導體、資訊電子業公司執行資訊安全風險管理，資訊安全架構設計、資訊系統安全評估（包含弱點掃描、滲透測試），建置ISO 27001資訊安全管理制度，並取得國際認證
- 負責過20個以上資訊安全/機敏資料保護/個人資料保護專案，協助客戶建置資訊安全管理制度、個人資料保護管理制度，並取得國際認證
- 主要的客戶群包含半導體、資訊電子、電信、金控、銀行、證券與保險、汽車、零售等產業

專業能力

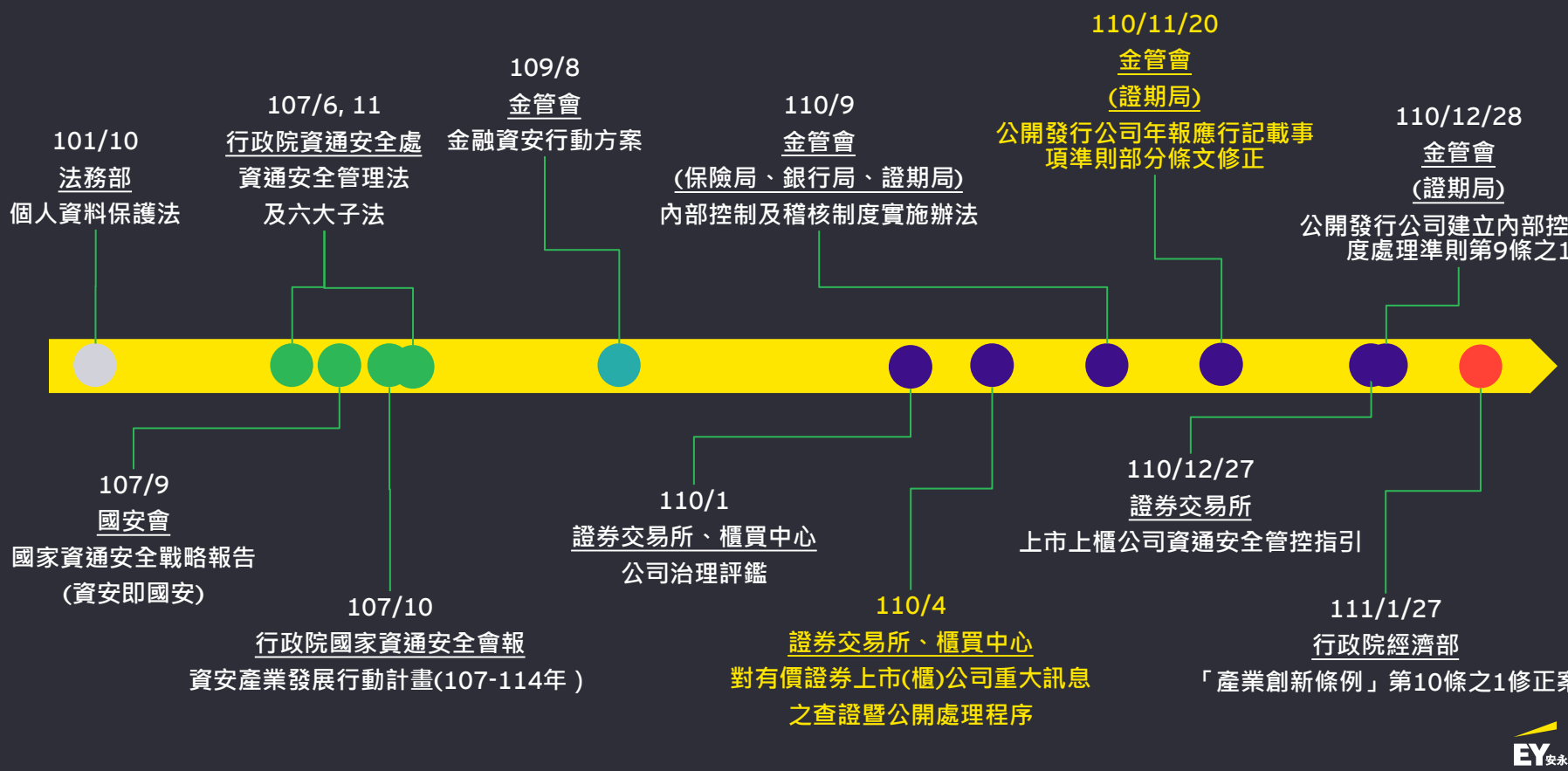
- 資訊安全風險管理制度建置
- 資訊安全架構設計與評估
- 資訊安全解決方案設計
- 機敏資料保護與管理
- 個人資料保護/隱私權管理
- 供應鏈風險管理評估
- 資訊科技環境控制諮詢
- 一般資訊循環及應用系統查核
- 資訊循環控制度設計及覆核
- 資安/SOC確信

報告大綱

1. 近期資安法規發展分享
2. 年報揭露資安管理作為分析
3. 資安管理作為資訊揭露的良好範例
4. 觀察與建議
5. 問題與討論

1 近期資安法規發展分享

我國近年與資通安全相關法律、法規



「公開發行公司年報應行記載事項準則」強化資通安全管理之資訊揭露

依據	修正條文	揭露重點
（一）資通安全已為公司營運重要議題，為強化資通安全之管理，爰明定公司應敘明**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。（修正條文第十八條）	第十八條 營運概況應記載下列事項： 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。	• 資通安全管理架構 • 資通安全政策 • 具體管理方案 • 投入資通安全管理之資源 • 重大資通安全事件之損失、可能影響及因應措施 • 資通安全保險
（二）目前公司雖可自行辨認及揭露其資通安全風險暴露情形，惟為落實公司對資通安全之風險揭露，爰明定公司應揭露**資通安全風險對公司財務業務之影響及因應措施，及因重大資通安全事 件所遭受之損失、可能影響及因應措施**。（修正條文第十八條及第二十條）	第二十條 公司應就財務狀況及財務績效加以檢討分析，並評估風險事項，其應記載事項如下： 六、風險事項應分析評估最近年度及截至年報刊印日止之下列事項： （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**。	• 風險管理架構與分析結果 • 影響與因應措施

上市公司發生重大資安事件應揭露於重訊

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	揭露重點
第二章 重大訊息 第四條 上市公司重大訊息，係指下列事項： 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。	• 營運衝擊分析 • 營運持續規劃 • 資通安全保險
第三章 重大訊息說明記者會 第十一條 上市公司重大訊息說明記者會之重大訊息，係指上市公司主動提供或經本公司主動查證之下列事項： 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股本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。	

「公開發行公司建立內部控制制度處理準則」第9條之1 (110/12/28修正)
提升公開發行公司對資訊安全之重視（規範資安組織與專責主管）

- 上市（櫃）公司應配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全維護作業。其符合一定條件者，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，並設置資訊安全專責單位、主管及人員。
- 應配置資訊安全人力之一定條件，其實施範圍及時程如下：

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： 1. 資本額100億元以上 2. 前一年底屬臺灣50指數成分公司 3. 經由網際網路或其他電子方式媒介從事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（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。	資安專責主管及至少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

2

年報揭露資安管理作為分析

揭露資安管理作為的規劃 ...

- 資通安全管理架構
- 資通安全政策
- 具體管理方案
- 投入資通安全管理之資源
- 重大資通安全事件之損失、可能影響及因應措施
- 科技改變及產業變化對公司財務業務之影響及因應措施
- 資通安全事件

- 公開發行公司年報應行記載事項準則

- 年報
- 企業官方網站

- 法令、法規規範
- 證交所、櫃買中心查核

- 落實公司對資通安全之風險揭露

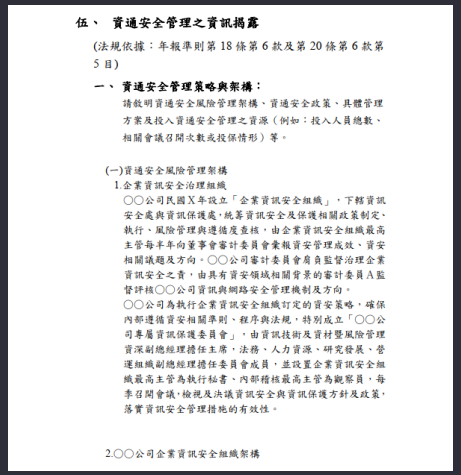
股東會年報最佳實務參考範例 - 資通安全管理之資訊揭露 (1)

章節大綱

一、資通安全管理策略與架構
(一)資通安全風險管理架構
1.企業資訊安全治理組織
2.企業資訊安全組織架構
3.專屬資訊保護委員會架構
(二)資通安全政策
1.企業資訊安全管理策略與架構
2.企業資訊安全風險管理與持續改善架構
3.具體管理方案
4.投入資通安全管理之資源

二、 資通安全風險與因應措施
(一)資訊技術安全之風險及管理措施

三、 重大資通安全事件



伍、 資通安全管理之資訊揭露

(法規依據：年報準則第 18 條第 6 款及第 20 條第 6 款第 5 目)

一、 資通安全管理策略與架構：

請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（例如：投入人員總數、相關會議召開次數或投保情形）等。

(一)資通安全風險管理架構

1.企業資訊安全治理組織

○○公司民國X年設立「企業資訊安全組織」，下轄資訊安全處與資訊保護處，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由企業資訊安全組織最高主管每年向董事會審計委員會彙報資安管理成效、資安相關議題及方向。○○公司審計委員會肩負監督治理企業資訊安全之責，由具有資安領域相關背景的審計委員A監督評核○○公司資訊與網路安全管理機制及方向。

○○公司為執行企業資訊安全組織訂定的資安策略，確保內部遵循資安相關準則、程序與法規，特別成立「○○公司專屬資訊保護委員會」，由資訊技術及資材暨風險管理資深副總經理擔任主席，法務、人力資源、研究發展、營運組織副總經理擔任委員會成員，並設置企業資訊安全組織最高主管為執行秘書、內部稽核最高主管為觀察員，每季召開會議，檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。

2.○○公司企業資訊安全組織架構

3.○○公司專屬資訊保護委員會架構

(二)資通安全政策

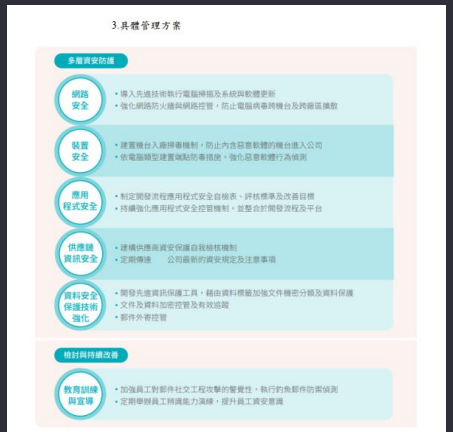
1.企業資訊安全管理策略與架構

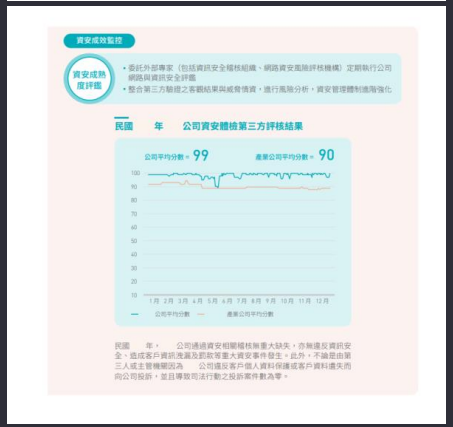
企業資訊安全組織為有效落實資安管理，透過涵蓋台灣廠區與海外子公司各單位的「資訊保護工作推動團隊」，每月召開例行會議，依據規畫、執行、查核與行動（Plan-Do-Check-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施，並定期與專屬資訊保護委員會回報執行成效。

「規畫階段」著重資安風險管理，建立完整的資訊安全管理系統(Information Security Management System, ISMS)，推動各廠區持續通過國際資安管理系統認證（ISO/IEC 27001、ISO/IEC 15408），從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求、最高規格的機密資訊保護服務。「執行階段」則建構多層資安防護，持續導入將資安防禦創新技術，將資安控管機制整合內化於軟硬體維運、供應商資安管理等日作業流程，系統化監控資訊安全，維護○○公司重要資產的機密性、完整性及可用性。「查核階段」積極監控資安管理成效，依據查核結果進行資安指標衡量及量化分析，並透過定期模擬演練資安攻擊進行資訊安全成熟度評鑑。「行動階段」則以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效；當員工違反相關規範及程序時，依據資安違規處理流程進行處置，並視違規情節進行人事處分（包括員工當年度考績或採取必要的法律行動）；此外，亦依據績效指標及成熟度評鑑結果，定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，確保○○公司重要機密資訊不外洩。

2.企業資訊安全風險管理與持續改善架構

股東會年報最佳實務參考範例 - 資通安全管理之資訊揭露 (2)






4.投入資通安全管理之資源

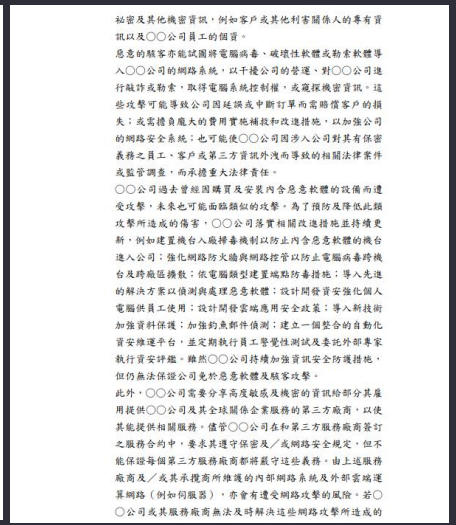
民國 X 年企業資訊安全措施推動執行成果

二、 資通安全風險與因應措施：

請敘明科技改變（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。

(一)資訊技術安全之風險及管理措施

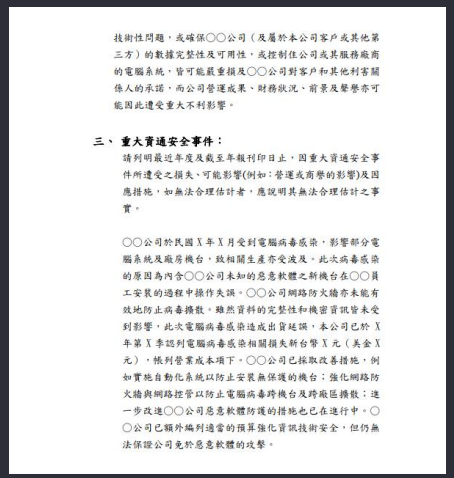
○○公司已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵○○公司的內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，○○公司的系統可能會失去公司重要的資料，生產線也可能因此停擺。○○公司透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業


秘密及其他機密資訊，例如客戶或其他利害關係人的專有資訊以及○○公司員工的個資。

惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入○○公司的網路系統，以干擾公司的管理、對○○公司進行敲詐或勒索，取得電腦系統控制權，或竊探機密資訊。這些攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統；也可能使○○公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。

○○公司過去曾經因購買及安裝內含惡意軟體的設備而遭受攻擊，未來也可能面臨類似的攻擊。為了預防及降低此類攻擊所造成的傷害，○○公司落實相關改進措施並持續更新，例如建置機台入廠掃毒機制以防止內含惡意軟體的機台進入公司；強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散；依電腦類型建置端點防毒措施；導入先進的解決方案以偵測與處理惡意軟體；設計開發資安強化個人電腦供員工使用；設計開發雲端應用安全政策；導入新技術加強資料保護；加強釣魚郵件偵測；建立一個整合的自動化資安維運平台，並定期執行員工警覺性測試及委託外部專家執行資安評鑑。雖然○○公司持續加強資訊安全防護措施，但仍無法保證公司免於惡意軟體及駭客攻擊。

此外，○○公司需要分享高度敏感及機密的資訊給部分其雇用提供○○公司及其全球關係企業服務的第三方廠商，以使其能提供相關服務。儘管○○公司在和第三方服務廠商簽訂之服務合約中，要求其遵守保密及／或網路安全規定，但不能保證每個第三方服務廠商都將嚴守這些義務。由上述服務廠商及／或其承攬廠商所維護的內部網路系統及外部雲端運算網路（例如伺服器），亦會有遭受網路攻擊的風險。若○○公司或其服務廠商無法及時解決這些網路攻擊所造成的


技術性問題，或確保○○公司（及屬於本公司客戶或其他第三方）的數據完整性及可用性，或控制住公司或其服務廠商的電腦系統，皆可能嚴重損及○○公司對客戶和其他利害關係人的承諾，而公司營運成果、財務狀況、前景及聲譽亦可能因此遭受重大不利影響。

三、 重大資通安全事件：

請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(例如：營運或商譽的影響)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。

○○公司於民國 X 年 X 月受到電腦病毒感染，影響部分電腦系統及廠房機台，致相關生產亦受波及。此次病毒感染的原因為內含○○公司未知的惡意軟體之新機台在○○員工安裝的過程中操作失誤。○○公司網路防火牆亦未能有效地防止病毒擴散。雖然資料的完整性和機密資訊皆未受到影響，此次電腦病毒感染造成出貨延誤，本公司已於 X 年第 X 季認列電腦病毒感染相關損失新台幣 X 元（美金 X 元），帳列營業成本項下。○○公司已採取改善措施，例如實施自動化系統以防止安裝無保護的機台；強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散；進一步改進○○公司惡意軟體防護的措施也已在進行中。○○公司已額外編列適當的預算強化資訊技術安全，但仍無法保證公司免於惡意軟體的攻擊。

資本額百億以上公司資安作為揭露分析 (1)

上市櫃公司資本額達百億以上公司 **119** 家，其中取得 **115** 家公司年報

年報頁數	資安作為揭露頁數	揭露內容最豐富
平均 317 頁 最薄 66 頁 最厚 709 頁	平均 2.5 頁 最薄 0.5 頁 最厚 6~7 頁	兆豐金控 中華電信 中信金控 中國鋼鐵

揭露資安架構	揭露資安政策	揭露管理方案	揭露科技改變及產業變化對財務業務之影響及因應措施
113 家	113 家	113 家	111 家

資本額百億以上公司資安作為揭露分析 (2)

揭露資安人數	揭露資安經費	揭露重大資安事件
27 家	13 家	14 家

資安人數最多

台積電
500+ 資安相關
1000+ 警勤資安

資安經費最多

- 台積電：10 億元
- 玉山金控：3 億元
- 聯發科： 2.4 億元
- 富邦金控：資安經費占資訊經費5%

最高損失金額

元大金控 1950 萬

資本額百億以上公司資安作為揭露分析 (3)

取得ISO 27001認證

68 家

揭露資安會議次數

52 家

揭露教育訓練計劃

82 家

其他資安相關標準

NIST CSF
ISO 27701
BS 10012
ISO 22301
ISO 15408
ISO 62443
FFIEC CAT
TISAX
……

會議型態

審計委員會
PIP委員會
資訊安全管理委員會
處務會議
ISMS例會
金控資安主管會議
風險管理會議
資安聯防會議
……

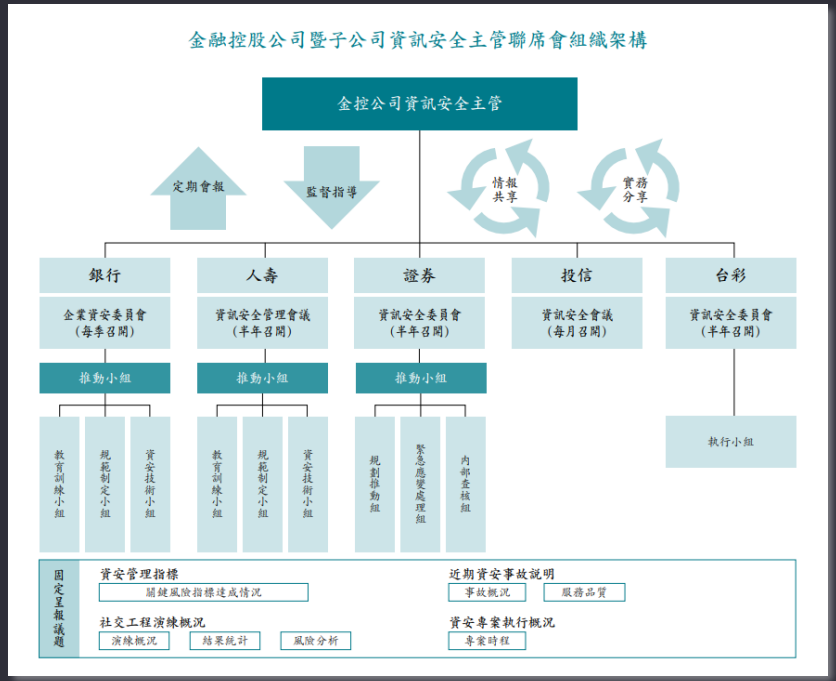
投保或評估資安險

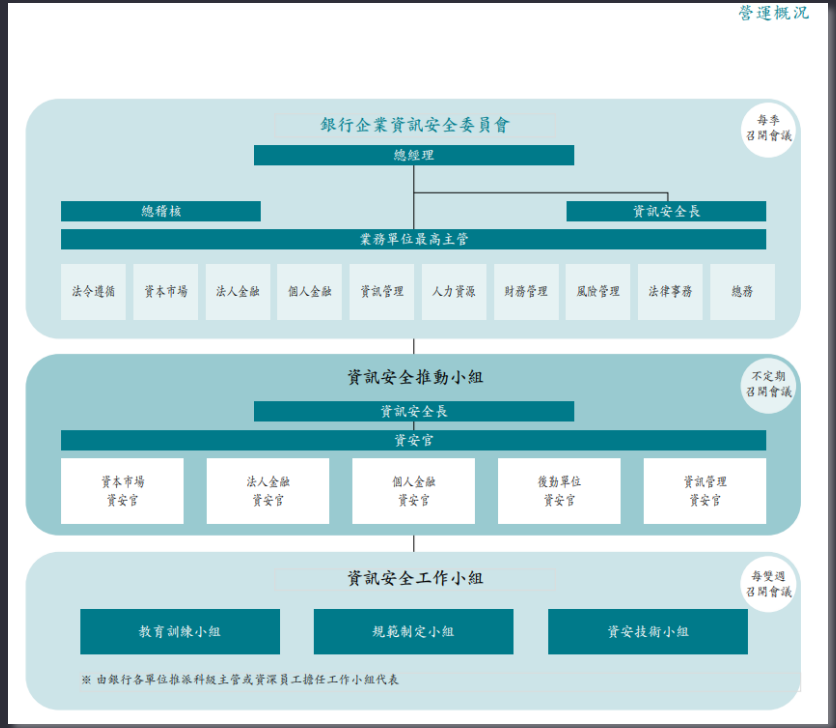
12 家

3

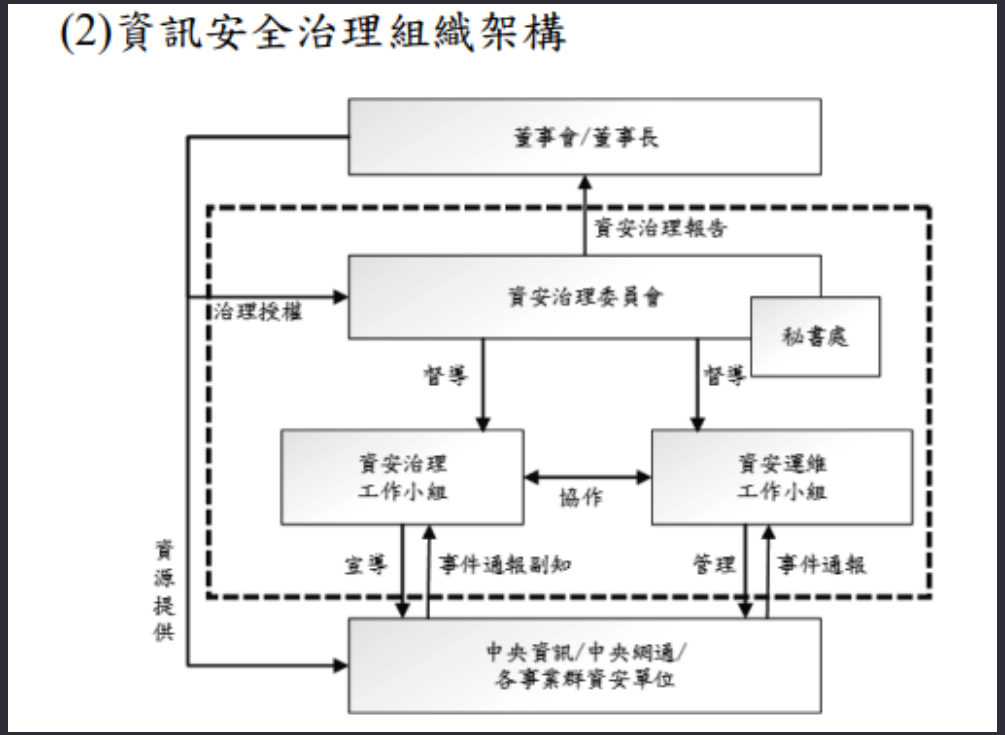
資安管理作為資訊揭露的良好範例

明確的資安政策與管理組織（中信金控）



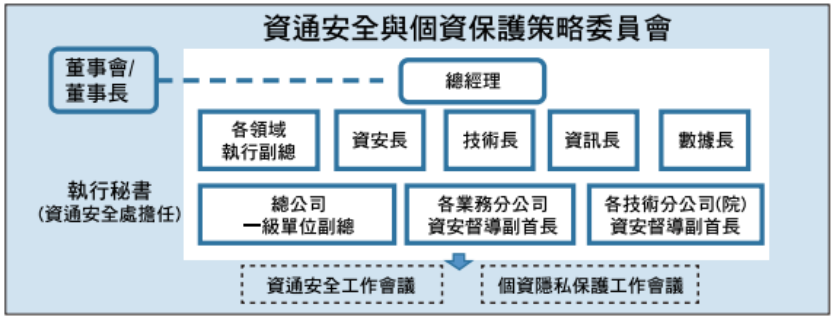


資安治理與管理的溝通模式（鴻海）

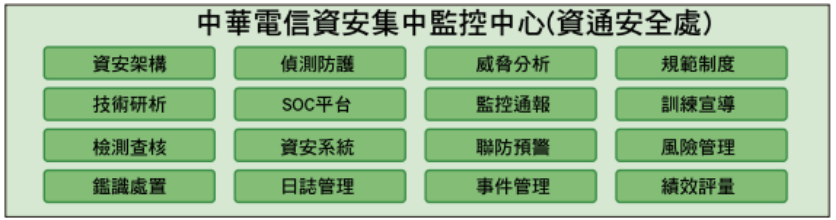


明確定義各層級角色與職掌（中華電信）

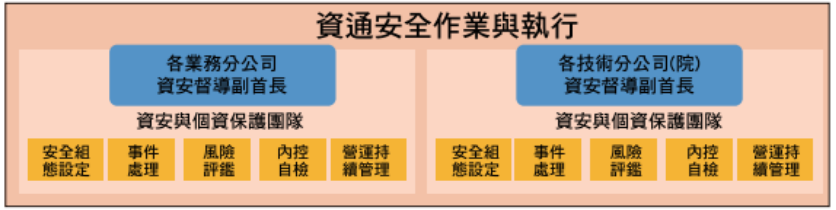
2. 資通安全組織架構



- 資安與個資隱私保護策略及治理
- 資安與個資隱私保護政策及目標制定
- 資安與個資隱私保護責任分配及資源協調
- 資安與個資隱私保護管理指標量測與監控
- 資安與個資隱私保護管理成效審查
- 資安與個資隱私保護新興風險與改善方針



- 貫徹「資通安全與個資保護策略委員會」政策方向
- 新興風險議題與對策制定
- 制定、推動公司資安與個資隱私規範與制度
- 檢視及彙報資安與個資隱私管理成效
- 監督、評核資安管理措施之合規與有效性



- 日常資通安全與個資保護執行作業，如網路設備安全設定、資訊系統安全管理、稽核日誌檢視、安全性更新與漏洞修補等

數據化績效指標並具可比較性（三商美邦人壽、緯創資通）

（四）投入資通安全管理之資源：

投入資源	110 年	109 年	108 年
資安預算編列	5,030 萬元	4,949 萬元	3,308 萬元
資安專責人力配置	資 安 長/專責主管：1 人 專責人員：10 人	專責主管：1 人 專責人員：9 人	專責主管：1 人 專責人員：8 人

策略	目標	108年成果	109年成果	110年成果
每半年執行社交工程演練	員工點擊社交工程的信件，點擊率<15%	上半年：14.5% 下半年：12.9%	上半年：10.6% 下半年：10.5%	上半年：10.8% 下半年：10.7%

（五）最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施：

	截至 111 年 2 月 28 日止	110 年度	109 年度	108 年度
(1)資安事件	0 件	0 件	0 件	0 件
(2)已發生之損失金額	0 元	0 元	0 元	0 元
(3)預計未來可能損失金額	0 元	0 元	0 元	0 元
(4)公司因應措施	雖無重大資通安全事件發生但公司仍持續強化資通安全防護：導入委外資安預警事件處理服務、強化端點防護、強化郵件防護、強化系統日誌分析告警及持續執行偽冒官網釣魚	雖無重大資通安全事件發生但公司仍持續強化資通安全防護：導入委外資安預警事件處理服務、強化端點防護、強化郵件防護、強化系統日誌分析告警及持續執行偽冒官網釣魚	雖無重大資通安全事件發生但公司仍持續強化資通安全防護：導入資安相關作業自動化、資料庫稽核系統升級、強化郵件 APT 防禦機制、強化及改善系統日誌分析告警、改善個	雖無重大資通安全事件發生但公司仍持續強化資通安全防護：升級入侵防禦系統、導入偽冒官網釣魚網站監控服務、導入防火牆政策管理軟體、執行資安治理成熟度委外評

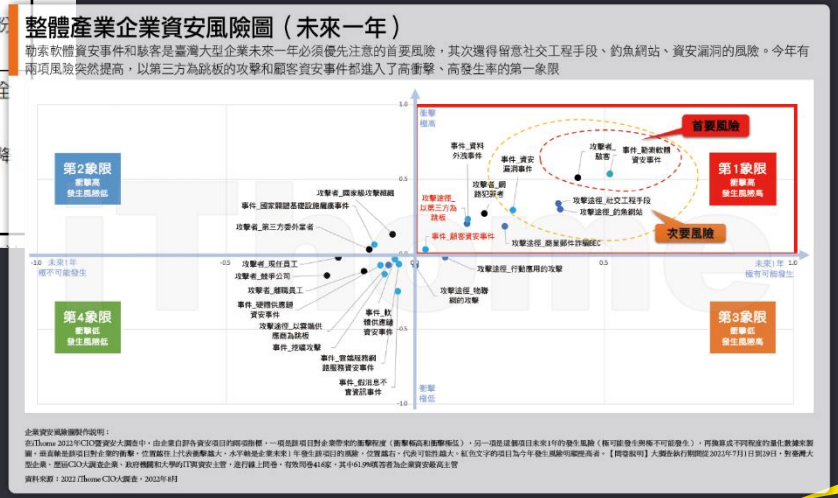
策略	目標	108年成果	109年成果	110年成果
每年執行關鍵應用系統災難復原模擬演練，確保能持續運作以保證企業的營運不中斷	關鍵應用系統RPO<=4小時 關鍵應用系統RPO<=24小時	RPO=0.9小時 RPO=19.95小時	RPO=0.5小時 RPO=21.0小時	RPO=0.8小時 RPO=22.0小時

*RPO: Recovery Point Objective(災難事故發生時最大可容忍資料遺失時間)
*RTO: Recovery Time Objective(災難事故發生後，最大可容忍資訊服務復原時間)

具體管理方案與風險評鑑相連結（金寶電子）

資安風險種類	風險內容	因應措施
員工資訊安全意識不足	內部員工處理的資料、資訊及系統，與公司營運有直接的關係，因此稍一不慎即可能因下載或感染到惡意程式，而影響到公司內部資訊安全。	1. 編製資訊安全線上教育訓練課程，列為必修課程。 2. 定期蒐集最新資訊安全攻擊手法及安全防護訊息，發佈內部資安公告與實施演練。
網路攻擊	網路駭客攻擊對企業營運造成最直接的影響，因此建置資訊硬體防護措施，包括重要網段切割與存取授權管制、防火牆、入侵偵測及阻斷攻擊的機制。	1. 對外提供連線服務的網站定期／不定期進行弱點檢測與滲透測試。 2. 應用程式保護及透過資訊安全弱點通報機制與修補工作。 3. 建立定期異地主機備援及資料備份機制，以確保營運不中斷。
病毒威脅	電腦病毒來源可能是所瀏覽的網站、含惡意程式的電子郵件(E-mail)、移動式儲存媒體(USB)、惡意程式下載等，而導致公司伺服器或電腦遭受到攻擊。	1. 建立多層次的防禦及檢測，終端全面安裝防毒系統。 2. 採中控方式進行監控及防護，以降低遭惡意程式感染及攻擊的風險。

【iThome資安風險圖】



企業資安風險圖製作說明：
在iThome 2022年CIO暨資安大調查中，由企業自評各資安項目的兩項指標：一項是該項目對企業帶來的衝擊程度（衝擊極高到衝擊極低），另一項是該項目未來1年的發生風險（極可能發生與極不可能發生），再換算成不同程度的量化數據來製圖，垂直軸是該項目對企業的衝擊，位置越往上代表衝擊越大，水平軸是企業未來1年發生該項目的風險，位置越右，代表可能性越大，紅色文字的項目為今年發生風險明顯提高者。【問卷說明】大調查執行期間從2022年7月1日至29日，對臺灣大型企業、歷屆CIO大調查企業、政府機關和大學的IT與資安主管，進行線上問卷，有效問卷416家，其中61.9%填答者為企業資安最高主管

資料來源：2022 iThome CIO大調查，2022年8月

具體的項目與成效評估（中信金控）

資安成效評估

資安整體執行成效評估

- 定期委託外部顧問及專家(包括國際標準驗證組織及資訊安全顧問公司等)定期執行資訊安全整體執行情況評估與個人資料保護作為檢查。

認證

通過ISO 27001:2013 資訊安全認證

通過BS1002:2017 個人資訊管理認證

通過PCI DSS 支付卡產業資料安全標準認證

第三方評估

個資保護確信查核 | 電腦系統資訊安全評估 | SWIFT客戶安全計畫 | 電子支付機構查核 | 資訊系統滲透測試 | 紅隊演練 | DDOS攻防演練

規範增修

120 份制度文件增修

參考國際最佳實務，定期審閱資訊及資安相關政策及作業管理規範，並依風險趨勢及最佳實務增修相關管理要求。

教育訓練及宣導

100% 完訓率

所有員工均完成年度資訊安全與個資保護年度教育訓練，總數超過10,000名人員。

14 資安宣導函

依據風險趨勢及時事。製作14篇資訊安全宣導函，持續傳達資訊安全重要規定與事項。

86% 資安週活動參與率

鼓勵單位充分了解資安相關要求並正確辨識及評估業務風險，以落實資安當責文化。

5 場資安事故演練

業務單位及資訊管理等單位於年度內辦理資安事故演練，以促使同仁熟悉事故應變流程。

社交工程演練

12 個月

每月12,000 餘演練對象

每月均參考當下時事設計釣魚郵件主題，對海內外全體同仁進行無預警演練，並於演練後公告演練成績。

資安人力配置

29 人資安一道作業

27 人資安二道作業

除在資訊安全專責單位配置27名資安專業人力外。另配置29人辦理安控系統、帳號管理及資安設備維運等一道防線作業。

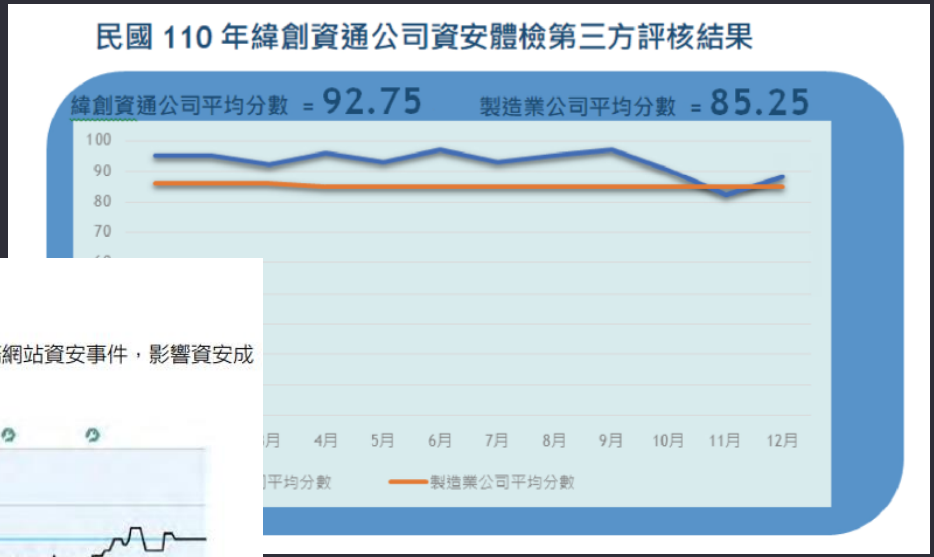
推動工作

30 餘項全行性資安工作

透過企業資安委員會轄下資安工作小組推動包含資安成熟度提升、關鍵風險防禦改善等工作，並定期呈報結果於委員會。

具體的項目與成效評估（中華電信）

透過第三方持續監控，提高揭露資訊可信度（宏碁、緯創資通）



產業標準為Industry Avg.， 分數約為84，成熟度為 B。

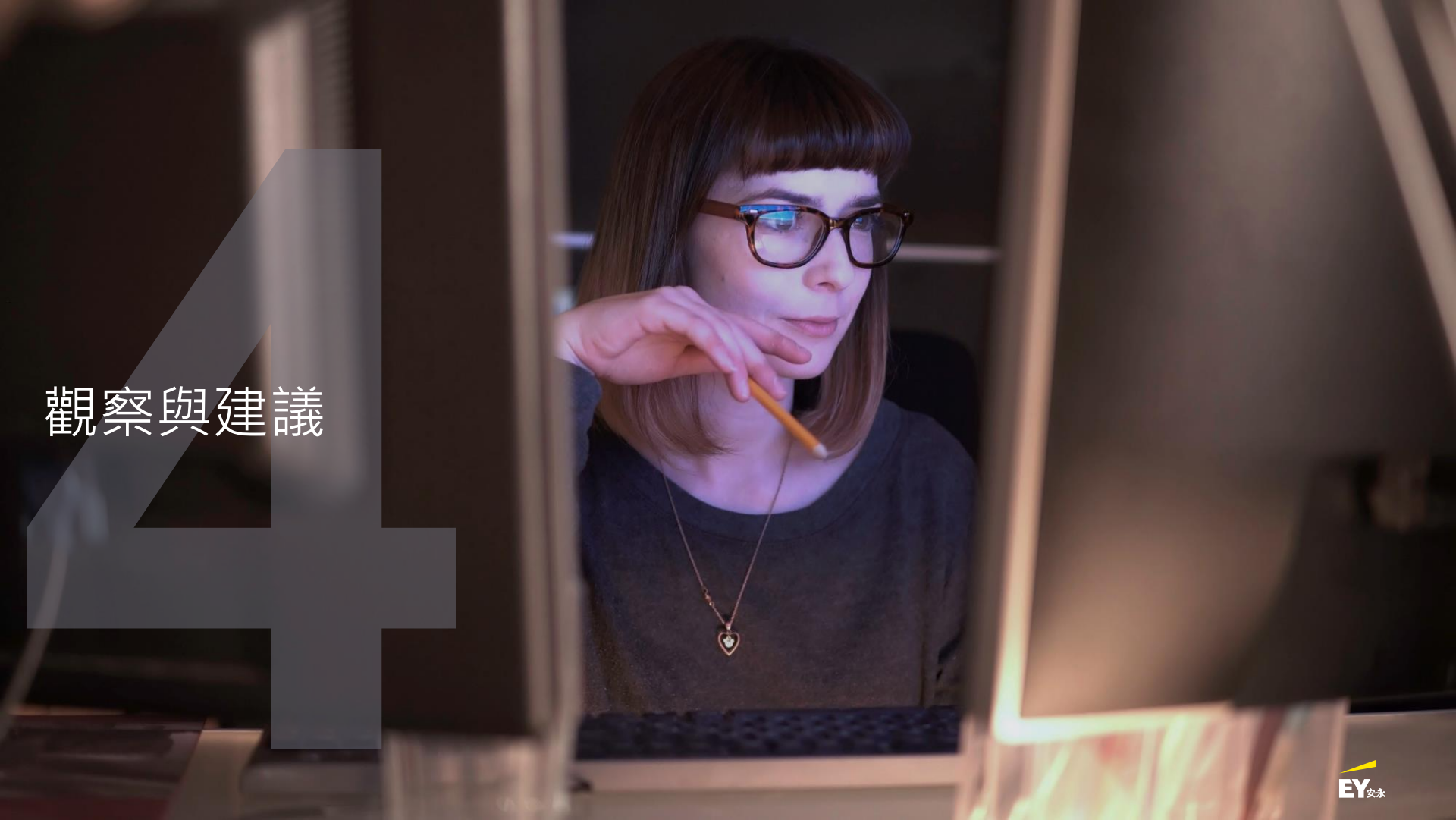
Acer為Acer Grade，除了因為2021年3月全球資安事件及10月因印度與台灣服務網站資安事件，影響資安成熟度被扣分，其餘均保持向上趨勢，與國際產業標準對齊。

最有彈性的揭露方式（台灣塑膠）

5. 有關本公司資訊安全管理更詳盡內容及未來規劃，請參考本公司永續發展網站。
http://csr.fpc.com.tw/FPC_CSR/coporate_governance/information_security.aspx

4

觀察與建議



觀察重點(1) - 主管機關的意向

- 資通安全管理架構
- 資通安全政策
- 具體管理方案
- 投入資通安全管理之資源
- 重大資通安全事件之損失、可能影響及因應措施
- 科技改變及產業變化對公司財務業務之影響及因應措施
- 資通安全事件

- 公開發行公司年報應行記載事項準則

- 年報
- 企業官方網站

- 法令、法規規範
- 證交所、櫃買中心查核

美國揭露資安作為的相關法規

- 國會
  - 建議修訂SOX法案：上市公司應提供對資訊系統的安全、網路安全風險評估的執行、內部記錄的維護進行評估說明，以及資訊系統與數據的風險管理計劃的管理評估與確信佐證。
  - Cybersecurity Disclosure Act of 2021 草案：要求上市公司在其年報或年度代理聲明中揭露董事會是否有任何成員具有資訊安全方面的專業知識或經驗。如果董事會成員沒有資訊安全專業知識，則需揭露提名和評估董事會成員的考量面向。

- 證券交易委員會（SEC）資訊安全揭露規則（預計2023 Q1）
  - 公司董事會是否有具備資訊安全專業知識成員，如果有，這些專業知識的性質
  - 整個董事會、特定董事會成員或董事會委員會是否監督資訊安全風險；董事會如何獲悉這些風險，包括討論該主題的頻率；以及董事會或相關董事會委員會如何將風險視為其對業務戰略、風險管理和財務監督的監督的一部分
  - 用於識別和管理資安威脅的政策、程序和策略（如果有）
  - 管理層評估和管理資安風險以及實施公司的資安政策、程序和戰略方面的效果，包括某些管理職位或委員會是否負責衡量和管理資訊安全風險，以及公司是否有指定的資安長（CISO）
  - 在確定重大資安事件後的四個工作日內以表格 8-K 披露重大資安事件，並且在定期報告中提供有關先前披露的重大事件的更新。此外，必須披露一系列先前未披露的個別非重大資安事件何時成為重大事件的總和。

Institutional Shareholder Services(ISS) 新增11項評估公司治理的資安風險因素

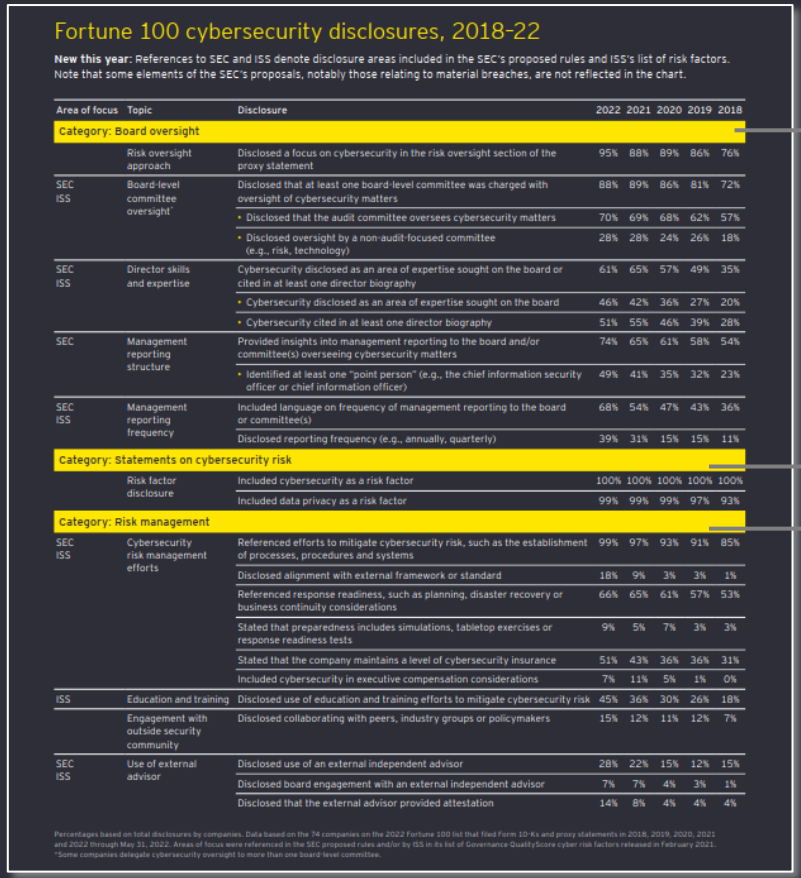
1. 負責資訊安全風險的委員會中有多少是獨立的？
2. 高層管理層多久向董事會通報一次資訊安全議題？
3. 董事會中有多少具有資訊安全經驗的董事？
4. 公司是否揭露識別和減輕資訊安全風險的方法？
5. 相對於總收入，過去三年因資訊安全漏洞而產生的淨費用是多少？
6. 公司在過去三年中是否發生過資訊安全漏洞？
7. 過去三年資訊安全違規處罰及和解所產生的淨費用佔總收入的比例是多少？
8. 公司是否簽訂資訊安全風險保險單？
9. 公司是否通過資訊安全標準認證或進行外部稽核？
10. 公司是否有資訊安全培訓計劃？
11. 最近一次資訊安全漏洞發生在多久前（以月計）？

Source： ISS ESG Unveils 2021 Methodology Enhancements for Governance QualityScore, February 8, 2021.

董事會成員具備資安專業範例 - Morgan Stanley

	DARLING	GLOCER	GORMAN	HERZ	JAMES	KAMEZAWA	LEIBOWITZ	LUCZO	MISCIK	MIYACHI	NALLY	SCHAPIRO	TRAQUINA	WILKINS	TOTAL
Experience, Qualifications and Skills															
Leadership	•	•	•	•	•	•	•	•	•	•	•	•	•	•	14
Global / International Perspective	•	•	•	•		•	•	•	•	•	•		•	•	12
Financial Services	•		•	•		•	•	•	•	•	•	•	•		11
Current or Former CEO		•	•			•		•	•		•	•	•	•	9
Accounting / Financial Reporting		•	•	•						•	•	•	•	•	8
Human Capital Management		•	•		•	•	•	•	•	•	•	•	•	•	12
Risk Management	•		•			•	•		•	•	•	•	•		9
Cybersecurity / Technology / Information Security		•				•	•	•	•		•			•	7
Academia / Government / Public Policy / Regulatory Affairs	•	•	•		•	•		•	•	•	•	•	•	•	12
ESG / Sustainability			•	•	•	•				•		•	•	•	8
Public Company Governance		•	•	•	•	•	•	•	•	•	•	•	•	•	13
Board Tenure and Diversity															
Years on the Board (from date first elected)	6	9	12	9	0	1	1	2	7	0	5	3	7	8	5.5

董事會關注資安議題 - EY Fortune 100大揭露調查 (2018-22)



Fortune 100 cybersecurity disclosures, 2018-22

New this year: References to SEC and ISS denote disclosure areas included in the SEC's proposed rules and ISS's list of risk factors. Note that some elements of the SEC's proposals, notably those relating to material breaches, are not reflected in the chart.

Area of focus	Topic	Disclosure	2022	2021	2020	2019	2018
Category: Board oversight							
	Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	95%	88%	89%	86%	76%
SEC ISS	Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	88%	89%	86%	81%	72%
		• Disclosed that the audit committee oversees cybersecurity matters	70%	69%	68%	62%	57%
		• Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	28%	28%	24%	26%	18%
SEC ISS	Director skills and expertise	Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	61%	65%	57%	49%	35%
		• Cybersecurity disclosed as an area of expertise sought on the board	46%	42%	36%	27%	20%
		• Cybersecurity cited in at least one director biography	51%	55%	46%	39%	28%
SEC	Management reporting structure	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	74%	65%	61%	58%	54%
		• Identified at least one "point person" (e.g., the chief information security officer or chief information officer)	49%	41%	35%	32%	23%
SEC ISS	Management reporting frequency	Included language on frequency of management reporting to the board or committee(s)	68%	54%	47%	43%	36%
		Disclosed reporting frequency (e.g., annually, quarterly)	39%	31%	15%	15%	11%
Category: Statements on cybersecurity risk							
	Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%	100%	100%
		Included data privacy as a risk factor	99%	99%	99%	97%	93%
Category: Risk management							
SEC ISS	Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	99%	97%	93%	91%	85%
		Disclosed alignment with external framework or standard	18%	9%	3%	3%	1%
		Referenced response readiness, such as planning, disaster recovery or business continuity considerations	66%	65%	61%	57%	53%
		Stated that preparedness includes simulations, tabletop exercises or response readiness tests	9%	5%	7%	3%	3%
		Stated that the company maintains a level of cybersecurity insurance	51%	43%	36%	36%	31%
		Included cybersecurity in executive compensation considerations	7%	11%	5%	1%	0%
ISS	Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	45%	36%	30%	26%	18%
	Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	15%	12%	11%	12%	7%
SEC ISS	Use of external advisor	Disclosed use of an external independent advisor	28%	22%	15%	12%	15%
		Disclosed board engagement with an external independent advisor	7%	7%	4%	3%	1%
		Disclosed that the external advisor provided attestation	14%	8%	4%	4%	4%

Percentages based on total disclosures by companies. Data based on the 74 companies on the 2022 Fortune 100 list that filed Form 10-Ks and proxy statements in 2018, 2019, 2020, 2021 and 2022 through May 31, 2022. Areas of focus were referenced in the SEC proposed rules and/or by ISS in its list of Governance QualityScore cyber risk factors released in February 2021.
*Some companies delegate cybersecurity oversight to more than one board-level committee.

董事會監督

- 風險監督方法
- 董事會層級的監督
- 董事技能與專業知識
- 管理報告結構
- 管理報告頻次

資訊安全風險聲明

- 風險因素揭露(資安、隱私保護)

風險管理

- 資訊安全風險管理工作
- 教育與培訓
- 與資安社群的聯繫
- 使用外部顧問

觀察重點(2) - 資安藍圖規劃與持續性的作為

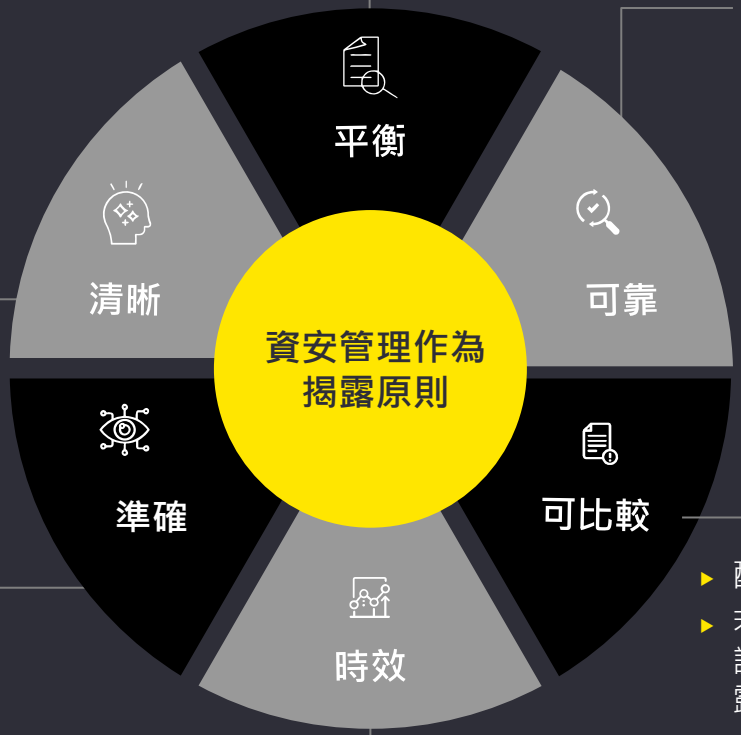
觀察重點(3) - 在有限的篇幅呈現優質的內容

- 除了揭露資安作為，若有資安事件，甚或造成財務影響，亦需充分揭露

- 報告書內容與資料應具備可靠度

- 章節編排架構清楚
- 版面設計與文字說明清晰易讀
- 善用圖表或指標的方式呈現

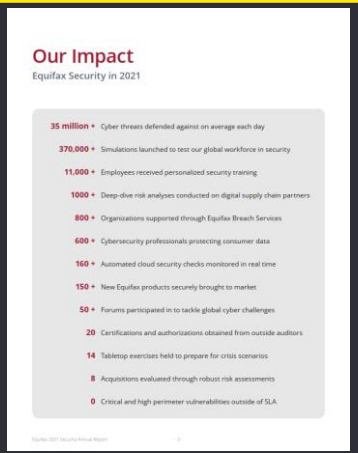
- 揭露內容與主軸可事前針對每年之進程與差異進行規劃
- 可參考同業或領先企業，評估與規劃未來執行方向

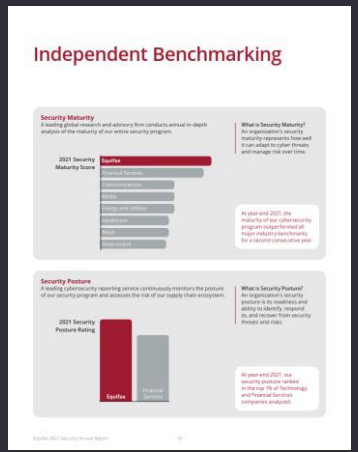


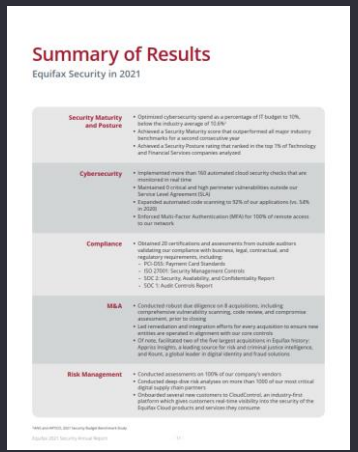
- 準確揭露要求內容
- 呼應主題，適時提供統計數據

- 配合年報製作時限，彙整最新現狀
- 若於非出版時間有特殊事件發生時，建議利用公開資訊觀測站或企業網站，揭露重大訊息

資安年報範例 - Equifax







2021-security-annual-report.pdf (equifax.com)

問題與討論

安永 | 建設更美好的商業世界

安永的宗旨是致力建設更美好的商業世界。我們以創造客戶、利害關係人及社會各界的永續性成長為目標，並協助全球各地資本市場和經濟體建立信任和信心。

以數據及科技為核心技術，安永全球的優質團隊涵蓋150多個國家的業務，透過審計服務建立客戶的信任，支持企業成長、轉型並達到營運目標。

透過專業領域的服務 - 審計、諮詢、法律、稅務和策略與交易諮詢，安永的專業團隊提出更具啟發性的問題，為當前最迫切的挑戰，提出質疑，並推出嶄新的解決方案。

加入安永**LINE@**好友
掃描二維碼，獲取最新資訊。

APAC no. (請填上SCORE number)
ED MMYY [填寫圖片版權到期日，若無到期日請寫上 ED None; 若無圖片請刪除]

ey.com/zh_tw