推動上市櫃公司強化資安的政策執行近況與推動事宜

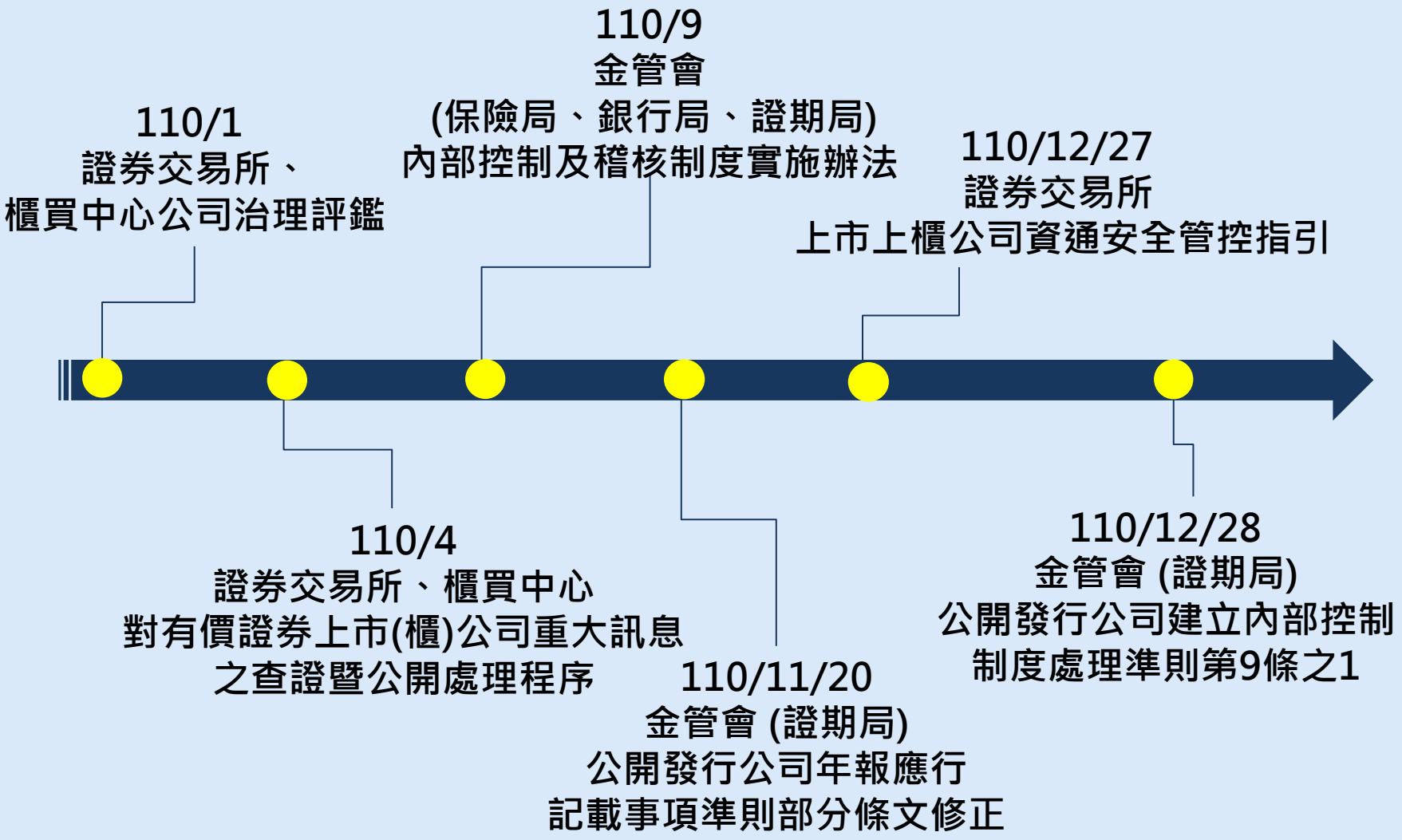
2023.5.11

TAIWAN STOCK EXCHANGE

2022全球資通安全威脅趨勢

資料來源：國家資通安全研究院 111年12月
政府機關資安威脅與防護重點

近年與資通安全相關法律、法規



上市(櫃)公司資安管理架構

公司治理

資訊公開

監理協助

上市櫃公司資通安全防護

上市(櫃)公司資安管理措施

竭誠為您服務

資訊公開

- 年報及公開說明書揭露重大資安風險
- 重大訊息即時說明重大資安事件
- 加強查核公司重大訊息資訊揭露內容之妥適性

公司治理

- 資安納入內部控制制度(含人員與系統)
- 資安納入公司治理評鑑項目
- 透過公司治理評鑑鼓勵取得資安管理標準相關驗證
- 依資安風險程度要求或鼓勵設置資安單位及人員

監理協助

- 將資安納入內部控制制度查核項目
- 教育宣導
- 成立任務型專案小組推動執行
- 制定上市上櫃公司資通安全管控指引
- 推動上市(櫃)公司加入領域ISAC或TWCERT/CC

資訊公開措施(1/2)

年報及公開說明書揭露重大資安風險

- 重大資安風險
  - 若資安風險為公司重大營運風險者，應於年報(定期)及公開說明書(不定期)中揭露資安風險及因應措施
- 資安管理之資訊揭露
  - 年報及公開說明書增加資安管理之資訊揭露

資安資訊揭露

1. 資安風險管理架構、資安政策、具體管理方案及投入資源
2. 重大資安事件所遭受之損失、可能影響及因應措施
3. 科技改變（含資安風險)對公司財務業務之影響及因應措施

資訊公開措施(2/2)

重大訊息即時說明重大資安事件

- 如發生對其股東權益或證券價格有重大影響之資安事件時，應即時發布重大訊息對外說明
- 加強查核上市(櫃)公司重大訊息資訊揭露內容之妥適性

公司治理措施(1/3)

內部控制制度(內控準則第8條、第9條、第13條)

- 公司應建立適當並有效之**內部控制制度**以確保**個人資料保護管理**及**資通安全檢查**作業之適法性與妥適性
- 應包括程式及資料存取等11項控制作業
- 應將「資通安全檢查」列為公司年度稽核計畫之稽核項目
- 內部稽核人員應持續進修，並參加電腦稽核相關講習

公司治理措施(2/3)

設置資安長、資安專責單位及資安人員

111年底前設置資安專責單位、資安長、資安主管及至少2名專責人員

112年底前配置資安主管及至少1名專責人員

鼓勵配置至少1名專責人員

第一級公司

- 資本額100億元以上
- 台灣五十成分股公司
- 主要經濟活動以電子式方式媒介商品或服務者

第二級公司

- 第一級以外的上市(櫃)公司
- 最近未連續3年虧損且每股淨未低於面額

第三級公司

- 第一級以外的上市(櫃)公司
- 最近連續3年虧損或每股淨值低於面額

公司治理措施(2/3表A)

資安長、資安專責單位及資安人員設置狀況

(截至112年4月30日)

		第一級公司		第二級公司	
		上市	上櫃	上市	上櫃
	合計	102	13	772	671
資安主管	已設置	102	13	170	125
	未設置	0	0	602	546
資安人員	已設置	102	13	170	138
	未設置	0	0	602	533
整體設置	皆已設置	102	13	154	118
	尚未完整	0	0	618	553

公司治理措施(2/3表B)

資安長、資安專責單位及資安人員設置狀況

(截至112年4月30日)

資安分級標準	家數		
	上市	上櫃	合計
第一級	102	13	115
第二級	772	671	1443
第三級	70	117	187
合計	944	801	1745

設置完成率	家數	
	上市	上櫃
第一級	100%	100%
第二級	20%	18%
第三級	0%	0%

公司治理措施(3/3)

調整公司治理評鑑項目鼓勵企業提升資安

評鑑項目

- 公司是否**建置資訊安全風險管理架構**、**訂定資安政策**（如成立資安委員會定期檢討資安政策，並定期向董事會報告等）、**具體管理方案及投入資安資源，並揭露於公司網站或年報**

加分項目

- **導入ISO27001、CNS27001等資訊安全管理系統標準**，或其他具有同等或以上效果之系統或標準，**並取得第三方驗證**

TAIWAN STOCK EXCHANGE

公司治理評鑑資安指標

竭誠為您服務

	DJSI	MSCI ESG Index	FTSE FTSE4GOOD	公司治理評鑑 第九屆
監督層級	●			
政策與機制	●	●	●	●
流程與基礎架構	●			●
引用國際標準 (e.g.ISO 27001、TRUSTe標準)	●	●		●
第三方驗證	●	●		●
定期弱點分析	●	●		
事件因應	●	●		
收集與留存數據最小化		●		
政策涵蓋供應鏈/合作夥伴		●		
資安教育訓練	●	●		

監理協助措施(1/4)

查核

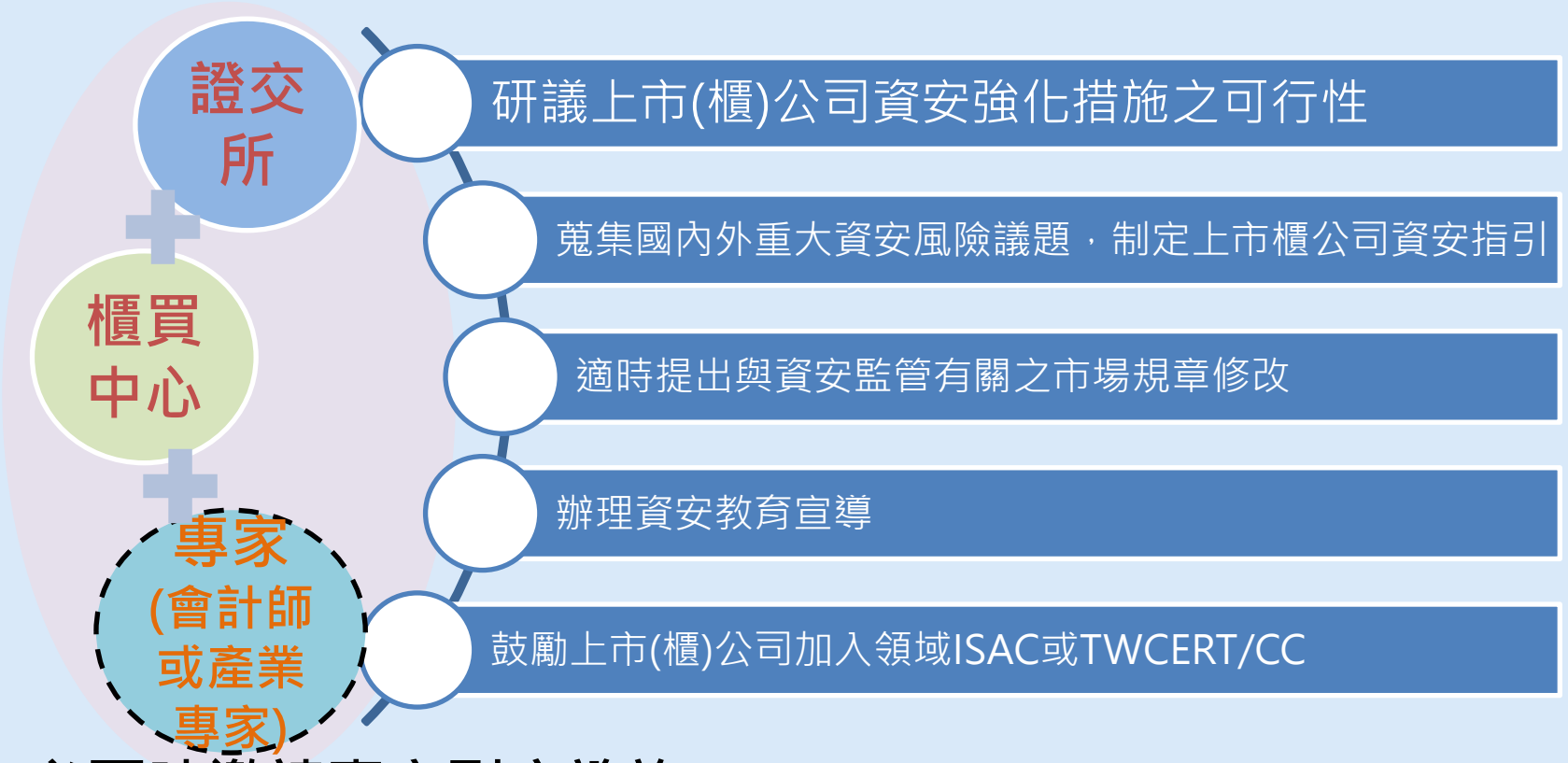
- 資安列入對上市(櫃)公司內部控制制度查核作業之選定稽核項目，視個案公司資安風險程度不定期納入查核

教育訓練

- 資安課程納入上市櫃公司董事進修課程
- 上市(櫃)公司資安宣導

監理協助措施(2/4)

成立任務型專案小組，協助公司落實資安防護



必要時邀請專家列席諮詢

監理協助措施(3/4)

制定上市上櫃公司資通安全管控指引
(可衡諸產業特性、規模大小及資安風險適度採行之)

- 資安政策及推動組織
- 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
- 資安防護及控制措施
- 資通系統或資通服務委外管理
- 資安事件通報應變及情資評估因應
- 資安之持續精進及績效管理機制

監理協助措施(4/4)

鼓勵加入資通安全情資分享平台

領域資安情資分享平臺	主管機關	可能參與之上市(櫃)產業
金融領域(F-ISAC)	金管會	金融保險業
科技領域(SP-ISAC)	科技部	電機機械、電器電纜、半導體業、電腦及週邊設備業、光電業、電子零組件業、電子通路業、資訊服務業、其他電子業
醫療領域(H-ISAC)	衛服部	生技醫療業(需為醫院)
能源領域(E-ISAC)	經濟部	油電燃氣業
通訊傳播(C-ISAC)	NCC	通信網路業
交通領域(T-ISAC)	交通部	航運業
TWCERT	NCC	未設參加限制，所有產業均得加入

監理協助措施(4/4表A)

鼓勵加入資通安全情資分享平台

- 上市櫃公司尚未加入各領域ISAC或TWCERT/CC之家數，及遞交申請加入TWCERT/CC之KPI

	上市公司			上櫃公司		
	截至第二次資安小組會議尚未加入家數	KPI		截至第二次資安小組會議尚未加入家數	KPI	
		%	家數		%	家數
第一級	73	80	58	8	80	6
第二級	577	50	289	552	25	138

監理協助措施(4/4表B)

鼓勵加入資通安全情資分享平台

監理協助措施	上市公司		上櫃公司	
	第一級	第二級	第一級	第二級
推動上市櫃公司加入資安情資分享組織期程	111年上半年	112年底前	111年上半年	112年底前
上市櫃公司原已加入家數(A)	24	76	3	44
上市櫃公司KPI(B)	58	289	6	138
目標加入總家數(A+B)	82	365	9	182
111年上半年已加入家數	82	--	10	--
截至112年3月7日加入家數	91	76+166=242	10	44+143=187

監理協助措施(4/4)

持續強化機構企業資通安全管理

證交所

持續追蹤112年底前全體第2級公司應完成資安專責主管與資安專責人員之設置

櫃買中心

每半年召開「強化上市櫃公司資安措施任務小組」會議，以強化上市櫃公司資安治理，並協助上市櫃公司落實資安防護

其他推動事宜

- 內控查核項目現已規劃"增加個資查核項目"，內控查核項目內容已報局，待主管機關核可後執行
- 國發會：防止非公務機關個資外洩精進措施

國發會：防止非公務機關個資外洩精進措施

◆強化業者防護能力、完備法制、落實執法，提升個資保護

策略一	策略二	策略三
強化 聯繫會議功能	提高 個資法相關 罰則	設立 個資保護 獨立監督機關

機關個資外洩情節重大最高罰1500萬

112年5月3日立院初審通過個人資料保護法部分條文修正草案

- 「個人資料保護委員會」為個資法主管機關，預計8月成立籌備處
- 非公務機關保有個人資料檔案者，未採行適當之安全措施，導致個人資料被竊取、竄改、毀損、滅失或洩漏，將處以新台幣2萬元以上200萬元以下罰鍰，並限期改正，若限期未改善或情節重大，將處以15萬元以上1500萬元以下罰鍰

簡報完畢
敬請指教