Deloitte.

勤業眾信

金融穩定與合規管理：銀行與證券法規的比較研究

勤業眾信聯合會計師事務所 風險諮詢服務部門 · 2024/09

Agenda

- 金融穩定與合規之重要性
- 銀行及證券產業資安法規比較
  - 各國銀行及證券產業資安法規比較
  - 我國證券及銀行產業資安法規比較
- 問題與討論

金融穩定與合規之重要性

金融穩定與合規之重要性

隨著金融科技和數位轉型的迅速發展，銀行及證券業已成為網路攻擊的主要目標之一，金融機構必須在資安法規合規方面展現高度的重視與能力。資安合規不僅保護金融機構內部的資料與系統安全，還直接關係到金融體系的穩定運作和投資者信心。

下面介紹先前國外一些知名金融機構因違反資安法規或資安漏洞而導致重大影響的新聞案例：

美國Capital One銀行個資外洩案遭罰8千萬美元

事件背景

Capital One 是美國的主要銀行之一，2019年遭到黑客入侵，超過1億名用戶的個人信息和信用卡申請數據被竊取。該事件的源頭是雲端數據庫設置錯誤，使得黑客得以輕易攻入。

違反法規

Capital One未能符合《NYDFS Part 500》的多項要求，特別是在雲端安全配置和數據保護措施上存在漏洞。此外，該事件還引發了對其網絡安全治理和雲端數據保護策略的質疑。

影響

- Capital One最終支付了8,000萬美元的罰款，並同意改善其資安控制機制和雲端數據管理策略。
- 事件曝光後，促使美國金融機構加強對雲端資安的重視，並提升資安治理結構，以避免類似事件再次發生。

荷蘭 ING Bank 資安法規違規遭罰7.75億歐元

事件背景

荷蘭的ING Bank在2021年被荷蘭中央銀行（DNB）調查，發現該行未能有效執行客戶盡職調查（KYC）和反洗錢法規（AML），且未能妥善保護客戶的數據安全，這被認為違反了歐盟《網路與資訊系統安全指令》（NIS 2 Directive）。

違反法規

ING被指責未能對客戶交易進行充分的監控，且在數據保護方面缺乏有效的內控機制，違反了歐盟的資安合規要求。

影響

- ING最終支付了超過7.75億歐元的罰款，成為歐洲金融機構面臨的重大資安罰款案例之一。
- 此事件加強了歐盟對金融機構在數據保護與網絡安全方面的監管，特別是在反洗錢、數據洩露風險控制等方面。

銀行及證券產業資安法規比較

各國銀行及證券產業資安法規比較

選取國家之比較基準 -全球金融中心指數

參考知名英國智庫機構Z/Yen Group及中國（深圳）綜合開發研究院於2023年9月發表之「全球金融中心指數」報告（GFCI 34）之結果，作為選擇國際知名金融中心所在國家作為本研究之參考之標的。

Centre	GFCI 34		GFCI 33		Change In	Change In
	Rank	Rating	Rank	Rating	Rank	Rating
New York	1	763	1	760	0	▲3
London	2	744	2	731	0	▲13
Singapore	3	742	3	723	0	▲19
Hong Kong	4	741	4	722	0	▲19
San Francisco	5	735	5	721	0	▲14
Los Angeles	6	734	6	719	0	▲15
Shanghai	7	733	7	717	0	▲16
Washington DC	8	732	11	713	▲3	▲19
Chicago	9	731	8	716	▼1	▲15
Geneva	10	730	23	701	▲13	▲29
Seoul	11	729	10	714	▼1	▲15
Shenzhen	12	728	12	712	0	▲16
Beijing	13	727	13	711	0	▲16
Frankfurt	14	726	17	707	▲3	▲19
Paris	15	725	14	710	▼1	▲15

國際相關資安法規

對全球現行資安法規進行簡要介紹，並介紹其在面對重大資安事件發生時的通報要求等等。

美國

- 《網路安全風險管理、策略、治理與事件揭露》
- 《關鍵基礎設施網路事件報告法》（CIRCIA）
- 《NYDFS Part 500》

歐盟

- 《歐盟網路安全法》（Cybersecurity Act）
- 《網路與資訊系統安全指令》（NIS 2 Directive）

新加坡

- 《網路安全法》（Cybersecurity Act）
- 《技術風險管理準則》（TRMG）
- 《NOTICE 655》

美國資安法規-《網路安全風險管理、策略、治理與事件揭露》
(Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure)

美國證券交易委員會 (SEC) 於 2023 年通過的另一項報告規定，此規則適用於遵守「1934 年證券交易法」報告要求的上市公司。

目標

加強和規範有關網路安全風險管理、策略、治理和事件的揭露，因為投資者需要更多有關公司網路安全風險狀況的實質和一致資訊來為投資決策提供資訊

要求

揭露網路安全事件的重大影響

- 在確定網路安全事件屬於重大事件後的四個工作天內提交表格 8-K
- 8-K 表必須描述 (1) 事件的性質、範圍和時間安排的重大方面，以及 (2) 對公司的重大影響或合理可能的重大影響
- 公司應建立並審查與網路安全風險或事件揭露相關的現有揭露控制和程序

揭露網路安全風險管理和策略

- 詳細描述其評估、識別和管理網路安全威脅重大風險的流程，以便投資者了解這些流程
- 描述網路安全威脅所帶來的風險（包括先前任何網路安全事件造成的風險）是否已產生重大影響或合理可能產生重大影響

揭露管理階層和董事會監督

- 描述董事會對網路安全威脅風險的監督以及管理階層在評估和管理網路安全威脅重大風險方面的作用

美國資安法規-2022年關鍵基礎設施網路事件報告法 (CIRCIA)

美國拜登總統於 2022 年簽署關鍵基礎設施網路事件報告法 (The Cyber Incident Reporting for Critical Infrastructure Act of 2022) ，以滿足針對重要基礎設施的網路事件快速回應和協調的迫切需求。

規範對象

16個關鍵基礎設施領域: **金融服務**、緊急服務、食品與農業、政府設施、醫療保健與公共衛生、資訊技術等

內容

要求關鍵基礎設施實體向「國土安全部網路安全暨基礎設施安全局」（CISA）報告 **(1) 重大網路事件**和 **(2) 支付贖金**

重大網路事件

重大網路事件的定義

導致此類資訊系統或網路的機密性、完整性或可用性嚴重喪失，或對作業系統和流程的安全性和彈性造成嚴重影響的任何事件

報告時間

確認網路事件發生後72小時內

支付贖金

贖金的定義

任何因勒索軟體而產生的付款，因此嚴格說來，它不需要報告針對其他類型的網路勒索而進行的付款

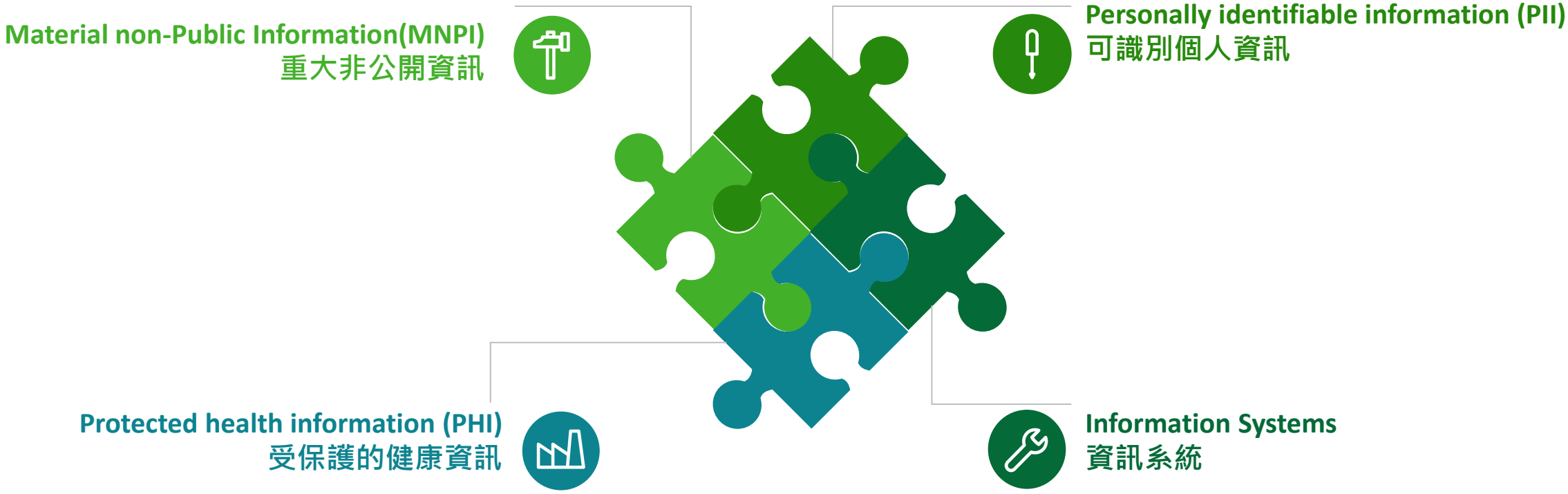
報告時間

支付贖金後 24 小時內

美國資安法規- NYDFS Part 500

紐約州金融服務部 (NYDFS) 於2017年發布了 23 條紐約 (NYCRR) 500 條例，以應對網路犯罪分子日新月異的犯罪手法以及美國金融機構面臨日益動盪的網路安全環境。該法規的目標是確保非公開資訊的安全，並確保金融服務機構資訊系統的完整性。因應不斷改變的環境，Part 500 條文內容也不斷更新，NYDFS已於2023年11月1日正式通過，將要求金融機構提供更全面的網路安全保護。

對象 | 根據《銀行法》、《保險法》或《金融服務法》授權在紐約州運營的任何組織。



美國資安法規- NYDFS Cybersecurity Regulations 23 NYCRR Part 500 修正概述

本次新版可大致分為六大修訂類別。

大規模金融服務機構義務與治理

大規模金融服務機構義務:

- 本次新版新增「**A級金融服務機構**」與其定義
- A級金融服務機構需要承擔幾項額外的網路安全義務，包含**定期獨立審查、風險評估和監控技術導入等。**

治理

- 新增針對於**CISO與董事會專業知識與認知要求**，以確保對網路安全進行有效監督風險
- **修訂合規、改善措施、補救計畫和教育訓練**之相關要求

風險評估與技術

風險評估:

- 本次新版**擴展風險評估的定義**，明確說明評估應針對特定金融服務機構進行調整
- 每當業務或技術的變化導致公司的網路風險發生重大變化時，都**必須進行風險評估**

技術:

- 本次新版要求**落實資訊資產盤點**，已追蹤資訊資產的相關資訊
- 本次新版擴大**特權帳號**相關要求

通報責任與罰責

通報責任:

- 網路安全事件發生**72 小時**內應通知 NYDFS，並應於**90天內**提供相關事件調查資訊。
- 網路安全事件發生於**第三方服務供應商**時應於**知曉事件後72小時**內通報NYDFS。

罰責:

- 規定實施任何此法規禁止的**單一行為，或不履行義務**，將構成違反法規條件。
- 本次新版提供了 NYDFS 在評估處罰時**可能考慮的幾個減輕因素的清單**

新版NYDFS Cybersecurity Regulations 23 NYCRR Part 500 主要要求

500.3 實施並保持一份書面網路安全政策，**需每年經由高階管理代表批准。**

500.4 金融服務機構的CISO應至少**每年**向其董事會或同等理事機構提交**書面報告**以及**發現事項改善計畫。**

500.5 應每年執行滲透測試及**定期**執行弱點評估。

500.6 金融服務機構應保存資訊安全事件檢測和響應的審查軌跡**不少於五年。**

500.7 應限制存取非公開的資料系統的使用者及特殊權限，並應**定期審查**及**即時刪除或停用不再需要的帳號權限。 A級金融服務機構應實施特權帳號管理方案。**

500.8 CISO應**每年**審查、評估和更新與網路安全計畫相關之系統發開管理制度文件。

500.9 應**每年**進行風險評估且風險評估應根據書面政策和程序進行，並應妥善記錄，**A級企業應至少每三年聘請外部專家進行一次風險評估。**

500.11應訂定**第三方服務提供廠商有關的盡職調查及合約保護的相關要求**，以確保第三方服務供應商存取或持有的資訊系統和非公開資訊的安全性。

500.12**多因子驗證機制應運用於可遠端存取非公開資訊的網路、企業及第三方應用系統**，除非其CISO已書面批准使用合理等效或更安全的存取控制。

500.13應制定書面政策和程序，說明如何定期安全處置與銷毀確定不再有業務利用需求或不再具有合法商業目的非公開資訊。並識別及管理機構所持有的資訊資產。

500.14 應提供定期資訊安全意識教育訓練並**監控和過濾電子郵件以阻止惡意程式影響權限用戶。A級金融服務機構應實施監控異常活動的端點偵測與回應解決方案及日誌集中及安全事件告警之解決方案。**

500.15 應針對非公開資訊進行**加密保護，若採用補償性控制，應至少每年由CISO進行審查。**

500.16 應建立一個**書面營運持續及事件響應計畫(BDCR計畫)。**

500.17 網路安全事件應於**72小時內**通報(含事件發生於第三方)，每年應在**4/15**之前向監督單位提交書面聲明，並於**遭勒索軟體攻擊及付贖金時進行通報與說明。**

500.21 每年準備並向監督單位提交一份符合紐約州金融服務資訊安全法規並根據2018年2月15日開始的第500.17（b）條規定的證書。

500.22 須自本部分的生效日期後計有**180天**之時間以符合本部所載的規定，除非另有要求。

法規比較-「關鍵基礎設施網路事件報告法」、「電腦安全事件通知要求」、「網路安全風險管理、策略、治理與事件揭露」

雖然三項法規的主要重點是報告和揭露，但也存在差異

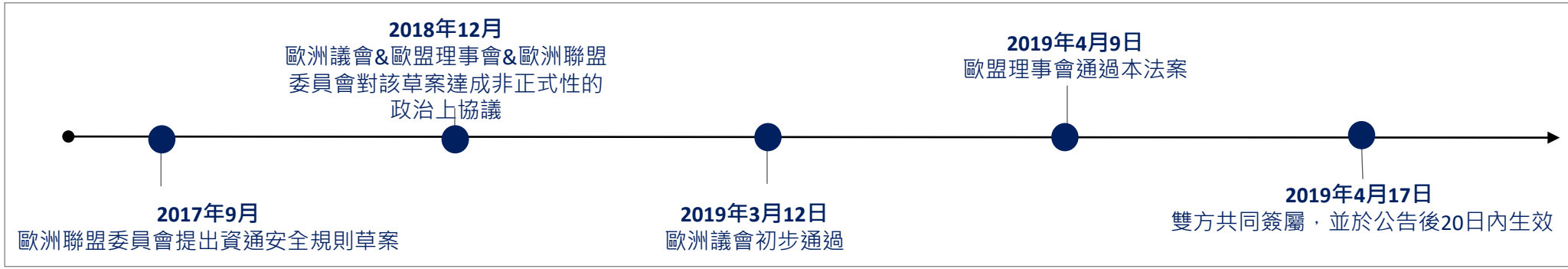
	關鍵基礎設施網路事件報告法	電腦安全事件通知要求	網路安全風險管理、策略、治理與事件揭露
發布機構	聯邦政府	聯邦銀行監理機構 （FDIC、FRB、OCC）	證券交易委員會 (SEC)
規範對象	關鍵基礎設施	(1)銀行機構 (2)第三方銀行服務提供者	遵守「1934 年證券交易法」報告要求的上市公司
報告內容	(1) 重大網路事件 (2) 贖金支付	電腦安全事件	(1) 網路安全事件 (2) 網路安全風險管理與策略 (3) 管理階層和董事會監督
截止日期	(1) 72小時內向國土安全部網路安全暨基礎設施安全局 (2) 24小時內向國土安全部網路安全暨基礎設施安全局	(1) 36小時內向聯邦銀行監理機構報告 (2) 「盡快」向提供者提供服務的銀行	(1) 4個工作天內向SEC

歐盟網路安全法（Cybersecurity Act）背景摘要

2018年5月29日，歐洲聯盟理事會發布了關於監管歐洲聯盟網路和資訊安全局（ENISA）和資訊和通信技術網路安全認證（歐盟網路安全法（Cybersecurity Act））的提案。本提案有兩項重點部分：

核心內容	▪ 第一個:通過使ENISA成為歐盟的常設機構，用以加強ENISA的權力旨在減少資訊安全事件對於組織資訊資產之機密性、完整性和可用性可能造成之影響。 ▪ 第二個:建立歐洲網路安全認證框架，以確保對資訊和通信技術（ “ICT”）商品之應用，將須通過網路安全認證。
規範標的	▪ 歐盟成員國，惟資安認證框架並不要求各國強制加入。

時間軸



資料來源: https://www.apra.gov.au/

歐盟網路安全法（Cybersecurity Act）-歐盟資安政策

ENISA將協助歐盟各國建立其各自的”電腦安全事件應變小組(Computer Security Incident Response Team, CSIRTs)”，以符合”指令(Directive 2016/1148)規範外，ENISA本身之業務，也做出些許調整。

ICT資安認證框架之職責

為準備歐盟資安認證計畫方案，將與資安領域專家與國家認證機構進行合作; 此外將對ICT標準化的政策發展，提供協助。

政策發展與執行

ENISA將協助歐盟各國與歐洲聯盟委員會，對歐盟的資通安全政策之發展、規劃等提出建議。並對指令所提及之能源、金融等資通安全政策，提供協助。

能力建構

ENISA將協助歐盟各國提高其資安相關之專業能力，平時之預防與事件發生時之應對策略，並對資安事件提供協助。

資安指導

ENISA將成為歐盟內資安方面之主要窗口，並協助歐盟組織了解與提高資安意識與新知。

歐盟網路安全法（Cybersecurity Act）-資安認證框架

資安認證框架是由歐盟各國以自願性方式採取，目的為確保產品與服務的資安是受到保護的。而其層級將高於歐盟各國現行的認證計畫。

本框架主要用於全歐盟的認證計畫，包含規定、技術層面要求、程序等內容

將由ENISA與歐盟資安認證小組(European Cybersecurity Certification Group, ECCG)合作，提出建議與草案。

歐盟成員國與歐盟資安認證小組，可主動向歐洲聯盟委員會提議，請求ENISA對某特定產品或服務，草擬資安認證計畫。

歐盟資安認證計畫通過後，ICT廠商即可提交申請，而其資格有效期間，最長為五年，並設有更新資格有效期的規範。

歐盟《網路與資訊系統安全指令》（NIS 2 Directive）

該指令（Directive）係於2023年1月16日正式生效，是一項資安監管措施，基於2016公布的《網路與資訊系統安全指令》（NIS Directive）進行擴展補充。

監管對象

對經濟或社會影響至關重要的中大型企業。

通報對象

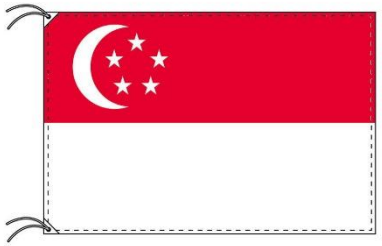
電腦資訊安全事件應變小組（CSIRT小組）或主管機關

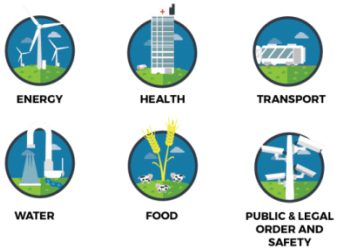
事件回應

重大事件24小時內進行初期通報，72小時內提供事件報告，並於一個月內提供最終報告（第四章第23條）

新加坡網路安全法(Cybersecurity Act)

法案通過時間：2018年02月05日、總統同意時間：2018年03月02日





CII

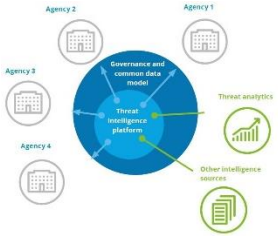
加強對重要資訊基礎設施(Critical Information Infrastructure, CII) 的保護，以防範網路攻擊

CII部門包括：能源、水源、銀行和金融、醫療健保、運輸（包括陸地、海事和航空）、資訊通信、媒體、安全和緊急服務以及政府。

CSA

授權CSA預防和應對網路安全威脅和事件

該法案授權網路安全專員(Cyber Security Agency) 調查網路安全威脅和事件，以確定其影響並防止進一步的傷害或網路安全事件的發生。



Sharing

建立共享網路安全資訊的框架

該法案促進資訊共享，這對於政府和系統的所有者可以即時的識別漏洞並更有效的防止網路事件是至關重要的。

PT&SOC

為網路安全服務提供商建立較寬鬆的許可框架

CSA目前只有兩種類型的服務提供商採取寬鬆的許可，即滲透測試 (Penetration Testing) 和資訊安全監控中心 (Security Operations Centre, SOC)。

新加坡技術風險管理準則（TRMG）

新加坡金融管理局（Monetary Authority of Singapore, MAS）頒佈了技術風險管理準則（Technology Risk Management Guideline, TRMG），以規範新加坡金融機構的資訊安全系統。該準則旨在促進採用合理、可靠的做法來管理技術風險。

科技風險管理準則 - 範圍

目的：

近年來金融服務的資訊科技（IT）基礎架構的範圍和複雜性都在增加，因此MAS列出了風險管理原則和最佳實踐，以指導金融機構建立健全而強大的技術風險治理和監督機制，並維護IT和網路的彈性。

建立健全而穩健的技術風險治理與監督：

金融機構的董事會和管理階層在技術風險的監督和管理中起著不可或缺的作用，應樹立強健的風險文化，並確保健全、穩健的技術風險管理框架。

維持網路彈性：

金融機構應採取深度防禦措施，以增強網路彈性。必須建立並持續改善其IT流程和控制，以保護數據和IT系統的機密性、完整性和可用性。

新加坡技術風險管理準則（TRMG） - MAS TRMG 框架

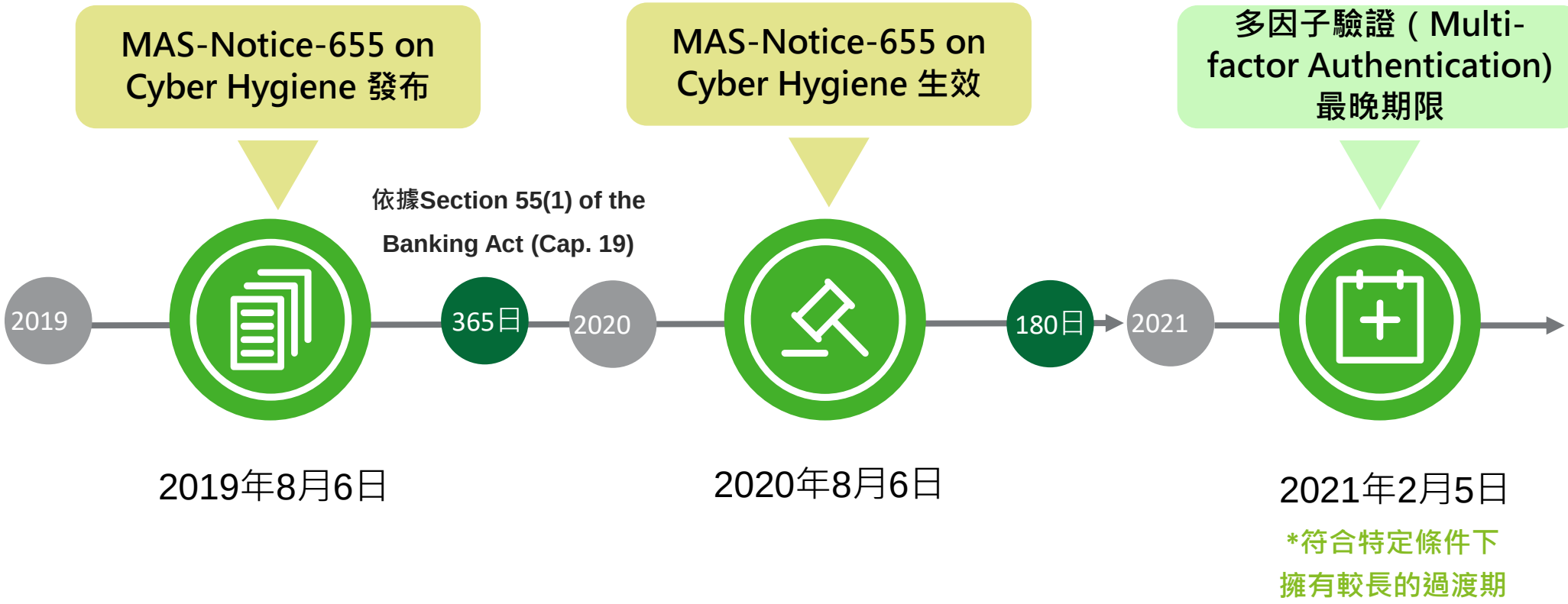
依據TRMG第2章節之說明，TRMG提供一般性指導，金融機構可依據服務風險水準與複雜度參考TRGM所提供之最佳實踐。

1. Preface			文件介紹
2. Application of the MAS Technology Risk Management Guidelines			適用範圍
3. Technology Risk Governance and Oversight	4. Technology Risk Management Framework		政策、職責、盤點、風險評鑑
5. IT Project Management and Security-by-Design	6. Software Application Development and Management	7. IT Service Management	安全開發、維護、變更
8. IT Resilience			營運持續
9. Access Control	10. Cryptography	11. Data and Infrastructure Security	系統、資料、網路安全
12. Cyber Security Operations	13. Cyber Security Assessments	14. Online Financial Services	管理審查、技術檢測、線上金融
15. IT Audit			稽核結果呈董事會及高階主管
A. Application Security Testing	B. BYOD Security	C. Mobile Application Security	SAST, DAST, IAST、行動裝置安全

新加坡 Notice 655 - 背景摘要

新加坡金融管理局(MAS)發布Notice 655 on Cyber Hygiene，針對所有銀行在資訊安全方面的規範，規定金融機構必須採取一系列基本網路安全措施，以管理網路威脅。

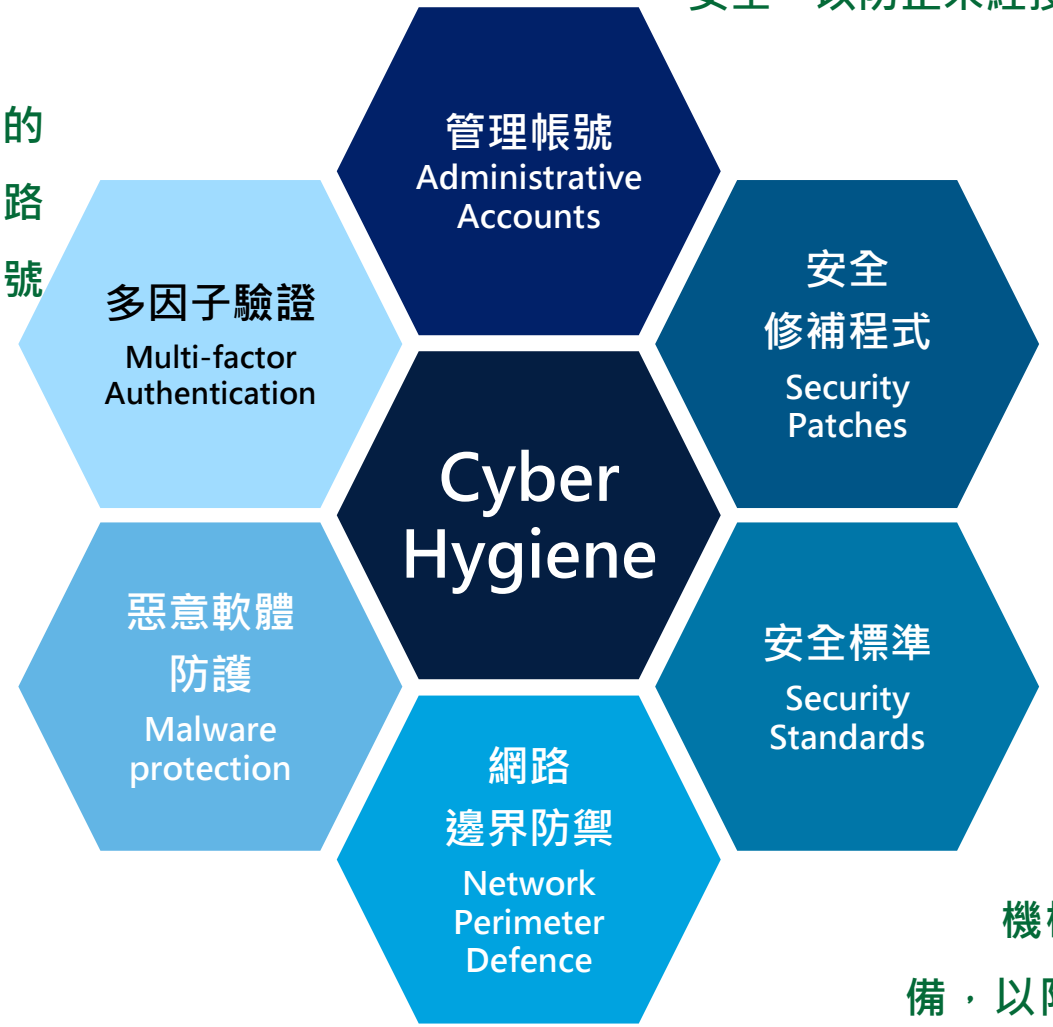
MAS Notice 655 on Cyber Hygiene 重要里程碑



新加坡 Notice 655 - Cyber Hygiene 概覽

機構應確保特殊權限帳戶的安全，以防止未經授權的存取。

機構應加強關鍵系統環境的管理帳號、以及能透過網際網路存取客戶資訊的系統的所有帳號的身分驗證。



機構應確保所有資訊系統及時更新，以解決系統的潛在漏洞。

機構應為所有資訊系統建立書面化的安全設定標準，並確保遵循性。

機構應實施相關措施，以降低被惡意軟體感染的風險。

機構應配置適當的安全設備，以限制未經授權的網路流量。

我國證券及銀行產業資安法規比較

法規比較-法規綜整

根據銀行及證券同業公會各自所發布的自律規範中，我們可以發現，兩者在監管主題面相上大致相同(請詳下方表格)。

以主題面向來說，差異之處通常為該產業特有之業務。

類別	證券業	銀行業
自律規範- 資通安全防護基準	《資通系統安全防護基準自律規範》	《金融機構資通安全防護基準》
	《建立證券商資通安全檢查機制》	
新興科技	《新興科技資通安全自律規範》	《金融機構運用新興科技作業規範》
	《建立證券商資通安全檢查機制》	《金融機構提供行動裝置應用程式作業規範》
		《金融機構使用物聯網設備安全控管規範》
供應鏈風險管理	《供應鏈風險管理自律規範》	《金融機構資通系統與服務供應鏈風險管理規範》
	《建立證券商資通安全檢查機制》	
資訊作業韌性	《資訊作業韌性自律規範》	《金融機構資訊作業韌性規範》
	《建立證券商資通安全檢查機制》	
重大資安事件通報	《證券期貨市場資通安全事件通報應變作業注意事項》	《金融機構通報重大偶發事件之範圍申報程序及其他應遵循事項》
	《建立證券商資通安全檢查機制》	
電腦安全評估	《資通系統安全防護基準自律規範》	《金融機構辦理電腦系統資訊安全評估辦法》
	《建立證券商資通安全檢查機制》	

銀行業特有自律規範

- **《金融機構提供自動櫃員機系統安全作業規範》**
- **《金融機構提供QR Code掃描支付應用安全控管規範》**
- **《電子支付機構資訊系統標準及安全控管作業基準》**

自律規範-資通安全防護基準

法規比較-自律規範-資通安全防護基準

本次證券業與銀行業在自律規範-資通安全防護基準方面，主要會分為13大類進行比較：

#	類別		比較說明	補充說明
一	資安政策檢視頻率		與銀行業規範一致之情形	證券商較佳，證券商應依其所屬資安分級辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。
二	資訊資產清冊盤點要求		與銀行業規範一致之情形	
三	人員管理與存取控管相關要求	1. 存取權限、帳號管理	與銀行業規範一致之情形	
		2. 帳號權限管理	與銀行業規範一致之情形	
		3. 身分確認	銀行業規範較為嚴謹	應確認人員之身分及存取權限，必要時得限定其使用之機器或網路位置（IP）。 依據「建立證券商資通安全檢查機制」存取控制（CC–18000，每月查核），已要求證券商針對各項系統之權限有相關要求，並符合證券商之產業特性。並此條款由金融機構自行認定為必要時執行，因此建議不須進行調整。
		4. 個人電腦設定	銀行業規範較為嚴謹	證券：公司應建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準（如密碼長度、更新期限等）。 條款描述範圍較不同，但若以個人電腦螢幕保護程式或登出系統之議題，目前證券業無直接要求具體時間(例如：十五分鐘)。因相關條款所規範之範圍不同，評估無須調整。
		5. 個人帳號管理	與銀行業規範一致之情形	

法規比較-自律規範-資通安全防護基準

本次證券業與銀行業在自律規範-資通安全防護基準方面，主要會分為13大類進行比較：

#	類別		比較說明	補充說明
三	人員管理與存取控管相關要求	6. 安全組態設定	與銀行業規範一致之情形	
		7. 加密規範	與銀行業規範一致之情形	
		8. 最高權限帳號管理	銀行業規範較為嚴謹	銀行：如為核心資通系統，應於該等帳號被使用時，每日覆核使用結果。 雖銀行業較為嚴謹，但依據目前建立證券商資通安全檢查機制中已有針對系統之最高權限帳號進行管控。
		9. 雙因子認證	銀行業規範較為嚴謹	銀行：提供網際網路服務之伺服器及 AD(網域服務)主機，對於最高權限帳號及特殊功能權限帳號，應採雙因子認證。 雖銀行業較為嚴謹，但依據建立證券商資通安全檢查機制之要求，已有針對網路下單登入時採多因子認證方式，以確保為客戶本人登入。
		10. 最小權限原則	與銀行業規範一致之情形	銀行產業與證券產業皆有針對定期審查權限與授權採最小權限原則有相關要求，惟目前未有針對系統權限異常存取紀錄進行審查之要求，但因在「建立證券商資通安全檢查機制-分級防護應辦事項附表」有要求證券商依據分級進行異常之監控，應能輔助降低相關風險。
四	個資保護相關要求		與銀行業規範一致之情形	
五	機敏資料隱密及金鑰管理		與銀行業規範一致之情形	

法規比較-自律規範-資通安全防護基準

本次證券業與銀行業在自律規範-資通安全防護基準方面，主要會分為13大類進行比較：

#	類別		比較說明	補充說明
六	營運管理相關要求	1. 原始碼管理	銀行業規範較為嚴謹	銀行：應評估避免於營運環境安裝程式原始碼，惟系統需具備程式原始碼，如：Python、SQL command 等方能運行之營運環境不在此限。 雖銀行業較為嚴謹，但依據目前建立證券商資通安全檢查機制中已針對原始碼管理有適當之安全規範。
		2. 連續假期資安防護	銀行業規範較為嚴謹	因證券市場與銀行產業特性不同，連續假期期間因證券市場未開盤，因此較無確保相關系統持續運作之議題，建議無須調整。
七	容量管理之要求		銀行業規範較為嚴謹	雖銀行業較為嚴謹，但依據目前建立證券商資通安全檢查機制中已規範需定期對系統容量進行壓力測試，並留存紀錄。
八	脆弱性管理之要求	1. 上網管制措施	與銀行業規範一致之情形	
		2. 電腦病毒及惡意軟體管制	與銀行業規範一致之情形	
		3. 弱點掃描	現有證券業規範較為完整	證券產業法規之要求關注於提供網際網路下單服務之證券商每半年執行弱點掃描之檢測。而銀行產業則是透過「金融機構資通安全防護基準」要求定期執行弱點掃描，並依據「金融機構辦理電腦系統資訊安全評估辦法」針對第一類（每年一次）、第二類（第三年一次）與第三類（每五年一次）系統由第三方檢視掃描作業執行情形。另外「金融機構提供自動櫃員機系統安全作業規範」針對自動櫃員機(ATM)伺服器應每半年執行一次弱點掃描。
		4. EOS/EOL	銀行業規範較為嚴謹	證券產業法規僅針對網路設備有相關規範。

法規比較-自律規範-資通安全防護基準

本次證券業與銀行業在自律規範-資通安全防護基準方面，主要會分為13大類進行比較：

#	類別		比較說明	補充說明
八	脆弱性管理之要求	5. 惡意網站偵測	與銀行業規範一致之情形	
		6. 入侵偵測	與銀行業規範一致之情形	證券產業依據「建立證券商資通安全檢查機制-分級防護應辦事項附表」之內容，針對第一至四級證券商皆要求建立入侵偵測及防禦機制。
		7. 社交工程	與銀行業規範一致之情形	
		8. DDoS	銀行業規範較為嚴謹	證券產業規範未要求每年進行演練。
		9. 防火牆	與銀行業規範一致之情形	
		10. 網頁與程式異動偵測	與銀行業規範一致之情形	
		11. 源碼掃描	與銀行業規範一致之情形	
九	測試環境之要求		銀行業規範較為嚴謹	因評估測試環境本身資產之特性其風險較低，因此建議無須調整。
十	辦公室管理之要求	1. 公用電腦管理	銀行業規範較為嚴謹	因辦公環境非為營運環境，其可能造成之風險較低。
		2. 視訊會議	銀行業規範較為嚴謹	因辦公環境非為營運環境，其可能造成之風險較低。
		3. 遠距辦公	與銀行業規範一致之情形	

法規比較-自律規範-資通安全防護基準

本次證券業與銀行業在自律規範-資通安全防護基準方面，主要會分為13大類進行比較：

#	類別		比較說明	補充說明
十	辦公室管理之要求	4. 虛擬桌面管理	銀行業規範較為嚴謹	
十一	網路管理之要求	1. DMZ區管理	與銀行業規範一致之情形	
		2. 網路服務	與銀行業規範一致之情形	
		3. 防火牆存取控管	銀行業規範較為嚴謹	證券產業規範未有應定期檢視高風險設定及六個月內無流量之防火牆規則評估其必要性及風險、已下線系統於半年內調整或停用防火牆規則之規則。
十二	系統生命週期之要求		銀行業規範較為嚴謹	依據「建立證券商資通安全檢查機制」， 已有系統開發之相關要求，並考量證券商之規模大小與人力規劃。
十三	資訊安全事故之要求		與銀行業規範一致之情形	證券產業有要求進行相關日誌及稽核軌跡之留存，但未有集中管理進行異常紀錄分析之要求。依據「建立證券商資通安全檢查機制-分級防護應辦事項附表」，證券商應建置建置資通安全威脅偵測管理機制(SIEM)，應能達成相關精神。

新興科技

法規比較-新興科技

本次證券業與銀行業在新興科技方面，主要會分為5大類進行比較：

#	類別		比較說明	補充說明
一	雲端服務	1. 資安政策檢視頻率	銀行業規範較為嚴謹	
		2. 獨立第三人查核	銀行業規範較為嚴謹	銀行雲端服務自律規範預計今年發布，建議證券業可參考雲端服務自律規範發布之結果進行相關規範。
		3. 加密傳輸規範	銀行業規範較為嚴謹	
		4. 資料存取	銀行業規範較為嚴謹	
		5. 儲存地管理	銀行業規範較為嚴謹	
		6. IaaS或PaaS雲端服務模式管理	銀行業規範較為嚴謹	
		7. 建立資通安全通報程序	銀行業規範較為嚴謹	依據「證券期貨市場資通安全事件通報應變作業注意事項」已有資通安全事件通報要求。
二	社群媒體	1. 資安政策檢視頻率	銀行業規範較為嚴謹	
		2. 內容監視管控	與銀行業規範一致之情形	
		3. 緊急應變程序	與銀行業規範一致之情形	
		4. 異常事件通報	現有證券業規範較完整	

法規比較-新興科技

本次證券業與銀行業在新興科技方面，主要會分為5大類進行比較：

#	類別		比較說明	補充說明
三	行動裝置	1. 管理辦法	現有證券業規範較完整	銀行有規範自攜裝置管理政策應每年檢視，證券則無規定檢視頻率。但證券除自攜裝置外，另規範須制定公務用行動裝置設備管理辦法。
		2. 列冊管理	銀行業規範較為嚴謹	
		3. 身分與裝置識別機制	銀行業規範較為嚴謹	
		4. 連網環境標準	銀行業規範較為嚴謹	
		5. 自攜裝置資料保護	銀行業規範較為嚴謹	
四	行動應用程式	1. 應用程式發布位置	現有證券業規範較完整	
		2. 應用程式發布程序	銀行業規範較為嚴謹	依據「建立證券商資通安全檢查機制」，涉及投資人使用之行動應用程式於初次上架前及每年應委由經財團法人全國認證基金會（TAF）認證合格之第三方檢測實驗室進行並完成通過資安檢測，且留存相關檢測紀錄。
		3. 版控	與銀行業規範一致之情形	
		4. 偽冒監測機制	與銀行業規範一致之情形	

法規比較-新興科技

本次證券業與銀行業在新興科技方面，主要會分為5大類進行比較：

#	類別		比較說明	補充說明
四	行動應用程式	5. 敏感性資料保護	現有證券業規範較完整	
		6. 行動應用程式檢測	與銀行業規範一致之情形	
		7. 金鑰管理	銀行業規範較為嚴謹	依據「建立證券商資通安全檢查機制」，其中對網路傳輸及連線安全管理有相關規範。
		8. 空中傳輸(OTA)管理	銀行業規範較為嚴謹	
		9. 安全元件儲存媒介(SE)管理	銀行業規範較為嚴謹	
		10. 近距離無線通訊(NFC)管理	銀行業規範較為嚴謹	依據「建立證券商資通安全檢查機制」，涉及投資人使用之行動應用程式於初次上架前及每年應委由經財團法人全國認證基金會（TAF）認證合格之第三方檢測實驗室進行並完成通過資安檢測，且留存相關檢測紀錄。

法規比較-新興科技

本次證券業與銀行業在新興科技方面，主要會分為5大類進行比較：

#	類別		比較說明	補充說明
五	物聯網設備	1. 設備盤點	銀行業規範較為嚴謹	
		2. 權限控管	銀行業規範較為嚴謹	
		3. 連線管控	銀行業規範較為嚴謹	
		4. 供應商管理	與銀行業規範一致之情形	
		5. 教育訓練	銀行業規範較為嚴謹	因證券商規模有差異，應予證券商自行考量教育訓練時數。
		6. 網路釣魚	現有證券業規範較完整	
		7. 電子交易	現有證券業規範較完整	
		8. 深度偽造	與銀行業規範一致之情形	

供應鏈風險管理

法規比較-供應鏈風險管理

本次在供應鏈風險管理方面，依證券業《中華民國證券商業同業公會供應鏈風險管理自律規範》與銀行業《金融機構資通系統與服務供應鏈風險管理規範》針對委外前、委外契約、委外中、委外後進行比較：

項目	銀行	證券
	《金融機構資通系統與服務供應鏈風險管理規範》	《中華民國證券商業同業公會供應鏈風險管理自律規範》
委外前	規範較為完整	證券業未納入： 1. 資訊安全要求之服務水準。(已規範納入合約，未要求納入建議書) 2. 供應商與其提供產品或服務位置。
委外契約	規範較為完整	證券業未納入： 1. 要求供應商遵守相關法令法規及其他適當資訊安全國際標準要求。 2. 非經金融機構書面同意，不得將作業複委託他人。委外契約中應定義委託業務得否複委託、得複委託之範圍與對象，及複委託受託者應具備之資訊安全措施。 3. 訂定供應商契約終止時，資訊資產與資料返還、移交、刪除或銷毀之要求。
委外中	規範較為完整	證券業未納入： 監督供應商針對其專案執行人員辦理資訊安全教育訓練。
委外後	銀行業、證券業規範一致	銀行業、證券業規範一致

資訊作業韌性規範

法規比較-資訊作業韌性規範

銀行業與證券業在資訊作業韌性規範上，針對以下四點進行比較說明：

人力配置與識別核心業務 銀行產業與證券市場皆要求組織應配置適當人力辦理持續營運管理事項，並識別核心業務、核心系統與相關資訊系統之復原時間目標 (RTO)、資料復原點目標 (RPO)	**制定營運持續計畫** 證券市場早期已將持續營運相關要求納入「建立證券商資通安全檢查機制」，同樣針對持續營運計畫有相關要求。
備份備援機制 證券市場之規範於備份備援機制描述較為細節，應考量「3-2-1備份原則」。而銀行產業之規範則要求應考量資料復原點目標(RPO)進行資料備份類型、方式之妥適性。	**營運持續演練** 證券市場則要求依據資安分級定期執行相關演練作業，第一級證券商應針對全部核心系統每年至少演練一次、第二級與第三級證券商應針對全部核心系統每二年至少演練一次，其餘證券商則依「建立證券商資通安全檢查機制」營運持續管理（CC-20000，半年查核）故障復原程序應週期性測試。

比較結果

比對銀行產業與證券市場之規範，於營運持續相關之要求，較大差異為證券市場有依證券商等級進行不同的演練要求，因證券商數量多、規模差異較大，現有規範要求符合證券市場之資訊作業韌性之規劃。

此外雖證券市場之規範無直接鼓勵異地備援演練時，納入對外實際運作驗證。但依據金管會所發布「金融行動方案2.0」之要求範圍，證券商仍為金管會所鼓勵之對象。

重大資安事件通報法規比較

美國通報及揭露法規比較 - 「電腦安全事件通知要求」、「網路安全風險管理、策略、治理與事件揭露」

	電腦安全事件通知要求	網路安全風險管理、策略、治理與事件揭露
發布機構	聯邦銀行監理機構 （FDIC、FRB、OCC）	美國證券交易委員會 (SEC)
規範對象	(1)銀行機構 (2)第三方銀行服務提供者	遵守「1934 年證券交易法」報告要求的上市公司
報告內容	電腦安全事件	• 網路安全事件 • 網路安全風險管理與策略 • 管理階層和董事會監督
通報時限	(1) 36小時內向聯邦銀行監理機構報告 (2) 「盡快」向提供者提供服務的銀行	4個工作天內向SEC繳交8-K通報表格，依風險嚴重程度可申請延長至7、30、60日

歐盟通報及揭露法規比較-「一般個人資料保護規則》（GDPR）」、「網路與資訊系統安全指令（NIS 2 Directive）」

	一般個人資料保護規則（GDPR）	網路與資訊系統安全指令（NIS 2 Directive）
發布機構	歐洲議會和歐盟理事會	歐洲議會和理事會
規範對象	歐洲所有握有其客戶或成員相關資料之企業	對經濟或社會影響至關重要的中大型企業
報告內容	遭侵害個資之事件	可能導致服務嚴重運營中斷或該實體經濟損失或影響其他自然人或法人的事件
通報時限	72小時內通報	24小時內提出預警 72小時內提交事件通知 30日內提交最終報告

台灣資安通報法規

《資通安全事件通報及應變辦法》為台灣針對資安事件的規範，適用範圍較為廣泛。由於金融機構通報規範要求更為緊急，故金管會增訂《金融機構重大偶發事件通報作業程序及其他應遵循事項》 ，包含更多與金融市場穩定性相關的事件。以下是兩者的比較：

法規名稱	資通安全事件通報及應變辦法	金融機構通報重大偶發事件之範圍申報程序及其他應遵循事項	證券期貨市場資通安全事件通報應變作業注意事項
規範對象	所有政府機關及特定行業，包括金融機構在內的資通系統運營者	金融機構，包括銀行、保險公司、電子支付機構等。	證券期貨業者
通報範圍	所有資通安全事件，區分成**四種級別**，不同事件類型有不同的通報級別和處理方式。	• 重大資安事件 • 金融詐騙 • 影響金融穩定性事件 • 其他重大事件：自然災害、突發公共衛生事件	• 資訊服務異常事件 • 資通安全事件
通報時限	一小時內	**三十分鐘內**	**三十分鐘內**
報告時限	一個月	**七日**	無

台灣資安通報法規-《資通安全事件通報及應變辦法》

資通安全事件發生後的通報和處理程序

通報要求

- 即時通報：公務機關在知悉資通安全事件後，應在一小時內按主管機關指定的方式和對象進行通報。如果通報方式受阻，需在相同時間內以其他適當方式通報，並註明原因。
- 等級變更：事件等級變更時，需依原通報方式續行通報。

審核

- 審核時間：

第一級或第二級事件：主管機關需在接到通報後八小時內完成審核。

第三級或第四級事件：主管機關需在接到通報後二小時內完成審核。

- 通知與覆核：審核完成後，需在一小時內通知主管機關。主管機關可根據提供的信息覆核事件等級，並進行必要的變更。

復原

- 完成時間：

第一級或第二級事件：需在知悉事件後72小時內完成損害控制或復原作業。

第三級或第四級事件：需在知悉事件後36小時內完成損害控制或復原作業。

- 後續報告：公務機關需在一個月內提交調查、處理及改善報告。此提交期限可經上級或主管機關同意後延長。

法規比較-國內外金融機構重大偶發資通安全事件通報法規比較

分別擷取台灣、美國、歐盟相關法規

國家	台灣-金融與證券機構	美國	歐盟
通報最低時限	30分鐘內 	1. 網路安全事件：72小時內 2. 勒索贖金支付：24小時內	24小時內提出預警 72小時內提交事件通知報告
報告最低時限	七日內	1. 90日內 2. 30日內	30日內提交最終報告

與國外法規相比建議可參考之項目：

- 依事件級別規定於36、72小時內完成損害控制或復原作業 -- 台灣《資通安全事件通報及應變辦法》
- 要求年度合規性之提交，每年4月15日前需上交一年內重大(不)合規證明 -- 美國《NYDFS Part 500》

法規比較-重大資安事件通報

銀行業與證券業在重大資安事件通報上的比較說明：

	證券業	銀行業
資安事件通報法規要求	《證券期貨市場資通安全事件通報應變作業注意事項》	《金融機構通報重大偶發事件之範圍申報程序及其他應遵循事項》
通報時限	證券期貨業者於發生影響客戶權益或正常營運之資訊服務異常事件或資通安全事件，應於知悉事件 **30 分鐘內**至通報系統，辦理事件初步通報。若查明原因為錯誤通報，應填寫「取消通報」原因，始得辦理取消該通報作業。	金融機構應於確認後**三十分鐘內**，先以電話向銀行局通報，再儘速續以網際網路申報系統辦理通報。

小結建議

分析與討銀行和證券商都被要求在**30分鐘內的時間通報事件**，這確保了相關單位能夠在第一時間獲取資訊並採取相應措施。這種即時性通報機制是防止事態惡化的關鍵，特別是在現代金融市場中，資訊傳遞和市場反應速度都非常快。

論以上法規皆針對重大資安事件進行相關要求，兩份規範皆強調了迅速反應的重要性。

其次，這些規範提供了明確的通報流程和細節要求，這有助於避免混亂和誤報。通過規範化的程序，銀行和證券商可以有條不紊地進行通報，確保資訊的準確性和一致性。 這不僅有助於主管機關做出正確的決策，也能提高市場參與者對金融體系的信心。

金融機構辦理電腦系統資訊安全評估辦法

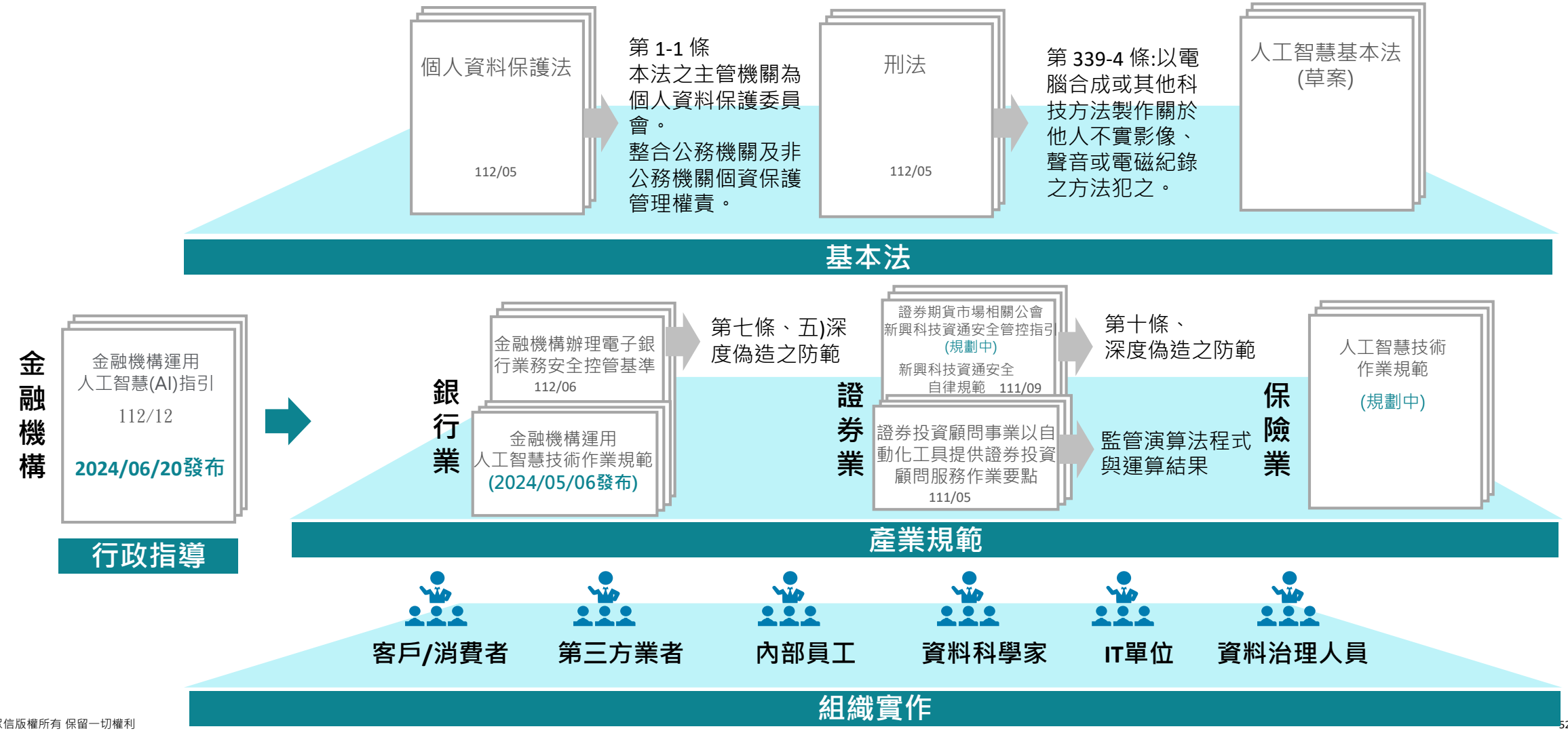
法規比較-金融機構辦理電腦系統資訊安全評估辦法

比較面向	銀行業 《金融機構辦理電腦系統資訊安全評估辦法》	證券業
電腦系統分類方式	**分為三類**，第一類為直接提供客戶自動化服務或對營運有重大影響之系統；第二類為經人工介入以直接或間接提供客戶服務之系統；第三類為未接觸客戶資訊或服務且對營運無影響之系統或設備。	**建立證券商資通安全檢查機制：** 於資產分類與控制（CC–14000，半年查核）中要求證券商應至少區分核心與非核心系統。 **資通系統安全防護基準自律規範：** 於名詞定義中定義核心系統之定義為：係指直接提供客戶交易或支持交易業務持續運作之必要系統(如交易系統、報價系統、中台風控、盤後結算系統、帳務系統等維持交易業務之必要系統)，其餘皆為非核心系統。
資訊安全評估作業	評估單位可委由外部專業機構或由金融機構內部單位進行。如為外部專 業機構，應與提供、維護資安評估標的之機構無利害關係，若為金融機構內部單位，應獨立於電腦系統開發與維護等相關部門。	**「證券暨期貨市場各服務事業建立內部控制制度處理準則」第36-2條之要求：** 各服務事業每年應將前一年度資訊安全整體執行情形，由資訊安全長或負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過。 除此之外，臺灣證券交易所券商輔導部也透過年度查核執行證券商合規之辦理情形。
技術面要求	資訊安全評估作業區分為資訊架構檢視、網路活動檢視、網路設備/伺服器/端末設備及物聯網等設備檢測、網路設備/伺服器及物聯網等設備且連線至Internet者應辦理相關事項、客戶端應用程式檢測、安全設定檢視、合規檢視等作業。	**建立證券商資通安全檢查機制-分級防護應辦事項附表：** 針對不同等級證券商有訂定相關資訊安全評估作業與技術面之評估內容。

人工智慧(AI)

法規比較-台灣人工智慧監管重點－AI相關法規及產業規範發展情形

因應國內人工智慧技術運用普及和持續性發展，其所引發之負面效應及風險，如隱私侵害、偏見歧視、不公平競爭、安全性疑慮，國內監管機構正在積極介入和制定/修訂相關要求及規範



法規比較-台灣人工智慧監管重點－金管會公布金融業運用人工智慧(AI)之核心原則

組織架構及問責機制 | 風險管理機制 | 人員知識及能力

建立治理及問責機制

- 應對其使用之AI系統承擔相應之內、外部責任(內部:指定高階主管負責AI相關監督管理並建立內部治理架構、外部:保護消費者之隱私及資訊安全)。
- 應建立全面且有效的AI相關風險管理機制。
- 培養及增進人員對AI的知識、風險辨識及管理能力。

落實公平性 | 以人為本及人類可控原則之落實方式 | Gen AI 產出資訊之風險管控

重視公平性及以人為本的價值觀

- 使用AI系統之過程中，應避免演算法之偏見，故使用AI系統的數據、資料庫及模型，應進行定期審查及驗證準確性，以減少偏差。
- AI系統之運用應符合以人為本及人類可控之原則，故為協助人類、對人類無危害及確保人類之自主權與可控制權。
- 生成式AI產出資訊，金融機構需就其風險進行客觀且專業的最終判斷。

隱私保護及資料治理 | 尊重客戶選擇的權利及替代方案

保護隱私及客戶權益

- 應充分尊重及保護消費者之隱私，並妥善管理及運用客戶資料。
- 如運用AI系統向客戶提供金融服務，應提供客戶退出AI服務之選項，或提供相應之人工替代方案。

資料來源:金管會公布金融業運用人工智慧(AI)之核心原則與相關推動政策 | 勤業眾信整理

落實系統穩定性 | 落實系統安全性

確保系統穩健性與安全性

- 金融機構在運用AI系統時，必須確保其系統之穩健性(robustness)與安全性，以避免對消費者或金融體系造成損害。
- 運用第三方業者開發或營運之AI系統提供金融服務，應對第三方業者進行適當之風險管理及監督、亦須針對第三方之責任範疇予以明定及要求針對AI相關運算規則並留存軌跡紀錄，俾利後續驗證與管理。

落實系統透明性 | 落實系統可解釋性

落實透明性與可解釋性

- 運用AI系統時，應確保其運作之透明性及可解釋性，理解AI如何做出決策，以確保對AI的運作之有效管理。
- 使用生成式AI作為辦理業務或提供金融服務輔助工具時，應適當揭露，並確保可解釋性的程度與其AI系統應用之重要性相稱。

落實永續發展 | 員工培育及培訓

促進永續發展

- 應確保其AI的運用策略與實施方式，均符合永續發展的原則，包括減少經濟、社會等不平等現象，保護自然環境，從而促進包容性成長、永續發展及社會福祉。
- AI系統運用過程中，宜對一般員工提供適當之培育及培訓，使員工能適應AI帶來之變革，尊重並保護一般受僱員工的工作權益。

資料來源:金融業運用AI指引/勤業眾信整理

法規比較-台灣人工智慧監管重點－金融業運用人工智慧(AI)指引

彈性選擇適宜的風險管理措施

- 金融機構可依AI系統具體使用情境所涉風險，依各核心原則宜注意之事項，合理選擇緩解風險之機制及落實方法

第三方業者的監督管理

- 金融機構運用AI系統時宜辨識可自行監控風險的程度，並對自身較無控制權或事項，透過契約等方式明訂風險監控的責任分工

外部審查機制

- 金融機構可於評估AI系統風險、內部資源及專業程度後，視需要得建立由具AI專業之獨立第三人進行審查、評測之機制

以風險為基礎落實核心原則

運用AI系統之風險高低仍由金融機構綜合考量各風險評估因素後自行判斷

AI系統公平性及人類可控

- 金融機構使用第三方業者開發之生成式AI，如無法掌握訓練過程及確保其數據或運算所得出之結果符合公平性時，金融機構對其產出之資訊，仍需由其人員就其風險進行客觀且專業的管控

資料最小化原則

- 採用「資料最小化原則」，避免蒐集過多或不必要的資訊
- 蒐集個人資料必須適當、相關且於資料處理目的之必要範圍內

AI系統運作的可解釋性及透明性

- 金融機構可清楚說明「自行或委託研發並使用之AI系統」如何運作及其預測或決策過程背後之邏輯
- 主動讓利害關係人(stakeholder)知悉其運用AI系統之做法

台灣人工智慧監管重點 – 銀行公會公布金融機構運用人工智慧技術自律規範

第三條
金融機構於第一條所載範圍內運用人工智慧，作為與消費者直接互動並提供金融商品建議、或提供客戶服務且影響客戶金融交易權益、或對營運有重大影響者，適用本規範。
本條所指之營運重大影響可參考「金融機構作業委託他人處理內部作業制度及程序辦法」第四條第五款之重大性定義，自行評估。

本辦法所稱之重大性，係指下列情形之一：
一、委外作業無法提供服務或有資訊安全疑慮，對金融機構之業務營運有重大影響者。
二、委外作業涉及客戶資料安全事件，對金融機構或客戶權益有重大影響者。
三、其他委外作業對金融機構或客戶權益有重大影響者。

治理政策及風險管理

金融機構於使用人工智慧服務技術作業時應規劃及注意之治理制度與風險管理事項，包含指定高階主管或委員會負責人工智慧相關監督管理並建立內部治理架構及適當之風險管理及定期檢視機制

永續發展

依據國際永續發展目標及自訂之永續發展原則，適當列入永續發展綜合指標

客戶權益保護及緊急應變措施

應採取措施以符合金融服務業公平待客原則，與消費者直接互動時，應告知該服並揭露相關資訊，並提供消費者選擇使用與否之權利，評估使用資料之治理方式、資通安全、監督機制、消費者權益保障及發生非預期事件時之應變措施，該評估由資安、法遵及風控等單位對於上開內容提出意見。

隱私保護及資訊安全

應注意保護所有相關個人和組織的資料隱私權，具備適當的保護措施確保其系統和資料的安全，避免資料洩露，並使用相關安全技術防止、偵測和回應各種安全威脅和攻擊

風險基礎及定期查核

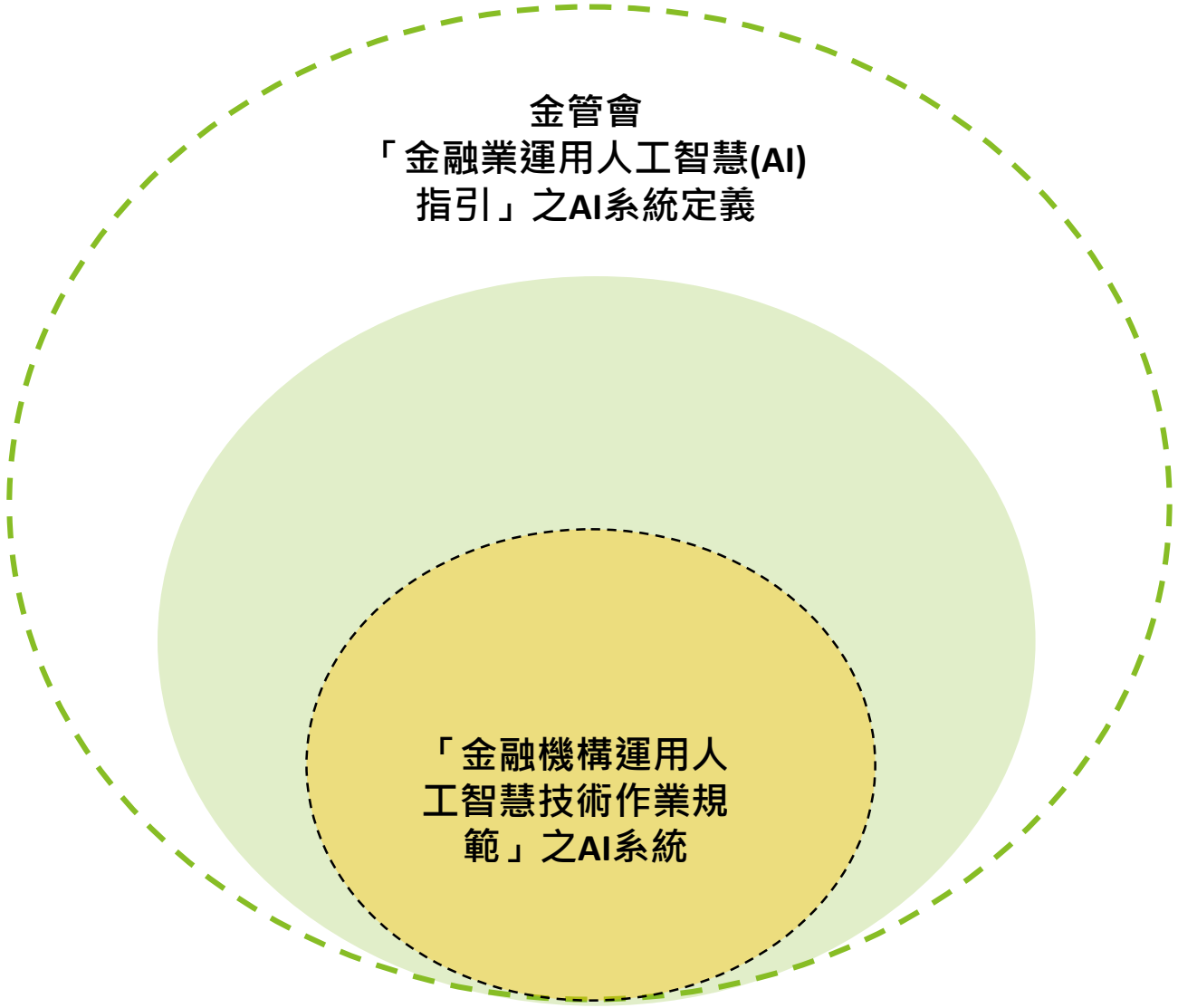
應以風險基礎為導向，視其營業規模及運用人工智慧技術之程度建立適當之風險管理制度及定期檢視機制，得由具人工智慧專業之獨立第三人出具評估報告。並應加人工智慧規範要求納入內控內稽制度中，並定期辦理查核。

人才培訓

人工智慧專業能力之訓練及能力提升、人力提升計畫。

資料來源: 金融檢督管理委員會/ 勤業眾信整理

金融機構運用人工智慧技術作業規範—適用範圍



AI系統：係指透過大量資料學習，利用機器學習或相關建立 模型之演算法，模仿人類學習、思考及反應模式之技術
生成式AI：係指可以生成模擬人類智慧創造之內容的相關AI 系統

「金融業運用人工智慧(AI)指引」以風險為基礎(RBA)評估方法

1. 是否面對客戶
2. 使用個人資料
3. 自主決策程度
4. 複雜性
5. 影響程度
6. 救濟選項

「金融機構運用人工智慧技術作業規範」適用範圍

1. 與客戶直接互動&提供金融商品建議
2. 提供客戶服務&影響金融交易權益
3. 對營運有重大影響(參考作業委外)

法規比較-人工智慧(AI)

銀行業訂定的「金融機構運用人工智慧技術作業規範」與各國AI法規規範比較

類別	銀行業「金融機構運用人工智慧技術作業規範」	與各國AI法規比較說明	
治理層面	強調對AI技術應用的監管和審查機制，確保金融機構在使用AI技術時能夠遵守相關法律法規，並維持高標準的治理結構。	**美國和歐盟**	皆有強調AI應用的透明度和問責性。 透過參考這些國家的經驗，台灣可以進一步完善其治理框架，確保AI技術在金融領域的應用能夠更加合規和有效。
風險評估層面	要求金融機構在使用AI技術時必須進行全面的風險評估，包括資料風險、技術風險和操作風險等。這些要求旨在識別和管理可能出現的風險，保護金融市場的穩定性。	**新加坡**	相關法規要求金融機構建立完善的風險評估和管理機制，以應對AI技術帶來的各種挑戰。
客戶權益層面	特別強調保護客戶的隱私和資料安全，確保AI技術的應用不會對客戶造成不必要的損害。這與全球其他國家在AI法規中的重點一致。	**歐盟與美國**	歐盟《通用數據保護條例》（GDPR）對個資保護提出了嚴格要求，美國的相關法規也在強化對客戶資料的保護。 通過參考這些國家的經驗，台灣可以進一步提升其客戶權益保護的標準，確保在使用AI技術時不會侵犯客戶的權利。

小結建議

針對證券市場的發展，建議可以先參考銀行產業的人工智慧技術作業規範，制定適合證券產業的指引與方向。這不僅有助於確保證券市場在使用AI技術時能夠遵守相關規範，還可以促進證券市場的技術創新和發展。同時，應當參考各國對於AI應用的定義和情境，逐步滾動式地調整證券市場的法令法規內容，確保其能夠與時俱進，適應不斷變化的技術環境。

問題與討論

Deloitte.

勤業眾信