金融監督管理委員會銀行局

《各國監理機關如何因應 Big Tech提供銀行服務之挑戰》

專題研究期末報告

勤業眾信聯合會計師事務所

中華民國 113 年 10 月 15 日

摘要

本研究旨在探討各國監理機關如何因應大型科技業者(Big Tech)提供銀行服務之挑戰。隨著 Big Tech 憑藉其規模及數據優勢，雖為金融業帶來創新與商機，卻也引發集中度、資訊安全及金融穩定性等議題，亦對於金融監管帶來挑戰。

研究採用標竿研究、文獻分析、專家交流與問卷調查等多元方法進行。透過分析標竿國家與國際金融組織對銀行業採用 Big Tech 服務衍生風險的監管框架與措施、並蒐集國內外相關研究資料，以及邀請國際專家進行交流。此外，亦透過問卷對本國銀行與外國銀行在台分行進行調查，瞭解其使用 Big Tech 服務的情況及合作中面臨的機會與挑戰，為未來監管政策的制定提供實證依據，並針對相關風險提出應對建議。

報告聚焦於由金融監管機構主導的 Big Tech 監管模式，深入分析我國面臨的 Big Tech 相關風險，並探討國際重大風險事故，如美國 Capital One 銀行資料外洩及南韓 Kakao 服務中斷事件等。針對這些風險，報告提出了具體的應對建議，並針對國際重大事故提出監理機關可於事前、事中、事後所採取的策略，強化對相關風險的管理。

延伸國際清算銀行（BIS）提出的基於業務活動（Activity-Based, AB）與基於實體（Entity-Based, EB）的監管方針，本研究提出針對台灣市場的短期、中期及長期監管框架。短期內金融監理機關應要求 Big Tech 加強其對金融產業相關服務風險的揭露，以及收集金融機構之服務供應商與服務狀況資訊；中期則應制定產業自律規範，確保 Big Tech 服務的透明度與風險控制；長期則建議採取 AB/EB 混合式監管，針對特定業務活動進行監管，同時強化對 Big Tech 作為第三方服務提供商所帶來的系統性風險管理，從而提升監管靈活性與市場穩定性。

本研究對國際上間接監理及直接監理措施進行分析，並建議在台灣現行間接監管框架的基礎上，借鏡國際作法，提出加強控管力度監理措施，包含在治理架構、風險管理、事故通報、測試演練及變更管理等領域，提升控管的精細度。同時，報告也探討了直接監理的優勢與國際上的控管措施，並建議監理機關未來可評估將 Big Tech 納入更全面的監管框架，以確保其與服務符合金融穩定性需求，為監管政策制定提供參考。

Abstract

This research aims to examine how national supervisory authorities are handling the challenges of Big Tech, both when it provides services to the banking industry and when it directly offers banking services. With its advantages in scale and data, Big Tech has brought innovation and business opportunities to the financial industry, but it has also raised issues such as market concentration, information security and financial stability, as well as challenges for financial regulators.

The study was conducted using multiple methods such as benchmarking approach, document analysis, expert sessions and surveys. It involved analyzing the regulatory frameworks and measures of benchmark countries and international financial organizations regarding the risks associated with the use of services provided by Big Tech in the banking industry. The study also collected relevant research findings from both domestic and international sources, and invited international experts to share their insights. In addition, a survey was conducted on domestic banks and branches of foreign banks in Taiwan to understand their use of Big Tech services and the opportunities and challenges they face when cooperating with Big Tech, providing an empirical basis for the formulation of future regulatory policies and offering suggestions for dealing with related risks.

The research focuses on the Big Tech regulatory framework led by financial regulators. It provides an in-depth analysis of Big Tech-related risks faced by Taiwan and discusses global risk events, such as the Capital One data breach in the United States and the service disruption of Kakao in South Korea. In response to these risks, the report offers specific suggestions for countermeasures and outlines strategies that can be adopted by supervisory authorities before, during, and after such incidents to mitigate the risks of these global risk events, strengthening the management of related risks.

Extending the Bank for International Settlements' (BIS) Activity-Based (AB) and Entity-Based (EB) regulatory approaches, this study proposes a short-term, medium-term, and long-term regulatory framework for the Taiwan market. In the short term, financial regulators should require Big Tech companies to strengthen disclosure of the risks associated with their financial industry-related services, as well as collect information on the service providers and service status from financial institutions. In the medium term, industry self-regulatory norms should be formulated to ensure the transparency and risk control of Big Tech services. In the long term, it is recommended to adopt an AB/EB hybrid approach to supervision, targeting specific business activities while simultaneously enhancing the systemic risk management that Big Tech introduces as a third-party service provider, thereby improving regulatory flexibility and market stability.

This research analyzes international indirect and direct supervision measures and recommends strengthening supervisory controls in Taiwan by drawing on these international practices. It proposes enhancing control measures in areas such as governance structure, risk management, incident reporting, testing exercises, and change management to improve regulatory precision under the current indirect supervision framework. Additionally, the report discusses the advantages of direct supervision and international control measures, suggesting regulators consider including Big Tech in a more comprehensive regulatory framework to ensure their services meet the requirements for financial stability, while also providing a reference for regulatory policy development.

目錄

表目錄

1. 緒論

1.1. 研究動機與目的

近年大型科技業者(Big Tech)興起，憑藉其規模及數據優勢，透過與金融機構合作、受金融機構委託、取得金融執照或虛擬資產等途徑，跨業提供銀行服務，雖為金融產業帶來各種商業機會，然其所衍生之服務集中度、資訊安全及金融穩定等議題，亦對於既有金融監管帶來挑戰。

Big Tech 挾其成本及彈性之優勢，使許多金融創新服務集中於少數業者，如亞馬遜(Amazon)、谷歌(Google)或微軟(Microsoft)等，其衍生之風險如過度集中風險、系統性風險及消費者保護風險等，對金融穩定造成影響。各國監理機關為應對相關風險，已研議相關監理政策，如金融機構與 Big Tech 合作或委外時應建立妥適風險控管機制等；更甚者近年並研議將此類 Big Tech 納入監管，如英國金融監理機關研議將銀行之關鍵第三方業者納入監管，印度亦發布草案定義國內「系統性重要數位企業」並建立相關控管制度。

據悉現行臺灣已有多家金融機構表示將更廣泛採用第三方服務或進行跨業合作，以提升金融服務品質及業務創新。於前述背景下，希冀藉由本委託研究案瞭解各國就銀行業採用 Big Tech 等第三方服務所關注之主要風險，及為應對該等風險所採取之監理措施；並對我國未來監理政策之方向及法制層面之作業提供具體建議。

1.2. 研究範圍

本研究範圍涵蓋 BIS、FSB、IMF、歐盟、英國、德國、美國、日本、印度等國家與國際金融組織對於 Big Tech 涉及金融相關產業之規範，與本國現有法規進行差異分析並歸納比較。

1.3. 研究方法

針對如上研究議題，本報告之研究方法主要包括標竿研究、文獻分析、專家交流、問卷調查，要述如下。

1.3.1. 標竿研究法(Benchmarking Approach)

本研究針對標竿國家與國際金融組織對銀行業採用 Big Tech 等第三方服務衍生風險之重要議題，包含所採取之監管原則、設計之風險監管架構及法制作業等進行分析，對 BIS、FSB、IMF、歐盟、英國、德國、美國、日本、印度之重要標竿案例進行重點歸納與深入比較與分析，以做為我國未來監理政策設計之參考。

1.3.2. 文獻分析法(Document Analysis)

透過國內外相關研究資料之文獻蒐集與分析，檢視標竿國家於銀行業採用 Big Tech 等第三方服務衍生的風險之重要議題: 發展背景、現況、提供金融業的服務類型、對金融業造成的影響、與 Big Tech 相關的重大風險事件、國際組織與先進國家關注的主要風險、採取之監管原則、設計之風險監管架構及法制作業。

1.3.3. 專家交流

本研究針對銀行業採用 Big Tech 等第三方服務的重要議題，委由勤業眾信與國際團隊相關領域專家進行交流，俾以匯集專家見解，凝聚共識，並進一步探討各國對於 Big Tech 監管的現況、規劃與挑戰。

本所邀請了英國、美國、德國、印度、日本與歐盟的專家參與此研究與進行交流，我們將專家分享之內容彙整、且與本研究案之研究資料與結果進行參照與比對，並將具獨特性且未已涵蓋於各國法規分析之內容，整合於本研究報告書第六章之各國分析段落，以專家意見呈現。

1.3.4. 問卷調查

金融機構在採用 Big Tech 服務及與 Big Tech 的合作方式上不盡相同。本研究將透過問卷對本國銀行與外國銀行在台分行進行調查，以瞭解銀行使用 Big Tech 服務情形及與 Big Tech 合作所帶來的機會與挑戰，以利監理機關瞭解銀行業面臨的痛點及潛在風險，為監理機關制定相關政策時提供依據，確保金融體系的穩定性與安全性。

2. Big Tech 針對金融服務產業之發展背景與現況

2.1. 國際間對 Big Tech 的界定摘要

目前國際金融組織與各國主管機關對 Big Tech 的定義與界定不完全一致，就監管層面而言，雖 Big Tech 提供創新金融服務逐漸興起，不過 Big Tech 作為金融機構之第三方服務提供商仍為主流，例如歐盟與英國的金融主管機關僅定義與規範「具關鍵角色」與「提供關鍵服務」之關鍵第三方服務提供商，由於上述之關鍵第三方服務提供商不一定都是 Big Tech，但若 Big Tech 作為金融機構的第三方委外服務提供商時，通常會是關鍵第三方服務提供商，也因此 Big Tech 往往僅在作為金融機構關鍵第三方服務提供商時，受到金融主管機關之監管。此外，國際金融組織亦有探討 Big Tech 公司作為金融機構第三方服務提供商的重要性，在關鍵服務集中在少數大型服務提供商的情況下，隨之而來的營運風險(Operational Risk)、依賴性風險(Dependency Risk)、資料保護風險(Data Privacy Risk)、資訊安全風險(Cybersecurity Risk)，以及系統性風險(Systemic Risk)皆為潛在的監管挑戰。

表 1 國際金融組織對 Big Tech 的界定摘要

國際金融組織	Big Tech 的界定摘要
國際清算銀行(BIS)	透過數位服務平臺(如電子商務、社交媒體與搜尋引擎)，獲取大量用戶資料與用戶基礎的大型科技公司，並具備數據分析(Data analytics)、網路外部性(Network externalities)及多元商業活動(Interwoven activities)等彼此可相互強化效益之內在條件因素，例如 Alibaba(阿里巴巴)、Amazon(亞馬遜)、Facebook(臉書)、Google(谷歌)和 Tencent(騰訊)。
金融穩定委員會(FSB)	在電子商務、社交媒體與搜尋引擎等方面具明顯優勢，且擁有運作成熟的平台和廣泛存取客戶資料的大型科技公司，例如 Alibaba(阿里巴巴)、Amazon(亞馬遜)、Facebook(臉書)、Google(谷歌) 和 Tencent (騰訊)。
國際貨幣基金組織(IMF)	擁有豐富的資料資源、技術能力、龐大客戶網路的大型科技公司，例如 Alibaba(阿里巴巴)、Amazon(亞馬遜)、Facebook(臉書)和 Google(谷歌)。

表 2 各國主管機關對 Big Tech 或關鍵第三方服務提供商的界定摘要

國家	近 Big Tech/關鍵第三方服務提供商的界定摘要
歐盟	關鍵資訊通信技術(ICT)第三方服務提供商(Critical Third-party ICT Service Providers)的評估標準包括是否提供關鍵服務、在市場的影響力、可替代性、對金融服務的穩定性、持續營運能力或品質等系統性影響、以及金融機構對服務提供商的依賴程度等方面。
英國	關鍵第三方(Critical Third Parties, CTPs)的評估標準包括服務重大性（如是否提供關鍵服務、對金融系統的穩定性與系統性影響）、服務集中度（如金融機構對服務提供商的依賴程度）、可替代性以及對金融機構重要資源的存取權限等方面。
美國	無特別規範。
德國	在 IT 委外服務的範疇中，僅針對雲端服務供應商特別規範。
印度	提供核心數位服務(Core Digital Services)的系統性重要數位企業(Systematically Significant Digital Enterprises, SSDE)的評估標準包括財務與商業規模、使用者數量、市場影響力，以及企業與使用者的依賴程度等面向。
日本	無特別規範。
台灣	Big Tech 是指大型科技公司，例如從事電子商務的 Amazon(亞馬遜)及 Alibaba(阿里巴巴)、搜尋引擎 Google(谷歌)及手機製造商 Apple(蘋果)等。

2.2. Big Tech 在金融產業的定位

Big Tech 為在資訊科技產業具領導地位的大型科技公司，提供以資訊科技與數位服務為主的業務活動，並且在各個市場擁有廣泛的客戶和顯著的市場影響力，通常包含以下公司：

(1) Apple：主要以 macOS 作業系統、iOS 作業系統、iWork 辦公室應用軟體，以及 iPhone、iPad、Macbook 等軟、硬體和 App Store、iCloud 等數位服務著稱。

(2) Alphabet：為 Google 母公司，以 Google 搜尋引擎、Google Ads 廣告業務、Android 作業系統、GCP 雲端服務和 YouTube 影音串流平台聞名。

(3) Microsoft：以 Windows 作業系統、Office 辦公室應用軟體、Azure 雲端服務等產品著稱。

(4) Amazon：主要以其電商平台、AWS 雲端服務和 Prime Video 影音平台著稱。

(5) Meta：為 Facebook 前身，以 Facebook、Instagram、WhatsApp 等社交軟體聞名。

雖目前 Big Tech 尚未有公認且一致的定義，包含我國中央銀行在內，較常見將下列大型科技公司視為 Big Tech，如 Amazon(亞馬遜)、Alibaba(阿里巴巴)、Google(谷歌)、Apple(蘋果)、Microsoft(微軟)等，而上述本業非屬金融業的 Big Tech，在龐大的用戶基礎與逐漸成熟的產品服務生態圈背景下，從一開始作為提供金融機構科技導向解決方案(Technology-Based Solution)的第三方服務提供商，到為滿足使用者於平台交易衍生之金融服務需求，跨足金融產業，漸次提供支付、融資、保險、儲蓄及投資商品等創新金融服務。

2.3. Big Tech 提供之服務

2.3.1. Big Tech 作為金融機構的第三方服務提供商

2.3.1.1. 金融機構對 Big Tech 的委外服務需求

金融機構在降低成本與提升效益的同時，可能將公司的某些業務或職能委託給外部服務供應商，由委外服務供應商負責執行與維運受託之業務。Big Tech 作為金融機構的委外服務供應商，主要以提供雲端服務為大宗（如 Amazon Web Services、Microsoft Azure、Google Cloud Platform 等雲端服務），包含金融機構所需的雲端服務和運算資源，協助處理與分析大量的資料和複雜的金融應用運算。在金融機構通常需要大量的資訊基礎設施的情況下（如伺服器與資料儲存設備），使用雲端服務除成本效益考量外，可以根據實際需求靈活調整資源，具備擴充性和彈性的優勢。不過也因為 Big Tech 本身在產業的高市占率，由少數服務供應商支援企業資訊科技基礎架構的情形，可能導致新型的集中度風險，再加上金融產業為受高度監管的行業，主管機關亦須加強金融機構在委外與使用雲端服務的監管強度。

2.3.1.2. 金融機構對 Big Tech 的外部服務採購需求

金融機構在支援或增強業務營運的情況下，可能會以訂閱或購買等採購方式使用外部服務來滿足具體需求，且金融機構通常會保留更多的控制權，僅使用外部服務來支援或增強業務營運。Big Tech 作為金融機構的第三方服務供應商，提供的服務涵蓋但不限於辦公室應用軟體、通訊與團隊協作工具、資料保護與備份服務、人工智慧與機器學習平台等多個領域，而常見的採購服務有 Microsoft Windows 作業系統、Microsoft Office 辦公室應用軟體、Microsoft Teams 通訊與團隊協作工具、Apple App Store 與 Google Play 應用程式商店，以及 Microsoft

Azure Active Directory 身分識別和存取權管理解決方案等多樣化的產品與服務。與委外服務相比，往往採購之外部服務在金融機構的使用範圍更廣泛，也和金融機構日常營運的關係更加緊密。

2.3.2. Big Tech 與金融機構的合作以及直接提供類金融服務

隨著 Big Tech 在金融服務領域的成長，從推動金融產業創新到提供創新金融服務，包含與金融機構合作提供服務，以及由 Big Tech 直接提供類金融服務，展示了 Big Tech 和金融機構既是競爭者也是合作夥伴，在金融機構和 Big Tech 之間的合作越來越普遍的同時，Big Tech 也對傳統金融機構構成了競爭威脅。

Big Tech 具備龐大的使用者基礎，期望在既有的產品與服務生態圈建立嵌入式金融服務，將金融服務融入應用程式與平台之中，以此完善 Big Tech 生態圈的消費體驗。在 Big Tech 與金融機構的合作方面，Apple 自 2014 年推出 Apple Pay 行動支付服務，並與銀行及信用卡發卡機構合作，使用者可將簽帳卡或信用卡加入錢包(Apple Wallet)，且經身分驗證通過後，即可透過 Apple 產品在線上或實體店面進行支付，另於 2019 年 Apple 與美國投資銀行高盛(Goldman Sachs)聯手推出 Apple Card 信用卡，除了提供簡化的信用卡使用體驗，亦彌補了原本不支援 Apple Pay 的支付場景，不過因金融產品在不同國家的監管要求，Apple Card 的服務範圍仍僅限於美國。而在 Big Tech 直接提供類金融服務方面，Amazon 於 2012 年針對其電商平台的中小賣家推出 Amazon Lending 商業貸款服務，透過分析商家的銷售歷史與業績表現等條件評估放款，無須額外的信用檢查即可提供賣家短期的優利貸款，幫助其擴展業務，而還款方式將從賣家在 Amazon 平台上的銷售收入中自動扣除，亦無需賣家執行額外的還款作業，不過在經歷了 10 年的服務提供期間，可能在缺乏對信貸市場的瞭解以及貸款管理的掌握等因素下，Amazon 已於 2024 年 3 月終止這項商業貸款服務[1]。

[1] *Digital Disruption in Banking and its Impact on Competition* (2020).

2.4. Big Tech 對傳統金融業造成的影響

Big Tech 在多面向數位化技術的應用，為金融服務帶來的許多機會及潛在效益。對於銀行而言，業務數位化將有望擴大金融服務、降低交易成本、改善使用者體驗和增加市場競爭力。對於客戶也能獲得更完善、更便利的金融服務。然而，Big Tech 提供的強大科技技術可使銀行及客戶受益，卻也可能因迅速主導市場，造成有害市場競爭的行為，提高銀行、客戶和金融穩定所面對的既有風險。

2.4.1. 集中度風險

Big Tech 帶來的集中度風險，主要以平台（如乙太坊區塊鏈）、模型（如基礎人工智慧模型）或第三方（如雲端服務供應商和人工智慧模型開發商）等形式出現，英格蘭銀行在 2020 年調查估計，超過 70% 的銀行和 80% 的保險公司僅依賴兩家雲供應商的 IaaS[2]。在新興市場地區，Big Tech 亦表現出強大的壟斷能力，在肯亞(Kenya)，行動支付服務的市場領導者擁有超過 2500 萬用戶，佔肯亞總人口的一半以上。

在全球範圍內，市場研究機構 Synergy Research Group 於 2024 年 4 月發布的報告[3]顯示，目前全球最大的雲服務供應商為亞馬遜 AWS，市場占有率為 31%；微軟 Azure 位居第二，市場占有率 25%；Google 排行第三，市場占有率 11%，若前述公司發生服務中斷，將可能會導致整個銀行和金融系統的重大中斷。

2.4.2. 系統性風險

Big Tech 提供新技術及應用進入金融服務領域迅速擴展業務活動的同時，也將提高銀行體系和金融穩定的系統性風險，包括：

- 服務提供的互聯性大幅增加：Big Tech 提供強大的科技技術，與銀行之間產生更多的相互依賴關係，然 Big Tech 公司可能對金融產業運作欠缺經驗及專業知識，風險管理文化亦與金融業嚴謹的法令遵循要尚有差距，將增加金融體系複雜性和不透明性，使監理機關更難識別、評估和應對風險。

- 金融傳染：Big Tech 主要作為網路多邊平臺（Multi-Sided Platforms, MSP），支援和促進兩組或多組使用者（例如買家和賣家）之間的直接互動，加快金融市場建立連結的速度。然，若兩造其中一方積欠另一方某種有價資產，使得另一方的處於無力償債狀態，負債壓力將可能藉由借款人傳染給銀行、保險公司，再到許多與借款人

[2] 基礎架構即服務 (IaaS) 是一種雲端運算服務類型，可透過網際網路以依用量計費的方式提供隨需存取如伺服器、儲存空間、網路和虛擬化等運算資源的服務。

[3] ‘’*Huge Cloud Market Sees a Strong Bounce in Growth Rate for the Second Consecutive Quarter*’’ RENO, NV, April 30, 2024

沒有商業往來的公司，由於網絡涵蓋的範圍極大，將可能造成災難性後果。

- 羊群效應：在 Big Tech 提供市場大多數金融機構同一組深度學習或其他相關技術演算法的情況下，將可能導致整體金融市場因過度集中依賴於同一演算模型而造成行為一致性的系統性問題。將可能再度重演歷史事件的連鎖性效應及對金融市場造成的重大衝擊，在過往相似的歷史經驗包括 1980 年代末的美國儲蓄貸款危機、互聯網泡沫和 2007 年的量化危機。除了在美國，日本也曾因信貸商品太過一致造成泡沫破裂而讓銀行業受到衝擊。

2.4.3. 消費者保護風險

相較於金融機構已建構較嚴謹的監管規範下，Big Tech 現有的監管要求相對鬆散許多，在客戶資料的保護上容易面臨較高的風險，特別是新興市場或開發中國家，在相對薄弱的消費者保護和監督框架，以及普遍用戶金融知識水準不足的情況下，Big Tech 與該國金融服務用戶的互動，以及相關的業務行為和數據隱私考量，有可能對該區域內的金融穩定構成較大的風險。如 2009 年，印度最大的電信公司 Reliance Jio 即外洩 1.1 億客戶的個人資訊，包含姓名、地址、手機號碼，以及指紋、相片、虹膜掃描等高度敏感個人資訊，有心人士可透過 WhatsApp 匿名群組以低廉的價格取得客戶個人資訊。

此外，雖 Big Tech 通常不會直接提供資金予用戶，然若 Big Tech 公司倒閉或突然離開運營所在國，將結清存放於該國銀行的現金儲備或維持營運的資金帳戶，仍可能會對銀行的財務狀況造成流動性壓力。再者，從電子商務業務發展起來的 Big Tech 公司通常與商家和消費者間有大量的準備金交易，在相關規範控管不足的情況下，可能發生準備金不足造成的流動性風險，並影響消費者權益。

3. 銀行使用 Big Tech 服務之重大風險事故分析

3.1. 美國 Capital One 銀行

3.1.1. 背景、裁罰、集體訴訟

2019 年 7 月前 AWS 員工利用美國 Capital One 銀行於在 Amazon AW 雲端系統上的防火牆漏洞駭入侵系統，並竊取上億用戶個資及企業資訊，導致美國約 1 億人口、加拿大約 600 萬人口的資料外洩。事後 Captial One 遭監理機關處以 8 千萬美元民事罰金，且還須面對索償 3.5 億的集體訴訟。

根據 A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned 對 Capital One 事件分析，導致此次資料洩漏事件源頭可追溯至 2014 年 Capital One 在雲端策略的佈局，相比金融業傳統的策略，該公司做了較前瞻性的創新決定，以支持其雲端策略，包括對開源技術的承諾、採用敏捷開發理念以及公有雲架構等。因應企業轉型策略，該公司積極招募技術人才，並將公司目標放在快速開發新功能以利增強客戶體驗。該公司於轉型策略過程中並非僅於 2019 年發生資料外洩事件，然此事件係直接針對雲端基礎架構進行攻擊所造成的重大個資外洩風險事件。

Capital One 在 2015 年公佈雲端策略之前，公司管理階層為了保持競爭力，制定的策略是將銀行重塑為具有前瞻性的科技公司，該策略包含降低技術（資料中心）成本，並同時利用雲端可快速擴展性和不斷增加應用服務的優勢。由於策略的成功與否取決於該公司獲取技術人才的能力，故高階管理階層做出了較大膽的決定，包括開源技術、敏捷開發理念以及將服務佈署至公有雲。這種策略（敏捷、開源和公有雲）將開發新應用程式的速度和成本作為最優先考量，而犧牲這些應用程式的安全性。鑑於高階管理階層雖瞭解遷移到雲端會增加風險，但不排除其對雲端共同責任模型的誤解，而且造成內部對於雲端資訊安全管理流程的疏漏。

3.1.2. 責任釐清

共同責任模式常使人們誤以為目前供應商提供的雲端基礎建設已有足夠的安全控管措施，便對自身的資訊安全防禦掉以輕心，忽略了若雲端供應商的安全性不足可能導致資訊安全事故，且租用雲端服務的客戶也有責任確保其應用程式安全。儘管 Capital One 外洩事件最終被歸咎於「防火牆配置錯誤」，但高階管理階層採取的許多政策和決定對洩漏事件也產生了相當的影響。因為高階管理階層的主要職責是提供有意義的網路安全策略，並根據充分的風險評估和管理流程分配足夠的資源，以實現雲端安全目標。

首先，AWS 未提供租用雲端服務之客戶足夠的指導以防範資安漏洞，但在共同責任模式下，Capital One 使用的 IaaS 及 PaaS 雲端服務所產生雲端內部安全由其自行負責。託管 Capital One 後端系統的雲端服務供應商 AWS，在 Capital One 資料外洩事件發生後，明確否認對此次駭客攻擊負有任何責任，因其表明此並非雲端本身的安全所產生的漏洞。根據共同責任模式，AWS 作為雲端服務供應商提供雲端基礎架構，並負責雲端基礎設施的安全(雲端本身安全[4])，而客戶即 Capital One 則負責雲端服務的安全(雲端內部安全[5])。AWS 指出這種共同責任模型可有助減輕客戶的營運負擔，AWS 除了提供安全可靠的基礎設施服務外，亦負責提供各種工具、服務以及充分有效的指導，以協助客戶實現其安全性和合規性目標。在此次資料外洩事件中，儘管雲端基礎設施未受到損害，但攻擊者卻利用了基礎設施架構中的弱點。即使 AWS 在 2018 年就意識到此漏洞，仍未實施具體對策。直到 2019 年 11 月，AWS 才宣布更新修復上述漏洞。

其次，Capital One 董事會層級僅遵守網路風險管理原則，雖滿足合規要求但不足以有效防止資料外洩。從 Capital One 的年報中可以確認其董事會承擔了網路風險監督的責任，並成立了風險委員會，負責監督公司的資訊安全風險概況、高風險的資訊安全議題、企業資訊安全計畫和關鍵企業資訊安全管控措施。然而，高階管理階層卻未能為其雲端策略建立適當的風險管理流程，「包括適當的設計和實施網路安全控制、充分的資料遺失預防控制以及有效的入侵偵測和監控控制」。然，其管理制度仍存在兩個關鍵弱點。第一點，董事會在事件發生前，雖然已經在技術面運用了完整的五項原則，但董事會沒有與 CISO（Chief Information Security Officer）的直接溝通管道，無法及時從公司主要安全防禦者接收有關潛在風險的資訊。儘管建立了網路安全管理措施，但這些控管措施的成熟度不足以識別和解決因採用新技術而出現的風險，另一方面，內部稽核運作存在缺失，OCC[6]發現內部稽核未能識別雲端營運環境中的許多控制弱點，也沒有向董事會、審計委員會報告已識別出的弱點和差異。此外，對於內部稽核提出的一些安全控管的擔憂點並未得到董事會的回饋。

最後，雲端提供者不受任何特定網路安全法規的約束，且對金融業者實施過多的監管和多個機關的監督並不能有效防止資料外洩。Capital One 遵守《Gramm-Leach-Bliley Act[7]》（GLB

[4] AWS 負責之雲端本身安全係指雲端基礎設施的安全，負責營運、管理和控制主機作業系統和虛擬化服務的設施實體安全。

[5] Capital One 負責之雲端內部安全係指於企業內部使用雲端設施的安全，如負責為其雲端策略建立適當的風險管理流程，包括適當的設計和實施網路安全控制、充分的資料遺失預防控制以及有效的入侵偵測和監控控制等。

[6] 在美國，金融機構的監理機關包括: 美國貨幣總核查辦公室 (OCC)、聯邦存款保險公司 (FDIC)、儲蓄機構管理局 (OTS) 以及各州銀行部門在內的眾多聯邦和州機構。 OCC 負責特許、監管和監督國家特許銀行，而 FDIC、美聯儲和州銀行當局負責監管州特許銀行。聯準會對擁有一家或多家銀行或擁有控股權的銀行控股公司和金融服務控股公司進行監管。同時，OTS 則審查聯邦和許多州特許的儲蓄機構，其中包括儲蓄銀行和儲蓄貸款協會。目標是強制金融部門建立強大的資訊安全實踐，以保護消費者並確保經濟穩定。

[7] 《Gramm-Leach-Bliley Act》亦稱《Financial Services Modernization Act of 1999》(金融服務法現代化法案)，是 1999 年 11 月 12 日美國頒布的法案，該法案消除銀行、證券和保險公司之間的市場壁壘，使商業銀行、投資銀行、證券公司和保險公司得以合併為大型金融控股公司，並且允許同時擔任證券和銀行公司兩方的董事或員工。此外，它還要求金融機構須確保客戶數據安全保密，且須採取特定的安全措施來保護數據存儲及傳輸安全。

Act）第 501(b) 條[8]和《Fair and Accurate Credit Transactions Act of 2003[9]》（FACT Act）第 216 條[10]。金融機構須遵循相關法令要求[11]，制定和實施全面有效的資訊安全計畫來保護資訊系統和非公開資訊免受網路威脅並測試其資訊安全計畫的關鍵控制措施、系統和程序的有效性，以確保客戶資訊的安全性、機密性和完整性。

該要求規定了資訊安全計畫所有主要領域的期望，包括風險評估、滲透測試、稽核追蹤、限制存取權限、每年向董事會提交的資訊安全報告、加密、多因素身分驗證和供應商合規性。基於這些規定， Capital One 的董事會對網路安全更加關注。然而，儘管董事會相當關注網路安全並且該銀行明顯遵守了所有要求，但 Capital One 還是產生了重大違規。多數組織通常僅採取最低限度的措施以使監管稽核合規。

許多監理機關會使用不同的詞彙和框架來規定內容相似的資訊安全要求，造成了不必要的複雜性，使得組織耗費大量人力及時間以符合監理機關對資訊安全期望及報告審查要求。另外，由於近年金融服務機構增加了對雲端服務供應商的依賴，應正視雲端服務供應商缺乏監管的問題。主要風險之一來自金融業者對共擔安全責任模式的誤解，正確理解評估和實施適當控制的職責分工至關重要，特別是因為雲端提供者不受任何特定網路安全法規的約束，且與第三方相關的各項資訊安全風險預計未來將由金融機構進行管理。2019 年 8 月受侵害的用戶對 Capital One 和 AWS 提起的集體訴訟，聲稱 Capital One 和 AWS 都沒有充分保護數據，這證實了在未來呼籲對雲端服務提供者問責將獲得更多關注。

3.1.3. AWS 的責任

在此次資料外洩事件中，攻擊者有利用了基礎設施架構中執行個體中繼資料服務 (IMDSv1)並不會驗證來自 EC2 執行個體的 API 請求合法性的漏洞，雖無法直接證明該漏洞是導致資料外洩事件的原因，但的確存有安全漏洞未修補事實。AWS 即便在 2018 年已意識到此設計漏洞，卻將焦點放在發布創新的功能及服務，並未考量與提供修補漏洞的因應對策。然而，根據共同責任模式，AWS 作為雲端服務供應商提供雲端基礎架構，並負責雲端基礎設施的安全(雲端本身安全)，而客戶即 Capital One 則負責雲端服務的安全，故 AWS 表明，由於此次資料外洩事故並非雲端本身的安全所產生的漏洞，故否認對此次駭客攻擊負有責任。

另外，AWS 除了提供基礎設施服務外，市場亦有聲浪表示其應負有提供針對各種工具和服務之充分有效的指導之責，以協助客戶實現安全性與合規性目標。在此資料外洩事件中，

[8] 此條目內容為列述金融機構之保障措施，包含以下三點：(1)確保客戶紀錄和資訊的安全和保密；(2)防止此類紀錄的安全性或完整性受到任何可被預期的威脅或危害；(3)防止未經授權存取或使用此類紀錄或訊息，以免對任何客戶造成重大傷害或不便。

[9] 《Fair and Accurate Credit Transactions Act of 2003》是美國國會於 2003 年頒布的一項聯邦法律，旨在修訂 1970 年通過的《Fair Credit Reporting Act》(公平信用報告法案)。其目的是加強消費者保護，特別是身份竊取方面。該法案最著名的特點是，它允許消費者每年至少一次能免費查閱個人的信用報告。

[10] 此條目內容主要列述針對消費者其報告資訊和紀錄的處理規範。

[11] 相關法令要求如《Interagency Guidelines Establishing Standards for Safeguarding Customer Information》，該準則建立了與管理、技術和實體保護相關的標準，以確保客戶資訊的安全性、機密性和完整性。

AWS 未向 Capital One 提供足夠的指導來防範這些漏洞，尤其公有雲的雲端部屬模式加劇了伺服器端請求偽造(Server Side Request Forgery, SSRF)的安全威脅影響，而 AWS 卻沒有採取任何措施來解決此安全議題。此後，AWS 在發生該資料外洩事件的四個月後(2019 年 11 月)，宣布更新執行個體中繼資料服務(IMDSv1)的漏洞並發布更新後的第二版本(IMDSv2) 服務提供「針對未經授權的元資料存取的深度防禦」。

3.1.4. 主管機關處分及訴訟結果

根據共同責任模式，客戶即 Capital One 應負責「雲端內部的安全」，包含客戶在執行個體上安裝的所有應用程式軟體或公用程式，以及 AWS 在每個執行個體提供的防火牆組態。此外洩事件最終被歸咎於 Capital One 在雲端的「防火牆配置錯誤」，且高階管理階層採取的許多政策和決定對洩漏事件也產生了相當的影響，Capital One 後續遭監理機關處以 8 千萬美元民事罰金，並於 2021 年底同意支付 1.9 億美金予受資料外洩事件影響的 9,800 萬個用戶。而此次事件的攻擊者，前 AWS 員工則受美國地方法院判處犯有七項詐欺罪，罪名是從儲存在雲端亞馬遜網路服務的不安全帳戶中竊取超過 1 億客戶的個人資料，於 2022 年 10 月受陪審團裁定她犯有電信詐欺、未經授權存取受保護電腦和損壞受保護電腦的罪名，最終被判處緩刑五年。

3.2. 南韓 Kakao 純網銀

3.2.1. 背景

2022 年 10 月 15 日，SK 集團旗下一棟大樓發生火災，該大樓是韓國兩家網路公司 Kakao 和 Naver 的資料中心。這場大火在當日深夜被撲滅，但 Kakao 的停電持續至隔日，影響了韓國境內的金融和交通，導致銀行交易、線上線下支付系統以及海外支付服務等 17 項 Kakao 服務大規模中斷。受影響的服務包括行動支付系統 Kakao Pay、交通應用程式 Kakao T、Kakao Games、Daum 入口網站和 Melon 音樂服務。多方消息管道指出 Kakao 缺乏災難復原準備工作，另韓國時報引述當地 IT 專家表示「如果 Kakao 用備份站點保護其數據，服務中斷問題就會很快得到解決」。但 Kakao 表示若消防單位未於起火時即刻關閉電源，將能更有效執行災難應變措施，從而搶救更多資料，大幅降低此次災害影響範圍和時間。

3.2.2. 責任釐清

Kakao 表示起火原因為 SK 集團子公司 SK On 所生產鋰電池發生問題，SK 集團也於事後表示願意承擔火災的所有責任，但其賠償僅能於 Kakao 衡量完損失後才能受理。

3.2.3. 集體訴訟賠償

在 2022 年 10 月中資料中心火災導致服務中斷後，客戶向 Kakao 尋求賠償委請律師對 Kakao 提起集體訴訟，理由是該公司的「疏忽」導致韓國各地的交通和金融受到嚴重干擾。Kakao 表示向 10 月火災造成影響的小型企業提供 30,000 韓元(23.70 美元)至 50,000 韓元（39.28 美元）的賠償，範圍包括社交媒體、商業、金融及交通。該公司於 2023 年 1 月 5 日也開始向 KakaoTalk 用戶發送表情包作為進一步的補償，並為前 300 萬名申請者提供一個月免費使用資料備份服務的優惠券。該事件也促使韓國政府加強對平台和資料中心營運商的措施。

3.2.4. 小結

資料中心火災事件發生後，金融監督院表示與國家消防局簽署了一項協議，以加強溝通管道，以便及早採取預防措施撲滅資料中心火災。資訊通信技術部表示，政府批准了法律修正案，從 2023 年 7 月 4 日起，政府將承擔新的災害預防和應對管理義務。2023 年 10 月，資訊通信技術部表示將更審慎管理防災工作，並將關鍵數位基礎設施的風險降至最低。金融監督院還承諾成立專家小組來製定相關策略，以提高該南韓資料中心的安全性和可靠性。該專家小組提出透過三大階段來改善現有制度和措施：第一階段將要求提供金融相關服務的大型科技公司建立災害復原中心；第二階段將對於過於細節的規範進行修改，著重於提出原則和目標以利大型科技公司有效遵循；第三階段則期望將現行正面表列的安全法規轉變為透過負面表列以因應快速變化的市場環境。金融監督院於 2024 年 2 月初宣布近期將公布《數位金融監督條例》修正案，旨在透過上述三階段的調整加強數位金融營運韌性，有效減緩系統性風險可能帶來的負面影響。

4. 國際金融組織之關注重點、監管原則及法制作業

4.1. 國際清算銀行 (Bank for International Settlements, BIS)

BIS 對於 Big Tech 的定義為在數位技術方面具有相對優勢的大型全球性且活躍發展的科技公司。這類科技公司具備全球性的業務運營，擁有大量客戶基礎，並能利用關於客戶的大量資訊來為其個別提供量身定制的數位服務，Big Tech 具備數據分析(Data analytics)、網路外部性(Network externalities)及多元商業活動(Interwoven activities)(簡稱「DNA」)等彼此可相互強化效益之內在條件因素，同時結合非金融業務與金融服務，其業務規模及競爭能力已逐漸對傳統銀行業形成挑戰，並引起國際間金融監理機關的關注。

根據 BIS 近年的報告[12]，Big Tech 在金融領域的業務性質使其涵蓋於多個監理機關的管轄範圍，包括中央銀行、市場競爭監理機關和資料保護監理機關。形成了特定產業監管和跨國監管的複雜組合。BIS 建議對於 Big Tech，各國監理機關可先以基於業務活動（Activity-Based, AB）的監管方向開始設立相關監管措施，此方法旨在讓所有經營相同特定業務活動的公司都應遵守一致的規則和標準，無論其組織結構或商業模式如何，確保 Big Tech 和傳統金融機構在公平的競爭環境中運作。基於業務活動的監管方式具有以下特點：

- **公平競爭環境**：透過對所有從事特定業務行為的公司一視同仁應用相同規則，可以確保同一業務內的公平競爭，防止監理強度差異導致不公平的情況。
- **靈活性**：可以隨著新技術和新業務模式的出現而迅速調整監管要求。
- **風險聚焦**：可以更直接針對特定業務活動所涉及的風險，而不必考慮整個公司的業務範圍和結構。
- **協調性**：從業務層面的角度訂定規範，較容易配合跨行業和跨國監理的協調。

AB 監管方針在應對 Big Tech 能夠提供高靈活性和針對性監管。然而，為了充分應對 Big Tech 所帶來的風險，通常需要與基於實體(Entity-Based, EB)的監管方針結合使用，形成混合的監管框架。如此一來既可以考量到特定業務活動的風險，又能整體掌握公司的營運方向。EB 監管有以下特點：

- **全面性**：涵蓋受監管公司的所有業務活動範圍，提供全面性的風險管理機制，有助於識別和管理跨業務線的風險。

[12] *"Digitalisation of finance"* May 2024;*"Principles for Operational Resilience"* March 2021;*"BIS Working Papers No WP1129 Big techs in finance"* October 2023.

- **組織結構考量**：考慮受監管公司的治理結構、資本充足率、風險管理框架和內部控制等因素，有助於確保公司的整體穩健性。
- **系統性風險管理**：從公司實體的角度建立控管規範，能夠更具體的識別和管理系統性風險。
- **一致性和穩定性**：監理機關若針對整體相同類型公司設立長期穩定的監管框架，有助於維護市場信心和穩定。

根據 Big Tech 在各區域業務活動的不同背景，目前各國監理機關優先考慮的規範面向不盡相同。對於中國，Big Tech 在電子支付和金融市場參與度較高，監管重點在於解決金融穩定問題[13]。美國更關注於市場競爭政策，而不是金融穩定，因為與其他國家市場相比，Big Tech 能左右金融服務市場的程度較低。在歐盟，監理機關已經制定了一個框架，重點關注營運韌性和資料保護。然而無論從何種面向，BIS 認為就國內層面，建議中央銀行、金融監理機關、市場競爭和資料保護機關應共同討論對於 Big Tech 和數位市場的監管。

從跨境的角度來看，由於 Big Tech 的總部只設在少數幾個國家和地區，母國監理機關（即 Big Tech 總部所在國的公部門）應對於 Big Tech 的業務活動有相對更深入的瞭解，並且在收集資料、影響商業行為、課稅等方面擁有更大的權力，然實際業務所在國因個別業務佔 Big Tech 在市場的總業務量較小，該國監理機關（即 Big Tech 運營的其他市場公部門）對其影響力可能很小，因此母國與各業務運營國的監理合作將日益重要。

4.2. 金融穩定委員會 (Financial Stability Board, FSB)

根據 FSB 對於 Big Tech 在新興市場和發展中經濟體（Emerging Market and Developing Economies, EMDEs）[14]中提供金融服務情況的研究[15]，Big Tech 在 EMDEs 地區通常比在先進國家更迅速擴展其規模，主要可歸因於 EMDEs 的金融系統發展及對於經濟弱勢族群的服務包容度相對較低，而 Big Tech 提供這些人群較容易能取得金融服務的機會，因而在許多地區獲得龐大的客群基數。

然而，在消費者保護制度相對薄弱的 EMDEs，缺乏如已開發國家較嚴格的數據資料使用規定，在普遍金融知識水準不足的情況下，用戶可能會為了獲得 Big Tech 提供的服務而忽略個人資訊安全的重要性。根據 FSB 調查顯示，76%的受訪者認為在新興市場，Big Tech 與金融服務用戶的相關業務行為持續擴張，與目前當局對於數據隱私監管要求的差距之下，在未

[13] 2019 年，中國人民銀行對 Big Tech 電子支付賬戶的用戶餘額規定 100%的準備金要求。隨後在 2021 年發布相關規範，限制 Big Tech 透過提供信貸或投資有息資產來轉移風險，並要求將用戶的資金存放在指定的銀行賬戶中。

[14] 包含阿根廷、巴西、智利、哥倫比亞、埃及、匈牙利、印度、印度尼西亞、哈薩克斯坦、黎巴嫩、馬來西亞、墨西哥、尼日利亞、秘魯、菲律賓、波蘭、俄羅斯、南非、土耳其和烏克蘭。(參考來源：IMF, International Financial Statistics database)

[15] "Big Tech Firms in Finance in Emerging Market and Developing Economie" October 2020.

來有可能會對其國內的金融穩定構成風險。

為因應 Big Tech 在金融服務領域的迅速擴展，FSB 強調國際合作和雙向溝通的重要性，包括加強銀行、證券和保險監理機關之間的國內合作，以及國際合作，國際間監理機關在跨境支付和匯款方面若可達成共識，將大大提高各國平台之間的互動性。此外，對於當金融業務活動由 Big Tech 等新型態金融服務機構執行時，監管單位應遵循「同樣風險-同樣監管」的原則，以確保對有金融穩定影響的活動進行適當和一致的控管。

對於用戶資訊管理，若擁有系統性金融服務業務的 Big Tech 服務中斷，可能對其服務區域的經濟以及周遭其他經濟體產生重大影響，FSB 建議各國監理機關應建立涵蓋跨境資訊交換相關規範的資訊治理框架，議題建議包含：

(1) 數據權利的明確性；

(2) 在鼓勵適當資訊共享的同時，保護資訊機密性、可用性和完整性的保障措施；

(3) 隱私考量；

(4) 風險管理；

(5) 資訊倫理。

適當的資訊治理框架有助於各機構對客戶資訊使用的明確性，確保個人機敏資訊保護，可幫助定義消費者權利並提高消費者信心。此外，部分國家引入監管框架協助發展開放銀行業務，或支持銀行與其他機構（包括 Big Tech）共享相關數據。如新加坡和香港，發布指導意見和 API 框架、標準和技術規範，鼓勵市場參與開放銀行業務並在許可範圍之內共享資訊。

此外，消費者保護制度亦是促進金融穩定的重要因素之一，FSB 建議各國監理機關訂定針對 Big Tech 金融業務行為監管框架時，應確保 Big Tech 遵守用戶資金隔離和保證不會被挪作他用要求，以避免其資金流動性發生問題或面臨倒閉時，讓用戶資金面臨風險。

4.3. 國際貨幣基金組織 (International Monetary Fund, IMF)

IMF 的報告[16]認為，Big Tech 與金融科技新創公司的關鍵區別在於用戶數量、營運所在區的數量以及收入和活動範圍。考慮到實體的規模，Big Tech 提供的金融科技往往對市場產生更大的影響。與現有金融機構相比，Big Tech 可以推動更大的變革，更快、更便宜地將新想法和技術推向市場，並具有更大的覆蓋範圍和可用性。

Big Tech 在金融服務領域的擴展，可能會在三個構面上對金融穩定性造成風險，包含：

(1) 所提供的金融服務過度被過多金融機構使用，導致所提供的金融服務產生集中性集中的金融服務多項業務使風險增加。(單一企業、產業同一服務集中)。

(2)與現有金融機構的營業行為互聯性(interconnectedness)過高。

(3)與現有金融機構的財務互聯性(interconnectedness)過高。

IMF 建議，為因應 Big Tech 涉足金融業務領域，監理機關應透過企業實體和業務活動基礎的治理方針進行控管，母國監理機關應建立基於企業實體的監管方針以利制度上涵蓋 Big Tech 的全球性業務活動，包含公司治理、審慎規範和行為要求；而業務所在國監理機關原則上可主要針對業務活動的監管來解決當地風險和不公平競爭。現有的監管框架中，相較於 Big Tech，銀行為滿足監管要求，須承擔較多的法規遵循義務並投入相應的資源以安排適當的治理和風險管理規劃。如今 Big Tech 在部份業務面向已跨入金融體系的風險範圍，各國監理機關應對現有框架進行修訂或引入新的標準和指引，以因應 Big Tech 對金融穩定帶來的潛在衝擊。

IMF 對監管 Big Tech 的建議，短期、中期和長期監管框架如下。

(1) 短期監管框架，加強揭露：雖然 Big Tech 目前可能尚未面臨與金融服務相關的信用風險和流動性風險，但隨著 Big Tech 業務的擴展，個人或法人將漸漸基於對 Big Tech 服務品質和聲譽的信任，而開始廣泛的使用這些由 Big Tech 提供的金融服務。然在沒有足夠的監管力道下，如果具有系統重要性的 Big Tech 倒閉或突然撤出業務所在國時，對直接使用其平台服務的自然人或委託外部服務項目的法人將面臨巨大的風險。

目前，由於缺乏透明度，這種服務中斷的成本尚無法準確估量。在可能導致消費者權益受損或合作的金融機構無法繼續提供服務的情況下，應有相關機制要求 Big Tech 提供協助以維持該項金融服務的持續性。為了緩釋這類風險，應要求 Big Tech

[16] "Big Tech in Financial Services Regulatory Approaches and Architecture" January 2022.

加強接露其所提供之金融服務風險(包括無法量化的風險，如協助金融機構提供相關服務對於金融機構的營運風險和聲譽風險)，包括商業活動的資訊和風險，如貸款、消費者風險和公司義務等。

(2) 中期監管框架，制定產業行為準則(或稱產業自律規範)：

產業行為準則可以幫助監理機關控管 Big Tech 的各種市場行為，有助於在尚未完善監管資源的同時即時提供一些市場保護，限制未受監管的業務所產生的風險，例如要求管理應承擔的風險、保障消費者資金或資料等等。產業行為準則通常可以比實施大規模政策更快能夠執行，監理機關可以針對自身作為母國或業務所在國不同監管角色的需求，訂定符合國情的產業行為準則。

建立行為準則可以及時解決 Big Tech 原先未受監管的業務活動對於金融系統產生的風險，然而，產業行為準則並不能取代完整的監管框架。監理機關須注意行為準則可能會產生光環效應（Halo Effect），即服務使用方得知 Big Tech 已受到相關準則監管時，可能直覺認為金融市場已建立完整的監理框架與控管機制。若此時發生 Big Tech 相關重大事件導致市場或使用者權益受損，將為監理機關帶來聲譽風險。

(3) 長期監管框架，混合式監管：

Big Tech 在金融領域的業務性質使其受到多個監理機關的管轄，包括中央銀行、市場競爭監理機關和資料保護監理機關，形成同時由國內和國際各機關監管的複雜組合。鑑於 Big Tech 的跨產業別的性質，IMF 建議各國在長期規劃上應朝金融監理機關和其他國內監理機關之間的密切合作前進。

此外，國際監管合作和資訊分享也是緩釋 Big Tech 跨境營運所帶來風險的方式之一，同時可減少 Big Tech 跨足不同市場時所產生的監管摩擦，IMF 建議各國在規劃長期監管框架上，可明確的劃分出 Big Tech 企業實體母國及商業活動所在國，個別根據 AB 及 EB 的監管方針適當的混合調整，Big Tech 的母國監理機關須加強與世界組織、其他國內監理機關和全球業務所在國監理機關的監管交流與合作。

	國際清算銀行 (BIS)	金融穩定委員會 (FSB)	國際貨幣基金組織 (IMF)
對 AB/EB 監管框架看法	● 建議為了充分應對 Big Tech 所帶來的風險，通常需採 AB 與 EB 結合的混合監管框架	● 並未提及相關看法	● 建議在規劃長期監管框架上，可明確的劃分出 Big Tech 企業實體母國及商業活動所在國，個別根據 AB 及 EB 的監管方針採

			適當的混合調整
主要關注重點	● 各國監理機關可先以基於 AB 的監管方向開始設立相關監管措施，最終採 AB 與 EB 結合的混合監管框架	● 金融監理機關國內合作與國際雙向溝通的重要性	● Big Tech 的母國監理機關須加強與世界組織、其他國內監理機關和全球業務所在國監理機關的監管交流與合作 ● 建議採短期、中期和長期監管框架 短期：加強 Big Tech 接露所提供之金融服務風險 中期：制定產業行為準則 長期：採 AB 與 EB 混合式監管
執行方式	● 國內層面：建議中央銀行、金融監理機關、市場競爭和資料保護機關應共同討論對於 Big Tech 和數位市場的監管 ● 跨境層面：母國監理機關應對於 Big Tech 的業務活動有相對更深入的瞭解及監管	● 對於當金融業務活動由 Big Tech 等新型態金融服務機構執行時，監管單位應遵循「同樣風險-同樣監管」的原則，以確保對有金融穩定影響的活動進行適當和一致的控管	● 監理機關應透過企業實體和業務活動基礎的治理方針進行控管 ● 母國監理機關應建立基於企業實體的監管方針以利制度上涵蓋 Big Tech 的全球性業務活動

5. 主要先進國家之關注重點、監管原則及法制作業

各國監理機關正逐步調整既有法規和指引來監督 Big Tech 提供金融服務的營運風險，包含受銀行委託之金融相關服務的治理和控制、資訊安全、營運風險和營運韌性等。部分監理機關制定更具體的指引，如涵蓋銀行即服務(Banking as a service)模式或通過社交媒體平台提供銀行服務的相關控管要求。在某些國家，銀行在與第三方建立某些合作關係或重大安排之前，可能需要事先獲得監理機關的核准。

監管議題除包含科技、網路安全、委外和營運韌性等要求外，越來越多的監理機關還發佈了針對雲端的相關要求，包括傳輸到雲端的資訊應受合約條款的約束，以及考慮不同的雲端特定問題以確保資料安全等，關於雲端中可以儲存的內容和資料位置、資料隔離、資料使用限制、資訊安全和退場機制，以及對雲端服務供應商(Cloud Service Provider，簡稱 CSP)在內的關鍵第三方廠商實施直接監督機制。然而，大多數監理機關尚不具備這種監督權，因此監管通常僅限於銀行如何管理其服務提供者。僅少數監理機關有能力要求包括 CSP 在內的銀行第三方服務供應商提交報告並進行現場檢查，或有權直接監督關鍵第三方向金融機構所提供的服務。

在各國許多監理機關依靠指引來指導銀行使用新科技，相關指引涵蓋科技風險管理、營運風險管理和營運韌性、模型風險管理、資訊安全和 IT 風險管理、委外/第三方風險管理和公司治理要求，或引入針對特定領域的指引，本章將針對各國的監理指引進行說明。

5.1. 歐盟

本章節參考歐盟條例《2022/2554》(Regulations (EU) 2022/2554) (DORA)，《歐盟條例 2024/1502》(Regulations (EU) 2024/1502)，《歐盟條例 2024/1505》(Regulations (EU) 2024/1505)。

歐盟於 2023 年 1 月頒布了《歐盟條例 2022/2554》(Regulations (EU) 2022/2554)，即《數位營運彈性法案》(The Digital Operational Resilience Act)[17]，以下簡稱 DORA。該法案是基於業務活動的監管措施。DORA 希望於 2025 年 1 月前完善相關二階法案(詳下表 3)，這些立法旨在制定金融機構與資訊通信技術（ICT）服務具體相關的營運風險。根據 DORA，當 Big Tech 提供金融機構第三方服務，Big Tech 需要遵循相關的技術標準，並且進行第三方風險的評估和監控；「關鍵」第三方服務的供應商，更會受到直接監督與額外的監管要求。

雖然無任何官方文件佐證，但是現今歐盟境內的金融機構與第三方服務提供商達成共識，將 DORA 內法條所描述的主要業務分成五大支柱: ICT 風險管理、ICT 相關事故管理、數位營運韌性測試、ICT 第三方風險管理、以及監理機關監督指南。每一支柱都有相對應條例，這些條例或已經生效或尚在立法的過程中，預計在 2025 年 1 月前將全數通過。

目前，已有二個條例通過。一為《歐盟條例 2024/1502》(Regulations (EU) 2024/1502)[18]，此條例規範服務金融機構之關鍵 ICT 之「篩選條件」，亦即關鍵 ICT 第三方服務提供商範圍界定與指定規則，詳細條文請參見 5.1.1.1。二為歐盟通過《歐盟條例 2024/1505》(Regulations (EU) 2024/1505)[19]，此條例指出，當第三方服務提供商之業務對金融機構影響過於顯著，而透過前條例之「篩選條件」歸類為關鍵第三方 ICT 服務提供商時，需繳交「監管費用」給監理機關，詳細條文請參見 5.1.1.6。其餘相關條例之內容與其對應之支柱請參見下表:

表 3 DORA 支柱、相關主題、與其目前立法狀況

支柱	相關主題	目前立法狀況
ICT 風險管理	ICT 風險管理架構與簡易架構	最終報告出爐
ICT 相關事故管理	事故與網路安全分類	最終報告出爐
	事故通報時程與範例	最終報告出爐
	大型事故總花費與損失指南	最終報告出爐
數位營運韌性測試	威脅導向滲透測試	最終報告出爐
ICT 第三方風險管理	指定支持關鍵或重要功能的 ICT 服務政策	最終報告出爐
	註冊資訊	最終報告出爐
	關鍵或重要功能的在委外	最終報告出爐

[17] Regulation (EU) 2022/2554 of the European Parliament and of the Council | European Union
[18] COMMISSION DELEGATED REGULATION (EU) 2024/1502 | European Union
[19] COMMISSION DELEGATED REGULATION (EU) 2024/1505 | European Union

監理機關監督指南	關鍵 ICT 第三方服務提供商範圍界定與指定規則	Regulations (EU) 2024/1502
	關鍵 ICT 第三方服務提供商監管費用	Regulations (EU) 2024/1505
	歐洲監理機關（ESAs）及監理機關監督合作指南	最終報告出爐

5.1.1 對第三方廠商(Big Tech)要求

5.1.1.1. 篩選標準

依據現有歐盟條例，在提供銀行服務之條件內，最接近 Big Tech 之名詞為關鍵 ICT 第三方服務提供商 (Critical ICT third-party service providers)。根據 DORA 第 31 條指出，歐洲監理機關（ESAs）應制定對金融機構至關重要的 ICT 第三方服務提供商 (ICT third-party service providers) 相關篩選標準，包括但不限於：

(1) 相關 ICT 第三方服務提供商提供服務之金融機構的數量及總資產價值、對金融服務的穩定性、持續營運能力或品質等系統性影響。《歐盟條例 2024/1502》(Regulations (EU) 2024/1502) 第二章提出以下兩個衡量 ICT 第三方服務提供商對金融機構的**關係程度**。根據 EU 境內金融機構種類劃分:

   i. ICT 第三方服務提供商提供關鍵服務的同種類金融機構數量，與對所有同種類金融機構數量之比例

   ii. ICT 第三方服務提供商提供關鍵服務的同種類金融機構資產總值，與對所有同種類金融機構資產總值之比例。

(2) 相關 ICT 第三方服務提供商對金融機構的系統性特徵或重要性。《歐盟條例 2024/1502》(Regulations (EU) 2024/1502) 第三章提出以下二個衡量 ICT 第三方服務提供商對金融機構的**重要程度**:

   i. 提供關鍵或重要功能的 ICT 服務中，同一 ICT 第三方服務提供商為全球系統性重要機構 (G-SIIs) 及其他系統性重要機構 (O-SIIs) 所提供服務的數量。

   ii. 由同一 ICT 第三方服務提供商提供 ICT 服務，且該服務支持關鍵或重要功能的金融機構數量。

(3) ICT 第三方服務提供商的可替代性。《歐盟條例 2024/1502》 (Regulations (EU) 2024/1502) 第五章提出以下二個衡量 ICT 第三方服務提供商對金融機構的替代程度:

i. 無法找到其他提供相同服務能力的替代 ICT 第三方服務提供商以達成關鍵或重要功能的金融機構數量，占市場金融機構總數的比例。

ii. 實務上要將關鍵或重要功能的委外項目轉換到另一家 ICT 第三方服務提供商難度極高的金融機構數量，占市場金融機構總數的比例。

5.1.1.2.事故下通報金融機構及監理機關

根據 DORA 第 6 條指出，ICT 第三方服務提供商需建立向金融機構的報告管道，確保金融機構能夠及時通報給監理機關，並且瞭解與 ICT 第三方服務提供商相關的安排、重大變更及其對關鍵功能的潛在影響，包括但不限於：

(1) 與 ICT 第三方服務提供商協議之的服務計畫

(2) 重大變更與其對關鍵功能的潛在影響、風險分析

(3) 重大 ICT 事件的影響評估及相應的應對、恢復和改善措施。

5.1.1.3.服務終止應對流程

根據 DORA 第 18 條指出，當第三方服務提供商有以下等情形，金融機構可提出終止服務：

(1) ICT 第三方服務提供商嚴重違反法律、法規或合約；

(2) 風險監控中發現可能影響合約功能或服務表現的情況；

(3) 第三方服務提供商在 ICT 風險管理，特別是資料保護方面出現明顯缺失；

(4) 監理機關無法達到有效監管。

雙方在終止服務時需考慮可能出現的風險，包括但不限於: 如第三方服務提供商停止營運、服務品質下降、業務中斷或重大風險。

5.1.1.4.是否硬性要求第三方服務商須在歐盟境內設立分支機構

DORA 第 31 條指出當第三方服務提供商設立於第三國時，若符合 6.1.1.1 篩選標準的關鍵 ICT 第三方服務提供商，需在該歐洲國家/該聯盟（歐盟）境內設立分支機構。

如果 ICT 第三方服務提供商進一步將支持關鍵或重要功能的 ICT 服務分包給其他 ICT 第三方服務提供商，金融機構應權衡此類分包可能帶來的效益和風險，特別是在 ICT 分包商設

立於第三國的情況下，當與設立於第三國的 ICT 第三方服務提供商簽訂使用支持關鍵或重要功能的 ICT 服務的合約時，金融機構除了考慮 6.1.1.1 所提及的事項外，還應考慮遵守歐盟數據保護規則和該第三國法律的要求。

5.1.1.5.演練測試

根據 DORA 第 26、27 條指出相關 ICT 第三方服務提供商為金融機構執行威脅導向滲透測試(Threat-led Penetration Test, TLPT)的相關規定。每次執行的 TLPT 應包含:

(1) 金融機構多個或所有關鍵或重要功能，並支援在正式環境上進行測試，識別所有相關的基礎 ICT 系統、流程和技術。

(2) 測試人員應由認證機構認證具備專業技能與擁有在網路威脅情資、滲透測試和紅隊測試方面的專業知識，可提供與 TLPT 相關風險管理的獨立驗證、稽核報告、和專業賠償保險。

(3) 若測試由金融機構人員進行，需獲得相關監理機關的核准，確保適當人力資源並避免利益衝突，且威脅情資需由 ICT 第三方服務提供商提供。

5.1.1.6.監管費用

根據 DORA 第 43 條指出，為涵蓋監管之成本，監理機關得向關鍵 ICT 第三方服務提供商收取費用，費用應涵蓋本節所列職責執行所產生的所有成本，並且應與其營業額成比例。

根據以上之原則，歐盟通過《歐盟條例 2024/1505》(Regulations (EU) 2024/1505)，於第 3 條對監管費用做出以下定義與限制:

(1) 對於每個關鍵 ICT 第三方服務提供商，某一年 (n) 的年度監管費用應為當年整體年度成本，並根據營業額系數進行調整，基於其適用於年 (n-2) 的營業額。營業額系數應基於適用營業額計算，如下：

$$\text{某關鍵 ICT 在 n 年營業額係數} = \frac{\text{某關鍵 ICT 第三方服務提供商在 } (n-2) \text{ 年 的適用營業額}}{\text{所有關鍵 ICT 第三方服務提供商在年 } (n-2) \text{ 的適用營業額}}$$

(2) 在任何情況下，關鍵 ICT 第三方服務提供商支付的年度監管費用不得少於 50,000 歐元。

5.1.1.7.外部稽核機制

根據 DORA 第 31 條指出，監理機關 (ESAs) 需要為每個關鍵 ICT 第三方服務提供商設立主要監督者(Lead Overseer)，並且管理和計算使用該關鍵 ICT 第三方服務提供商服務之總

資產占所有使用該服務的金融機構總資產價值的最大比例，以及這些金融機構的個別資產負債表的總和證明。

主要監督者也應每年制定其負責之關鍵 ICT 第三方服務提供商的年度監督目標和主要監督行動。該監督計畫應每年通報給關鍵 ICT 第三方服務提供商。根據 DORA 第 38 條及 39 條指出，主要監督者對關鍵 ICT 第三方服務提供商查核的之檢查權力與方針，內容包括一般查核與檢查。

一般查核為對 ICT 第三方服務提供商進行非實地考察之檢查。一般查核中，主要監督者及其他查核人員具備以下權力：

(1) 查核與該服務相關的記錄、數據資料、流程規範及其他相關文件；

(2) 取得可證明上述資料真實性和正確性的證明文件；

(3) 召集關鍵 ICT 第三方服務提供商的代表，參照相關實際執行做法或書面文件進行訪談與說明，並記錄回答；

(4) 訪談相關個人或法人，以收集相關資訊；

(5) 取得通話和其他相關通訊記錄。

查核人員應出示書面授權書，說明查核的主題和目的。關鍵 ICT 第三方服務提供商的代表應根據監督機構的決定提交查核說明，該決定應包含查核主題、目的、法律救濟及查核權利。

當查核程序需要進行現場考察，查核升級成檢查。檢查過程中，主要監督者及其他檢查人員應具備以下權力：

(1) 進入任何商業場所、土地或財產；

(2) 必要時，查封商業場所、書籍或紀錄。

這些人員在行使權力時應出示書面授權書，說明檢查的主題和目的，並提及若關鍵 ICT 第三方服務提供商不配合檢查可能面臨的罰款。檢查範圍應涵蓋所有相關 ICT 系統、網路、設備、資訊和數據。關鍵 ICT 第三方服務提供商需根據監理機關的檢查結果執行後續改善，該結果應說明檢查的主題、目的、開始日期，並指示可能的罰款及可用的法律救濟。如果查核過程中遭到阻擾或不配合，監理機關應告知服務提供者相關懲罰，包括要求終止合約。

5.1.2. 對金融機構要求

5.1.2.1.第三方治理

根據 DORA 第 5 條指出，金融機構應建立內部治理和控制措施，管理層應定義、核准、監督並負責 ICT 風險管理框架的實施，包含：

(1) 制定資訊安全管理政策。

(2) 定期確認並核准金融機構對於 ICT 業者的查核規劃，並於查核後確認執行結果及 ICT 可能影響金融機構的重大調整。

(3) 除微型企業外，應指定高階管理階層或委員會負責督導管理 ICT，並授權相關人員角色、職責及權限，以協助監督及推動 ICT 管理。

(4) 應有使用 ICT 服務營運持續政策及復原計畫。

(5) 定期確認並分配適當預算，作為金融機構內部 ICT 服務相關維運使用。

(6) 定期審核企業所使用的 ICT 服務。

(7) 建立 ICT 業者重大變更的溝通機制。

(8) 應確保管理層具備足夠的知識和技能，包括定期參加專業教育訓練課程。

除微型企業外，金融機構應建立相關組織或指定一名高級管理人員來監督與 ICT 第三方服務提供商服務項目執行情況。此外，金融機構的管理層成員應具備理解和評估 ICT 風險及判斷對金融機構運營影響的知識和技能，包括通過定期參加專業教育訓練。

5.1.2.2.風險管理

根據 DORA 第 6 條指出，ICT 風險管理框架至少應包含必要的策略、政策、程序、ICT 合約事項和風險管理工具，以適當和充分地保護所有資訊資產和 ICT 資產，包括電腦軟體、硬體、服務器，以及保護所有相關的物理組件和基礎設施，如場地、數據中心和敏感指定區域，確保所有資訊資產和 ICT 資產免受包括損害和未經授權的訪問或使用等風險的侵害。

ICT 風險管理框架應至少每年定期記錄和審查一次，以及在發生重大 ICT 相關事件後，根據監管指示或來自相關運營持續演練測試或查核過程的結論進行修正。除微型企業外，金融機構的 ICT 風險管理框架應定期由查核人員根據金融機構的年度計畫進行內部查核。根據內部查核的結論，金融機構應建立正式的追蹤計畫，包括及時驗證和補救關鍵 ICT 查核發現的規則。

5.1.2.3.變更管理

根據 DORA 第 9 條指出，當 ICT 管理變更發生時，金融機構應實施有據可查的政策、程序和控制措施，以管理 ICT 變更，包括軟體、硬體、組件、系統或安全參數的變更。這些措施應基於風險評估方法，並成為整體變更管理流程的一部分，以確保所有對 ICT 系統的變更都在受控管的情況下記錄、測試、評估、核准、實施和驗證。ICT 變更管理流程應由適當的管理層核准，並制定具體的協議。

5.1.2.4.事故管理

根據 DORA 第 17 條指出，金融機構應建立 ICT 相關事故管理流程，內容包含但不限於：

(1) 預警指標；

(2) 根據事件的優先級和嚴重性以及受影響服務的重要性，建立識別、追蹤、記錄、分類和分級相關風險事件的書面程序。

(3) 分配不同 ICT 相關風險事件類型和情境所需要之角色與其職責；

(4) 制定向員工、外部利益相關者和媒體進行的溝通計畫，並制定內部管理流程，包括 ICT 服務相關的客戶投訴，以及在適當情況下向作為對手方的金融機構提供資訊；

(5) 確保相關高階管理階層知悉重大 ICT 相關風險事件報告與等級；

(6) 建立 ICT 相關風險事件應對程序，確保關鍵服務能夠安全地及時恢復運行。

5.1.2.5.事故通報監理機關

根據 DORA 第 19 條指出，ICT 事故發生時，金融機構應在規定時間內向相關監理機關提交以下文件：

(1) 初步通知；

(2) 期中報告：在初步通知後，當原事件狀況發生重大變化或基於新的資訊改變應變處理方式時，需提交期中報告，每次有相關更新或應監理機關要求時需提供更新相關資訊；

(3) 最終報告：根本原因分析完成後，無論是否已實施緩解措施，當實際影響程度可取代原先估計結果時，需提交最終報告。

金融機構可以根據相關法律，將報告義務委外給第三方服務提供商，但仍需對履行事件報告的要求負全責。在收到初步通知和每份報告後，監理機關應根據適用情況，及時將重大 ICT 相關事件的詳細資訊提供給：

(1) 歐洲銀行管理局（EBA）、歐洲證券和市場管理局（ESMA）或歐洲保險和職業養老金管理局（EIOPA）；

(2) 歐洲央行（ECB），適用於特定金融機構；

(3) 相關之電腦資安事件應變小組（Computer Security Incident Response Teams, CSIRTs）；

(4) 清算機構和單一清算委員會（Single Resolution Board, SRB）；

(5) 相關團體；

(6) 其他依據國家法律的相關公共機構。

5.1.3. 主要合約指南

根據 DORA 第 30 條指出，配合以上所述之監管原則，金融機構與第三方 ICT 服務提供商主要合約應最低應涵蓋的條款與注意事項如下：

(1) 金融機構與 ICT 第三方服務提供商的權利與義務應、服務協議應於合約中載明，並以書面文件記錄。該文件應以可供各方以紙本或其他可下載、耐久且可查閱的形式提供。

(2) 使用 ICT 服務的合約，應至少包括：

(a) ICT 第三方服務提供商針對該項委外服務提供的所有功能和 ICT 負責之服務須明確且完整的描述，並敘明是否允許委託外部協助關鍵或重要功能的 ICT 服務或其重要部分，以及此類服務項目能否委託外部的適用條件；

(b) 提供實際服務執行以及資料處理的地點（區域或國家），包括資料倉儲位置，並要求 ICT 第三方服務提供商在預計變更這些地點時提前通知金融機構；

(c) 關於資料保護的可用性、真實性、完整性和機密性的條款，包括個人機敏資訊安全控管要求；

(d) 確保在 ICT 第三方服務提供商破產、清算或停止業務運營，或其他合約被迫終止的情況下，個人和非個人資料能夠以易於解讀的格式傳遞、恢復和返還金融機構處理的條款；

(e) 詳述服務項目和範圍，包括服務提供項目相關更新和修訂條款；

(f) 在發生涉及提供給金融機構的 ICT 服務相關之風險事件時，ICT 第三方服務提

供商在無需額外成本或預先確定成本的情況下向金融機構提供援助的義務；

(g) ICT 第三方服務提供商應完全配合金融機構內部規範及監理機關之要求，包括其派駐人員的權利義務；

(h) 符合金融機構及監理機關規範的合約終止規則和相關事件最低通知期限；

(i) ICT 第三方服務提供商參與金融機構的 ICT 資訊安全意識計畫和相關運營持續演練的條件。

(3) 金融機構對於關鍵或重要功能的 ICT 服務委託外部處理的合約要求，除上述條款外還應包括：

(a) 對於服務項目和範圍的詳細描述，包括服務提供項目相關更新和修訂條款，具有明確的定量和定性目標，允許金融機構有效監控 ICT 服務，並在未達到約定服務水準時能夠迅速採取適當的改善措施；

(b) ICT 第三方服務提供商向金融機構通報的通知期和報告義務，包括通報任何可能對 ICT 第三方服務提供商有效提供支持關鍵或重要功能的 ICT 服務的能力產生重大影響的發展；

(c) 要求 ICT 第三方服務提供商實施和測試業務應變計劃，並具備符合其監管框架的 ICT 安全措施、工具和政策，以提供適當的安全水準；

(d) ICT 第三方服務提供商參與並完全配合金融機構的威脅導向滲透測試 (Threat-led Penetration Test, TLPT) 的義務；

(e) 持續監控 ICT 第三方服務提供商的權利，包括以下內容：

i. 金融機構以及監理機關或其指派的第三方應有不受限制的訪問、調查、稽核以及直接取得相關文件的權利，如果這些文件對 ICT 第三方服務提供者的運營至關重要，則另作討論；

ii. 如果其他客戶的權利受到影響，有權商定替代的方案；

iii. ICT 第三方服務提供商在監理機關、金融機構或其指派的第三方進行查核期間應完全配合；並配合提供有關查核範圍所需之服務流程、內部章程或其他詳細資訊的義務；

(f) 須建立合約中止或結束前的強制過渡期條款：

i. 在過渡期間，ICT 第三方服務提供商將繼續提供相關的功能或 ICT 服務，以避免金融機構的服務中斷並確保所有資訊的有效交接；

ii. 金融機構可以根據服務的複雜性，選擇轉移到另一個 ICT 第三方服務提供商或內部自行解決。根據(e)點規定，ICT 第三方服務提供商和微型企業的金融機構可以同意將訪問、檢查和稽核的權利委託給由 ICT 第三方服務提供商指定的獨立第三方。金融機構可以隨時向該第三方索取有關 ICT 第三方服務提供商相關資料。

5.2. 英國

本段落主要參考英國徵詢文件(Consultation Paper)「CP26/23 - 營運韌性：英國金融產業的關鍵第三方[20]」，針對主題進行篩選及歸納，提出英國對於關鍵第三方相關監管態度及要求。惟 CP26/23 為徵詢文件仍屬於草案諮詢階段，故和最終版本可能有所落差。

英國的監理機關包含 Bank of England (BoE)、Prudential Regulation Authority (PRA), 和 Financial Conduct Authority (FCA) ，三者以下簡稱「監理機關」，2023 年，英國監理機關對金融服務業營運持續，尤其是與關鍵第三方 (Critical Third Party, CTP) 相關的韌性監管力道越來越大且層面也將更加廣泛。2023 年 12 月，英國發佈了一份徵詢文件「CP26/23 - 營運韌性：英國金融產業的關鍵第三方」，主要目的是管理由 CTP 提供金融機構服務失效或中斷時，可能對英國金融體系穩定性或信心產生的潛在風險，詳述了監理要求和期望，該法案於 2023 年 12 月 7 日發布，並於 2024 年 3 月 15 日結束徵詢。此份徵詢文件的前身是 2022 年 7 月發佈的同名討論文件(DP3/22[21])，該討論文件的目的是分享並獲取針對第三方監管潛在措施的意見和想法，以充分管理第三方帶來的潛在系統性風險。

CP26/23 內容涵蓋 PRA、英國金融行為監督局(Financial Conduct Authority, FCA) 和英格蘭銀行的相關規範，研擬了與關鍵第三方相關規則變更。其中包括關於關鍵第三方的高層次基本規則和業務要求、資訊和通知要求。監理機關在命名潛在的關鍵第三方候選人的過程中將發揮積極作用，扮演識別和推薦關鍵第三方給英國財政部 (His Majesty's Treasury, HMT) 的重要角色。英國監理機關將採用技術中立原則，換句話說只要廠商符合該法案對於關鍵第三方的標準皆受其列管，而不僅適用於科技技術服務的提供商。此次徵詢為關鍵第三方的監理規則帶來更清晰的輪廓，例如任命關鍵第三方的流程和標準，以及關鍵第三方在多個領域（包括風險管理、治理、資源盤點(mapping)和演練）需要遵守的規則。這使金融服務業者的第三方供應方更明確判斷自己是否可能被任命為關鍵第三方，並為其預先做準備。

CP26/23 建議關鍵第三方在提供服務過程中必須遵守六項基本規則。包含：

1. 誠信經營；

2. 以專業、謹慎和盡職盡責的方式執行業務；

3. 審慎行事；

[20] CP26/23 - Operational resilience: Critical third parties to the UK financial sector | Bank of England，該徵詢文件源於《2023 年金融服務與市場法案》(The Financial Services and Markets Act 2023)，給予相關監理機關權利訂定此關於規範關鍵第三方之徵詢文件。

[21] DP3/22 – Operational resilience: Critical third parties to the UK financial sector | Bank of England

4. 有效的風險策略和管理制度；

5. 負責任和有效地規劃和控制活動；

6. 以開放和配合的方式與監理機關互動，應要求揭露相關資訊。

5.2.1. 對第三方廠商(Big Tech)要求

5.2.1.1. 篩選標準

CP26/23 明確指出，關鍵第三方在第三方服務供應商中所佔的比例將非常低，理論上將僅限於具有系統重要性的第三方供應商。監理機關將在實務上扮演積極角色，在評估以下三個標準後，向英國財政部推薦可能被任命為關鍵第三方的潛在候選人。

(1.)服務重大性

即第三方服務供應商提供給金融業者及金融市場的服務之重大性，判斷標準包含：

i. 如果該服務中斷，可能會威脅到英國金融服務的穩定性。

ii. 如果在單一第三方服務供應商提供的多種不同服務中，單一或多項服務中斷的情況下，整體而言可能威脅到金融穩定。

iii. 監理機關判斷第三方服務供應商提供之該項服務係支援金融服務業者提供重要業務。

(2.)服務集中度

即第三方服務供應商向金融機構提供服務之集中度，判斷標準包含：

i. 根據第三方服務供應商對金融服務業者提供的服務數量和類型多寡。

ii. 監理機關應考慮第三方服務供應商的使用狀況，包含從整個金融體系的角度，以及特定個別金融服務市場的角度。

iii. 針對金融服務業者，個別或整體依賴特定第三方服務供應商，所形成的系統性本質進行分析。

(3.)其他因素

包含潛在系統性衝擊的其他驅動因素：

i. 第三方服務供應商的可替代性，例如是否缺乏替代方案或移轉服務的難度較高。

ii. 第三方服務供應商是否能夠直接存取金融服務業者用於支援重要商業服務的資源，例如技術和資料等。

監理機關將以全面性的角度考慮上述各種標準，以決定是否建議英國財政部任命該第三方服務供應商為關鍵第三方。而在上述標準的結構下，即可避免第三方服務供應商為了不被視為關鍵第三方而單純避開量化門檻的可能。

5.2.1.2.第三方治理

CP26/23 內提及要求關鍵第三方確保其服務提供之韌性，並明確規範相關面相要求關鍵第三方遵守，除針對內部控制進行規範外，也針對管理人員提出相關監管建議。

(1.)監理機關建議要求每個關鍵第三方透過以下方式確保其治理促進其服務的韌性：

i. 任命一名具有適當資格的員工（或其管理機構成員），該員工具有適當的權力、知識、技能和經驗，作為與具有監督職能的監理機關聯繫的中間人；

ii. 為參與提供服務的各級員工建立明確的角色和職責，並提供清晰且易於理解的管道來溝通和呈報問題和風險；

iii. 建立、監督和實施涵蓋關鍵第三方服務的方法：

iv. 預防、回應、適應任何導致服務中斷的事件並從中恢復；

v. 從事件和進行的任何演練測試中學習；

vi. 確保對向監理機關提供的任何資訊進行適當的審查和核准。

(2.)監理機關也建議要求關鍵第三方以書面通知其指定人員的姓名、辦公地址以及其他最新聯絡方式，包括電子郵件地址、電話號碼和非工作時間聯絡資訊。

(3.)在監管聲明草案中，英國監理機關也提出對於關鍵第三方的資料管理，也應有適當審查機制和核可標準的想法。

5.2.1.3.風險管理

CP26/23 提出建議要求關鍵第三方有效確保服務持續提供，並建議關鍵第三方主動建立明確風險管理框架。

(1.)監理機關建議要求每個關鍵第三方透過以下方式有效管理其繼續提供服務的能力的風險：

i. 識別並監控相關的外部和內部風險；

ii. 確保其具備有效管理上述風險的管理機制；

iii. 定期更新風險管理機制，以反映其對於下列問題的持續改善：

- 服務中斷；
- 與監理機關的接觸；
- 新出現的風險；
- 任何相關演練測試。

(2.) 關鍵第三方提供服務商可能存在許多營運風險。然而，監理機關建議關鍵第三方也應考慮可能影響其提供服務能力的財務風險，例如破產風險。

(3.) 為符合上述規範，監理聲明草案建議關鍵第三方應擁有健全的風險管理框架，以管理提供服務的風險。監理機關預計風險框架將包含：

i. 識別、衡量、監控和報告相關風險（包括風險偏好）的策略、政策和程序；

ii. 在關鍵第三方風險偏好範圍內控制和管理風險的政策和程序；

iii. 定期檢視並確保上述策略、政策和程序得到有效設計和運作的機制。

(4.) 關鍵第三方也需要持續監控相關風險，包括透過系統性地監控和分析外部環境變化，識別潛在風險的前瞻掃描和對威脅情資的分析處理。

5.2.1.4. 依賴關係和供應鏈風險管理

CP26/23 代表監理機關提出要求關鍵第三方須有效識別並管理其服務供應鏈中可能影響服務提供之各項風險，並確保其服務提供之韌性。

(1.) 監理機關建議要求每個關鍵第三方識別和管理其供應鏈中可能影響其提供服務能力的任何風險。關鍵第三方須採取合理步驟，確保其供應鏈中的每個人：

i. 瞭解因「關鍵第三方職責」而適用於關鍵第三方的要求（這是監理機關規則草案中的總括術語，涵蓋 FSMA 賦予關鍵第三方的所有職責和義務，包括擬議的規則和其他監理機關的任何同等規則）；

ii. 採取行動促進關鍵第三方滿足這些要求；

iii. 使監理機關能夠取得與其行使監督職能相關的任何資訊。

(2.) 儘管 CP 26/23 已針對風險管理提出關鍵第三方應遵循之相關建議及規範，詳 6.2.1.3 風險管理，然考量依賴關係和供應鏈具有值得單獨考量之風險特徵，監理機關建議關鍵第三方額外關注存在於服務提供內的依賴關係和供應鏈風險，已確保其風險控管之完善性。

(3.) 為了遵守上述規範，監理機關建議關鍵第三方應：

i. 在委外承包對於其服務具重大影響之部分前，對於承包商進行適當盡職調查，並於後續持續或定期 (至少每年) 監控這些服務承包商；

ii. 對監理機關及其服務的客戶保持透明，同步瞭解其提供之服務對於客戶供應鏈中哪些部分至關重要；

iii. 持續瞭解與其服務有關之客戶供應鏈中風險事件相關資訊；

iv. 在演練測試中納入涉及客戶供應鏈中斷的場景；

v. 將供應鏈中斷和演練測試中所學到的經驗教訓納入風險管理和事件管理流程。

5.2.1.5.科技和資訊安全韌性風險管理

CP26/23 除前述針對服務供應鏈做出規範外，詳 6.2.1.4 依賴關係和供應鏈風險管理，也針對資訊安全提出相關管理建議，考量資訊科技應用之快速變化及複雜性，定期檢視和測試為其核心概念，同時須確保其營運韌性以滿足規範要求。

(1.) 監理機關提議要求關鍵第三方必須確保任何提供、維護或支援服務的技術的韌性，包括：

i. 技術和資訊安全管理以及營運韌性措施；

ii. 定期演練測試這些措施；

iii. 確認演練測試結果發生異常的流程和改善方法；

iv. 及時傳達相關資訊以協助調整風險管理和決策過程的程序。

(2.) 作為遵守風險管理流程的一部分，關鍵第三方需要滿足監理機關對技術和資安韌性的建議要求。

(3.) 監理機關認為，與依賴性和供應鏈風險管理以及變更管理一樣，技術和資安韌性由於其技術複雜性，值得在擬議要求中明確考慮。此外，在過去幾年中，英國央行每半年進行一次的系統性風險調查，一直將網路攻擊風險視為對英國金融體系影響最大的首要風險或首要風險之一。

(4.) 為了達到上述規範，監理機關在監管聲明草案中提出了一系列監理期望，包含關鍵第三方技術和資安韌性措施應遵循的內容。相關內容包含：

i. 明確闡明關鍵第三方如何確定其技術和資安韌性目標，以及如何識別、評估、抵減、衡量和管理技術和資訊安全的框架。除了技術之外，這個框架還應該涵蓋關鍵第三方的資產（包括資料）、人員和流程；

ii. 保護、偵測、回應和恢復關鍵資產免受服務中斷和網路攻擊的措施；

iii. 確保服務在設計上具有韌性的文化和流程；

iv. 資料控制：最大限度地減少相關事件對服務及其支援資源的可能性和影響；

v. 安全控制：最大限度地降低網路攻擊對服務及其支援資源的影響機會和程度；

vi. 監控異常活動的能力（即時或接近實際發生時間）；並發現事件；

vii. 辨識、評估和及時修復漏洞的能力；

viii. 全面、定期的測試，以驗證其技術和資安韌性的有效性 (包括但不限於監管機構規則要求的測試)；

ix. 建立在有效網路威脅情報為基礎上的情勢判斷，使關鍵第三方能夠瞭解其網路威脅環境以及其資安韌性和網路安全措施的充分性。

(5.) 最後，監理機關建議關鍵第三方應確保網路和技術回應及復原措施被視為遵循事件管理的一部分。

5.2.1.6. 變更管理

CP26/23 要求關鍵第三方確保服務變更時仍能維持服務之提供，同時建議關鍵第三方於服務變更後於適當時間內持續監控其營運狀況，以應對意外事故之發生。

(1.) 監理機關建議關鍵第三方透過以下方式確保其擁有系統的方法來處理重大服務的變更（包括用於交付、維護或支援該服務的流程或技術的變更）：

i. 實施適當的政策、程序和控制，確保服務變更仍可供客戶正常運作的韌性；

ii. 以盡量避免不當中斷風險的原則進行服務變更；

iii. 確保在實施任何變更之前都經過適當的風險評估、記錄、測試、驗證和核准流程。

(2.) 為符合上述規範，監理機關在監理聲明草案中建議關鍵第三方應評估整個服務變更過程的風險變化。並列舉建議關鍵第三方應評估變更的類型清單如下：

i. 固有風險；

ii. 需要投入適當的資源來確保變更的韌性和成功；

iii. 未來將實施的新流程；

iv. 人員變化，包括員工、主要第三方服務提供商和供應鏈的其他重要部分；

v. 現有服務風險狀況的變化（包括風險閾值或限制）；

vi. 使用適當的指標來評估和監控變更相關的風險；

vii. 擬定適當的實施時間框架，不鼓勵過度倉促的決策；

viii. 實施適當的控制、風險管理流程和風險抵減。

(3.) 監理機關建議，在開始對重大服務進行變更之前，關鍵第三方應訂定變更失敗時的應變措施，包括但不限於撤銷變更或回溯。

(4.) 監理機關也建議，關鍵第三方應在實施後的適當時間內繼續監控服務的變化，以識別和管理任何意外風險。

5.2.1.7. 應確保營運持續下所需資源(盤點)

CP26/23 期待關鍵第三方透過盤點營運所需資源(Mapping)以確保其營運韌性，並建議盤點內容包含其服務中的依賴關係和脆弱性評估。同時，監理機關期待關鍵第三方主動提出其盤點框架，以避免統一框架導致盤點不完全。

(1.) 監理機關建議要求關鍵第三方：

i. 根據服務變更的相關要求和以下要點確認並記錄：

ii. 資源，包括用於交付、支援和維護其提供的每項服務的資產和技術；

iii. 與該服務相關的資源之間的任何內部和外部互連以及相互依賴性。

iv. 在英國財政部指定為關鍵第三方後，於 12 個月內完成了指定資源的識別和記錄，並在此後隨時保持更新。

(2.) 盤點是公司和金融機構營運韌性框架中的關鍵概念。DP3/22（為 CP26/23 前身）的受訪者表示監理機關應適時調整對於關鍵第三方盤點的相關要求。一些受訪者質疑關鍵第三方盤點的精細程度，其他人則建議盤點應包括所有服務的依賴關係和脆弱性。

(3.) 將其提議的應用盤點到關鍵第三方的目標是使關鍵第三方能夠透過以下方式識別脆弱性（然後應通知其情境測試）：

i. 區分整個供應鏈中對於關鍵第三方提供服務至關重要的資源以及資源間的相互關聯（監管聲明草案包含非詳盡的說明性資源清單）；

ii. 確定這些資源是否適合其用途；

iii. 考量如果資源無法使用所產生的後果。

(4.) 監理機關不建議要求關鍵第三方為其盤點使用固定格式，期望由關鍵第三方自行規劃的盤點程序能：

i. 專注於盤點對於關鍵第三方提供服務至關重要的資源；

ii. 細節說明如何實現上述目標；

iii. 每年更新或在某些事件發生後更新（例如，關鍵第三方供應商的變更）。

5.2.1.8. 事故管理

考量意外事故往往會對服務提供產生極大影響，CP26/23 要求關鍵第三方針對可能產生不利影響之事件預先規劃因應措施，同時定期更新其假設事件和因應方案，以有效將事故影響降至最低。

(1.) 監理機關建議關鍵第三方應適當管理對服務的提供產生不利影響或合理預期會對服務的提供產生不利影響的事件，包括：

i. 採取適當措施，以盡量降低衝擊的方式回應事件並從中恢復服務；

ii. 設定服務中斷的最大容忍水準；

iii. 維護及運作金融產業事件管理手冊；

iv. 協調並參與服務公司、金融機構、當局或其他人員制定的安排，以協調對影響英國金融產業的事件的回應。在這種情況下，「當局」可能包括：

- 參與回應架構(ARF)中的監理機關。
- 非英國金融監理、監督或監督機構，例如《數位營運韌性法案》(Digital Operational Resilience Act)下的關鍵第三方主要監督者；
- 金融服務業以外的監理機關和其他公共機構，可能在關鍵第三方方面具有重疊的職責或利益。

(2.) 在監理聲明草案中，監理機關建議關鍵第三方的回應和恢復措施應涵蓋事件的生命週期，包括但不限於：

i. 在事件發生前設定服務中斷的最大容忍水準；

ii. 根據標準對事件進行分類，例如預期恢復時間以及（如果已知）對關鍵第三方公司和金融機構客戶的潛在影響；

iii. 恢復服務和恢復資料的程序和目標，例如恢復時間目標(RTO)、資料恢復點目標(RPO)等，這些目標應盡可能與公司和金融機構為任何重要因素設定的影響承受程度相一致；

iv. 內部和外部溝通計畫；

v. 透過結合從先前的事件和演練測試中學到的經驗教訓來持續改進。

(3.) 監理聲明草案就關鍵第三方應如何設定最大可容忍干擾程度提出了進一步建議，包括使用適當的指標和目標。

(4.) 監理機關建議關鍵第三方也應：

i. 定期（至少每年一次）測試並更新其應對和恢復措施；

ii. 確定事件的根本原因，並採取一切合理措施解決問題，以降低事件再次發生的風險。

(5.) 監理機關建議關鍵第三方的回應和復原措施應涵蓋具有潛在跨境和跨部門影響的事件。

(6.) 根據對 DP3/22（為 CP26/23 前身）的答覆，金融產業事件管理手冊的主要目標是讓關鍵第三方考量、計劃、記錄、測試和定期審查，在發生影響其一項或多項服務的事件期間，如何與監理機關及其服務的公司和機構進行溝通和合作。

(7.) 監理機關理解每起事件都會有所不同，不可能有統一做法。然而，監理機關建議該事件管理手冊仍應包括規定關鍵第三方：

i. 與其提供服務的公司和金融機構協調危機溝通，以減輕金融體系穩定性和信心的風險；

ii. 確保其服務之公司和金融機構，以及監理機關在整個事件生命週期中獲得準確、一致和及時的資訊和支援。

(8.) 為了遵守上述要求，監理機關建議要求關鍵第三方至少每年使用其服務具有適當代表性公司或金融機構進行樣本測試，確保其金融產業事件管理手冊符合時宜。

(9.) 監理機關建議關鍵第三方應根據要求向他們提供其金融產業事件管理手冊。

(10.) 監理機關建議關鍵第三方參與其服務公司及金融機構、監理機關或其他人員制定的安排，以協調對影響英國金融市場事件的回應。央行關於金融市場營運韌性的網頁提到包括但不限於跨市場業務連續性小組（CMBCG）、金融產業網路協作中心（FSCCC）以及部門回應框架（SRF）。監理機關不建議直接規定關鍵第三方必須參與的特定金融產業事件。

(11.) 監理機關對事件通知的建議須涵蓋要求關鍵第三方在事件通知中指定一名負責與為其提供相關服務的公司進行溝通的人員。監理機關建議此人也應負責溝通安排，以協調對影響金融產業的事件的回應。

5.2.1.9.服務終止應對流程

CP26/23 要求關鍵第三方對於服務終止提出適當應對措施，同時遵守相關規範以滿足監管期待。

(1.) 監理機關建議要求關鍵第三方採取適當措施來應對其任何服務的終止，包括採取以下措施：

i. 擬定有效、有序和及時終止這些服務的規劃，包含但不限於將該服務轉移

予原先使用服務的公司或金融機構；

ii. 應有相關規定確保其原先服務的公司或金融機構在適用的情況下，以易於使用的格式取得、回收和返還該項服務下相關資產。

(2.) 監管聲明草案列出一系列可能發生終止的原因，包括但不限於公司重組、控制權變更、法律或監管問題、破產、法院程序或不可恢復的中斷。移轉後原服務公司和金融機構應繼續遵守原先該項服務應遵守的營運韌性和原第三方風險管理的適用要求和期望。關鍵第三方應採取相關措施協助促進原服務公司和金融機構能夠遵循這些要求。

5.2.1.10. 自我評估

CP26/23 要求關鍵第三方定期向監理機關提交自我評估報告，除提供相關獨立認證報告外，同時應包含相關缺漏及其補救措施，以助於監理機關有效評估關鍵第三方營運狀況。

(1.) 監理機關建議要求每個關鍵第三方在被指定為 CTP 後三個月內以及最後一次提交自我評估報告後 12 個月內，向監理機關提交書面自我評估報告。關鍵第三方應根據要求向監理機關提供自我評估報告中引用的任何文件（例如獨立確信報告、認證等），監理機關提議要求關鍵第三方保留自我評估報告副本至少三年。同時，監理機關希望關鍵第三方的自我評估報告是平衡、徹底和透明的，並公開已發現的漏洞、需要改進的領域和建議的補救措施。

5.2.1.11. 演練測試

CP26/23 要求關鍵第三方定期進行模擬情境測試，以有效確保服務提供受影響時盡量降低對客戶產生影響之風險，並要求關鍵第三方提出相關測試報告並與監理機關分享。

(1.) 根據監理機關的建議，關鍵第三方需要：

i. 定期進行情境測試，測試其在發生嚴重但合理的中斷時在其最大可容忍中斷水平內可繼續提供每項服務的能力。

ii. 確定與其業務、風險狀況和供應鏈相關的一系列不同性質、嚴重程度和持續時間的不利情況，並考慮在這些情況下提供服務的風險。

(2.) 建議的關鍵第三方情境測試要求和期望改編自公司和金融機構營運韌性架構中的要求和期望。關鍵第三方在設計測試場景時應該假設中斷是不可避免的。

(3.) 監理機關期望關鍵第三方情境測試的複雜程度與其系統重要性一致，同時盡量減少對其營運或客戶造成干擾的風險。

(4.)監理機關提議要求關鍵第三方每年測試其金融產業事件管理手冊,並在合理的範疇下(如發生重大服務中斷後)要求關鍵第三方在不同時間或比每年一次更頻繁地重新測試其策略。監理機關希望測試能夠：

i. 由關鍵第三方集中組織和協調；

ii. 包括關鍵第三方公司和其提供服務的金融機構客戶的適當樣本；

iii. 並在關鍵第三方的適當層級進行審查和核准。

(5.)監理機關也建議要求每個關鍵第三方在每次測試其金融產業事件管理手冊後產生一份報告，並與監理機關分享。該報告內容應納入：

i. 測試的主要結果；

ii. 對關鍵第三方金融產業事件管理手冊或更廣泛的關鍵第三方事件管理提出修訂；

iii. 向其客戶（相關企業或金融機構）揭露一般性非歸因性測試結果。

(6.)除了擬議的年度自我評估和測試要求外，在合理需要的情況下，監理機關還可以要求關鍵第三方根據 s312P FSMA 提供資訊。監管聲明草案列出了關於關鍵第三方應如何遵守這些要求的期望。

5.2.1.12. 盡職調查(金融業者對第三方)

CP26/23 除針對關鍵第三方進行規範外，也提醒業者需進行盡職調查，英國財政部認列關鍵第三方之考量因素並無法完整取代各業者自行進行之風險評估，同時提醒業者須自行承擔確保營運韌性之義務及責任。

(1.)監理機關將根據與關鍵第三方向公司和金融機構提供的服務集中度和重要性等相關標準指定關鍵第三方，然相關標準並不包含營運韌性，因此被列為關鍵第三方的供應商並不代表具備較其他供應商更完善的營運持續規劃。

(2.)監理機關也強調，公司委外項目和營運持續義務的最終責任不能歸責於關鍵第三方。接受提供服務之公司或金融機構需要對其聘用的第三方供應商(無論是否為被指定的關鍵第三方）進行盡職調查並進行持續監控。此外，與關鍵第三方簽訂合約並不能免除公司或金融機構應承擔的任何責任。

監理機關強調將建立一個以服務為基礎的制度，重點專注於監督關鍵第三方向金融服務

業者提供的重大服務。一旦被任命為關鍵第三方，將受到六項基本規則的約束，詳 6.2，適用於向金融服務業者提供的所有服務，概述了關鍵第三方在該制度下的基本義務，並表達監理機關控管關鍵第三方帶來的相關風險的目標。同時，也提供更細緻的營運風險和營運韌性要求期望關鍵第三方能遵守並主動進行控管。

為了滿足現有的監管要求，包括營運韌性、委外和第三方風險管理，關鍵第三方制度被期待要用來彌補受監管金融業者問責制度的不足之處，而不是用來減少金融業者的責任。其他監理機關也在擴大他們的監管網絡，以管理數位平台和關鍵服務供應商。

5.2.2. 專家意見與分享

(1.)歐盟和英國的監管機構目前已經發布有關監督金融服務行業關鍵第三方（CTPs）提案的文件和草案。英國的金融服務監管機構預計將在 2024 年底前確定關鍵第三方（CTPs）的詳細要求；而歐盟將透過 DORA 對 ICT 關鍵第三方進行控管，預計於 2025 年 1 月全面施行。

(2.)預期相當大部分的關鍵第三方（CTPs）將同時受到歐盟和英國體系的監管。例如，主要的雲端服務提供商很可能會將會同時受到歐盟和英國的監管。另外，市場數據服務供應商、人工智慧（AI）應用例如模型或數據服務供應商，預計也很可能被指定為關鍵第三方。

(3.)歐盟和英國定義關鍵第三方（CTPs）的方法不盡相同，將影響兩個管轄權在 CTPs 監管上的差異，彙整如下：

i. 英國在 CTPs 的定義上採技術中立，關注所有對金融服務業至關重要的第三方，並且可能涵蓋非 ICT 服務供應商；而歐盟關注的 CTPs 聚焦於 ICT 服務供應商，未涵蓋非 ICT 服務供應商。

ii. 英國監管機關表示，其 ICT 服務供應商不太可能涵蓋其他已受充分監管的行業（例如電信和能源業者），將更聚焦於對於金融服務業至關重要、但尚未受到同等強度監管的服務供應商。然而，歐盟關注的 CTPs 涵蓋所有 ICT CTPs，原則上涵蓋已受監管的行業如電信業者。

iii. 在判定服務供應商是否為 CTPs 的方法上，在英國，政府可根據金融服務監管機構之建議來進行 CTPs 認定，因金融服務監管機構主要考量因素通常為質化的標準，這也意味著服務供應商無法僅僅透過未達量化門檻來避免在英國被指定為 CTPs。然而，歐盟對於 CTPs 的定義標準包括質化和量化門檻，只有當所有標準都滿足時，才可能在歐盟被指定為 CTPs。

5.3. 美國

本章節參考《銀行服務公司法案》(Bank Service Company Act, BSCA) 第一章至第七章 和《The Financial Service's Sector's Adoption of Cloud Services》第四章

美國國會於 1962 年通過《銀行服務公司法案》(Bank Service Company Act, BSCA)，該法案旨在專門規範銀行服務公司（Bank Service Companies, BSC）的設立、運營及監管，以確保其服務符合監管標準，從而維護金融體系的整體安全與穩定。《BSCA》制定的背景是美國金融體系快速發展與變革的需求。BSC 作為提供銀行服務的專門機構，其運營品質與金融體系的穩定性密切相關。

根據《BSCA》，BSC 被定義為任何執行 BSCA 授權服務的公司或有限責任公司，其所有成員或資本股票持有者為一家或多家受保存款機構。這一定義涵蓋了多種類型的金融服務提供商，並為其提供了一個明確的監管框架。與歐盟《數位運營韌性法案》(Digital Operational Resilience Act, DORA) 對關鍵第三方供應商（如 Big Tech）的明確規範不同，《BSCA》並未特別針對 Big Tech 制定監管框架或限制其特定業務活動。這反映了美國與歐盟在監管思路上的差異，即美國更側重於對金融機構和 BSC 的監管，而非對 Big Tech 進行專門約束。

自《BSCA》頒布以來，該法案經歷了多次修訂，以適應金融行業不斷變化的格局。最初，《BSCA》主要針對傳統銀行業務進行規範，隨著金融科技的崛起，法案的適用範圍逐步擴展到涵蓋金融科技公司提供的數位服務。這種法規的動態演進反映了監理機關對新興金融業態風險的高度關注與應對能力。該法案確立了對金融機構和其第三方服務提供商（即本法所稱之銀行服務公司，Bank Service Company, BSC）的直接監管與規範框架。

5.3.1. 對第三方廠商要求

5.3.1.1. 第三方治理

《BSCA》授權美國銀行監理機關對 BSC 進行與銀行相同程度的監管與檢查。根據該法案，BSC 必須遵守資本充足性、業務合規性及風險管理等一系列監管要求。此外，BSC 需定期向監理機關提交運營報告，並接受定期的監管與檢查，以確保其運營的透明度與合規性。根據《BSCA》第七節，對 BSC 的監管和檢查應遵循以下規範:

(1) BSC 應接受其主要投資者的相應聯邦銀行監理機關的檢查和監管，監管程度應與其主要投資者相同。該監理機關可以授權任何其他監管該 BSC 其他股東或成員的聯邦銀行監理機關進行此類檢查。

(2) BSC 應如同其他受保存款機構一樣，需遵守《聯邦存款保險法》(Federal Deposit

Insurance Act)第八節的相關規定。

(3) 任何定期接受相應聯邦銀行監理機關檢查的存款機構或其任何子公司或附屬機構，若欲通過合約或其他方式委託第三方執行本法授權的任何服務，應遵守下列規則：

i. 第三方服務項目的執行應受到該機構的監管和檢查，監管程度應與存款機構於內部執行該服務時相同；

ii. 存款機構應在訂立此類服務合約或服務執行後 30 天內（以較早者為準）通知每個此類機構該服務關係的存在。

(4) 聯邦儲備系統理事會(Board of Governors of the Federal Reserve System)和相應的聯邦銀行監理機關被授權發布必要的法規和命令，以使其能夠管理和實施本法的目的並防止規避。

5.3.1.2.事故下通報金融機構或監理機關

根據聯邦規則彙編 (Code of Federal Regulations, CFR)第 12 篇第 1 章第 53.4 節，當銀行服務提供商確定其遭遇了(或有合理可能)實質性中斷或降低提供給某銀行機構服務的電腦安全事件，而該事件持續時間為四小時或更長時，該銀行服務提供商有責任儘快通知受影響的每位銀行機構客戶的一位銀行指定聯絡人。 銀行指定聯絡人是一個電子郵件地址、電話號碼，或由銀行機構客戶先前提供給銀行服務提供商的其他聯絡方式。如果銀行機構客戶先前未提供銀行指定聯絡人，則該通知應通過任何合理方式，發送給銀行機構客戶的首席執行官和首席資訊官，或兩位具有相當責任的人。

5.3.1.3. 營運原則

《BSCA》對於 BSC 為其他人提供的允許活動設定了必須遵守的條件和地區限制，確保股東或成員的利益受到保護。根據《BSCA》第四節 ：

(2) BSC 可以向任何人提供本節授權的任何服務，但不得接受存款。

(3) 除非根據以下(3)(4)(5)項規定或監理機關根據本法去事先核准：

i. BSC 不得在其股東或成員所在州以外的任何州執行本節授權的服務；

ii. 所有受保存款銀行的股東或成員必須位於同一州。

(4) 在某州內有州銀行或州儲蓄協會作為股東或成員的 BSC，僅應執行該州法律授權或可授權執行的服務，並且僅應在該州銀行或州儲蓄協會股東或成員可授權執行此類服

務的地點執行此類服務。

(5) 在某州內有國家銀行或聯邦儲蓄協會作為股東或成員的 BSC，僅應執行該國家銀行或聯邦儲蓄協會根據美國法律授權或可授權執行的服務，並且僅應在該國家銀行或聯邦儲蓄協會股東或成員可授權執行此類服務的地點執行此類服務。

(6) 若州銀行和國家銀行都是股東或成員，BSC 僅可執行：

i. 每個存款機構股東或成員根據任何適用的聯邦或州法律授權執行的服務；

ii. 僅在此類股東或成員可授權執行此類服務的州內執行此類服務。

(7) 儘管有本節或任何其他法律條文的規定，除適用於銀行或儲蓄協會分支機構位置的聯邦和州法律條文外，BSC 可以在董事會根據《金融服務法現代化法案》(GLBA) 授權的規定下，選擇在任何地理位置（除存款接受地點外）執行本節授權的任何活動，前提是這些法律條文適用於 BSC 並且該活動在法律條文範圍內允許控股公司執行。

《BSCA》對於 BSC 向非股東或非成員提供服務的運營原則制定了相應的規範。根據《BSCA》第六節，任何 BSC 在依據本法提供服務時，不得因某存款機構與擁有該 BSC 股份或為該 BSC 成員的機構存在競爭關係，而對該未持有股份或非成員的存款機構進行不合理的歧視。唯有在以下情況下例外：

(1) 若 BSC 向非持股或非成員機構提供服務時，僅按照能夠充分反映提供該等服務的所有成本（包括資本成本及合理回報）的價格收費，則不應被視為不合理的歧視。

(2) BSC 可以拒絕向非持股或非成員機構提供服務，若該機構可以從其他來源以具競爭力的整體成本獲得類似服務，或若提供該服務將超出服務公司的實際能力範圍。

5.3.2. 對金融機構要求

美國財政部於 2023 年 2 月發布《The Financial Service's Sector's Adoption of Cloud Services》，該報告概述美國金融服務行業在採用雲端服務的優勢與面臨的主要問題，以及監理機關需要仔細審查的風險。

(1) 雲端營運風險對金融機構而言不夠透明

(2) 具雲端與資安專業的人力資源不足

(3) 市場集中度問題

(4) 監管碎片化

報告中指出，美國的金融服務監管和監督制度對於受監理機關在其運營或提供的金融服務中使用的技術服務類型通常持中立態度。適用的聯邦監管要求無論是否將任何特定活動或運營委外給第三方，金融機構對於技術運營和相關風險（如網路安全）皆應具備有效和適當管理。金融機構通常可以自行決定選擇供應商、服務和技術架構的其他方面。在某些情況下，金融機構需要通知其監理機關技術系統或技術服務提供商的變更或計劃變更。針對 Big Tech 雲端服務在金融業的部分，目前並未有較為完善的法規或約束。

不同的金融機構通常由不同的監管機構進行監管。金融及銀行基礎設施聯絡委員會（Financial and Banking Information Infrastructure Committee, FBIIC）由來自聯邦和州級財務監管機構的 18 個成員組織組成，該委員會由財政部金融機構助理部長擔任主席。FBIIC 的成員通過每月例會，共同處理與金融服務業中的關鍵基礎設施相關的營運和策略問題，包括網路安全等議題。FBIIC 的高級領導層由各成員組織的負責人構成，每年召開三次會議，為 FBIIC 的工作提供戰略和政策層面的指導。會議討論的議題涵蓋了從消除資訊共享障礙、加強事件應對計劃到檢視金融機構中網路安全控制的最佳實務等多個方面。

5.3.2.1.風險管理

金融機構的監督和審查工作包括對技術運營和相關風險管理計劃的評估。根據各機構的職權範圍，FBIIC 成員監理機關，如聯邦存款保險公司（Federal Deposit Insurance Corporation, FDIC）、聯邦儲備委員會（Federal Reserve Board, FRB）和貨幣監理署（Office of the Comptroller of the Currency, OCC）等機構在對金融機構進行監督和檢查時，可能會涵蓋金融機構的技術營運和相關風險管理計劃。這些機構負責檢查金融機構的技術和資訊安全風險治理、資訊技術（IT）安全及韌性風險管理計劃，並審查營運恢復計劃的測試結果，以評估機構的營運和服務韌性。此外，這些監理機關還會審查金融機構的第三方關係和風險管理控制措施，以確保其符合安全性和穩健性的標準。這些審查可能包括瞭解機構如何管理由第三方服務提供商帶來的風險。

聯邦金融機構檢查委員會（Federal Financial Institutions Exmaination Council, FFIEC）和聯邦住房金融局（Federal Housing Finance Agency, FHFA）等機構發布了支持安全使用雲計算的風險管理實務指南，包括相關警報和檢查清單。雖然不同機構的規則、指導方針、審查實踐和資源可能有所不同，但通常基於或對應於一些共同的標準和框架，如美國國家標準與技術研究院（National Insititue of Standards and Technology, NIST）網路安全框架、資訊和相關技術控制目標（Control Objectives fo Informationn Technologies, COBIT）、國際標準化組織（International Organization for Standardication, ISO）標準、互聯網安全中心（Center for Inernet Security, CIS）關鍵安全控制以及美國網路安全和基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）的網路安全績效目標。FHFA 還通過定期審查和風險計劃檢查，來監管受監理機關雲端技術的採用情況。

5.3.2.2.個人資訊安全

《金融服務法現代化法案》(GLBA)通常要求金融機構通知消費者其非公開個人資訊（NPI）披露給非關聯第三方，並要求金融機構允許消費者選擇退出此類披露，某些例外情況除外。一個顯著的例外是向代表金融機構執行服務或功能的第三方提供 NPI。在這種情況下，金融機構必須披露這些資訊的共享，並與第三方訂立合約協議，要求第三方保持資訊的機密性。GLBA 還要求 FDIC、FRB、 國家信用合作社管理局(National Credit Union Administration , NCUA)、OCC、證卷交易委員會(Securities and Exchange Commission , SEC)、聯邦貿易委員會和州保險監理機關為受其管轄的金融機構建立適當的標準，這些標準涉及管理、技術和物理保障措施，包含：

(1) 確保客戶紀錄和資訊的安全性和機密性

(2) 防範任何預期的對這些記錄或資訊的安全性或完整性構成的威脅或危害

(3) 防止未經授權的訪問或使用這些記錄或資訊,這可能會對任何客戶造成實質性傷害或不便。

每個金融機構都應具備應對其國內外服務提供商所管理的客戶資訊系統中未經授權訪問事件的能力。因此，根據本指引中所規範的責任以及機構現行的指導方針，機構與其服務提供商的合約應明確要求服務提供商在發生未經授權訪問金融機構客戶資訊事件時，採取適當行動。這包括要求服務提供商儘快向金融機構報告任何此類事件，以便機構能迅速啟動其回應計劃。

美國監管機構針對金融機構的網路安全和第三方風險管理的規則、法規和指導方針，可能會根據各機構的法定權限而有所不同。例如，聯邦存款保險公司（FDIC）、聯邦儲備委員會（FRB）和貨幣監理署（OCC）根據《金融服務現代化法》（GLBA）和《聯邦存款保險法》共同發布了《資訊安全標準的跨機構指南》（Interagency Guidelines Establishing Information Security Standards）。該指南適用於代表銀行機構維護的、受這些銀行機構監管的單位內的客戶資訊。指南為涵蓋的單位設定了實施全面書面資訊安全計劃的標準。根據該指南，金融機構應至少每年向其監管機關或相關的委員會提交一次報告。報告應詳細說明資訊安全計劃的整體狀況以及機構對這些指導方針的遵循情況。報告的內容會根據各機構計劃的複雜性而有所不同，但應涵蓋與計劃相關的重要事項，包括以下內容：

(1) 風險評估

(2) 風險管理和控制決策

(3) 服務提供商的管理

(4) 測試結果

(5) 安全漏洞或違規行為

(6) 管理層的回應

(7) 資訊安全計劃變更的建議

5.3.2.3.盡職調查要求(金融機構對第三方)

根據《資訊安全標準的跨機構指南》，金融機構應遵循以下規定：

(1) 適當的盡職調查：在選擇服務提供商時，應進行充分的盡職調查，以確保服務提供商具備合規和安全管理的能力。

(2) 合約要求：應通過合約明確要求服務提供商實施與《資訊安全標準的跨機構指南》目標一致的適當安全措施，以保障資訊安全。

(3) 監督與審查：根據機構的風險評估，金融機構應對其服務提供商進行持續監督，以確保服務提供商履行合約中規定的義務。作為監督的一部分，機構應定期審查服務提供商的稽核報告、測試結果摘要或其他等效的評估報告。

5.3.2.4.事故管理

每個機構應能夠處理其國內和國外服務提供商維護的客戶資訊系統中發生的未經授權訪問客戶資訊的事件。因此，根據《資訊安全標準的跨機構指南》指引中與這些安排相關的義務，以及機構發布的現有指導意見，機構與其服務提供商的合約應要求服務提供商採取適當行動，以應對未經授權訪問金融機構客戶資訊的事件，包括儘快向機構通報任何此類事件，以便機構迅速實施其回應計劃。

根據美國證券交易委員會（SEC）制定的系統合規與完整性規則（Regulation Systems Compliance and Integrity, Reg SCI），受其監管的 SCI 單位須具備維護業務連續性和災難恢復計劃，包括保持足夠強韌和地理多樣性的備份和恢復能力，並且這些計劃合理設計以實現下個工作日恢復交易並在廣泛中斷後兩小時內恢復關鍵SCI系統。SEC還發布了一項建議規則，禁止註冊投資顧問在未達到最低要求的情況下將某些服務或職能委外。

除了 GLBA 適用於某些美國商品期貨交易委員會(CFTC) 監管的單位規定以外，CFTC 對某些其他註冊單位實施了系統保障要求。這些單位必須建立並維持風險分析和監督計劃，以識別和減少運營風險的來源，通過開發可靠、安全且具備足夠可擴展能力的控制和程序及自動化系統來實現。系統保障要求這些註冊單位擁有足夠的業務連續性和災難恢復計劃，以確

保及時（通常為下一個工作日內）恢復和重啟營運。而對於被金融穩定監督委員會（FSOC）指定為系統重要性的衍生品結算組織（Derivatives Clearing Organization, DCO），要求是在中斷後兩小時內恢復運營。如果 DCO 決定使用與另一個 DCO 或其他服務提供商的合約安排來滿足任何系統保障要求，則 DCO 應對未能滿足相關保障要求承擔全部責任，並且 DCO 必須僱用具備必要專業知識的員工，以使其能夠監督服務提供商的服務交付。

5.3.2.5. 系統變更的通知要求

多個聯邦金融監理機關要求金融機構通知適當的監理機關其技術系統的變更。例如，美國的銀行被要求向其主要聯邦監理機關提供某些類型服務關係存在的事後通知。某些 CFTC 註冊單位必須通知 CFTC 計劃對影響可靠性、安全性或容量的自動化系統進行的變更，並計劃對註冊單位的風險分析和監督計劃進行的變更。SCI 單位必須每季度向 SEC 報告已完成、正在進行和計劃的對 SCI 系統的重大變更以及間接 SCI 系統安全的變更。

5.4. 德國

本段敘述參考並擷取德國聯邦金融監理局 Bafin 於其官方網站發布之文章【Outsourcing in the financial sector: Greater transparency means greater security】之觀點，近年來，德國聯邦金融監理局 BaFin 正密切監控 Big Tech 以及金融科技帶來的發展，要求企業報告其委外情形，並指出 IT 服務委外領域集中化的潛在影響，作為今年特別關注的風險領域之一。企業的委外情形報告揭示了企業間的密切關聯，有助於識別和預防潛在的系統性風險，而 BaFin 就該等委外資料進行了詳細的分析，以監控和評估金融市場中的委外風險。

根據《Financial Market Integrity Strengthening Act[22]》（Finanzmarktintegritätsstärkungsgesetz – FISG）和《The German Securities Institutions Act[23]》（Wertpapierinstitutsgesetz – WpIG），自 2022 年起，金融業者必須向 BaFin 報告其委外活動的安排。該等法規要求通報內容涵蓋委外活動及流程的意圖、執行、重大變更及重大事件等。此舉旨在提高金融市場的透明度和風險管理。以下說明相關監管法規：

根據《Payment Services Supervision Act[24]》第 20 條針對委外的規定，其表明機構如有意委外支付服務或電子貨幣發行業務的重要營運任務，應通知德國聯邦金融監理局和德意志聯邦銀行。

以下列出《Banking Act》第 25b 條關於委外活動和流程的法規內容：

(1) 根據委外活動和流程的性質、範圍、複雜性和風險，機構應採取適當安排，以避免承擔過多的額外風險。委外活動不得損害機構業務和服務的正常執行，也不得損害業務組織。機構應確保持續進行適當且有效的風險管理，其中需涵蓋委外的活動和流程。

(2) 委外活動不應導致管理董事會的責任轉移給外部服務提供者。在進行委外活動時，機構仍應對遵守法律規定負責。

(3) 委外活動不得妨礙 BaFin 履行其職責；應透過相關委外活動和流程來確保 BaFin 的資訊請求權、審查權和監督能力，此包括委外給其他 EEA 國家或非 EEA 國家的機構的情況。該規範同樣適用於機構稽核師的職責履行。委外需簽訂書面協議，規定機構遵守上述條款的權利，包括指示權和通知權，以及外部服務提供者的相應義務。

(4) 如果 BaFin 在委外過程中其審查和監督權受到損害，BaFin 可在個別情況下發出適當

[22] 《Financial Market Integrity Strengthening Act》該法於 2021 年 7 月 1 日生效，首次從法律上要求建立充分、有效的內部控制系統和風險管理系統。

[23] 《The German Securities Institutions Act[23]》該法於 2021 年 6 月 26 日生效，係德國聯邦議院和聯邦參議院為投資公司創建之獨立的監管框架。

[24] 《Payment Services Supervision Act》允許支付服務提供者和機構提供支付服務，主要係為實現和加強德國支付服務的監管。

和必要的命令，以消除這種損害。

截至 2022 年 11 月，大約有 1,900 家公司通報了約 20,800 項委外活動和流程。報告顯示，通報的委外數量在不同類型的金融機構間存在差異。例如，投資公司和保險公司提交的委外報告數量相對較少，而德國資產管理公司報告的委外活動數量則最多，係因其涉及之相關監管法律不同，需向 BaFin 提交的報告範圍包括所有的委外活動。此外，BaFin 利用委外資料分析出金融市場中企業間的委外關係，發現銀行業內銀行與外部服務供應商有著緊密的業務關係。

除了分析銀行業與第三方供應商的關係外，BaFin 識別出部分外部服務供應商提供服務予多種金融機構，如德國資產管理公司、保險公司和信貸機構，此多客戶服務供應商對金融市場的系統有相當重要性，該等供應商如發生問題可能將對整個金融市場造成系統性影響。委外活動中，尤其是 IT 服務的委外，可能導致風險的複雜性和缺乏透明度，故 BaFin 特別關注雲端服務供應商，並在 2024 年 2 月份更新了對雲端服務委外的監管指導（Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter）。該指導旨在確保雲端服務供應商的韌性，並提高金融產業對這些服務的監管水平。

5.4.1. 德國整合 DORA 準備態度與方向

BaFin 正在等待 2025 年 1 月 DORA 落地，並將採行非強制性指導，旨在幫助德國金融機構和 ICT 服務公司實施 DORA 的標準化 ICT 風險管理以及 ICT 第三方風險管理，並補足德國在 DORA 所缺失之相關規範。誠如前面所說，德國目前只針對金融市場有重要系統性風險之產業 (例如雲端服務供應商) 有相關 IT 服務規範。德國希望透過整合 DORA，將有相關規範與無相關規範之產業歸類為 DORA 所謂 “ICT 第三方服務提供商” ，並將德國的相關法規與歐盟的數據韌性生態系做銜接。

BaFin 於 2024 年 4 月發布專家專欄[25]，提供未來整合 DORA 的相關展望。以下兩個領域尤為重要，他們在德國已有相似法律在運行，BaFin 在此提供整合方向。

5.4.1.1. 整合事故管理流程

在德國，事故管理流程在幾個金融服務產業已有先例。舉例來說，支付服務提供商須遵守《Payment Services Supervision Act》，網路安全相關服務提供商須遵守《Directive (EU) 2022/2555》，資訊安全相關服務提供商則須遵守《German Act on the Federal Office for Information Security》(Gesetz über das Bundesamt für Sicherheit in der Informationstechnik)，等等。在此，DORA 將提供其第 18 條作為整合標準化事故管理報告形式與通報主管機關名單之依據，除原本通報德國的主管機關之外，因應 DORA 也應通報歐盟層級之主管機關，以及

[25] BaFin Federal Financial Supervisory Authority – *DORA: the countdown has begun*

必要時通報歐洲央行。

5.4.1.2.強制執行威脅導向滲透測試

另外 DORA 第 16 條規定金融機構與第三方需要執行威脅導向滲透測試 (Threat-led Penetration Test, TLPT)。德國聯邦財政部（BMF）與德國聯邦銀行依循歐盟紅隊滲透演練測試框架 TIBER-EU，於 2019 年推出滲透測試框架 TIBER-DE，適用對象主要為銀行、保險公司、金融市場基礎設施及其關鍵服務提供商。透過這個框架，企業可以讓道德駭客 (ethical hackers)[26] 檢視機構的資訊系統在面對網路攻擊的防禦韌性。測試的目是在真實情境下測試系統防禦能力，識別潛在的安全漏洞，以利機構採取相應改善措施。[27]

因 TIBER-DE 非屬監管工具，執行 TIBER-DE 測試為自願性質。然在 DORA 實行後，TIBER-DE 將會根據其第 16 條從自願性變為強制性要求，BaFin 也會提供 TIBER-DE 執行指南給須執行 TLPT 的金融機構。[28]

5.4.2. 雲端服務委外的監管指導：對金融機構要求

在 DORA 於明年實施之前，德國目前尚未有針對第三方廠商(Big Tech)的具體方針要求，惟其發布之對雲端服務委外的監管指導《Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter》針對採納雲端服務之金融機構受監管公司有詳細的規範，以下篇章內容為對金融機構的相關規範。

5.4.2.1. 篩選標準

BaFin 於 2024 年 2 月更新之《Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter》，此監管通知的主要目的是使合約條款中各項措辭的監管評估透明化，並提供有關雲端委外監控和受監管公司應確保的要求的資訊。

此監管通知所指金融機構受監管公司包括信貸機構、金融服務機構、保險公司、公司退休金計畫、退休基金、證券機構、其他投資服務公司、資本管理公司、支付機構和電子貨幣機構等。[29]

5.4.2.2. 第三方治理

[26] 道德駭客（又稱「白帽駭客」）根據 TIBER-EU, TIBER-DE 框架進行紅隊演習滲透測試，進而模擬潛在威脅、評估防禦能力、和網絡攻擊，以找出金融機構系統中的漏洞。

[27] Deutsche Bundesbank. TIBER-DE: Threat Intelligence-Based Ethical Red Teaming.

[28] BaFin Federal Financial Supervisory Authority – *DORA: the countdown has begun.*

[29] 雲端服務模式可分為三種，1. 基礎設施服務（IaaS，提供運算能力和儲存空間）；2. 平台服務（PaaS，提供開發者平台）；3. 軟體服務（SaaS，提供軟體應用程式/Web 應用程式）。雲端運算佈署模式則可分為四種，1. 私有雲：只能由單一公司使用的雲端基礎架構；2. 社群雲：只能由特定公司社群（包括單一群組中的多個受監管公司）使用的雲端基礎架構；3. 公有雲：可供公眾免費使用的雲端基礎架構；4. 混合雲：由兩個或多個特殊雲端基礎架構組成的雲端基礎架構。

此監管指導提及監控委外雲端供應商的相關規範，針對資訊網絡與責任共擔模式，首先受監管公司和雲端供應商之間在雲端運營責任存在分工模式，而根據所選的雲端服務和服務模型，職責劃分也有所不同，受監管公司應針對所使用的所有雲端服務的資訊網路營運功能和活動，定義並記錄明確的任務和責任分配。

受監管公司應採取適當的、以風險為導向的技術和程序預防措施來監控雲端供應商提供的服務，以便能及時、完整和全面地收集、分析和評估必要的資訊。

5.4.2.3. 風險管理

受監管公司應在制定雲端架構規範，以便在開發雲端應用和配置雲端環境時能夠在技術上實現其架構。

因未執行相關架構而產生的風險亦應作為風險管理的一部分進行記錄和控制，尤其應考慮以下面向：

(1) 限制許可的雲端服務和資料中心位置或區域

(2) 根據所處理資料的保護要求，定義雲端服務和雲端環境的安全標準設置，使用許可的加密程序，以確保機密性、完整性、可用性和真實性此保護目標

(3) 對不面向公眾的雲端存取通道進行限制，例如明確批准具有已定義安全功能的硬體、軟體和網路區域，並根據各個雲端應用程式的重要性進行區分

(4) 將生產環境與開發、測試及其他環境分開

(5) 對非技術使用者執行多重身分驗證

(6) 定期（自動）執行備份

(7) 使用紀錄和監控資料並保護其免受未經授權的存取、操縱或未經授權的刪除

5.4.2.4. 依賴關係和供應鏈風險管理

受監管公司應在其 IT 策略中體現對雲端服務使用的考量，並且應建立相關控管程序，涵蓋委外給雲端供應商相關的所有步驟，包含從策略到遷移到雲端和退出策略。此外，受監管公司應首先檢查所有相關的內部流程，以確保在進行委外決策之前已做好準備。除了委外事項外，還應考量受監管公司自身的風險管控流程。在做出向雲端供應商採購第三方事務的策略決策後，受監管公司應在流程開始時根據適用的監管要求逐案審查是否可執行委外。

風險分析部分應考慮受監管公司委外給雲端供應商相關的所有方面，分析的強度取決於

委外事務的類型、範圍、複雜性和風險內容。受監管公司應使用風險分析來評估和記錄何項風險與委外相關以及是否屬於重大性委外。

風險分析部分應考量以下因素：

(1) 所使用雲端服務的設計

(2) 服務品質不足（業務活動的健全性或持續性）的影響

(3) 委外項目的重要性，即評估該項目對受監管公司的持續業務是否至關重要

(4) 對所選服務和交付模式所產生的風險評估

(5) 對財務、營運（例如系統故障、破壞）風險的評估，包括法律風險（例如執法風險、資料保護風險）以及聲譽風險和可能影響財務績效的風險

(6) 對雲端提供者的適用性進行評估（能力、基礎設施、經濟狀況、公司和監管狀況等）；在適當的情況下，可以從雲端供應商取得基於通用標準的憑證/證書（例如國際標準化組織的國際安全標準 ISO/IEC 2700X、聯邦資訊安全辦公室的 C5 要求）、來自認可第三方的測試報告或其內部測試報告

(7) 集中風險評估，包括將多項事務委外給雲端供應商時的風險

(8) 評估不遵守監管和處理要求的風險

(9) 對資料儲存或處理位置、雲端供應商公司總部位置、地緣政治局勢（整體政治和安全穩定性）以及相關司法管轄區適用法律（包括資料保護法）的評估，以及這些司法管轄區適用的法律執行法規，包括雲端供應商倒閉時適用的破產法規

(10) 對處理或儲存資料的完整性、可用性、機密性和真實性的風險進行評估，應考慮以下要點：

i. 其他司法管轄區可能存取數據

ii. 自身和第三方系統之間的介面不同而產生的風險

iii. 異常、甚至是無意和意外終止合約而導致的風險，例如資料遺失、資料傳輸到新服務提供者的能力有限

(11) 對雲端供應商轉移的風險進行評估

若已知委外的重大缺陷或重大變化，應注意此可能將對委外的風險狀況產生影響，從而對委外公司的風險狀況產生影響。在該等情況下，至少應檢查或重新進行風險分析。

受監管公司的監控措施應基於與委外事項相關的風險，採取不同的形式，而定期監控活動應由受監管公司的專業技術負責部門和控制職能部門根據監測計畫安排和實施。此外，應視情況採取臨時監控措施，特別是在發生事件、雲端的某些方面運作存在不確定性或為能更好地瞭解風險情況時。

對此適當的措施如下所示：

(1) 與雲端供應商的顧問進行討論

(2) 對雲端供應商的技術文件和白皮書進行評估

(3) 測試報告及證書

(4) 與雲端供應商的專家就特定主題進行深入分析

以上監控措施應記錄在案，並可促成進一步措施的協議，而這些措施的實施則應由受監管公司進行監控。

5.4.2.5. 科技和資訊安全風險管理

受監管公司應在雲端的書面規範訂定包括雲端應用程式的開發和營運之要求。在適當的情況下，應區分適用於所有應用程式和提供者的標準適用要求以及基於各個雲端供應商及其雲端服務的具體情況的特定法規。

標準要求下，受監管公司應制定符合受監管公司 IT 策略及其資訊安全和 IT 指導方針和政策的適當規範，且應根據風險分析、雲端供應商的資訊、自身的風險降低措施和其他調查結果制定特定於供應商和服務的法規。

此外，受監管公司應避免實務運作上與標準要求不一致的情況。另外需特別注意應根據資料的保護需求以及儲存和處理的位置制定基於風險的雲端使用規範。雲端使用要求至少應涵蓋雲端合規性、身分和權限管理、加密和金鑰管理、開發和營運、應用程式、介面和環境的強化、相關服務供應商控管和 IT 緊急應變措施等主題管理。

5.4.2.6. 變更管理

受監管公司應確保各自的雲端供應商確實將服務項目的變更（例如介面、雲端服務效能、SLA 或計畫維護或內部流程變更）告知受監管公司，並提前通知必須符合與雲端供應商商定

的最後期限。受監管公司應持續監控服務項目的變更和計劃變更，並定期與雲端供應商進行討論。

在實施變更之前，必須將變更項目記錄下來並作為影響分析的一部分進行評估。此外，亦須特別關注資訊安全目標，並採取必要措施，例如更改應用程式架構。若發生重大變化，也必須規劃受監管公司增加支援工作的時期。

5.4.2.7. 應確保營運持續下所需資源

受監管公司應對受監管公司搭建的雲端環境、使用的雲端服務以及開發的雲端應用進行持續監控，包括受監管公司和雲端供應商之間的定期交流，例如效能和容量管理或生命週期管理的主題。

由於雲端應用程式通常包含敏感資料，因此若發生故障可能會影響關鍵業務流程，且雲端應用的開發、運作和使用往往伴隨著網路攻擊的顯著增加。由於雲端技術被許多公司使用，複雜的攻擊方法也可能被頻繁使用，而雲端的複雜性可能會導致錯誤配置，以及無法全面瞭解所使用的基礎設施和資源（包括供應商提供的雲端管理工具和介面），從而加劇網路攻擊頻率。

除了對潛在攻擊者、攻擊目標和攻擊方法的分析，還應蒐集包括公司和應用程式特定的威脅情資，並將該等資訊在開發、營運和使用的各階段中納入考量。受監管公司應確保其網路連接免受干擾和未經授權的監控，例如透過傳輸加密或與雲端供應商的專用連接。應用程式和基礎設施架構的建構方式應盡可能阻止未經授權的存取的滲透或擴展，例如透過使用防火牆、網路分段、多因子身份驗證或零信任架構，以及透過資料外洩防護措施(DLP)偵測和預防未經授權的資料外洩。

在評估潛在的資訊安全事件時，應確實調查資訊安全相關事件和由此產生的其他資訊安全事件的責任和流程。在此背景下，受監管公司也應同意雲端供應商及時向其通報受監管公司的安全相關事件和資訊安全事件。若發生資訊安全事件，應採取適當的措施，確保即使主要連接路徑和終端設備中斷也可以進行管理存取。關鍵業務資料和配置的備份也應定期儲存在雲端外部，例如本地或其他雲端供應商。作為關鍵服務或對其提供重要支援的雲端應用程序，以及在保護需求分析中被歸類為特別重要的雲端應用程序，應定期進行滲透測試。所有使用雲端應用程式的內部和外部員工都應強制接受網路和資訊安全培訓，培訓內容應為員工過往的知識、任務和潛在風險。

此外，受監管公司應持續監控服務品質，無論雲端服務是由雲端供應商或其分包商提供。應使用適當的分析或測量來檢查雲端提供者提供的數據的合理性。對於持續監控，受監管公司應在接近不可接受的服務水準時定義內部流程和警告等級閾值。若超過閾值，則必須啟動

與內部利害關係人和雲端供應商的溝通和升級流程。如實際服務品質低於原約定，受監管公司應臨時評估由此產生的限制和風險，並在必要時採取措施降低風險。而若服務品質低於原預期，且在相當長的一段時間內不再可接受，則受監管公司應在採取降低風險措施的同時，檢查更換供應商的準備步驟，必要時發起終止委外關係。

5.4.2.8. 事故管理

雲端供應商和受監管公司的緊急理念和 IT 緊急計畫應協調一致，若兩者不一致，受監管公司應瞭解雲端供應商應對緊急情況的方法，並相應地調整自己的流程、架構和其他預防措施。作為風險管理的一部分，必須對與雲端供應商流程不一致可能帶來的風險進行相應管理。IT 應急計劃必須定期測試，受監管公司亦應使用適當的測試場景。若無法與雲端供應商進行聯合測試，則應確保其測試結果充分涵蓋所有受影響的要素。

受監管公司亦應確保其雲端供應商應立即報告計劃外的中斷和資訊安全事件，並進行初步、預先的準備。必要時雲端供應商應提供暫時規避錯誤的措施。根據預先定義的事件升級等級和閾值，受監管公司應識別資訊安全事件並與雲端供應商一同處理。若受監管公司和雲端供應商在處理資訊安全事件時存在分歧，則應商定事件升級程序，並在必要時商定指示內容。在首次報告後，雲端供應商應及時向受監管公司提供完整的事實解釋和錯誤原因分析，包括採取的所有額外安全措施，後續應由受監管公司進行評估，並在必要時在風險管理中予以考慮。

5.4.2.9.服務終止應對流程

受監管公司應根據所使用的雲端服務制定服務終止計劃，並評估替代解決方案，其應不中斷業務活動、限制監管合規性或影響客戶服務的使用和品質。服務終止計劃應充分紀錄和測試，且必須在內部和雲端供應商面向考量必要的資源、時間段、責任和支援服務。

5.4.2.10. 外部稽核機制(第三方查核或授權金融機構查核)

受監管公司有義務透過合約確保委外項目獲得適當的資訊和稽核權。監管機構提供了企業稽核機制選項，旨在使權利的實施更為容易，例如聯合查核、委託第三方進行查核或來自雲端供應商的外部或內部查核報告。受監管公司的內部稽核部門可採納第三方的查核報告，惟這些替代稽核方法以及在執行稽核程序時使用的認證亦須滿足監管要求。此類方式不得導致受監管公司的資訊和稽核權利受到限制。

聯合查核：

稽核工作可以由受監管公司的內部稽核部門或受監管公司委託的第三方代表多家委外廠商及受監管公司進行「聯合查核」。目的係為確保受監管公司對於服務供應商的稽核規劃和實

施有足夠的影響力。所有參與聯合查核的受監管公司都應可取得結果報告，若此報告儲存在共享資料室中，則必須受到保護。

使用雲端供應商內部稽核部門的報告：

受監管公司對雲端委外的稽核工作，在符合受監管公司內部稽核部門本身監管要求的情況下，可以由雲端供應商的內部稽核部門提供。報告應直接從雲端供應商的內部稽核部門傳送至受監管公司的內部稽核部門。此外，為了避免稽核過程出現漏洞，稽核範圍不應僅限於委託的事項，還應包括執行稽核所需的資源和流程，委外公司的內部稽核部門則必須定期確保遵守這些要求，例如通過適當的認證（例如 DIIR 稽核標準 3 號或 IDW PS983）或遵守其公司的稽核程序。

使用獨立第三方的報告/證書和查核結果：

受監管公司的內部稽核部門可以使用獨立第三方的報告，但如為重大委外的情況，則不能僅採納此報告。使用此類報告的先決條件是確認其與所使用的雲端服務具體相關，涵蓋相關時間段，並且由合適的獨立第三方團隊根據一般的稽核標準所產出。此規定亦適用於雲端供應商的內部稽核報告。對於複雜性低和風險低的主題領域（例如實體安全、資料中心的滅火系統），提供查核結果可能即已足夠，對於較複雜或較高風險的主題，則需要採取額外、單獨的控制和監測措施。

5.4.3. 金融機構使用雲端服務情境下，對金融機構的要求

5.4.3.1. 草擬委外合約

根據監管要求，屬於重大委外者，委外合約中應特別約定以下內容：

(1) 服務對象

合約應指定並在必要時界定雲端提供者提供的服務。一般應規定以下內容：

i. 委外事項及其實施內容，例如服務類型和提供模式、提供的服務範圍（如運算能力或可用儲存空間、可用性要求、回應時間）

ii. 在合約期間需求變更時調整服務的選項，例如若需求發生變化，或根據效能和容量管理的需求報告調整服務提供者承諾的服務水平，則增加額外的安全措施

iii. 支援服務

iv. 合作和提供的責任、義務（如更新）

v. 服務提供、資料處理和資料儲存的位置（例如資料中心的位置）

vi. 委外合約的起始時間

vii. 用於持續審查服務品質的關鍵指標

viii. 用於識別不可接受的服務品質的指標，例如與不可用性和資料遺失相關的指標

(2) 受監管公司的資訊和稽核權

受監管公司的資訊權、稽核權、控制權不得受到合約限制。須確保受監管公司及時收到所需訊息，以適當管理和監控與委外相關的風險。該資訊一般應由受監管公司保留至少五年。

(3) 監督資訊和稽核權

資訊和稽核權以及監督控制選項可能不受合約或雲端供應商內部實施指南的限制。監管機構必須能夠根據相關法律以與受監管公司相同的方式控制雲端供應商的委外事務。因此，必須透過合約約定監管機構能夠適當且不受限制地行使其對委外事項的資訊權、稽核權以及控制權；這也適用於監管機構用來進行檢查的人員。另外，監管機構應能夠在合約終止後至少五年內行使資訊和稽核權。

為保證監管機構的資訊和稽核權利，合約中應特別約定以下內容：

i. 雲端供應商有義務與監管機構充分合作。

ii. 允許不受限制地存取資訊和資料以及雲端供應商的營業場所，包括用於提供委外事務的所有資料中心、設備、系統和網路。

iii. 有效的控制和稽核選項以及在雲端供應商進行現場稽核的可能性。

(4) 發出指示的權利

應約定受監管公司的指示權。這些指示旨在確保能夠給予履行約定服務所需的所有指示，即需要能夠影響和控制委外事務。

受監管公司應有權隨時向雲端供應商發出有關數據更正和刪除的指示，雲端供應商只能在受監管公司指示的範圍內收集、處理或使用數據。發出指令的權利也應包括隨時發出指令的可能性，如要求雲端供應商立即且不受限制地將處理的資料回傳給受監管公司。

(5) 資料安全/保護

必須就法規達成一致，以確保遵守資料保護法規和資訊安全法規要求。受監管公司應瞭解提供服務的地點，尤其是資料中心的位置。另外，應根據保護需求，確保資料和系統的冗餘，以便在資料中心發生故障時，雲端服務仍能正常運作。

受監管公司應能隨時存取雲端供應商儲存的數據，並在必要時將其匯回，並確保所選的回傳格式不會限制或導致資料的使用有困難。因此，需考慮不同系統的兼容性，並就獨立於平台的標準資料格式達成一致。

(6) 終止方式

必須商定終止權和適當的通知期限，特別是應為受監管公司約定特殊的終止權，如監管機構要求終止合約，則應終止合約。若出於正當理由亦可終止合約，特別是在以下情況：

i. 雲端供應商違反與委外事宜相關的適用法律或合約條款

ii. 存在可能影響委外事宜之事項或對服務品質產生不可接受影響的障礙

iii. 發生影響委外協議或雲端供應商的重大變更（例如委外或分包商變更）

iv. 機密、個人資料或其他敏感資料的處理和安全方面出現漏洞

終止後應確認所有委外給雲端供應商的事務完全轉移到其他雲端供應商。另外，須確保原雲端供應商充分支援受監管公司將委外事務轉移給其他雲端供應商或直接轉移給受監管公司。為確保在計劃或非計劃終止合約時委外事務得以維持，受監管公司應制定終止策略並審查其可行性。

(7) 委外事務轉移

須就委外事務轉移的可能性和方式達成一致，以確保持續滿足監管要求，特別是應確保受監管公司和監管機構在進一步委外時的資訊和稽核權以及控制權也適用於委外廠商。受監管公司應確認可以進行轉移的委外事務，針對不可行的事務，應提前達成協議。委外事項如有轉移，應事先以書面形式告知受監管公司，必要時應徵得受監管公司的同意。受監管公司應瞭解潛在的委外廠商以及委外的事項。

在有新的或變更的委外的情況下，應該注意這會對委外的風險以及委外公司的風險狀況產生影響。因此，如發生新的或變更的委外事項，至少應檢查或重新進行風險分析。這也適用於已知委外廠商提供的雲端服務有重大缺陷或重大變更的情況。

(8) 雲端供應商

必須議定規範，以確保雲端供應商向受監管公司通報可能影響委外事務的正確處理

進度。提供資訊的義務包括報告在提供雲端服務過程中發生的中斷和資訊安全事件，此目的是確保對公司的委外事務進行適當的監控。雲端供應商應向受監管公司通報可能對受監管公司資料處理造成安全風險的情況，例如透過第三方措施。

(9) 適用法律說明

出於法律確定性的原因，在商定法律選擇條款時，應確保歐盟或歐洲經濟區國家的法律適用於合約（除商定德國法律）。如不適用，則應保證法律可執行性的所有要求。

5.4.3.2.證照/資格要求

受監管公司應為雲端的使用提供充足的定量和定性資源，並在組織上進行資源適當配置（人力、預算和其他資源）。這尤其適用於治理、風險管理和委外管理。必須適當考量雲端委外的監控、控制和測試以及雲端應用和雲端環境的開發、運行和安全。

在雲端環境中承擔任務的人員應具備適當且相關的技能和知識，瞭解雲端的工作原理、與之相關的風險以及與雲端操作相關的技術和組織功能。必要知識的程度取決於該人員擬執行的任務。任務的技術性越強，雲端供應商和雲端服務的知識就應該越具體。必要的知識可以透過認證、參與相關教育訓練措施或相關實務經驗來證明。

5.4.4. 專家意見與分享

(1.)Big Tech 提供服務給銀行業方面的現況與風險

i. 以德國來說，Big Tech 若沒有銀行執照，銀行法規對其並不適用；在 AI 方面，他們則需要遵守《人工智慧法案》（AI Act）。然而，如果銀行將受監管的服務委外給 Big Tech，Big Tech 仍需遵守相應的相關法規，然銀行需對這些服務負責，且監管只涵蓋銀行本身，不包含 Big Tech。

ii. 另外，有些規範不僅適用於銀行監管，也適用於不受監管的 Big Tech。例如，在德國和歐盟，反洗錢（AML）和數據保護等規範是由非金融服務監管機構進行監督。

iii. 因服務供應商不遵守監管要求的風險是存在的，為了最小化相關風險，對供應商進行盡職調查並確保持續監控是至關重要的，並需建立全面性的服務水準協議（SLA），包含詳細的描述服務範圍、時程、以及監控/控管步驟。

(2.)差異化的監管方式

i. 對於重大和非重大的委外服務，在監管要求上有做區分。對於被識別為重大的委外，監管機構有權對供應商進行調查，且在銀行與供應商之間的委外合約中，供應商必須同意讓外部審計人員可以對其進行直接監管檢查。然而對於非重大委外，這點則不適用。

ii. 委外受到德國《銀行法》和歐盟《EBA 指導原則》的監管，適用於被認定為重大和非重大的機構。

(3.)供應商管理

i. 服務水準協議（SLA）應包括服務範圍、服務期間、監控/控制步驟、營運韌性、數據保護等，以將銀行的委外風險降至最低，且對於被歸類為風險較高的重大委外，必須納入銀行的內部風險管理。

ii. 整體流程和委外的責任不能轉移給委外服務提供商，必須由銀行董事會/管理層負責。

5.5. 印度

本章節參考數位競爭法委員會 (Committee on Digital Competition Law)所發布的《數位競爭法案》(Digital Competition Act)。

2024 年 3 月 12 日，印度企業事務部 (Indian Ministry of Corporate Affairs) 發布了數位競爭法委員會 (Committee on Digital Competition Law) 的草案報告，同時公開徵求對《數位競爭法案》(Digital Competition Act) 草案的意見。這一舉措是基於議會財政常務委員會 (Parliamentary Standing Committee on Finance) 對大型科技公司(Big Tech)反競爭行為的建議。值得注意的是，該草案與歐盟的《數位市場法案》（DMA）有著顯著相似之處，這表明該法案在印度議會通過的可能性很高。該法案的主要目的是為提供核心數位服務 (Core Digital Services) 的「系統性重要數位企業」(Systematically Significant Digital Enterprises, SSDE) 建立一個前置的監管制度。印度目前僅針對符合界定規則之大型科技公司 SSDE 之反競爭行為提出規範

5.5.1. 對第三方廠商(Big Tech)要求

5.5.1.1. 篩選標準

《數位競爭法案》對於 SSDE 的定義主要依據企業的財務門檻或其在核心數位服務中的市場影響力來進行判斷。根據《數位競爭法案》第三章所制訂對於 SSDE 的篩選標準，符合以下標準之企業將被認定為 SSDE :

(1.) 在前三財政年度內達到以下任一財政閾值：

i. 印度內營業額大於等於 400 億 INR

ii. 全球營業額大於等於 300 億 USD

iii. 印度內商品交易總額大於等於 1600 億 INR

iv. 全球資本市值大於等於 750 億 USD

(2.) 即使企業沒有達到以上 (1) 中的財務門檻，其仍有機會被委員會以下列要素判定其在核心數位服務中是否帶有顯著影響力，並被界定為 SSDE：

i. 商業規模

ii. 企業規模及資源

iii. 商業及終端使用者數

iv. 經濟實力

v. 企業與市場多面向的互聯性

vi. 商業及終端使用者的依賴度

vii. 壟斷地位

viii. 進入或擴張門檻，包含高合規、技術、數據需求、規模或範圍經濟門檻、財政風險、高啓動或行銷成本、高價替代產品或服務

ix. 使用者綁定產品的程度，包含轉換成本和影響轉換的行為習慣

x. 網路效應和數據優勢

xi. 活動規模和範圍

xii. 制衡購買力

xiii. 商業或服務結構性特徵

xiv. 社會責任和社會成本

xv. 市場結構及規模

xvi. 任何委員會認定相關之內容

符合上述篩選標準的企業將被認定為 SSDE，且此認定的有效期限為三年。當企業被列為 SSDE，或當委員會考慮將其列為 SSDE 時，如果該企業為集團成員或其核心數位服務與其他企業存在直接或間接的關聯，委員會在給予企業解釋機會後，可能將相關企業認定為「關聯數位企業」（ADE）。該 ADE 的認定期限將持續至 SSDE 的認定期滿為止。

關於 SSDE 的重新指定和撤銷規定，主要包括以下幾點：

(1) SSDE 在重新認列有效期的最後 6 個月內，若未達以上 SSDE 篩選標準，應向委員會申請不再認列為 SSDE。

(2) SSDE 在被認列或重新認列後的一年內，若市場環境發生重大變動，得隨時要求委員會撤銷認列。

(3) 委員會需在收到申請後的 90 天內決定是否撤銷該企業的 SSDE 認列，且在此期間企業仍被視為 SSDE。

(4) 在 SSDE 認列或重新認列之有效期限過期時，若沒有收到撤銷認列之決定，應將其重新認列為 SSDE，有效期限一樣為 3 年。

根據《數位競爭法案》第四章，委員會可以在企業被認定為 SSDE 生效 90 天後隨時要求企業提供有關資料以確認其是否符合 SSDE 篩選之標準。在審視過 SSDE 的資料後，若判定企業達到篩選標準中之財務門檻，委員會可以在給予企業辯解機會後將企業列為 SSDE 或要求企業解釋為何其不應被判罰。此外，若判定企業符合其在核心數位服務中帶有顯著影響力，委員會應通知企業回報不應將其列為 SSDE 之理由。委員會可以在給予企業解釋機會後：

(1) 認為企業在核心數位服務中帶有顯著影響力，將其列為 SSDE。

(2) 認為企業在核心數位服務中不帶有顯著影響力，則結案。

若企業不遵循委員會所給出之指示、提供不完整或錯誤資訊。若其達到篩選標準的任一財務門檻或符合核心服務影響力任一要素，委員會得在給予企業辯解機會後將其列為 SSDE。此外，企業應在達到篩選標準中財務門檻後的 90 天內主動通知委員會。同時提供和其核心數位服務有直接或間接關聯的企業之資訊以讓委員會將其列為 ADE。

為避免防篩選之規避，《數位競爭法案》指出企業不應以合約、商業、技術或任何其他手段直接或間接地將服務分割、區塊化或碎片化以規避以上篩選標準。委員會得在任何時候要求企業提供其所需資訊以確認企業是否有防篩選規避之嫌疑。

5.5.1.2. 第三方治理

根據《數位競爭法案》，SSDE 在限制第三方應用程式、反引導以及綁定銷售和捆綁銷售方面應遵循以下原則：

(1) SSDE 不得限制或妨礙終端用戶和商業使用者上下載、安裝、執行或使用第三方程式或軟體，並應允許其自由選擇、設置及調整預設設定。

(2) 除非是維持核心數位服務的必要舉動，否則 SSDE 不得直接或間接地限制商業使用者向其終端使用者推廣或通知他們的服務、或將其終端使用者導向其或第三方之服務。

(3) 除非某項產品或服務是提供核心數位服務的必要產品或服務，否則 SSDE 不得要求

或鼓勵核心數位服務終端及商業使用者使用一個或多個 SSDE 的其他產品或服務，或以下方產品或服務：

i. 關聯方

ii. 和 SSDE 簽訂產品生產和銷售、服務提供合約之第三方

5.5.1.3. 科技和資訊安全韌性風險管理

根據《數位競爭法案》，SSDE 在數據使用方面須遵循嚴格的規範。首先，SSDE 不得直接或間接利用商業使用者在其核心數位服務上儲存的非公開資料與其他企業進行競爭。非公開資料為商業使用者透過商業活動或其終端使用者在 SSDE 的核心數位服務上產生的整合或非整合資料。此外，在取得終端用戶及商業使用者的資料後，SSDE 不得將這些資料混合或交叉使用於不同服務（包括核心數位服務），也不得將資料授權給第三方使用。

這些規範旨在保障用戶和商業使用者的數據隱私和公平競爭環境，避免資料被濫用或導致競爭不公的情況發生。在規定的時間段後，SSDE 應以規定的形式與方法向委員會報告其合規措施。

5.5.1.4.監管範圍和規範原則

根據《數位競爭法案》第四章，當某企業被指定為 SSDE 或委員會正在考慮是否將某企業指定為 SSDE 時，若該企業屬於一個集團，並且該集團內的一個或多個其他企業直接或間接參與在印度提供核心數位服務，委員會可在給予這些其他企業發表意見的機會後，發出命令指定它們為 ADE。此類 ADE 的指定將持續至該企業作為 SSDE 的指定期結束。

在《數位競爭法案》第七章中提到關於 SSED 及其 ADE 遵守義務的要求：

(1) ADE 須遵從和 SSDE 一樣的義務責任，違規將面臨和 SSDE 同等級的判罰。

(2) 委員會應針對不同的核心數位服務擬定執行規範。委員會可根據市場特性、印度使用者數或其他適用因素對同一項核心數位服務對個別 SSDE 制定不同的要求。ADE 也適用於 SSDE 規範。

(3) 委員會在制定規範時，將根據以下一個或多個因素來調整執行規範：

i. 營運的經濟可行性

ii. 詐欺防治

iii. 資訊安全

iv. 智慧財產權的違反防治

v. 其他法律機關要求

vi. 其他因素

5.5.1.5.營運原則

SSDE 應以對商業及終端使用者公平、非歧視、透明的原則營運。根據《數位競爭法案》第十一章，SSDE 不得直接或間接地偏袒自家產品、服務或業務、或偏袒以下各方之產品、服務或業務：

(1) 關聯方；

(2) 和 SSDE 簽訂產品生產和銷售、服務提供合約之第三方，而這些產品、服務或業務超過第三方商業用戶在核心數位服務中提供的產品、服務或業務。

5.5.1.6.判罰標準及尺度

在根據《數位競爭法案》第二十八章，若委員會發現 SSDE 或其 ADE 未能遵守該法制定的規則和法規的任何義務時，委員會可判罰 SSDE 或其 ADE 不超其全球營業額 10%的罰緩。若企業未能通知委員會其符合篩選標準，委員會可判罰不超過全球營業額 1%的罰額。在大多數情況下，若未能提供或提供不完整、錯誤或誤導性之該法相關資訊，委員會可判罰企業不超過全球營業額 1%的罰額。

根據《數位競爭法案》第二十九章，如果 SSDE 或其 ADE 違反本法或任何規則、法規、命令或指示，且該違規行為得到確認，則在違規行為發生時負責並對該企業的業務運作負有責任的相關人員。除非本法另有規定，委員會可以對這些相關人員處以其認為適當的罰款，該罰款不得超過當事人於過去三個財政年度平均收入的 10%。

5.6. 日本

本章節主要參考《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks)，《金融機關 IT 治理相關對話論點實行整理，2023 修正》(Discussion Paper on IT Governance at Financial Institutions, 2023 Revision)，《經濟安全保障推進法》(经済安全保障推進法)。

日本金融廳於 2018 年開始捨棄舊有的金融監督方案，並提出《金融檢查・監督基本方針》(FSA's Supervisory Approaches (Replacing Checklists with Engagement)) 制定一系列金融廳的監督方案改革。其中最為顯著的改革為包括 IT Governance 等主題之年度報告（discussion paper），可視為日本金融廳對金融科技之重視的起點。

2018 年 6 月，日本金融廳發行《金融廳的監管方法——用對話取代檢查表》（JFSA's Supervisory Approaches - Replacing Checklists with Engagement），概述了日本金融廳對於整體檢查和監管的基本概念和方法，針對每個特定主題和領域的監管概念和方法以主題/領域專門以「討論文件」的形式展示，這些文件作為日本金融廳與金融機構溝通的參考。

2023 年 4 月， 日本金融廳發佈了名為《確保運營韌性的基本方法討論文件》（Basic Approach to Ensuring Operational Resilience, Discussion Paper）的草稿，該文件將運營韌性定義為「金融機構在系統故障、恐怖主義或網路攻擊、傳染病、自然災害以及其他事件發生時，能夠以最低水平的韌性持續提供關鍵業務的能力」。

對金融機構要求方面，日本金融廳於 2019 年提出《主要行綜合監督指針》(Comprehensive Guidelines for Supervision of Major Banks) ，對於大型銀行(主要行)先行列出監督指南，其中包括委外、電子支付、IT 等第三方服務委外相關之監督準則。對 Big Tech 直接監督方面，目前資料甚少，僅於 2019 年發行《金融機關 IT 治理相關對話論點實行整理》針對 IT 企業與金融機構合作時的潛在風險與作業框架做相關說明，並於 2023 年對此整理進行修正。

綜上所述，日本對數位營運韌性管理的相關規範還處於草創階段。大部分可列入參考範圍之文件皆為討論文件或監督指南，並無詳細規範。再者，金融廳身為金融機構之監管機關，極度難以規範相關第三方服務提供商，這也是在討論文件內金融廳強調的主要規範難處之一。

5.6.1. 對第三方廠商(Big Tech)的要求

5.6.1.1. 篩選標準

日本對於 Big Tech 並無明定篩選條件與定義。從《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks) 發現，與 Big Tech 相關之專有名詞，以及有相關監

管機制的第三方供應商，為 IT 服務提供商、委外承包商、與電子支付服務提供商。需要注意的是，《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks) 為日本金融廳對金融機構之監管指南，其中提及金融機構對第三方廠商的監管，而非直接對第三方廠商進行定義與監管。

5.6.1.2. 第三方治理

根據《金融機關 IT 治理相關對話論點實行整理，2023 修正》(Discussion Paper on IT Governance at Financial Institutions, 2023 Revision)，金融機構對於第三方供應商應制定治理框架，包括:

(1) 董事會和高級管理層的領導
董事會和高級管理層是否採取領導態度，以建立良好的 IT 治理。

(2) 與公司和業務戰略相一致的 IT 戰略和數位轉型戰略
無論 IT 戰略和數位轉型是否與公司和業務戰略保持一致，金融機構是否不僅致力於創新，包括新服務的發展，而且很快進行運營改革，如降低成本和提高生產力。

(3) 實施 IT 戰略的 IT 組織和數位轉型推進組織
IT 戰略和數位轉型戰略的負責人是否適當部署，而不是全權給予 IT 部門或委外承包商，無論角色和職責是否在 IT 部門、數位轉型推進部門和銷售部門等不同部門之間明確。

(4) IT 資源的優化配置和資源管理
IT 資源（即人力、設備、預算）的位置是否與 IT 戰略和數位轉型戰略相協調。

(5) 提升企業價值的 IT 投資戰略和管理
戰略性 IT 投資（包括對數位轉型相關項目的投資）是否是為了提高企業價值，IT 投資是否遵循品質管理。

(6) 適當的 IT 風險管理
IT 風險，包括與應用新技術的錯失機會相關的風險以及與數位轉型相關的風險，是否得到妥善管理

5.6.1.3. 事故下通報金融機構及監理機關

根據《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks) III-3-3-4-3 指出，當金融機構與委外承包商之間 IT 服務發生事故，如果在承包商的運營中發現問題，日本金融廳將通過該項服務委外的銀行進行調查，根據《銀行法》第 24 條，先行與

銀行要提交報告或業務改進令。關於日本金融廳對金融機構之監管請見 6.6.2。

當日本金融廳認為僅憑金融機構提出之委外服務調查報告與實際情況尚資訊不足時，將通過與委外承包商進行直接面談來掌握實際情況。在認為特別必要的情況下（例如多家金融機構將類似業務委託給該委外承包商，或委外可能影響整個銀行結算系統的情況），金融廳將根據《銀行法》(Banking Act) 第 24 條第 2 項的規定，要求該委外承包商就必要事項（如問題發生事實、問題發生原因的分析及改進措施）提交報告。

5.6.1.4.服務終止應對流程

根據《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks) III-11-4 指出 Critical Shared Services (CSS) 相關服務終止之指南。關鍵共享服務 (CSS) 指提供給金融機構或其集團實體的服務，這些服務的失敗將導致無法或實質性阻礙執行關鍵功能。不同於其他服務，此類服務必須採取合約措施，確保 CSS 的提供在採取這些措施時仍能持續。除非是合約下的支付義務違約，雙方不得因任何服務取消或終止原因而終止合約。

5.6.1.5.須在該國有分公司

根據《經濟安全保障推進法》(经济安全保障推进法）第三章指出，為了防止第三方濫用來自日本境外的服務而干擾關鍵基礎設施服務，第三方必須經過主管當局對關鍵基礎設施服務的委外、維護和管理等的預先審查後，建立關鍵基礎設施服務系統。

5.6.2. 對金融機構之要求

5.6.2.1.篩選條件

根據《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks)，其主要行代表日本三大巨型銀行：新生銀行、青空銀行、日本郵便。目前日本金融廳僅針對使用第三方服務之重大系統性銀行進行篩選，再對其第三方服務之性質進行規範。

5.6.2.2.風險管理

根據《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks) III-3-7-1-2 指出，金融機構須針對以下方面重點進行監管:

(1) IT 系統風險管理: 風險識別與評估、故障預防和恢復、快速報告和對故障的回應、技術改進、測試新服務、IT 控制環境的客觀基準

(2) 資訊安全管理: 政策和組織準備情況、角色和職責、防止未經授權的訪問、重要使用者資訊管理、資訊管理規則、防止未經授權的訪問和資料洩露、機密資訊控制、

定期監控和安全教育、評估雲服務、個人資訊保護

(3) 網路安全管理: 網路安全的重要性、網路安全系統、多層防禦、網路攻擊期間的損害控制、及時更新和安全評估、應急預案、IT 系統委外管理、委外合約、委外工作中的風險管理、定期監測、防止損害蔓延的措施、系統故障期間的使用者指南、最壞情況準備、系統故障的分析和預防、風險評估和緩解

5.6.2.3. 事故下通報金融機構及監理機關

對 6.6.1.3 進行補充，根據《主要行綜合監督指針》 (Comprehensive Guidelines for Supervision of Major Banks) III-3-3-4-3 指出，如果在檢查結果和不當行為通知等中發現銀行的內部控制環境與委外有關的問題，金融廳將根據需要要求銀行提交根據《銀行法》第 24 條的報告。如果發現嚴重問題，金融廳將根據《銀行法》(Banking Act) 第 26 條發出業務改進命令或實施其他措施。

5.6.3. 專家意見與分享

日本對於 Big Tech 的監管基本上還處於非常初步的階段，透過資料彙整以及與日本金融廳（JFSA）的會議，以下統整雲端運算、人工智慧使用與金融科技三個面向之監管現況與趨勢：

(1.) 雲端運算

i. 日本金融廳（JFSA）自 2011 年起即積極監督（而非直接監管）銀行業使用雲端運算的情況。日本金融廳看到雲端服務在金融服務中的潛力，並選擇不直接進行監管，而是與金融產業資訊系統中心（FISC）合作，為雲端運算的使用提供指引。相關指引於 2014 年前後發布，並持續更新，且目前仍然有效。

ii. 服務提供者與金融機構之間主導能力的不平衡為日本金融廳的一個顧慮之一；在一般的委外/供應商合作中，金融機構更具主導地位，而與雲端服務提供者的關係則相反（即雲端服務提供者佔有優勢）。日本金融廳透過 FISC 來應對雲端服務提供者與金融機構之間的這種權力不對等。

(2.) 人工智慧的使用

i. 對金融機構使用人工智慧（AI）的監管仍處於早期階段。日本政府已設立一個由政府贊助的工作論壇，討論 AI 的使用及其本質上的風險。日本對於 AI 方面通常採取了較為適應市場情境的立場，並會由日本金融廳與政府主導論壇的討論共同發展與商議。

(3.) 金融科技

i. 日本金融廳對於金融科技一向採取平衡型的措施；在有助於/有益於金融市場的情況下促進和推動金融科技的使用，但在有潛在風險的情況下進行監管。而現在的趨勢是朝向更嚴格的監管。

5.7. 歸納與比較

綜上述調研結果，目前歐盟及英國對於 Big Tech (或稱關鍵第三方)相對於其他國家，已建立較為完整的監理框架，兩大監理框架關鍵性的差異在於：歐盟 DORA 條款指示大多以金融機構為控管主體，英國則主要皆對 Big Tech 直接進行要求。美國和日本現階段仍以整體第三方服務供應商為範圍進行控管，尚未釋出以 Big Tech 為主要議題的相關規範草案。印度針對 Big Tech 法規主要為數位競爭法草案，與其他國家較不具可比性，因此不納入下列彙整比較表。德國則以 DORA 監理框架作為其主要的控管標準，另獨立雲端廠商列示額外的控管規範。相關彙整結果係參考下表。

5.7.1. 監理機關對第三方廠商(Big Tech)的要求

主題	歐盟	英國	美國	日本
法規依據	《數位營運韌性法案 》(DORA)	CP26/23	《銀行服務公司法案 》 (BSCA)	《主要行綜合監督指針 》
篩選標準	1. 相關 ICT 第三方服務提供商提供服務之金融機構的數量及總資產價值、對金融服務的穩定性、連續性或質量等系統性影響。 2. 金融機構的系統性特徵或重要性。 3. 對金融機構的可替代程度。	監理機關以服務重大性、服務集中度、其他因素(可替代性、移轉難易度等)決定是否被指定為關鍵第三方。	任何執行銀行授權服務的公司或有限責任公司。	IT 服務提供商、委外承包商、與電子支付服務提供商。
第三方治理 (GOVERNANCE)		1. 關鍵第三方應具備治理架構及適當人員，確保其服務提供之韌性。	1. BSC 應遵守與銀行相同程度的監管與檢查。	

主題	歐盟	英國	美國	日本
		2. 關鍵第三方應以書面通知其指派與監理機關聯繫的窗口相關資訊。	2. BSC 需定期向監理機關提交運營報告，並接受定期的監管與檢查。	
風險管理 (RISK MANGEMENT)		1. 關鍵第三方應建立其所提供服務相關風險控管框架及流程，並定期檢視。 2. 關鍵第三方應持續監控風險。		
依賴關係和供應鏈風險管理 (DEPENDENCY AND SUPPLY CHAIN RISK)		1. 要求關鍵第三方須有效識別並管理其服務供應鏈中可能影響服務提供之各項風險。 2. 確保其服務提供之韌性。 3. 關鍵第三方在提供對金融機構至關重要的服務前，應對該機構進行適當盡職調查，並持續審查。		
科技和資訊安全韌性風險管理 (TECHNOLOGY AND CYBER RESILIENCE)		1. 應確保技術和網路風險管理及營運韌性措施。 2. 關鍵第三方應確保事件管理包含網路和技術回應及復原措施。		

主題	歐盟	英國	美國	日本
變更管理(CHANGE MANAGEMENT)		1. 確保透過系統性的方式處理重大變更。 2. 預先研擬變更的風險控管措施。 3. 變更計畫開始前應訂定變更失敗補救措施。 4. 變更計畫實施後應定期監控。		
應確保營運持續下所需資源(MAPPING)		1. 要求關鍵第三方於 12 個月內完成記錄資源安排、內外部資訊交流網絡。 2. 建議資源盤點應包括服務的依賴關係和脆弱性。 3. 關鍵第三方應依實際服務供應狀況建立資源盤點架構。		
事故管理(INCIDENT MANAGEMENT)		1. 關鍵第三方應建立風險事件應對及復原措施，措施應涵蓋完整事件週期。 2. 相關措施應定期 (至少每年一次) 測試並更新，且使用具有代表性的法人樣本。		
事故下通報金融機構及主管機關	ICT 第三方服務提供商應建立可向金融機構即時報告的管道。		符合以下情形之一者，BSC 須儘快通知受影響銀行機構： 1. 電腦安全事件持續四小時以上	1. 當金融廳認為僅憑金融機構提出之說明尚資訊不足時，將與委外承包商直接面談來掌握實際情況。

主題	歐盟	英國	美國	日本
(NOTIFICATION DUTIES)			2. 該事件可能對提供給銀行機構的服務造成實質性影響。	2. 必要時將要求該委外承包商就必要事項提交報告。
服務終止應對流程 (TERMINATION OF SERVICES)		1. 建立服務終止應對程序。 2. 建立服務終止後，原委託機構對服務內容的取得、回收、返還的相關規定。		
需在該國有分公司	需在該國有分公司			
自我評估 (SELF-ASSESSMENT)		要求關鍵第三方在被指名後限期內提交書面自我評估報告，並保留相關副本至少三年		
演練測試 (TESTING)	(1)測試應涵蓋金融機構委外第三方的所有關鍵系統、流程和技術，並在其實際運行的系統上執行測試。 (2)測試人員應具備相關專業條件，確保該人選已利益迴避並且經主管機關核准。	1. 定期進行情境測試，測試其最大容忍程度及持續提供服務之能力，並確保情境與實際狀況一致 2. 依據測試結果調整應對措施，並產出測試結果報告提供主管機關 3. 監理機關如有需要可要求關鍵第三方提供相關測試資訊		

主題	歐盟	英國	美國	日本
向監理機關繳交監管費用	1. 向關鍵 ICT 第三方服務提供商收取的費用應涵蓋其職責執行所產生的所有成本，並且應與其營業額成比例。 2. 關鍵 ICT 第三方服務提供商支付的年度監管費用不得少於 50,000 歐元			
外部稽核機制	監理機關需為每個關鍵 ICT 第三方服務提供商設立主要監督者，並且管理和計算使用該關鍵 ICT 第三方服務提供者服務之總資產占所有使用該服務的金融機構 r 價值總額額，以及這些金融機構的個別資產負債表的總和證明。Lead Overseer 應每年制定其負責之關鍵 ICT 第三方年度監督目標和主要監督行動			1. 金融廳將視外部稽核結果和不當行為通需要，要求銀行提交報告。 2. 若發現嚴重問題，金融廳將發出業務改進命令或實施其他措施。

主題	歐盟	英國	美國	日本
營運原則			1. BSC 不得接受存款。 2. BSC 只能在股東或成員所在的州內執行服務，並遵守相關法律規定。 3. BSC 在提供服務時不得進行不合理的歧視。 4. 若非持股或非成員機構可以從其他來源獲得類似服務，或該服務已超出 BSC 的能力範圍，BSC 可拒絕提供服務。	

5.7.2. 金融機構使用 Big Tech 服務情境下，監理機關對金融機構的要求

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
治理架構	金融機構應建立內部治理和控制措施，管理層需負責定義、批准並監督 ICT 風險管理框架的實施，包含： 1. 訂定資訊保護政策 2. 定期核准並執行對於 ICT 業者的監督查核。 3. 除微型企業外，應建立 ICT 治理組織及角色權責。 4. 應有使用 ICT 服務營運持續政策及復原計畫。 5. 定期確認並分配資源。 6. 定期審核企業所使用的 ICT 服務。 7. 建立 ICT 業者重大變更的溝通機制。 8. 應規劃教育訓練或人員培訓計畫。			1. 董事會和高級管理層是否建立良好的 IT 治理策略。 2. 應對相關 IT 資源有良好的配置及投資，包含人力的部署。	

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
風險管理	1. ICT 風險管理框架至少應涵蓋策略、政策、程序、ICT 合約事項和風險管理工具，並包含資產及基礎設施的保護。 2. 應確保 ICT 業務、風險控管和內部稽核之間的獨立性。 3. ICT 風險管理框架應於重大事件後不定期，或至少每年一次記錄和審查，並根據內部審查結論或主管機關指示進行修正。		1. 通過合約確保服務提供商實施與資訊安全標準一致的安全措施 2. 根據風險評估持續監督與審查其表現，以確保其履行合約義務。	金融機構須針對以下方面重點進行監管: (1)IT 系統風險管理 (2)資訊安全管理 (3)網路安全管理	1. 金融機構應訂定其雲端架構規範。 2. 金融機構和雲端供應商之間在雲端運營責任存在分工模式，金融機構應採取適當的、以風險為導向的技術和程序預防措施來監控雲端供應商提供的服務。 3. 金融機構使用委外雲端服務前應建立委外給雲端供應商之相關內部控制規範。
變更管理	1. 金融機構應建立關鍵 ICT 第三方服務系統變更的相關控管措施，以確保在金融機構的控管下完成所有程序。 2. ICT 變更管理流程應由高階管理層批准，並制定具體的協議。				1. 金融機構應確保雲端供應商將服務項目的變更告知。 2. 金融機構應持續監控服務項目的變更和計劃變更，定期與雲端供應商討論。

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
					3. 在實施變更之前，必須將變更項目記錄下來並作為影響分析的一部分進行評估。
事故管理	金融機構應建立 ICT 服務的相關事件管理流程				1. 雲端供應商和金融機構的緊急理念和 IT 緊急計畫應協調一致。 2. IT 應急計劃必須定期測試。 3. 金融機構應確保其雲端供應商即時報告意外中斷和資訊安全事件及處理方式。 4. 金融機構應識別資訊安全事件並與雲端供應商一起處理。 5. 在初次報告後，雲端供應商應即時提供完整事件說明分析。
事故通知主管機關	金融機構須提出初步、中期及最終報告，並在收到每份		合約應要求 BSC 提供若發生未經授權調閱金融機構客戶		

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
	報告後提交至相關監管機關以及相關團體。		資訊事件的相關應對計畫，以便事件發生後機構能迅速實施其控管。		
服務終止應對流程	金融機構應制定 ICT 服務供應商退場機制，以應對必要條件下合約終止的情況。 金融機構應制定適當措施避免合約終止後業務產生重大影響。				1. 金融機構應根據與所使用的雲端服務制定廠商服務退場機制。 2. 退場機制應充分記錄和測試。在內部和雲端供應商方面考慮必要的資源、時間段、責任和支援服務。
盡職調查		金融機構無論第三方廠商是否為關鍵第三方，都應主動進行盡職調查，被認列為關鍵第三方不代表監理機關已負盡職調查之責任和義務	金融機構在選擇和管理服務提供商時，必須進行盡職調查。		
草擬委外合約	提供金融機構與關鍵 ICT 第三方服務提供商的合約最低要求				委外合約中應特別約定服務對象、金融機構的資訊和稽核權、提出請求的權利、資料安全/保護、終止方式、進一步變更、雲端

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
					供應商及適用法律說明等條目。
內部相關人員要求及培訓					1. 在雲端環境中承擔任務的人員應具備適當且相關的技能和知識。 2. 相關技能和知識可以透過培訓、參與相關措施或實務經驗來證明。
依賴關係和供應鏈風險管理					1. 金融機構應使用風險分析來評估和記錄該項雲端委外是否屬於重大性委外。 2. 金融機構對委外雲端服務的監控措施可採取不同的形式，而定期監控活動應由金融機構根據監測計畫安排和實施。
科技和資訊安全風險管理					1. 金融機構應在雲端的書面規範訂定包含雲端應用程式的開發和營運之要求。

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
					2. 雲端使用要求至少應涵蓋雲端合規性、身分和權限管理、加密和金鑰管理、開發和營運、應用程式、介面和環境的強化、分包商控制和 IT 緊急等主題管理。
應確保營運持續下所需資源					1. 金融機構應對雲端環境、使用的雲端服務以及開發的雲端應用進行持續監控。 2. 金融機構應確保其網路連接免受干擾和未經授權的監控或滲透。 3. 應確保即使與雲端主要連接路徑和終端設備中斷也可以進行管理存取。關鍵業務資料和配置的備份應定期儲存在受影響的雲端外部。 4. 金融機構應持續監控服

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
					務品質，應使用適當的分析或測量來檢查雲端供應商提供的數據資料是否合理。 6. 若實際服務品質低於合約約定，金融機構應評估因此產生的限制和風險。 7. 若服務品質低於原約定，金融機構應於必要時發起終止合約。
外部稽核機制					1. 金融機構應透過合約確保在重大委外項目獲得適當的資訊和稽核權。 2. 可以由金融機構的內部稽核部門或金融機構委託的第三方進行聯合查核(或稱彙總稽核)。 3. 使用雲端供應商內部稽核部門的報告： (1) 符合金融機構監管要求下，可由雲端供應商

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
					內部稽核部門提供。 (2) 報告應直接從雲端供應商內部稽核部門傳送至金融機構的內部稽核部門。 (3) 稽核範圍不應僅限於服務委託事項，還應包括執行稽核所需的資源和流程。 4. 使用獨立第三方的憑證/證書和測試結果： (1) 金融機構的內部稽核部門也可委託獨立第三方提供稽核結果報告，但在重大委外的情況下，不能只依賴於此。 (2) 可使用第三方稽核結果報告做為外部稽核證明文件的先決條件是該報告與雲端服務具體相關，

主題	歐盟	英國	美國	日本	德國摘要(針對雲端控管)
					涵蓋相同時間段，並且由合格的獨立會計師簽核。 (3)金融機構應分析第三方稽核結果報告，對於問題較複雜或較高風險，應採取額外的控制和監測措施。

6. 我國銀行所受影響、潛在風險與未來監理政策之具體建議

6.1. 我國銀行使用 Big Tech 服務之發展背景與現況

目前 Big Tech 涉足國內金融服務主要為行動支付領域，依照金管會 2023 年 11 月統計顯示，行動支付人數已達 2,679 萬人，其中街口支付、一卡通 MONEY 會員衝破 600 萬人，全支付也逾 400 萬，網路市調機構 Fincake 亦針對用戶進行了行動支付聲量調查，顯示出前三大聲量的行動支付排名別為 Line Pay、Apple Pay 及街口支付，其中通訊軟體 LINE(母公司為 LY Corporation，由韓國 Naver 集團與日本軟銀集團合資設立)及 Apple 已被 BIS 列為 Big Tech 公司。

此外，針對純網銀的部分，2019 年 7 月 30 日金管會核准將來商業銀行、樂天國際商業銀行及連線商業銀行等 3 家業者申設純網銀，而連線商業銀行由 LINE 持股 49.9%，樂天國際商業銀行由日本樂天(Rakuten)集團持股 51%，上述兩間公司亦已由 BIS 列為 Big Tech 公司；信用卡方面，Apple 公司與美國投資銀行高盛（Goldman Sachs）於 2019 年合作推出儲蓄帳戶 Apple Card，同年 7 月 15 日已向我國經濟部智慧財產局提交註冊 Apple Card 商標，未來計劃在我國推行此項服務。

6.2. Big Tech 於我國提供金融服務之發展背景與現況

根據金融研訓院 2022 年發表之「金融科技創新與數位轉型大調查」，國內有近九成銀行業者已經導入 AI、大數據及 機器人程序自動化（RPA）應用[30]，與金融機構建立合作關係的金融科技業者家數亦逐年增加，根據台灣金融服務業聯合總會「111 年金融業之金融科技投資運用情況」調查結果指出，國內金融業對金融科技投入總預算金額大幅提高至新台幣 312.15 億元，顯示出國內銀行業者與金融科技業者的合作日趨密切。

在國內金融業仰賴大量科技技術支援下，銀行與非銀行、科技公司之間有越來越多的合作，在銀行價值鏈的不同位置提供產品和服務，如透過 Big Tech 等第三方業者提供雲端服務，可協助傳統銀行進行資料處理、分析與管理、融資評分、資安系統控管、風險管理及災害事件之即時復原。隨著國內法規開放，金融機構已逐步朝上雲的目標邁進，甚至可能因而改變部分營運模式。此外，人工智慧近 20 年內深度學習演算法的重大突破，再加上雲端運算與大數據興起，成為當前在金融業應用最多元的技術，已有將近半數的國銀開始規劃、實驗或部分導入大型語言模型，未來應會有越來越多整合分析式 AI 與生成式 AI 的應用案例出現。

[30] RPA 全稱 Robotic Process Automation，即機器人程序自動化，是一種軟體工具或機器人。不管是在桌面應用程序、網頁或其他數位系統中執行的操作，RPA 都能模擬和執行人類在電腦系統中進行的重複性、規則性的任務，達到減輕工作者負荷、提高企業效率、降低錯誤率、拉高產出品質等效益。

6.3. 相關潛在風險

Big Tech 日漸掌握個別消費者及中小型企業等客戶之金流、物流及資訊流，將逐漸改變傳統金融中介運作方式，對金融服務市場影響力漸增，若 Big Tech 透過強大市場力量造成壟斷，除降低金融市場競爭性與公平性，亦將產生集中度風險與系統性風險，最終可能危及金融穩定及對經濟層面產生影響。

此外，因 Big Tech 具備強大科技能力，國內銀行在數位轉型逐漸倚賴 Big Tech 提供第三方服務，增加金融體系之複雜度與風險傳遞可能性，若委外業務集中在特定不易被取代之 Big Tech，其與銀行之緊密作業連結程度可能提升傳統銀行作業與資安風險，應確保當 Big Tech 發生作業失誤、遭受網路攻擊或發生財務危機，我國金融機構是否有相應風險控管機制，避免中斷銀行關聯性業務的正常運作，進而影響整體金融體系穩定。

6.4. 銀行業問卷結果彙整與分析

本問卷透過對本國銀行與外國銀行在台分行進行調查，以瞭解銀行使用 Big Tech 服務情形及與 Big Tech 合作所帶來的機會與挑戰，以利監理機關瞭解銀行業面臨的痛點及潛在風險。問卷共分為三大部份：第一部份聚焦於銀行業採用 Big Tech 大型科技公司所提供之服務情形；第二部份探討銀行業與 Big Tech 大型科技公司合作之風險與機會；第三部份透過問卷瞭解 Big Tech 跨足銀行業務對銀行業造成之風險與挑戰。

本研究案對於 66 間本國銀行與外國銀行在台分行進行問卷調查，共計回收 56 份問卷，回覆率達 84.8%。

6.4.1. 銀行業採用 Big Tech 大型科技公司所提供之服務情形問卷分析結果

在 56 間回覆問卷的銀行中，其中 60.7%有採用 Big Tech 所提供的服務，39.3%無採用 Big Tech 所提供的服務。

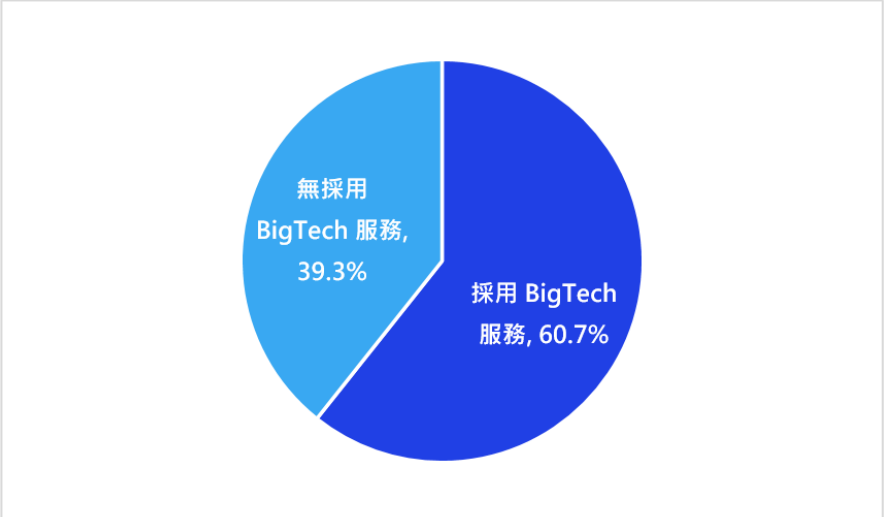

圖 1 銀行業採用 Big Tech 提供之服務現況

6.4.1.1. 已採用 Big Tech 服務之銀行現況

在問卷回覆有採用 Big Tech 服務的 34 家銀行中，採用雲端服務為最大宗。從問卷統計數據上顯示，其中 88.2%（30 家銀行）採用了雲端服務，且在排除只使用辦公室雲端工具如 Microsoft 365 等服務的銀行外，仍有高達約 70.6%使用雲端服務。此外，在 30 家於問卷中回覆有採用雲端服務的銀行中，93.3%採用了 SaaS 服務、56.7%採用了 IaaS 服務、46.7%採用了 PaaS 服務。

另外，在有採用 Big Tech 服務的銀行中，也有高達 50%採用了 AI 服務。常見應用包含聊天機器人/智能客服、數據分析與機器學習等，另有少數業者已開始測試與使用大型語言模型。

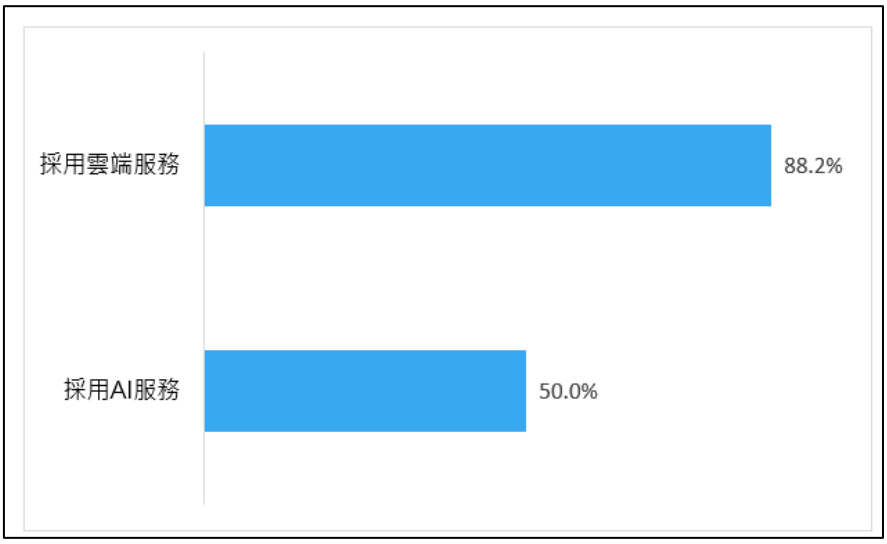

圖 2 採用 Big Tech 提供之雲端與 AI 服務情形

將銀行依資產總額分群，計算有採用 Big Tech 服務的占比，我們從統計數字可以看到資產總額大於 3 兆的銀行，高達 90%都有採用 Big Tech 提供之服務；資產總額在 100 億至 3 兆

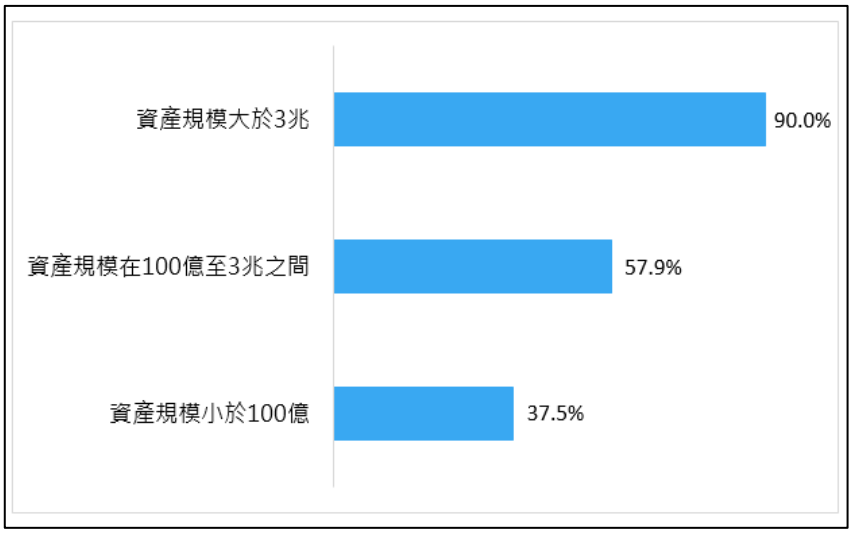

圖 3 不同資產規模銀行有採用 Big Tech 服務之百分比

之間的銀行，則有 57.9%有採用 Big Tech 提供之服務；而資產總額小於 100 億的銀行，有採用 Big Tech 提供之服務則為 37.5%。

對於已在使用 Big Tech 提供之服務的銀行來說，他們於問卷中主要分享的未來規劃除了包含持續擴大採用雲端與 AI 服務、並在生成式 AI 相關應用持續關注外，銀行也將進一步探索新技術以提升金融服務的創新和效率，例如採用區塊鏈技術、量子計算、物聯網整合和自動化技術。

6.4.1.1.1 期望 Big Tech 廠商配合事項

在問卷回覆中，有採用 Big Tech 服務之銀行表示希望能進一步要求廠商配合之事項主要包含以下三種情況：

(1) 82%之銀行希望要求廠商對於服務中止情況提出對應措施。

(2) 79%之銀行希望要求廠商配合緊急應變措施演練計畫。

(3) 76%之銀行希望要求廠商對於系統更新與事件通報措施。

另外，銀行也期望廠商能確保強而有效的應變措施、完善的資安偵測與防護。對於現行《金融機構作業委託他人處理內部作業制度及程序辦法》中所要求之事項，銀行能確保廠商全面配合再進行委外作業。然而，銀行期望能強化與進一步提升上述廠商管理措施，以降低委外風險。

6.4.1.1.2 管理 Big Tech 廠商之主要痛點

分析問卷中銀行提到對於管理 Big Tech 廠商之主要痛點與目前的解決方式，彙整十大類型如下：

(1) 數據安全與隱私：擔心數據外洩。目前主要透過加強加密和安全驗證來保護數據。

(2) 合規性與監管：不同地區的法律要求複雜。現行在銀行與科技公司合作上，會確保技術符合各地法律。

(3) 系統整合：新舊系統難以兼容。解決方式採以逐步遷移並進行系統現代化改造，確保整合順利。

(4) 技能缺口：員工缺乏新技術的知識，以及跨雲、跨應用之權限管理人才不足等。銀行通過教育訓練和文化變革提升員工適應能力。

(5) 廠商供應鏈管理挑戰：廠商的協力或複委託關係。目前解決方式主要透過盡職調查，盡量去降低風險。另外，因銀行較難要求 Big Tech 廠商直接回覆供應鏈廠商問卷，目前取而代之的作法為要求 Big Tech 廠商提供資訊安全相關之國際/產業認證。

(6) 資安風控：導入新型態服務時，不易以傳統的資安風控進行評估，缺乏業界共通標準，且 Big Tech 廠商多難以配合客製化調整。現行主要透過顧問或協力廠商花費更多時間與內外部進行溝通與諮詢，以確保符合金融業要求。

(7) 管理或稽核能力缺口：因 Big Tech 廠商具有高度科技水準，金融業較無相關管理或稽核能力與經驗。目前主要是透過第三方專業人員稽查或由廠商提出認證書作為信賴依據。另外，對於外商在台分公司來說，通常由總行統籌，本國管理上有因語言及時差等問題需要較多溝通。

(8) 事故風險：採用 Big Tech 服務雖因其龐大與較完善的基礎設備架構，有可能提供較穩定的服務，但若一旦有事故其影響層面極高，且因是跨國問題處理相關資訊及進度難以掌握。為降低風險，目前採以較不重要可替代之服務放置於 Big Tech（雲端服務）上，並建置本地端替代方案。

(9) 廠商配合度：廠商配合客戶需求的彈性應再加強，以及客服、技術支援等速度不佳，影響相關服務上線。目前解決方式為持續溝通或是找其他替代廠商。

(10) 合約談判能力：目前使用 Big Tech 服務多透過經銷商進行採購議約，部分採購服務需再簽原廠合約，此合約為該 Big Tech 公司制式合約（全球統一）故無法增刪其中條文，主管機關要求增加的資訊安全條款，供應商稽核條款皆無法增加其中。建議可比照與雲端 3 大 CSP 由銀行公會協助議約，例如消費者權益保障、複委託、經銷條款等，較能遵循相關委外辦法或自律規範。

6.4.1.1.3 期望納入合約之條款

(1) 客制化要求：希望針對其特定需求進行技術或服務的高度客制化，但大型科技公司往往更傾向於提供標準化的產品和服務，以維持其運營效率，銀行難以商議符合其營運需求之服務水準協議（SLA）入合約。

(2) 數據主權和控制：希望對存儲在雲端的數據保持完全控制和主權，但大型科技公司可能在數據存取、處理和存儲方面有自己的標準流程，導致銀行無法完全掌控。

(3) 責任和賠償條款：希望將更多的責任或賠償義務轉移給大型科技公司，特別是在數據洩露或服務中斷的情況下，但其往往有標準的責任範圍，且通常不會輕易改變。另外也希望增加對於服務異常之保證修復時效與對應賠償條款。

(4) 長期支持與維護：希望保障長期的技術支持與維護服務，但大型科技公司可能在合約中只提供有限的支持週期或強調自動化、自助式的支持模式。

(5) 對司法管轄權之要求。

(6) 資料隱私、查核及緊急應變措施：希望 Big Tech 廠商與國內代理商或金融機構得配合訂定相關合約條款，如資料或隱私保護、委外查核作業或緊急應變措施演練之配合等。

(7) 新興科技風險責任歸屬：與大型科技公司議約對於已知風險的責任範圍較能予明確敘明，但對於新興科技其風險分級及責任範疇均不甚明確，難以要求大型科技公司於溝通議約時即明確區分責任歸屬，例如 AI 技術均由第三方提供，訓練資料上雲（或資料在地化）及 AI 生成資料的相關個資保護議題、智財權的責任不容易約定責任歸屬。

6.4.1.2.未採用 Big Tech 服務之銀行現況

問卷回覆未採用 Big Tech 服務的 22 間銀行中，本國銀行與外國銀行在台分行各占一半。對於本國銀行來說，未採用 Big Tech 服務的主要原因包含對於資訊安全、隱私保護和適法性上的考量。另外，在未採用 Big Tech 服務的本國銀行中，約有 18.2%的銀行表示未來有考慮採用相關服務的規劃。

對於外國銀行在台分行來說，未採用 Big Tech 服務的主要原因主要為其在台業務未有相關需求，或採用 Big Tech 相關決策需依總行規劃辦理。

6.4.1.3.本國銀行海外分公司使用 Big Tech 服務情況

問卷回覆中共計 17 間本國銀行擁有海外分行，3 間有採用辦公室雲端工具如 Microsoft 365 等服務，其他皆無採用 Big Tech 提供之服務。

分行依所在國家之相關規定，分享參照之規範如下：在雲端委外相關規定，依循日本主管機關發布《FISC security guidelines》、新加坡主管機關制定《Guidelines on Outsourcing》；緬甸則無針對金融機構使用雲端服務的專門法規，但仍需遵守一般的數據保護法律和安全合規標準，以確保客戶數據的安全和隱私。在越南採用 Big Tech 相關服務時，會同時遵守台灣及越南「個人資料保護法」、「金融消費者保護法」、越南央行第 09/2020/TT-NHNN 號 Information System Security in Banking Operations 等相關法規。

6.4.2. 銀行業與 Big Tech 大型科技公司合作之風險與機會問卷分析結果

在 56 間回覆問卷的銀行中，其中 23.2%有與 Big Tech 合作，76.8%未與 Big Tech 合作。

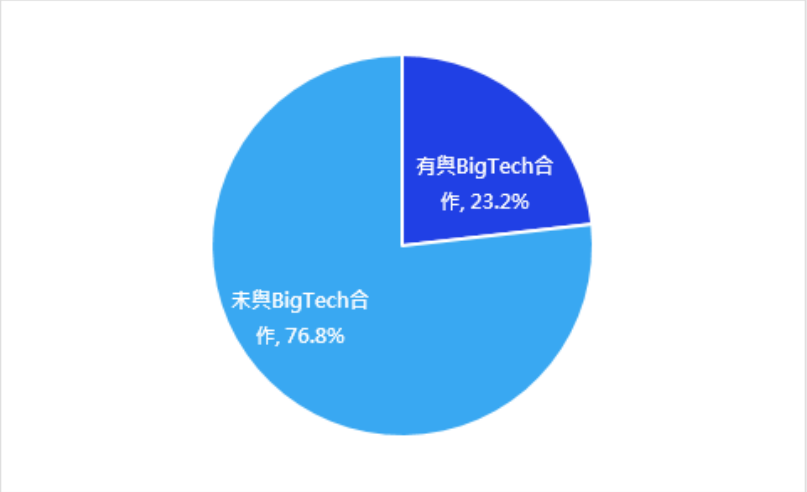

圖 4 銀行業與 Big Tech 合作現況

在 13 家回覆有與 Big Tech 合作的銀行中，90%以上之合作內容為行動支付如 Apple Pay、Google Pay、Samsung Pay，和上架 App 至 App Store 和 Google Play 等平台。另有一家銀行回覆有與 Big Tech 合作發行信用卡。而在未來考慮與 Big Tech 合作方向來看，進一步提升使用者體驗為主要合作動機。

在 43 家回覆未與 Big Tech 合作的銀行中，18.6%表示未來有考慮或規劃與 Big Tech 合作。而目前主要未有相關合作的原因為業務上無相關需求（約占 16.3%），以及為外國銀行在台分行，故 Big Tech 合作將依總行決策（約占 23.3%）。此外，資料安全與隱私保護、資安風險等議題也是未與 Big Tech 合作的銀行考量的要素。

對於銀行認為與 Big Tech 大型科技公司合作，能為其帶來的主要效益包含提升企業形象、增加用戶數、提升營收。60.7%的銀行回覆提升企業形象為與 Big Tech 合作主要能帶來的益處、57.1%的銀行回覆增加用戶數為與其合作之主要價值、46.4%的銀行回覆提升營收為與其合作之主要效益。另外，強化新興科技應用、提升內部效率、降低成本、以及創新皆為銀行認為與 Big Tech 合作能帶來的效益。

6.4.2.1.與 Big Tech 大型科技公司合作之主要風險

對於銀行與 Big Tech 大型科技公司合作帶來的主要風險，76.8%的銀行視資料隱私保護為其主要疑慮，25%的銀行認為市占下滑/市場瓜分為其考量之風險，23.2%的銀行視用戶流失為其主要風險之一。

除此之外，平台穩定性與安全性、資料保存與資安等議題，也是銀行認為與 Big Tech 大型科技公司合作上會面臨的風險。

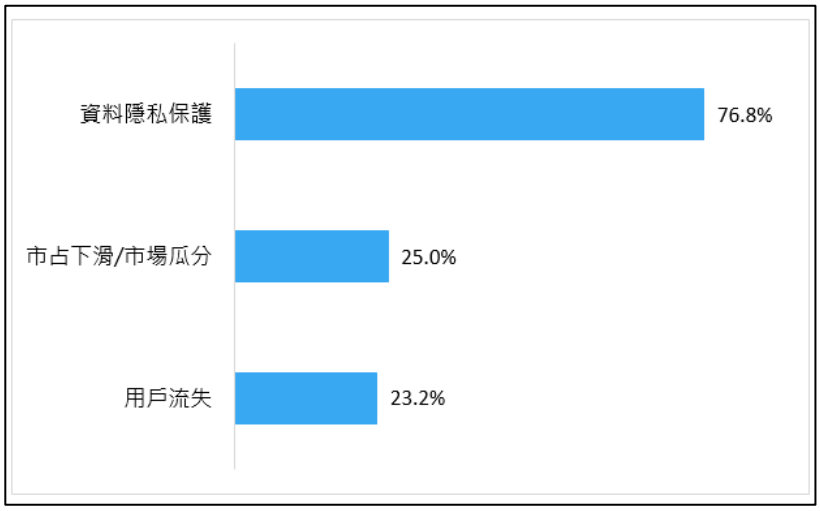

圖 5 與 Big Tech 合作對銀行之主要風險

6.4.3. Big Tech 跨足銀行業務對銀行業造成之風險與挑戰問卷分析結果

Big Tech 跨足銀行業務對銀行造成了潛在威脅與挑戰，以下彙整銀行於問卷中回覆之自身所具優勢與劣勢與其所採取的因應措施。

6.4.3.1.銀行相對 Big Tech 之優勢與劣勢

<u>優勢</u>

(1) 品牌信譽和客戶基礎：擁有悠久的銀行歷史和全球知名度，建立了廣泛的客戶基礎和信任，且具有在地化線下經營，主要客群黏著度高。

(2) 金融專業知識和經驗：在金融領域擁有豐富的專業知識和經驗，能夠提供複雜的金融產品和服務。

(3) 合規性和監管經驗：熟悉金融監管環境，具備處理合規要求的經驗，有助於應對各地的法規挑戰，且能夠有效保障客戶資金安全。

(4) 廣泛的全球網絡：擁有全球業務網絡，能夠提供跨境金融服務，滿足客戶多元化需求。

(5) 法規特許行業：銀行業為政府高度監管的特許行業，對於部分金融業務更關係國家的金融穩定，及影響廣大的民眾權益，故政府制定許多法令予以規範，有進入障礙優勢。

(6) 產品專業經驗：金融業務上擁有多元產品及多年經驗，能依照客戶不同需求提供專業且多元的金融服務。銀行能在不同平台和產品之間進行整合，提供更全面的解決方案，並且透過金控資源與業務整合，達成綜效。

劣勢:

(1) 靈活性不足：相較於靈活的 Big Tech 公司，銀行運營模式可能較為僵化，影響創新速度。

(2) 數位轉型挑戰：雖然銀行已在數位化方面做出努力，但在某些技術領域仍面臨與 Big Tech 公司相比的劣勢。

(3) 高運營成本：銀行業務運營成本較高，相對於 Big Tech 的低成本模式可能造成競爭劣勢。

(4) 技術創新速度：Big Tech 公司通常在技術創新方面速度更快，科技大廠通常擁有更強的技術基礎和研發能力，能快速採用最新的科技，如人工智慧、大數據、區塊鏈等。銀行可能需要更多時間和資源來追趕，無法及時滿足客戶對於數位化服務的需求。

(5) 人才不足：缺乏科技人才、技術創新速度慢、且金融業的人才招募相較於 Big Tech 較難吸引優秀人才的投入。

(6) 用戶數差距：因 Big Tech 具備龐大用戶數以及技術能力，勢必對客戶體驗、客戶滲透率、精準行銷能力等造成衝擊。

(7) 資源限制：Big Tech 擁有龐大的資金與技術資源，能夠快速擴展其金融服務，而傳統銀行在資源投入上可能受到限制。

(8) 跨界競爭：Big Tech 能夠結合其非金融業務與金融服務，提供一站式的解決方案，對於傳統銀行來說是一大挑戰。

(9) 法規限制：銀行業受限法規，服務項目的彈性受限。且因金融機構於資料安全等風險議題上較為謹慎，在創新金融技術與服務的應用上回應能力可能較不如 Big Tech 來的快速。

(10) 品牌優勢：銀行規模較 Big Tech 小、品牌優勢較為薄弱。

6.4.3.2.銀行所採取的因應措施

在 56 份回收的問卷中，約 76.8%表示已考慮或採取相對應之因應策略，以提升能與 Big Tech 競爭的優勢；約 23.2%表示未規劃因應策略、或將全權依循國外之總行決策進行應對。

在已考慮或採取因應策略的銀行中，71.4%聚焦於強化創新，69.6%致力於人才培育，

66.1%則以積極掌握市場趨勢來做應對，以提升與 Big Tech 大型科技公司競爭上的優勢。

面對 Big Tech 跨足銀行業務可能造成的潛在風險，以下彙整銀行業所採取的應對措施：

(1) 加速數位轉型：加快數位轉型步伐，投入資源於新技術的開發和應用，如雲端運算、人工智慧和大數據分析，以提升運營效率和客戶體驗。

(2) 加強創新能力：設立了創新實驗室和加速器，以促進金融科技創新，並與科技初創公司合作，探索新技術和業務模式。

(3) 增強客戶關係和服務：致力於提升客戶服務品質，提供更多個性化的金融產品和服務，以鞏固客戶忠誠度並滿足其多樣化需求。

(4) 強化合規與風險管理：加強了對監管要求的遵循，並提升內部風險管理和合規系統，以應對可能的法規挑戰和市場變化。

(5) 擴大合作與夥伴關係：積極尋求與科技公司和其他金融機構的合作，通過戰略聯盟來增強競爭力和拓展市場機會。

(6) 市場研究：加強金融市場與競業資訊收集，因應環境變化研擬對策與進行市場研究和競爭分析，且隨時追蹤觀察同業應對方式及採取必要行動。

(7) 人才招攬與培訓：引進外部資訊專業人才，並持續進行內部人員專業技能培訓，例如 AI 高階主管班課程，教授並引導主管們如何將 AI 技術與策略深度融合，制定有效的 AI 推動方案，推動組織轉型並實現業務目標。

(8) 跨界交流：邀請在人工智慧、數位賦能、電子商務、資訊安全等領域頂尖的專家學者參與交流，深化跨界、跨域、跨產業的交融，使能更好藉由科技的力量，打造新型態的金融服務。

6.5. 我國法規相關說明

我國依銀行法第四十五條之一第三項及信用合作社法第二十一條第四項訂定《金融機構作業委託他人處理內部作業制度及程序辦法》，旨在規範金融機構將內部作業委託給第三方處理的相關制度及程序，以確保業務的連續性、客戶權益的保障及金融穩定，辦法中規定金融機構將內部作業委託給第三方必須進行嚴格的風險評估，確保受託方具備處理相關業務的能力及資質。委託協議應包括服務範圍、品質標準、保密義務、風險分擔等內容，並應明確雙方的責任與義務。

其中第十八條已規範金融機構針對重大性消費金融業務資訊系統委託至境外處理，須檢

具詳細文件向監理機關申請核准，並且須確認受委託機構對客戶資訊的使用、處理及控管符合我國個人資料保護法，保留完整稽核紀錄。其次，應定期評估成本效益及集團內費用分攤的合理性，並報董事會通過。資訊系統的安全檢測應符合監理機關或銀行公會的規範，且每年至少應進行一次一般性查核和一次專案查核，在年度結束後四個月內將查核報告提報董事會。此外，金融機構亦須建立受委託機構服務中斷的營運備援計畫，並在契約中明確規定委外作業移轉或回轉的義務和責任。

第十九條規範金融機構在使用雲端服務時的原則，金融機構需訂定使用雲端服務的政策及風險管控措施，並注意雲端服務業者的適度分散。對雲端服務業者負有最終監督責任，並應具備專業技術及資源，監督其執行受託作業。金融機構可自行委託或與其他金融機構聯合委託具資訊專業的獨立第三人進行查核，確保查核範圍涵蓋重要系統及控制環節，並符合國際資訊安全及隱私保護標準。在資料保護方面，金融機構需確保客戶資料加密或代碼化，並訂定加密金鑰管理機制。對於委託雲端服務業者處理的資料，金融機構應保有完整所有權，並確保雲端服務業者無權存取或利用委託範圍外的客戶資料。此外，客戶資料及其儲存地應符合相關法律要求，重大性消費金融業務資訊系統的客戶資料儲存地應優先在我國境內，除非經監理機關核准。

6.6. 我國與主要先進國家之法規差異分析

根據本研究彙整結果及考察相關法律規範，我國目前關於第三方廠商的控管係依循「金融機構作業委託他人處理內部作業制度及程序辦法」,其針對屬金融機構涉及營業執照所載業務項目或客戶資訊之相關作業委外，要求金融機構需對於範圍內的委外事項進行控管。

不同於歐盟和英國，我國目前尚無針對 Big Tech (或稱關鍵第三方服務提供商)設立專法進行規範，然「金融機構作業委託他人處理內部作業制度及程序辦法」對於金融機構辦理服務項目委外第三方廠商的控管標準及要求，與歐盟 DORA 以金融機構為控管主體的規範框架有相對較高的連結性，故下列係以我國「金融機構作業委託他人處理內部作業制度及程序辦法」相關條例為主體，並以歐盟 DORA 為主，美國與日本為輔進行差異分析比較。除前述對於間接監理控管的差異分析外，歐盟、英國等國家亦採取直接監理的方式對第三方服務供應商進行控管。我國與主要先進國家之法規差異分析、歐盟與英國針對第三方服務供應商直接監理之法規摘要分析如下。

主題	間接監理	
	台灣作業委外辦法相關內容	各國法規摘要
治理架構	【第 4 條】 委外內部作業規範應載明下列事項： 一、作業委外之政策及原則，包括委外之決	【歐盟】 金融機構應建立內部治理和控制措施，管理層需負責定義、批准並監督 ICT 風險管理框

主題	間接監理	
	台灣作業委外辦法相關內容	各國法規摘要
	策評估、風險管理機制、核決層級及治理架構。 二、專責單位及相關單位對委外事項控管之權責分工。 三、委外事項範圍及委外程序。 四、客戶權益保障之內部作業及程序。 五、風險管理原則及作業程序。 六、內部控制原則及作業程序。 七、其他委外作業事項及程序。	架的實施，包含： 1. 訂定資訊保護政策 2. 定期核准並執行對於 ICT 業者的監督查核。 3. 除微型企業外，應建立 ICT 治理組織及角色權責。 4. 應有使用 ICT 服務營運持續政策及復原計畫。 5. 定期確認並分配資源。 6. 定期審核企業所使用的 ICT 服務。 7. 建立 ICT 業者重大變更的溝通機制。 8. 應規劃教育訓練或人員培訓計畫。 **【日本】** 1. 董事會和高級管理層是否建立良好的 IT 治理策略。 2. 應對相關 IT 資源有良好的配置及投資，包含人力的部署。
風險管理	**【第 8 條】** 第四條第二項第五款規定金融機構訂定之委外內部作業規範有關風險管理原則及作業程序，其內容應包括： 一、建立作業委外風險與效益分析之制度。 二、建立足以辨識、衡量、監督及控制委外相關風險之程序或管理措施： （一）評估委外事項之風險程度、重大性及對業務影響程度。 （二）確保金融機構及受委託機構具備足夠之專業知識與資源。 （三）考量相關風險因素，進行委外營運風險等級之評估，及降低風險之適當措施。 （四）定期評估風險等級，確保風險等級之更新。	**【歐盟】** 1. ICT 風險管理框架至少應涵蓋策略、政策、程序、ICT 合約事項和風險管理，並包含資產及基礎設施的保護。 2. 應確保 ICT 業務、風險控管和內部稽核之間的獨立性。 3. ICT 風險管理框架應於重大事件後不定期，或至少每年一次記錄和審查，並根據內部審查結論或主管機關指示進行修正。 **【美國】** 1. 通過合約確保服務提供商實施與資訊安全標準一致的安全措施 2. 根據風險評估持續監督與審查其表現，以確保其履行合約義務。

主題	間接監理	
	台灣作業委外辦法相關內容	各國法規摘要
	（五）辦理具重大性之委外事項依風險情境進行定期或不定期測試或演練。 三、訂定緊急應變計畫及終止委託之移轉機制。	
變更管理	尚無相關規範	**【歐盟】** 1. 金融機構應建立關鍵 ICT 第三方服務系統變更的相關控管措施，以確保在金融機構的控管下完成所有程序。 2. ICT 變更管理流程應由高階管理層批准，並制定具體的協議。
事故管理	**【第 18 條】** 五、應建立受委託機構發生無法提供服務情事或服務中斷之營運備援計畫。	**【歐盟】** 金融機構應建立 ICT 服務的相關事件管理流程
服務終止應對流程	**【第 18 條】** 六、應於契約中載明於委外作業移轉至其他受委託機構或移回金融機構之情況，原受委託機構有關系統遷移、資料處理之義務，及受委託機構服務中斷之賠償責任。	**【歐盟】** 金融機構應制定 ICT 服務供應商退場策略，以應對必要條件下合約終止的情況。 金融機構應制定適當措施避免合約終止後業務產生重大影響。
演練測試	**【第 8 條】** （五）辦理具重大性之委外事項依風險情境進行定期或不定期測試或演練。	**【歐盟】** (1)測試應涵蓋金融機構委外第三方的所有關鍵系統、流程和技術，並在其實際運行的系統上執行測試。 (2)測試人員應具備相關專業條件，確保該人選已利益迴避並且經主管機關核准。
外部稽核機制	**【第 18 條】** 一、應就受委託機構對客戶資訊之使用、處理及控管情形確認符合我國個人資料保護法相關規定，留存完整稽核紀錄，並列為重點查核項目。 四、每年至少應辦理一次一般性查核及一次專案查核，並應於每年年度終了後四個月內將當年度辦理跨境委外查核報告提報董	**【歐盟】** 監理機關需為每個關鍵 ICT 第三方服務提供商設立主要監督者，並且管理和計算使用該關鍵 ICT 第三方服務提供者服務之總資產占所有使用該服務的金融機構價值總額，以及這些金融機構的個別資產負債表的總和證明。 Lead Overseer 應每年制定其負責之關鍵 ICT 第三方年度監督目標和主要監督行動

主題	間接監理	
	台灣作業委外辦法相關內容	各國法規摘要
	（理）事會報告。前述查核之執行得委託具資訊專業之獨立第三人辦理。	
盡職調查	**【第 18 條】** 四、作業委外計畫書，其內容應包括： （一）風險評估及管理機制： 1.委外事項之風險程度、重大性及對營運及客戶權益影響之評估情形。 2.受委託機構盡職調查情形，確保提供作業之可靠性、遵法性，其中可靠性應包括對業務持續性、替代性及集中性之分析。 3.應具專業技術及資源，監督受委託機構執行受託作業之說明。 4.日常監督機制之計畫及執行單位。	**【歐盟】** 1. 金融機構在選擇和管理服務提供商時，必須進行盡職調查。 2. 通過合約確保服務提供商實施與資訊安全標準一致的安全措施 3. 根據風險評估持續監督與審查其表現，以確保其履行合約義務。
草擬委外合約	**【第 10 條】** 金融機構作業委外契約應載明下列事項： 一、委外事項範圍及受委託機構之權責。 二、金融機構應要求受委託機構配合遵守第二十一條規定。 三、消費者權益保障，包括客戶資料保密及安全措施。 四、受委託機構應依金融機構監督訂定之標準作業程序，執行消費者權益保障、風險管理、內部 控制及內部稽核制度。 五、消費者爭端解決機制，包括解決時程、程序及補救措施。 六、受委託機構聘僱人員之管理，包括人員晉用、考核及處分等情事。 七、與受委託機構終止委外契約之重大事由，包括主管機關通知依契約終止或解約之	**【歐盟】** 1. 金融機構與 ICT 第三方服務提供者的權利和義務應明確分配並以書面形式列出。完整的合約應包括服務層級協議，並以一份書面文件記錄，該文件應可供各方以紙質或其他可下載、耐久且可訪問的格式獲取。 2. 關於使用 ICT 服務的合約安排應至少包括以下要素： (a) ICT 第三方服務提供者提供的所有功能和 ICT 服務的明確且完整的描述，指出是否允許分包支持關鍵或重要功能的 ICT 服務或其重要部分，以及在允許的情況下，此類分包適用的條件； (b) 提供合約或分包功能和 ICT 服務以及數據處理的地點，即區域或國家，包括存儲位置，並要求 ICT 第三方服務提供者在預計變更這些地點時提前通知金融機構；

主題	間接監理	
	台灣作業委外辦法相關內容	各國法規摘要
	條款。 八、受委託機構就受託事項範圍，同意主管機關及中央銀行得取得相關資料或報告，及進行金融檢查，或得命令其於限期內提供相關資料或報告。 九、受委託機構對外不得以金融機構名義辦理受託處理事項，亦不得進行不實廣告或於辦理貸款行銷作業時向客戶收取任何費用。 十、受委託機構對委外事項若有重大異常或缺失應立即通知金融機構。 十一、其他約定事項。	(c) 關於數據保護的可用性、真實性、完整性和機密性的條款，包括個人數據； (d) 確保在 ICT 第三方服務提供者破產、解決或停止業務運營，或合約安排終止的情況下，能夠以易於訪問的格式訪問、恢復和返回金融機構處理的個人和非個人數據的條款； (e) 服務層級描述，包括更新和修訂； (f) 在發生與提供給金融機構的 ICT 服務相關的 ICT 事件時，ICT 第三方服務提供者在無需額外成本或預先確定成本的情況下向金融機構提供援助的義務； (g) ICT 第三方服務提供者完全配合金融機構的主管當局和解決當局，包括其指派的人員的義務； (h) 根據主管當局和解決當局的期望，合約安排的終止權利和相關的最低通知期； (i) ICT 第三方服務提供者參與金融機構的 ICT 資安意識訓練和數位營運韌性培訓的條件。

主題	直接監理
	各國法規摘要
篩選標準	【歐盟】 1. 相關 ICT 第三方服務提供商提供服務之金融機構的數量及總資產價值、對金融服務的穩定性、連續性或質量等系統性影響。 2. 對金融機構的系統性或重要性影響。 3. 對金融機構的可替代程度。
依賴關係和供應鏈風險管理	【英國】 1. 要求關鍵第三方須有效識別並管理其服務供應鏈中可能影響服務提供之各項風險 2. 確保其服務提供之韌性 3. 關鍵第三方在提供對金融機構至關重要的服務前，應對該機構進行適當盡職調查，並持續審查

科技和資訊安全	**【英國】** 1. 應確保技術和網路風險管理及營運韌性措施。 2. 關鍵第三方應確保事件管理包含網路和技術回應及復原措施
應確保營運持續下所需資源	**【英國】** 1. 要求關鍵第三方於 12 個月內完成記錄資源安排、內外部資訊交流網絡 2. 建議資源盤點應包括服務的依賴關係和脆弱性 3. 關鍵第三方應依實際服務供應狀況建立資源盤點架構
事故下通報金融機構及主管機關	**【歐盟】** ICT 第三方服務提供商應建立可向金融機構即時報告的管道
需在該國有分公司	**【歐盟】** 需在該國有分公司
自我評估	**【英國】** 要求關鍵第三方在被指名後限期內提交書面自我評估報告，並保留相關副本至少三年
向監理機關繳交監管費用	**【歐盟】** 1. 向關鍵 ICT 第三方服務提供商收取的費用應涵蓋其職責執行所產生的所有成本，並且應與其營業額成比例。 2. 關鍵 ICT 第三方服務提供商支付的年度監管費用不得少於 50,000 歐元

6.7. 監理機關可考量之監理工具

金融業隨著數位化的發展，監理框架、法規、監管方法和工具也持續在變化，根據 FSB 及 BIS 的報告[31]，其彙整相關監管方法及工具，旨在透過以可比較的、互通的監管方法，促進金融監管機關之間的合作，從而提高國家監管措施的有效性，使多種不同的監管制度能夠根據共同的期望與目標達到共存。

FSB 建議金融監理機關可以通過以下方式有效的瞭解第三方廠商及其提供給金融機構的服務營運持續的狀況：

(1) 週期性地監督金融機構，包括要求提供其委託第三方廠商服務的相關資訊、對單一金融機構或整個產業進行檢視與審核，以及審核金融機構從第三方廠商收到的保證和資訊，包括(如適用)獨立查核或協作保證工作的結果，例如聯合查核。

(2) 與第三方廠商進行對談與討論。

[31] *"Final Report on Enhancing Third-Party Risk Management and Oversight – a Toolkit for Financial Institutions and Financial Authorities"* December 2023；"Digitalisation of finance" May 2024

BIS 則建議監督方法可依下列原則持續調整，以應對與金融數位化相關的許多挑戰：

(1) 戰略和框架：一些監理機關已經採取了數位監理的策略，首先側重於瞭解和評估與數位化相關的風險，然後再尋求加強既有的監管框架。一些監理機關正在審查他們的框架，以確保他們在所有風險領域 (包括數位創新) 仍具備採取早期糾正措施的能力。

(2) 組織：一些監理機關已開始改變其內部監管功能的組織結構，組建了專業風險團隊 (例如資訊安全風險和營運風險) 或專業監管團隊，將注意力集中在銀行與金融科技公司之間的合作關係及各項新型態業務。許多監理機關還建立了金融科技或創新中心作為專注發展以下任務的核心，例如數位創新，與利害關係人舉辦工作坊，撰寫研究論文，進行實驗 (例如 techsprints) 並與業界互動，制定新的法規管理數位活動（例如關於加密貨幣或人工智慧）也要求監理機關分配更多資源用於實施和監控相關工作進行。

(3) 訓練和能力建構：許多監理機關已經實施了內部教育訓練計畫並支持員工參加外部研討會和專業訓練課程，以培訓和提高監管人員的能力，讓他們瞭解特定科技和傳統金融風險外更廣泛的主題，例如與資料保護、隱私、歧視和偏誤相關的主題。為了推動整個監管部門的專業知識水準，部分監理機關開始著重於招募具有 IT 和新興科技專業知識的員工，此外亦包含發表特定科技主題相關文章、引入金融監理學院課程或是建構內部專家團隊來持續強化人員相關監管能力。

(4) 事先通知或核准：多數監理機關要求銀行在採用部分較高風險之科技與第三方廠商建立合作關係或其他安排之前須先進行通知，或必須事先獲得核准。

(5) 審慎討論：許多監理機關在審慎檢討中更加重視和關注科技和資訊安全風險以及營運韌性的討論，並就資訊安全和 IT 風險等數位化相關主題進行專題討論。

(6) 商業模式分析：監理機關表示，他們越來越關注瞭解新興的商業模式，並評估和理解非傳統商業模式如何對銀行業的安全和穩健構成風險。

監理機關亦可更多的利用科技，包括監理科技工具，以增強其監督能力並提高監督決策的效率。監理科技工具有許多不同的形式，但一些常見的包括文本分析和摘要、情感分析、市場監控和風險識別、信用風險工具、反洗錢調查中的異常值檢測以及某些監管流程的自動化。一些監理機關正在使用監理科技解決方案來改善監管要求和期望的溝通和清晰度，包括互動聊天式的「監管即服務」，使用人工智慧來回應受監理機關的問題。

6.7.1. 金融監理機關對系統性第三方依賴關係和潛在系統性風險的識別、監控和管理

方法

系統性第三方依賴即金融機構或整個金融系統對外部服務提供商的關鍵性依賴，通常集中在技術、數據處理或基礎設施等領域，由於許多金融機構依賴 Big Tech 來獲取關鍵數位服務，若 Big Tech 發生服務失效或營運中斷等其他問題，其影響可能會波及整個金融系統，對整體金融市場造成衝擊。

監理機關應識別系統性第三方依賴關係，並評估是否可能引起系統性風險。例如在該項系統性第三方依賴關係中，供應商的服務中斷或故障時，若同時影響多個金融機構或一個以上系統重要性金融機構，便可能產生系統性風險。

6.7.1.1.識別系統性第三方依賴關係

作為識別系統性第三方依賴關係的第一步，金融監理機關可以根據金融機構現行的業務情況來收集和彙整其服務供應商和服務狀況的相關資訊，編製清單紀錄關鍵服務供應商及其提供的關鍵服務進行分析。金融監理機關可以利用下列方式取得相關資訊來源：

(1) 依據《巴塞爾委員會作業韌性原則》，可審查銀行「交付關鍵服務所必需建立的內部和外部相互連結和相互依賴關係」之個體關係，其應包含「依賴關係，但不限於第三方」之類別；

(2) 金融機構的災害復原和清算計畫中(特別是持續營運與清算有關的章節)通常皆會列出關鍵服務項目和服務供應商；

(3) 金融監理機關亦可依各國監理狀況考量其他條件和資料來源。

6.7.1.2.市場集中度評估

儘管金融監理機關為了識別系統性第三方依賴關係，會根據其司法管轄範圍內金融產業的特點，而有不同的集中度評估結果，但各國監理機關整體而言，在集中度評估過程中亦可考慮以下因素：

(1) 系統性第三方服務的數量和組成：各金融機構從單一或相互關聯的服務供應商，所獲得的關鍵服務與 (如果可行) 非關鍵服務之數量、組成和特性。

(2) 系統性第三方服務的金融機構數量及該金融機構系統重要性：系統性第三方所服務的金融機構總數，並分別歸納出國內及全球性的系統重要性金融機構 。

(3) 相互依賴關係和間接依賴關係：在識別系統性第三方依賴關係時，金融監理機關可考慮服務供應商用於向金融機構提供服務的供應鏈。然而，對於供應商向金融機構

提供關鍵服務而言，並非服務供應商的完整供應鏈都至關重要，有些甚至可能不相關。金融監理機關還可以查核關鍵服務之間潛在的相互依賴關係。例如，個別服務供應商是否向金融機構提供一系列關鍵服務，或者多個關鍵服務是否依賴於一個不容易分割或替代的通用基礎設施。

6.7.1.3.瞭解什麼特徵可能增加服務中斷對於關鍵服務的影響

金融監理機關在識別金融機構何種服務委託屬於系統性第三方依賴關係時，可以根據服務中斷時，對於下列項目產生影響的嚴重程度進行考量：

(1) 金融機構提供金融服務的持續性、品質或穩定性，包括對消費者的影響；

(2) 金融機構本身的安全性和穩健性；

(3) 整體金融市場的穩定性和完整性。

如果考慮限縮「服務中斷或故障的相關來源」的範圍，則識別系統性第三方依賴關係、金融產業關鍵服務供應商、和潛在的系統性風險將可能會有更高的效率，例如：

(1) 運營中斷或失效：金融監理機關應假設運營中斷可能發生。然而，上述中斷的程度和嚴重性可能取決於受影響的關鍵服務和服務供應商的應對和恢復能力，以及金融機構和服務供應商的風險抵減行動；

(2) 服務供應商財務狀況惡化：與金融機構的情況一樣，財務狀況惡化可能會成為持續向金融機構提供關鍵服務的一項挑戰，但可以通過適當的規劃和保障措施來減緩，類似於 FSB 發布之《Guidance on Arrangements to Support Operational Continuity in Resolution》中涵蓋的措施。

6.7.1.4.用於識別系統性第三方依賴關係的工具

全面且可靠的資料對於監理機關識別系統性第三方依賴關係至關重要。金融監理機關可以通過各種舉措獲取此類資料，包括但不限於：

(1) 金融機構主動對於重大服務委託第三方的通報：根據各國對於金融機構委託第三方服務的相關規範，當金融機構有關於涉及重大委外服務項目的申請核准、重大變更或合約終止時，監理機關應收到相關通報或請求核准的通知。

(2) 審視金融機構的登記清單：金融監理機關可以定期收到金融機構最新的第三方服務關係的完整或部分的登記清單，並檢視有關金融機構關鍵和/或非關鍵服務的資料。

(3) 事故通報：金融監理機關可能會不定期接獲通知並審閱影響關鍵服務或服務供應商的事故通報。

6.7.1.5.金融監理機關識別和管理潛在系統性風險的工具

鑑於各國的法律和監管制度不同，原則上金融監理機關可以通過以下方式來識別和管理第三方依賴關係引起的系統性風險：

(1) 金融監理機關、金融機構和相關服務供應商自願合作;

(2) 監理機關將相關要求直接規範在金融機構與第三方服務供應商的服務協議之中;

(3) 監理機關直接對金融產業關鍵服務供應商進行規範。

6.7.1.6.金融監理機關、金融機構和服務供應商之間的對話

金融監理機關可以發起或加強與金融機構和金融產業關鍵服務供應商的對話及交流 (在各別司法管轄區內以及跨境的基礎之上)，以識別整個產業的趨勢、良好作法、金融監理機關在管理潛在系統性風險的能力與所面對的挑戰、以及應對這些挑戰的可行方法。

6.7.1.7.金融業的服務中斷演練和事故回應協作框架

金融產業的關鍵服務供應商，可以參與旨在加強金融產業整體應對服務中斷並從服務中斷中復原的相關演練測試或計畫。例如：

(1) 金融產業的辦理演練；

(2) 確認復原計畫的有效性(如:透過桌面演練)聯合查核活動；

(3) 事故回應協作框架側重於金融產業或關鍵基礎設施 (包括但不限於金融服務)。

部分國家已制定相關框架，促進整個金融產業對運營中斷的協作與應對。這些框架同樣可以由金融監理機關、私部門、或兩者的結合來領導，並且通常與跨產業事故回應措施和在跨國的交易對手相連結。案例包括：

(1) 英國的 Cross Market Operational Resilience Group (CMORG) 和 Services Cyber Collaboration Centre (FSCCC);

(2) 美國的 Financial and Banking Information Infrastructure Committee (FBIIC)和 Financial Services Information Sharing and Analysis Center (FS-ISAC);和

(3) 義大利的 Unit for business continuity (Codise)和 Financial Sector Computer Emergency Response Team (CERTFin)。

各國監理機關亦可要求金融產業關鍵服務供應商通過以下方式參與：

(1) 要求金融產業關鍵服務供應商內部設置組織或指派相關人員，在發生相關服務中斷時配合國內營運中斷治理框架進行共同協作;

(2) 要求金融產業關鍵服務供應商為金融產業制定營運中斷相關協作和溝通計劃，後續可因應產業需求整合至範圍更大的危機應變計劃中。

6.7.1.8.金融監理機關的覆核

金融監理機關可以根據國際、特定司法管轄區或量身訂製的原則，評估金融產業關鍵服務供應商及其服務韌性。例如：

(1) CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) 的附件 F 概述了對關鍵服務供應商的五項監督期望，以支援 FMI 的整體安全性和效率。

(2) BCBS 營運韌性原則和 BCBS 的 Sound Management of Operational Risk 原則，包含幾項直接和間接相關的原則，與銀行使用服務供應商提供的關鍵服務有關。在金融監理機關視為產生系統性第三方依賴的關係之中，對服務供應商而言，從遵守這些原則有無助益的角度，考慮其向銀行提供服務的方式，可能會是一種好的做法。

(3) IOSCO《Principles on Outsourcing》（2021 年）包括一套針對證券市場參與者的基本準則和七項原則。基本準則涵蓋了最重要的問題，特別是符合比例原則以及對重要性和關鍵性的評估。七項原則規定了對金融機構的期望，並包括根據第三方服務的重要性和重要性實施指引。這些原則適用於在證券市場中廣泛的參與者，包括許多中小型金融機構，也因此對關鍵和非關鍵第三方服務，提供了一套符合比例原則的期望。

6.7.2. 跨產業監理

監理機關與其他公私部門參與者就數位化相關主題和感興趣的領域進行越來越多的接觸和交流，鑑於數位化的跨產業和全球化性質，國內外監理機關和國際標準制定機構的合作變得越來越重要。由於數位化的許多因素引發了更廣泛的公共政策問題，監理機關注意到審慎監管與下列議題之間的界限變得模糊，例如消費者保護、市場競爭/反壟斷、金融犯罪以及與監理機關密切合作的必要性。監理機關透過國際論壇和其他國家或組織交流，就共同關心的議題與同產業的監管者積極合作。

許多監管者也認知到與產業、科技專家和學術機構在數位化方面密切合作的重要性。其合作有多種形式可以參考，包括就特定主題 (例如資訊安全風險和營運韌性) 舉辦雙邊或全產業的交流，以及就創新議題進行公開討論以促進監理機關和產業之間的互動。一些監理機關建立論壇或產業夥伴關係，以探討特定科技和議題，並制定相對應風險管理原則或指引，其他監理機關則與業界合作開展特定主題的試行專案。一些監理機關還會定期與非銀行公司 (例如關鍵服務供應商) 進行交流，討論最新的風險、趨勢和發展。

如前所述，數位化引發的問題超出了審慎監管的範圍，包括公共政策目標，如保護資料隱私、資訊安全、消費者保護、促進市場競爭和遵守反洗錢/反恐怖主義融資。銀行監理機關和其他相關監理機關和公部門之間的溝通和協調，無論是在司法管轄區內還是在不同司法管轄區之間，對於解決上述議題而言都很重要。隨著科技發展出現越來越多跨境作業，國際合作也有助於促進有效應對措施，並減緩了監管不完善可能帶來的風險。可考慮通過改善現有的監督協調和資訊共享來加強金融穩定。

6.7.3. 跨境監理

通過各國監理機關之間的協調、協作和資訊共享，可以更有效地管理全球金融體系的系統性第三方依賴關係和潛在系統性風險。任何特定司法管轄區的金融監理機關在識別、監控和減輕系統性第三方依賴關係、以及國際運作的服務供應商構成的潛在系統性風險方面的能力都受到限制。然而，在加強第三方服務關係方面的合作可能會面臨挑戰，例如：

(1) 因金融監理機關的任務、立法、組織結構和框架間的差異，不同司法管轄區的金融監理機關通常有不同的監管框架、法律要求、監管做法和資源配置模式。因此各國對金融機構第三方服務供應商（或金融產業關鍵服務提供者）的控管可能大不相同；

(2) 因各國監理機關之間共同合作的經驗有限，故在協調各地監管活動以確保跨境監理的一致性和有效性上，將會是未來各國監理機關的一大挑戰；

(3) 第三方供應商資料庫留存資訊可能非常敏感，根據現有的合約條款或其他法律遵循要求，可能需要獲得額外權限以存取或使用資訊。未經同意共用機密資訊可能會使金融監理機關、金融機構或服務供應商面臨法律和聲譽風險，對機敏資訊的不當處理亦可能增加資訊安全和其他營運風險。

針對系統性第三方依賴關係，探討監管和監督框架之間更大程度融合的可能性。金融監理機關可考量直接參考其他地區金融監理機關的審查結果(例如查核、營運持續演練和測試)，如此便可更有效地利用各國金融監理機關的資源。從金融產業關鍵供應商的角度來看，亦可最大限度地減少重複受審的情況，可直接參考的條件如下：

(1) 服務供應商向兩個司法管轄區的金融機構提供的關鍵服務相同或非常相似；

(2) 金融監理機關願意分享自行或委託第三方機構執行審查之結果；

(3) 該項審查結果符合其他地區監理機關的目標、需求及所需資訊。

6.8. 具體監理建議

根據本次調研對國外監管方式的分析，結合對本國銀行及外國銀行在台分行進行的問卷調查結果，並考量金融監管機構直接監管 Big Tech 的適切性及我國現況，本章節聚焦於由金融監管機構主導的 Big Tech 監管模式，分析我國面臨與 Big Tech 相關之風險並提出因應措施，且針對台灣現況，提出具體的法規修正建議。

6.8.1. Big Tech 相關之風險與因應建議

在 Big Tech 提供多面向數位化技術應用的同時，為金融服務帶來了許多機會，但也同時對金融穩定帶來潛在風險。綜整本次調研所提及之國際關注風險、本國問券調查銀行業所反饋其面臨之風險，以及評估台灣現況，就 Big Tech 提供銀行服務，在銀行業所面臨之主要風險，提出因應建議如下。

6.8.1.1. 集中度風險

根據本次對本國銀行與外國銀行在台分行問卷調查的結果顯示，在 56 間銀行的回覆，有 60.7%採用 Big Tech 所提供的服務，且其中將進九成採用的是 Big Tech 所提供的雲端服務。市場研究機構 Synergy Research Group 於 2024 年 4 月發布的報告中指出，目前全球前三大雲端服務供應商(亞馬遜 AWS、微軟 Azure、Google)合計市占率接近七成，因此若前述公司發生服務中斷，將可能會導致整個銀行和金融系統的重大中斷。鑑於銀行業於問卷中也表示，未來規劃將持續擴大採用相關服務，故金融監管機構可採取對於潛在集中度風險的因應措施。

為因應此風險，各銀行業者僅能就自身使用 BigTech 所提供之銀行服務分析，尚不足以使個別金融機構瞭解產業整體及中度及業務關聯性等情形，需透過金融監管機構蒐集 Big Tech 服務提供情形以瞭解銀行產業總體概況，達強化對第三方服務提供商依賴關係及潛在系統性風險的識別、監控和管理，下列監理措施能協助金融監理機關有效追蹤及因應相關風險變化。

(1.) 金融監管機構可根據金融機構現行的業務情況，收集和彙整其服務供應商和服務狀況的相關資訊，編製清單紀錄關鍵服務供應商及其提供的關鍵服務進行分析，以識別系統性第三方依賴關係。金融監管機構可以通過各種方法獲取此類資料，包括但不限於：

i. 金融機構主動對於重大服務委託第三方的通報;

ii. 定期審視金融機構最新與第三方服務關係的完整或部分的登記清單

iii. 不定期接獲通知並審閱影響關鍵服務或服務供應商的事故通報

(2.)根據台灣司法管轄範圍內金融產業的特點進行集中度評估，而對各國監理機關而言，可能有不同的集中度評估結果。在集中度評估過程中，建議考慮以下因素，例如第三方所服務的金融機構總數及該金融機構系統重要性、相互依賴關係和間接依賴關係等。

(3.)瞭解哪些特徵可能增加服務中斷對關鍵服務的影響。建議根據服務中斷時對以下項目產生影響的嚴重程度進行考量：

i. 金融機構提供金融服務的持續性、品質或穩定性，包括對消費者的影響；

ii. 金融機構本身的安全性和穩健性；

iii. 整體金融市場的穩定性和完整性。

6.8.1.2. 系統性風險

當 Big Tech 提供新技術及應用迅速擴展至金融服務領域，因金融系統內部的互聯性與複雜性增加，將導致金融市場中的風險傳染性升高，提高銀行體系和金融穩定的系統性風險。雖然根據本次調研的問卷結果顯示，銀行業有 60.7%採用 Big Tech 所提供的服務，然其他尚未採用者也表示未來規劃將持續探索新技術，以提升金融服務的創新和效率，然而整體金融產業若存在集中化風險及依賴少數供應商的供應鏈風險時，將發生單一供應商無法提供服務時，可能發生連鎖效而造成多數金融機構面臨營運中斷風險，進而衍生營運、聲譽風險，並影響整個金融體系穩定。

為因應潛在的系統性風險，鑒於各國的法律和監管制度的差異，金融監管機構可以通過以下方式來識別和管理第三方依賴關係引起的系統性風險。

(1) 推動金融監管機構、金融機構和相關服務供應商之間自願合作。

(2) 監理機關將相關要求直接規範在金融機構與第三方服務供應商的服務協議中。

(3) 直接對金融產業關鍵服務供應商進行規範。

金融監管機構應發起或加強與金融機構和金融產業關鍵服務供應商的對話及交流，以識別整個產業的趨勢與良好作法，並分析金融監管機構在管理潛在系統性風險的能力與所面對的挑戰，以及應對這些挑戰的可行方法。此外，金融監管機構應確保並加強金融產業整體應

對服務中斷並從中復原的相關演練測試或計畫，例如：

(1) 辦理演練；

(2) 確認復原計畫的有效性聯合查核活動；

(3) 事故回應協作框架。

6.8.1.3.消費者保護風險

相較於金融機構已有較嚴謹的監管規範，對 Big Tech 在監管要求相對寬鬆，因此在客戶資料保護上容易面臨較高的風險。由於數位化帶來的挑戰超越了傳統審慎監管的範疇，涵蓋資料隱私保護、資訊安全及消費者權益等問題。從本次調研的問卷結果中也顯示，76.8%的銀行視資料隱私保護議題為銀行與 BigTech 合作上主要顧慮之一。

為有效應對上述風險，銀行監理機關可加強與其他相關監理機關例如消費者保護委員會、個人資料保護委員會、數位發展部與外國銀行監理機關等，建立更緊密的協作關係。隨著科技持續發展及跨境活動的增加，跨部會與國際間的合作不僅能推動有效的應對措施，還能減輕監管空隙所可能帶來的風險，建議透過加強現有的監督協調與資訊共享，具體包括建立跨監理機關的協調機制，定期舉行會議分享監管資訊與最佳實踐，以進一步提升金融穩定性。

6.8.1.4.銀行業於問卷中反映之主要風險、挑戰與期望

(1) 廠商服務中止風險

在已採用 Big Tech 服務之銀行中，82%表示希望要求廠商對於服務中止情況提出對應措施，以降低服務中止情況所造成的風險與衝擊。

針對服務終止應對流程，歐盟 DORA 強調金融機構應制定 ICT 服務供應商退場策略，以應對必要條件下合約終止的情況，並制定適當措施避免合約終止後業務產生重大影響。英國 CP26/23 則直接控管關鍵第三方，要求廠商建立服務終止應對程序並建立服務終止後，原委託機構對服務內容的取得、收回、返還的相關規定。

(2) 緊急應變措施演練計畫

在已採用 Big Tech 服務之銀行中，79%之銀行希望要求廠商配合緊急應變措施演練計畫，以進一步強化現行措施，降低委外風險，此與第 6.8.1.2 提到緩解系統性風險的措施相呼應。

歐盟 DORA 強調針對演練測試，測試應涵蓋金融機構委外第三方的所有關鍵系

統、流程和技術，並在其實際運行的系統上執行測試。同時，測試人員應具備相關專業條件，確保該人選已利益迴避並且經主管機關核准。英國 CP26/23 則直接控管關鍵第三方，其要求包括：

i. 廠商定期進行情境測試，以測試其最大容忍程度及持續提供服務之能力，並確保情境與實際狀況一致。

ii. 依據測試結果調整應對措施，並產出測試結果報告提供主管機關。

iii. 監理機關如有需要可要求關鍵第三方提供相關測試資訊。

(3) 系統更新與事件通報措施

在已採用 Big Tech 服務之銀行中，76%之銀行希望要求廠商對於系統更新與事件通報措施。

歐盟 DORA 對於事件通報，要求第三方服務提供商應建立可向金融機構即時報告的管道;美國則定義在電腦安全事件持續四小時以上或該事件可能對提供給銀行機構的服務造成實質性影響時，第三方服務供應商應儘快通知受影響銀行機構。此外歐盟 DORA 也要求金融機構對於事故須提出初步、中期及最終報告，並提交至相關監管機關以及相關團體。

(4) 資料隱私保護、市占下滑、用戶流失風險

對於銀行與 Big Tech 大型科技公司合作帶來的主要風險，76.8%的銀行視資料隱私保護為其主要疑慮，25%的銀行認為市占下滑/市場瓜分為其考量的風險之一，23.2%的銀行視用戶流失為其主要風險之一。

資料隱私保護議題與第 6.1.8.3 中提到的消費者保護風險相互呼應。為有效應對此風險，銀行監理機關必須加強與其他相關監理機關及公部門的合作，並強化國際間的合作，這不僅能推動有效的應對措施，還能減輕監管空隙所可能帶來的風險。針對可能造成的市占下滑和用戶流失風險，主管機關可透過鼓勵創新、促進資源交流如辦理研討會及人才培育等方式，協助提升銀行業的競爭力。

6.8.1.5.借鏡國際重大風險事件

鑒於國際所發生的 Capital One 資料洩漏事件、Kakao 服務中斷事件對金融服務所造成之影響，藉由歷史經驗的學習與反思，可借鏡國外監理機關面對此類事件從事前、事中及事後三面向強化相關風險的控管措施。

(1) Capital One 資料洩漏事件：

i. 事前：推動雲端服務相關規範和風險評估，確保金融機構在採用新技術前已建置充分的網路安全控制、強化人員專業能力培訓，並加強其董事會對網路安全的監督責任。

ii. 事中：建立即時通報機制和事故應變計畫，確保在資料外洩或安全事件發生時能迅速採取措施，減少對客戶資料和金融服務的影響。

iii. 事後：釐清責任歸屬，對應負責的金融機構和服務供應商採取懲罰或補救措施，檢討現行法規並加強對雲端服務供應商的監管，以防範未來類似事件。

(2) Kakao 服務中斷事件：

i. 事前：要求大型科技公司建立完善的災害復原中心並定期演練，推動資料中心防火安全規範，以確保關鍵金融服務的持續運作。

ii. 事中：確保金融機構建立即時通報機制和跨部門協調，以在事故發生時迅速啟動應變計畫，優先恢復關鍵金融服務，減少對客戶及其服務的影響。

iii. 事後：釐清事故責任並制定賠償機制，檢討現行法規並進行全面的事後評估以改善未來應變措施，提升數位金融營運的韌性。

6.8.2. 監理框架建議

鑒於 Big Tech 憑藉其在全球網路平台及數據主導優勢、龐大客群網絡、新技術創新的領先性等優勢，導致金融機構與 Big Tech 之間談判力道不足，除金融機構須對第三方業者進行監管外，更需透過金融監理機關的協助對 Big Tech 進行直接監理，以有效管理 Big Tech 所產生的系統性風險與依賴性。參酌國際清算銀行(BIS)提出基於業務活動(Activity-Based, AB)與基於實體(Entity-Based, EB)的監管方針結合使用，建議將監管框架分為短期、中期及長期逐步推進，最終達成混合的監管框架，既規範特定業務活動的風險，亦掌握 Big Tech 作為金融機構第三方服務提供商的系統性風險，以確保金融監管的靈活性、全面性與協調性，從而進一步維持市場的穩定性。

(1) 短期監管框架：加強揭露

金融監理機關應要求 Big Tech 加強其對金融服務風險的揭露，包括無法量化的風險，如提供相關服務對於金融機構的營運風險和聲譽風險等。此外，建議對於金融

機構與第三方服務提供商的依賴關係與供應鏈評估，根據金融機構現行的業務情況，收集並彙整其服務供應商及服務狀況的相關資訊，編製清單紀錄關鍵服務供應商及其提供的關鍵服務並進行分析，以識別銀行業對第三方服務供應商依賴關係與潛在風險，從而進一步規劃和設計符合台灣金融市場需求的監管指標及應對措施。

(2) 中期監管框架：制定產業自律規範

在短期監管框架下，透過資料蒐集與分析，若評估現行委外框架不足，可進一步訂定自律規範。產業自律規範能在監管資源尚未充分完善時，迅速提供市場保護，減少未受監管業務可能帶來的風險。例如，要求承擔風險管理責任、保障消費者資金與資料等。監管機關可根據其在母國或業務所在地的不同監管角色與需求，制定適合當地市場的自律規範。

然而，監管機關需注意自律規範可能產生的光環效應（Halo Effect），即當服務使用者瞭解到 Big Tech 已受此規範時，可能誤認為金融市場已具備完整的監管框架與風險控管機制。如果此時發生與 Big Tech 相關的重大事件導致市場或使用者權益受損，將可能對監管機關的聲譽帶來負面影響。

(3) 長期監管框架：混合式監管

在長期規劃上，應明確的劃分出 Big Tech 企業實體母國及商業活動所在國，個別根據 AB 及 EB 的監管方針適當的混合調整。鑑於 Big Tech 跨產業的特性，使其受到多個監理機關的管轄，形成涉及跨部會、跨監理機關管轄範圍、甚至跨國共同監管的複雜組合，故監理機關間需進行充分溝通協調，以推派最適的監理機關。

若採 EB 監管框架建議可參考 5.1.1.1 DORA 對關鍵 ICT 篩選標準、5.2.1.1 英國 CP26/23 對關鍵第三方篩選標準，定義符合台灣需求之具 Big Tech 標準的關鍵第三方，依據評估及對 Big Tech 在台灣業務發展觀察與經驗，評估進一步對該企業實體採取 EB 監管方針。若作為 Big Tech 母國的監理機關時，應加強與國際組織、國內其他監理機關及全球業務所在地的監理機關之間的監管交流。另外，國際監管合作與資訊共享是緩解 Big Tech 跨境營運風險的有效方式，可協助改善金融機構與國際間大型科技業者之間談判力道不足的問題，並可減少其跨足不同市場時所產生的監管摩擦，建議可明確劃分 Big Tech 企業實體的母國與商業活動所在國，並根據 AB 和 EB 的監管方針進行適當的混合調整。

6.8.3. 法規修正建議

主管機關往往針對金融機構使用之特定業務活動以專法或產業自律規範進行監管，也是現行在規範 Big Tech 業務活動上相對完整的部分，包含常見之委外服務、雲端服務

與 AI 服務等，如我國金融監督管理委員會已頒布之《金融機構作業委託他人處理內部作業制度及程序辦法》與《金融業運用人工智慧(AI)指引》、中華民國銀行商業同業公會全國聯合會公布之《金融機構運用新興科技作業規範》與《金融機構作業委外使用雲端服務自律規範》等，針對第三方業者的監督管理，金融機構應對自身較無控制權的部分或事項，與合作廠商明訂風險監控的責任分工。另借鏡國際間實務作法，現行國際間對 Big Tech 監管方式有分成透過金融機構間接監理及金融監理機關直接監管兩種方式，台灣現行金融機構對於第三方業者的管理係採透過金融機構間接監理模式，經分析、比較《金融機構作業委託他人處理內部作業制度及程序辦法》與國際間法規要求，將監管措施建議分類如下表：

與國際間接監理控管強度相同之監管措施	可借鏡國際提高間接監理控管強度之監管措施	對關鍵第三方直接監管措施
(1) 盡職調查 (2) 事故管理 (3) 委外合約 (4) 科技和資訊安全韌性風險管理	(1) 治理架構建議可增加要求規劃教育訓練或人員培訓計畫。 (2) 風險管理建議金融機構新增確保關鍵第三方業務執行端、風險控管和內部稽核之間的獨立性。 (3) 建議金融機構在事故通報上須提出初步、中期及最終報告，並在收到每份報告後提交至相關監管機關以及相關團體。 (4) 針對演練測試可增列較詳細之說明，如：測試應涵蓋金融機構委外第三方的所有關鍵系統、流程和技術，並在其實際運行的系統上執行測試；或測試人員應具備相關專業條件，確保該人選已利益迴避並且經	(1) 要求關鍵第三方辦理營運持續的資源盤點。 (2) 需在業務所在國設有分公司或指派與監理機關聯繫的窗口。 (3) 要求關鍵第三方提交書面自我評估報告。 (4) 在事故管理上，要求關鍵第三方服務提供商建立可向金融機構及時報告的管道。 (5) 關鍵第三方應研擬變更的風險控管與失敗補救措施，並在變更計畫實施後應定期監控。 (6) 要求關鍵第三方有效識別與管理依賴關係與供應鏈風險。

	主管機關核准等。 (5) 變更管理建議新增確保金融機構建立關鍵第三方服務系統變更的相關控管措施，以確保在金融機構的控管下完成所有程序，且變更管理流程應由高階管理層批准。	

在借鏡國際間接監理控管措施上，於表中提出在現行監管措施基礎上，可進一步加強控管力度的必要措施，鑑於台灣目前採間接監理形式，故此類措施可行性高。主要針對治理架構、風險管理、事故通報、測試演練及變更管理等領域，透過參考各國的控管要求，提升對於控管措施的細緻度。在治理架構方面，強調金融機構應規劃更完善的教育訓練與人員培訓；風險管理上，則著重於強化金融機構能確保其關鍵第三方的稽核獨立性；事故通報與演練測試上，要求金融機構提出事故報告至相關監管機關以及相關團體，且將測試演練增列較詳細之說明並確保測試人員之專業能力；變更管理上，則建議金融機構建立更嚴謹的控管機制，確保關鍵第三方服務的系統變更均在控管程序下完成，且流程需經由高階管理層批准，以降低系統之風險。

現行台灣對委外管理雖採間接監理方式為主，未來在中長期監管框架設計上，若評估需進一步強化對關鍵第三方之控管以全面提升監管效能與深度，可參考國際對於關鍵第三方的直接監管措施。金融監理機關對提供金融機構服務的關鍵第三方業者可參考下列控管建議：

i. 確保營運持續的資源盤點：資源盤點能協助識別並評估關鍵資源的充足性與可靠性，確保關鍵第三方擁有足夠的技術、基礎設施及人力資源來應對各種突發狀況以避免服務中斷。資源盤點有助於金融機構更好地評估第三方的應變能力，且及早發現潛在風險，防範於未然。英國已將確保關鍵第三方營運持續的資源盤點納入其監管措施。

ii. 需指派與監理機關聯繫的窗口：可參考英國 CP26/23 有要求關鍵第三方需設立與監理機關聯繫的窗口之要求，由關鍵第三方設置與該業務務活動所屬產業監理機關之聯絡窗口，能夠增強監理機關與第三方之間的溝通效率，這有助於提升監管透明度，並使第三方服務提供商能夠快速回應金融機構或監管要求。。

iii. 提交書面自我評估報告：定期提交自我評估報告可提升關鍵第三方之營運

透明度，能協助金融機構及時掌握第三方的合規狀況，並促使第三方服務提供商主動檢視並改善自身的運營和風險控管能力。英國 CP26/23 已將要求關鍵第三方提交書面自我評估報告納入其監管措施。

iv. 建立事故發生時向金融機構及時報告的管道：此機制能確保關鍵第三方迅速報告事故，確保金融機構能及時瞭解狀況並進行應對，以有效縮短事故回應時間，減少潛在損害，並有助於事後改進措施的制定。歐盟 DORA 與美國已將相關事故通報納入其監管措施。

v. 研擬變更的風險控管與失敗補救措施，並在變更計畫實施後定期監控：此措施能減少系統或服務變更帶來的潛在風險，有助於加強金融機構對第三方的風險掌控，並確保其服務穩定性。英國 CP26/23 已將相關變更管理措施納入其監管措施。

vi. 要求關鍵第三方有效識別與管理依賴關係與供應鏈風險：有效的依賴關係與供應鏈風險管理對於確保業務運作的穩定性至關重要。服務提供商可建立全面的風險識別系統，定期評估其供應鏈中各項依賴關係的可靠性，並確保擁有足夠的技術和資源來應對潛在的風險與挑戰。英國 CP26/23 已將相關變更管理措施納入其監管措施。

參考文獻

1. Sebastian Doerr, Jon Frost, Leonardo Gambacorta, Vatsala Shreeti. (2023) Big techs in finance (No WP1129). Bank for International Settlements.

2. Basel Committee on Banking Supervision. (2021). Principles for Operational Resilience. Bank for International Settlements.

3. Basel Committee on Banking Supervision. (2024). Digitalisation of finance. Bank for International Settlements.

4. The Financial Stability Board. (2023). Final Report on Enhancing Third-Party Risk Management and Oversight – a Toolkit for Financial Institutions and Financial Authorities.

5. The Financial Stability Board. (2020). BigTech Firms in Finance in Emerging Market and Developing Economies.

6. Parma Bains, Nobuyasu Sugimoto, and Christopher Wilson. (2022). Big Tech in Financial Services: Regulatory Approaches and Architecture. International Monetary Fund.

7. Borio, C, S Claessens and N Tarashev. (2022). Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs. SUERF Policy Brief, no 404.

8. Carstens, A, S Claessens, F Restoy and H S Shin. (2021). Regulating big techs in finance, BIS Bulletin, no 45, August.

9. Crisanto, JC, J Ehrentraud, A Lawson and F Restoy. (2021). Big tech regulation: what is going on? Bank for International Settlements, Financial Stability Institute.

10. Feyen, Erik, Jon Frost, Leonardo Gambacorta, Harish Natarajan, and Matthew Saal. 2021. “Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy.” BIS Papers No. 117, Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/ bppdf/bispap117.pdf.

11. IOSCO (2021), Principles on Outsourcing.

12. Parma Bains, Nobuyasu Sugimoto, and Christopher Wilson. (2022). Big Tech in Financial Services: Regulatory Approaches and Architecture. International Monetary Fund.

13. Richter, Felix. (2021). “Amazon Leads $150-Billion Cloud Market.” Statistica, July 5, 2021. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers.

14. Digital Disruption in Banking and its Impact on Competition (2020)

15. BIS Working Papers Big Techs in Finance (2023)

16. Deloitte. Critical third parties (CTPs) – a detailed UK regulatory framework emerges

17. Deloitte. Operational resilience and critical third parties: A year of real tests

18. Deloitte. DORA & Third-Party Risk Management

19. Deloitte. A key development in the regulation of critical third party suppliers to the financial services sector

20. Deloitte. Financial services on the Cloud: the regulatory approach

21. Deloitte. Cloud and regulation

22. Deloitte. Financial services cloud computing regulation: Cloud security risk management principles

23. Deloitte. FFIEC statement on risk management for cloud computing services

24. Deloitte. Regulatory barriers to the Cloud in financial services: perceived or real

25. Deloitte. All eyes on the cloud: Regulatory shake up agreed in EU, UK investigation ongoing

26. Deloitte. Federal banking agencies propose updated guidance on third-party risk management

27. Deloitte. Interbank ecosystems: Accelerating the transformation of banking services

28. Deloitte. Accelerating digital transformation in banking and capital markets with industry clouds

29. Deloitte. Realizing the digital promise: Transformation in an ecosystem of regulators, BigTech, FinTech and more