雲端共享責任與針對委外法令遵循之因應

AWS Compliance and Audit

Queena Tsai

FSI BDM, AWS

tsaiwan@amazon.com

© 2022, Amazon Web Services, Inc. or its Affiliates.

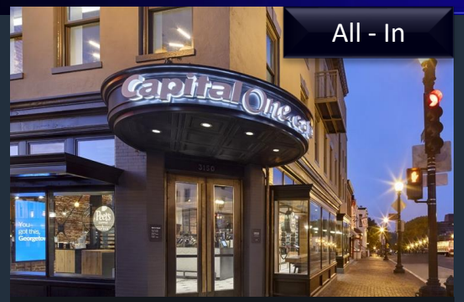
AWS re:Invent 2021 re:Invent 全球大型金融機構公開分享案例

數家大型金融機構持續將 AWS 作為長期數位轉型戰略合作夥伴

Outposts

Nasdaq 宣布將其部分交易平台遷移上雲, 因極低延遲的要求, 將使用Amazon Outposts建立全球地區之Private Local Zone.

All - In



Capital One 完成遷移其數據中心到 AWS

Capital One completes its data center migration to AWS

核心系統



Standard Chartered Bank搬遷其核心銀行系統Atlas上雲, 資料庫從DB2搬遷至Amazon Aurora, 增加系統穩定性與效能, 同時符合資安稽核規範.

模型運算

Globe Life

Global Life 打造雲端自助服務分析平台, 支持同時>10B紀錄與20個模型同時運算 (包含精算模型), 分鐘內產出助於業務決策之分析結果.

資料分析



CME Group 於雲端打造 data-ingestion pipeline, 使用事件導向與file-based設計架構 (AWS Step Functions, AppFlow, Lambda, EMR, Lake Formation)

核心系統



JPMorgan Chase 將其核心風控管理平台遷移上雲, 選用雲原生應用架構 (EKS, S3, RDS, ElastiCache for Redis), 加速 40% 運算效率.

交易查詢



Itaú Unibanco 搬遷其交易帳戶 Account Statement 系統上雲, 支持過去22年歷史資料文字查詢. (OpenSearch, Fargate, Lambda, DynamoDB)

應用搬遷



Guardian Life 建置Cloud-Native life insurance policy administration platform, 加速 time to market, 降低成本與增進客戶互動頻率

aws financial services

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

雲端服務於台灣金融市場常見的應用場景

隨著金融機構更好地了解在雲中運行的方法以及滿足法遵義務的能力，越來越多金融機構開始於雲端試驗各種應用場景與提出雲端合規需求。

As financial institutions better understand their ability to meet regulatory compliance obligations when operating in the cloud, they are increasingly focused on leveraging the cloud to transform existing businesses and bring innovative new solutions to market.



企業內部系統



開發測試環境



高效能運算



海外系統加速



公開網站
資安防護



公開圖資儲存
爬文平台



機器學習

現今被廣泛採用
Widespread adoption today

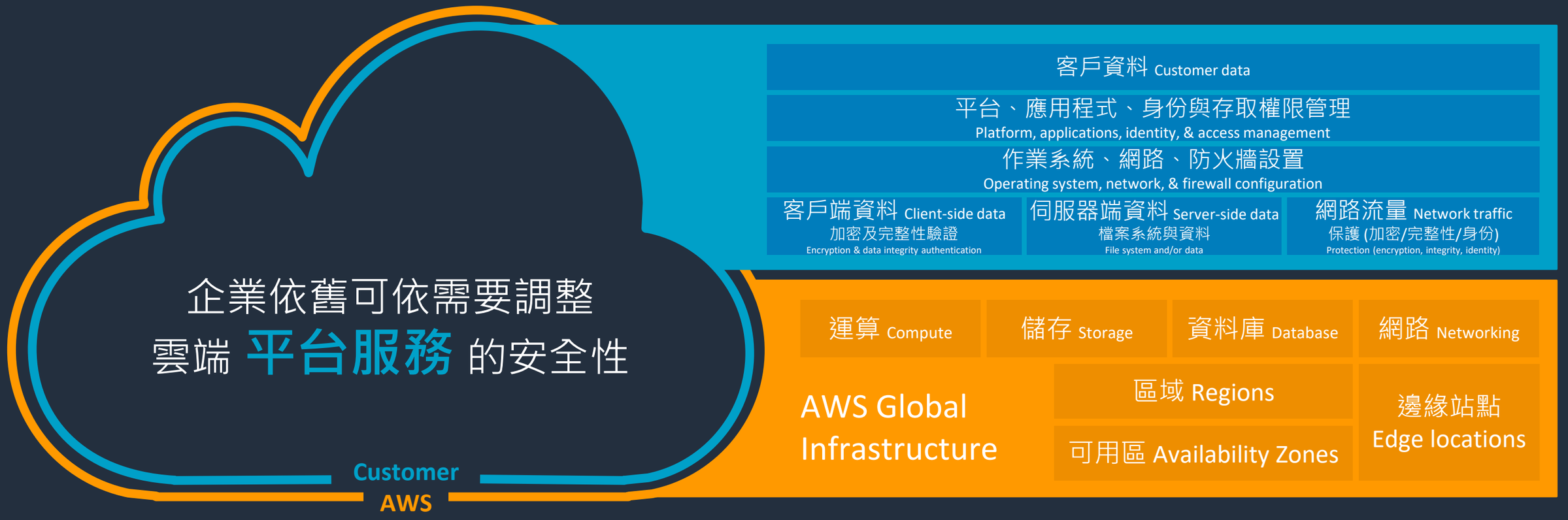
應用趨勢走向
Gaining traction

® 2021 Amazon Web Services Inc. or its Affiliates. All rights reserved.

aws financial services

AWS 共同責任模型 Shared responsibility model

AWS 協助打理基礎設施的安全，並保障企業完全控制雲端資產的自主性



Reference: https://aws.amazon.com/tw/compliance/shared-responsibility-model/

定期更新的雲服務安全性與合規認證

Inherit global security & compliance controls

SOC 1

SOC 2

SOC 3

CJIS

DoD SRG

FedRAMP

FERPA

SEC Rule 17a-4(f)

GxP

MPAA

My Number Act

VPAT Section 508

G-Cloud

https://aws.amazon.com/tw/compliance/programs/

https://aws.amazon.com/tw/compliance/data-privacy/

金融機構作業委託他人處理內部作業制度及程序辦法 第19-1條

行政 > 金融監督管理委員會 > 銀行目 | 修正日期：民國 108 年 09 月 30 日

風控與監督

金融機構將作業委託他人處理涉及使用雲端服務，應依下列規定辦理：

一、金融機構應確保作業風險控管，充分評估受託機構處理之風險，採取適當風險管控措施，確保作業委外處理之品質，並應注意作業委託雲端服務業者之適度分散。

二、金融機構對雲端服務業者負有最終監督義務，並應具有專業技術及資源監督雲端服務業者執行受託作業，並得視需要委託專業第三人以輔助其監督作業。



https://aws.amazon.com/tw/compliance/data-center/controls/

AWS 服務建構於完善規劃且高度安全的雲端基礎設施之上

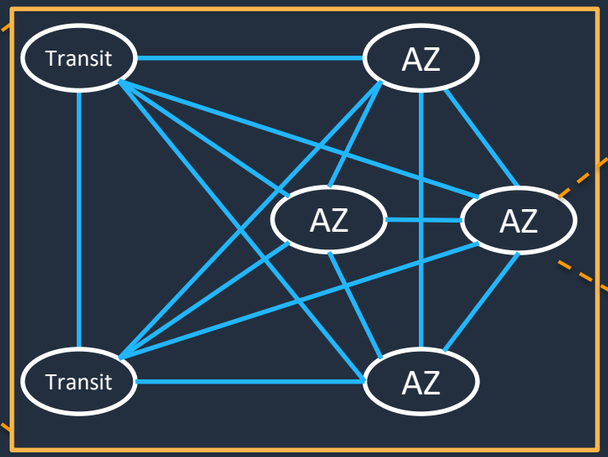
全世界最大的雲端基礎架構部署，採用一致的高可用性、可靠、耐用性及低網路延遲架構



地理區域 (Regions) 及
可用區域 (Availability Zones , AZ)

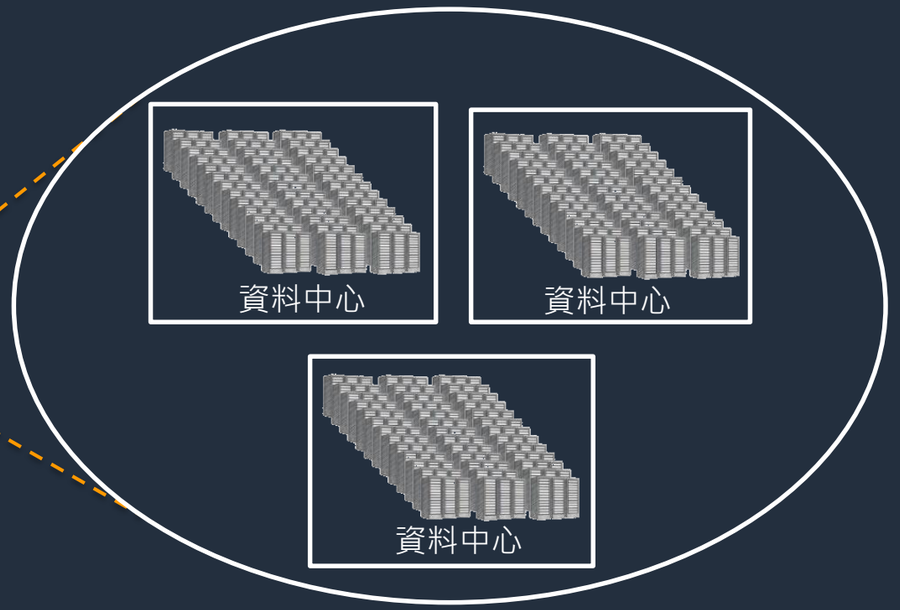
已公佈的佈建中地理區域
印尼、西班牙、日本

AWS Region



地理區 (Region) 是實際的地理區域，
在每個地理區域中建置有兩個(含)
以上的可用區域 (Availability Zones)

AWS Availability Zone (AZ)



可用區域 (AZ) 由一至多個獨立的資料
中心組成，且每個數據中心都具備有
冗餘的電源、網路與連線。

26 個地理區域 (Regions) 、 84 個可用區域 (Availability Zones, AZ)
410+ 個入網點 (Points of Presence, PoP)

https://www.infrastructure.aws/

aws

金融機構作業委託他人處理內部作業制度及程序辦法 第19-1條

行政 > 金融監督管理委員會 > 銀行目 | 修正日期：民國 108 年 09 月 30 日

認證及查核

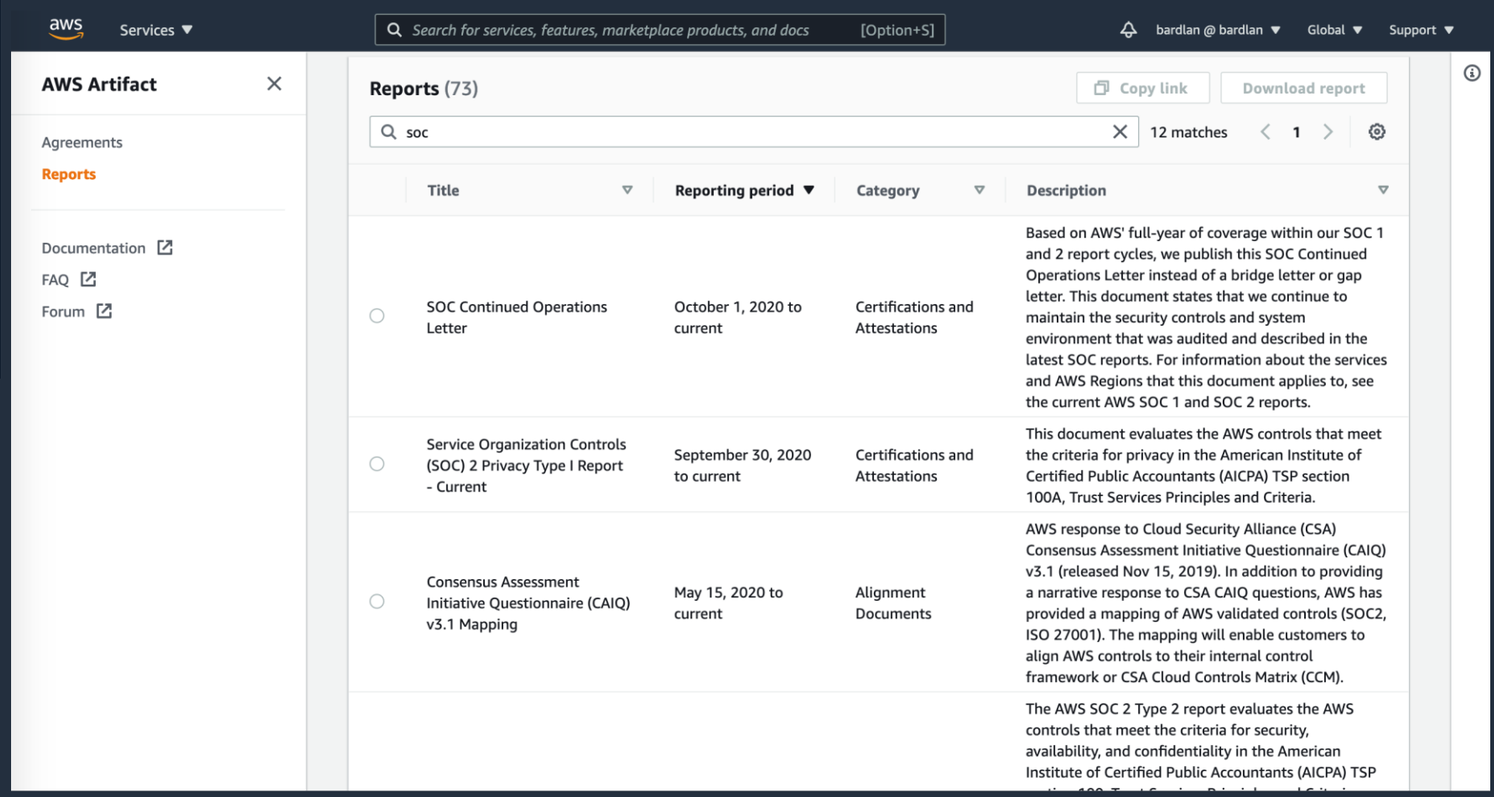
三、金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行受託作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。

四、金融機構得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核，並應符合下列規定：

（一）確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節。

（二）應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。

（三）應針對金融機構所委託作業範圍進行查核並出具報告。



https://aws.amazon.com/tw/artifact/

金融機構作業委託他人處理內部作業制度及程序辦法 第19-1條

行政 > 金融監督管理委員會 > 銀行目 | 修正日期：民國 108 年 09 月 30 日

資料加密保護

五、金融機構傳輸及儲存客戶資料至雲端服務業者，應採行客戶資料加密或代碼化等有效保護措施，並應訂定妥適之加密金鑰管理機制。



https://aws.amazon.com/tw/kms/faqs/



資料保護
Data Protection

除了自動數據加密與管理外，亦提供多種數據保護功能 (包含數據管理、安全性與加密金鑰保存)

In addition to our automatic data encryption and management services, employ more features for data protection (including data management, data security, and encryption key storage)



AWS Key Management Service (KMS)
輕鬆建立與控制用於加密數據的密鑰

Easily create and control the keys used to encrypt your data



AWS CloudHSM
AWS 雲上的託管硬體安全模組 (Hardware Security Module, HSM)

Managed hardware security module (HSM) on the AWS Cloud



Amazon Macie
大規模發現並保護企業的敏感數據

Discover and protect your sensitive data at scale



AWS Certificate Manager
輕鬆配置、管理與部署 SSL/TLS 證書以用於 AWS 服務

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services



AWS Secrets Manager
在生命週期內，輕鬆更換 (rotate) 管理與取得資料庫憑證、API密鑰及其他機密參數

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle



AWS VPN
將企業的在地網路延展到雲，並從任和地方安全的訪問

Extend your on-premises networks to the cloud and securely access them from anywhere



Server-Side Encryption
靈活使用 AWS 服務託管密鑰、AWS KMS 託管密鑰或客戶管理密鑰進行數據加密

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

金融機構作業委託他人處理內部作業制度及程序辦法 第19-1條

行政 > 金融監督管理委員會 > 銀行目 | 修正日期：民國 108 年 09 月 30 日

資料所有權

六、對委託雲端服務業者處理之資料應保有完整所有權，除執行受託作業外，金融機構應確保雲端服務業者不得有存取客戶資料之權限，並不得為委託範圍以外之利用。

七、委託雲端服務業者處理之客戶資料及其儲存地以位於我國境內為原則，如位於境外，應依下列規定辦理：

（一）金融機構須保有其指定資料處理及儲存地之權力。

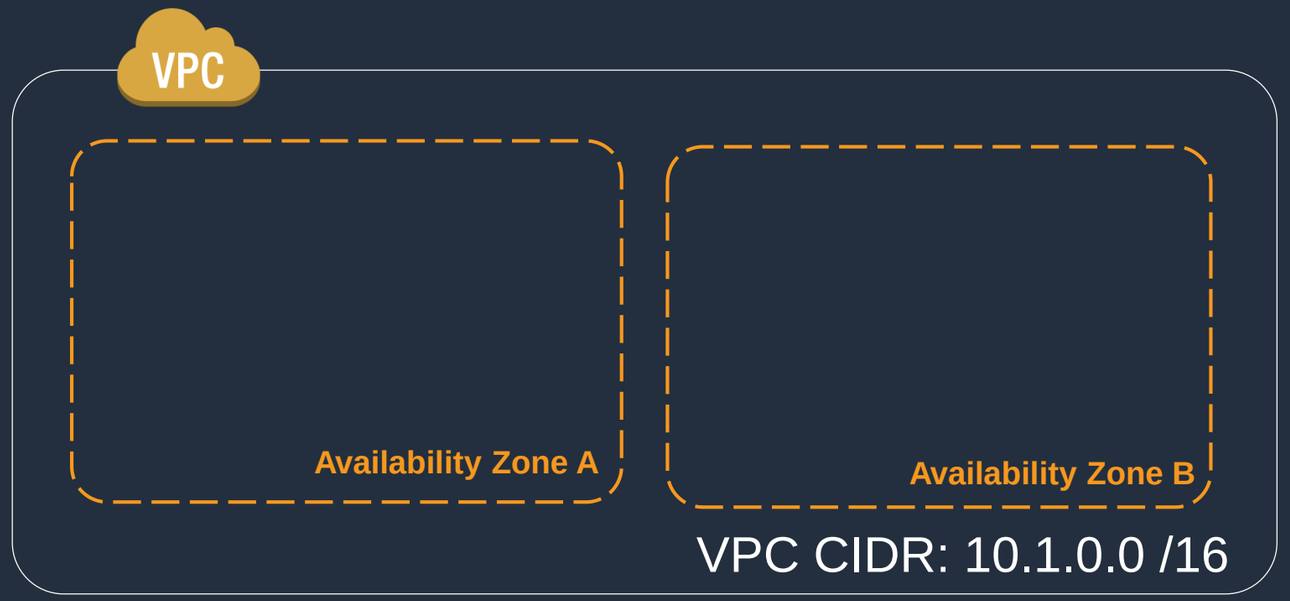
（二）境外當地資料保護法規不得低於我國要求。

（三）除經主管機關核准者外，客戶重要資料應在我國留存備份。



https://aws.amazon.com/tw/compliance/data-privacy-faq/

客戶指定AWS資料存放與處理之所在地



資料所在地

第 19–1.7 條允許委託雲端服務供應商在台灣境外儲存和處理客戶資料，但須符合下列條件：(一) 金融機構須保有其指定資料處理及儲存地之權力，(二) 境外當地資料保護法規不得低於台灣的要求，以及 (三) 除經主管機關核准者外，客戶重要資料應在台灣留存備份。

AWS 客戶自選其內容和伺服器所在的 AWS 區域。 這可讓客戶建立的環境符合特定地區的要求。 例如，台灣的 AWS 客戶可以選擇部署其 AWS 服務、或將其內容存放於亞太地區（日本、新加坡、南韓或香港）內的任何區域。 如果客戶做出選擇，除非客戶選擇移動該內容，否則其內容將位於所選區域。

AWS 區域的設計和建置是為了符合全球嚴格的合規標準，為所有AWS 客戶提供高水準的安全性。 所有 AWS 區域均符合適用的資料保護法規。

金融機構作業委託他人處理內部作業制度及程序辦法 第19-1條

行政 > 金融監督管理委員會 > 銀行目 | 修正日期：民國 108 年 09 月 30 日

作業應變

八、金融機構應訂定妥適之緊急應變計畫，降低因作業委託而可能有服務中斷之風險。金融機構終止或結束作業委託，應確保能順利移轉至另一雲端服務業者或移回自行處理，並確保原受託雲端服務業者留存資料全數刪除或銷毀，並留存刪除或銷毀之紀錄。

應變安排及退場規劃

根據雲端服務委外規定第 19-1.8 條，金融機構應訂定緊急應變計劃，降低因作業委託造成服務中斷的風險；終止或結束作業委託時，應確保能順利轉移至另一雲端服務供應商或移回自行處理。

AWS 基礎設施具有高度可用性，提供客戶功能以部署具有恢復力的 IT 架構。 AWS 系統的設計能容忍系統或硬體失效，將對客戶造成的影響降至最低。 每個可用區域都被設計為獨立的失效區域。 這表示，可用區域在典型的都會區域內實體位置是分散的，並且位洪泛

風險較低的區域（特定的洪泛區分類因區域而異）。除了分散的不斷電系統（UPS）和現場備用發電設施外，還透過獨立公用事業的不同電網供電，進一步減少單點失效。 可用區域都是冗餘連接到多個一級傳輸供應商。

AWS 業務連續性計劃詳述故障時 AWS 所依循的程序，從檢測到停用。 制定此計劃的目的是使用三階段的方法來復原和重建 AWS：啟用和通知階段、復原階段和重建階段。 此方法可確保 AWS 以有條不紊的順序進行系統復原和重建，將復原和重建工作的有效性最大化，並將因錯誤和遺漏而導致的系統中斷時間降至最低。欲取得更多資訊，請參閱 AWS 白皮書 Amazon Web Services: Overview of Security Processes 和 AWS Artifact 主控台內的 SOC 2 報告。

客戶負責為 AWS 上託管的系統實施妥善的應急計劃、培訓和測試。AWS 讓客戶能實施強大的連續性計劃，包括利用伺服器執行個體頻繁備份、資料備援複製，以及靈活地在多個地理區域以及每個區域內的多個可用區域放置執行個體和儲存資料。

客戶利用 AWS 使其重要 IT 系統能更快速地從災難中復原，而不需支付過往專用的第二實體站台的基礎設施費用。 AWS 雲端支援許多常見的災難復原（DR）架構，從隨時準備擴展的「指示燈」環境，到啟用快速容錯移轉的「熱待命」環境。 如需災難復原方法的詳細資訊，請參閱災難復原。

如果客戶決定將部分或全部系統和資料從 AWS 遷移到另一個 IT 環境，可以使用各種 AWS 服務，匯出其系統和資料。AWS 提供 AWS Import/Export 和 AWS Snowball 等服務，以便使用實體儲存設備將大量資料匯入和匯出 AWS。 如需詳細資訊，請參閱雲端儲存。 此外，AWS 還提供 AWS Database Migration Service，這項雲端服務讓客戶可將資料庫從 AWS 服務遷移到內部部署資料庫。

AWS擁有完整團隊協助進行金管會核准流程

AWS Team have rich experiences in Taiwan regulatory compliance process

Account Team



Queena Tsai

蔡宛霖

Sr. FSI BDM, AWS Taiwan



Reca Kuo

郭雅珍

Sr. FSI BDM, AWS Taiwan

Solution Architect & Professional Service



Bard Lan

藍元宏

Solution Architect, AWS Taiwan



JJ Sung

宋俊頡

Cloud Infrastructure Architect, AWS Taiwan

Public Policy



Cynthia Chyn

秦素霞

Principle Public Policy, AWS Taiwan & HK



Erica Lai

Public Policy PM, AWS Taiwan

協助與主管機關溝通雲端政策與提供教育訓練

FSI Compliance & Audit



Kelvin Leung

FSI Compliance Specialist, AWS WWCS FSI Business



Patrick Chang

APJ Audit, TW & HK Lead, AWS Security

協助合規相關規範要求與實地稽核安排，協助與主管機關溝通

Security Assurance & Legal



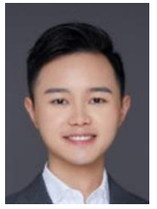
Brandon Lim

Principle FS Security, AWS Security(Compliance)



Alvin Li

Sr. Security Strategist, AWS Security(Compliance)



Kent Chow

Legal Counsel, AWS Legal

提供報部相關文件與雲端相關條款諮詢，協助與主管機關溝通

此團隊已具備協助金融同業報部成功與執行查核之經驗

We had successful reference cases to assist local and foreign financial institutions to get approval from Taiwan FSC.

AWS已具備相關文件供金融機構存留備查或是核准申請

All documents are ready to assist client to go through FSC approval process

- ✓ 金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行受託作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。(A letter of consent of Audit)

- ✓ 受委託機構所在地對客戶資訊之保護不低於我國之法律意見書。(The legal opinion indicates the protection of customer data where the service provider(AWS) is located is not below the condition in Taiwan.)

- ✓ 受委託機構出具近三年內未發生造成客戶權益受損或影響機構健全營運之人員舞弊、資通安全及其他事件之聲明書。(A statement issued by the service provider(AWS) certifying that no violation on customer interests, personnel malpractice, information and technology security and other occurrences that have impact on sound business operation in the last three years.)

- ✓ 作業委外計畫書，其內容應包括：(AWS user guide meet the requirements set out in Para 1 of Art 19-2 of the Outsourcing Regulations)

（一）風險評估及管理機制 (Risk assessment and management)
（二）資訊安全及稽核 (safety requirement for data transmission, backup storage etc.)
（三）資料所在地 (data residency & Audit right)
（四）緊急應變計畫及退場機制 (Emergency backup plan and exit right and plan)

AWS 使用者指南：台灣金融監督管理委員會銀行局雲端服務委外規定

指南資源

2020 年 1 月



目錄

引言 2

資安和共同的責任模型 3

- 雲端內部的資安 3
- 雲端本身的資安 4

AWS 合規確保計劃 4

AWS Artifact 6

AWS 區域 6

雲端服務委外規定第 19-1 條 6

- 風險管理及監控 7
- AWS 安全性與稽核系列 8
- 資訊保密及資料安全 10
- 資料所在地 13
- 應變安排及退場規劃 13

後續步驟 15

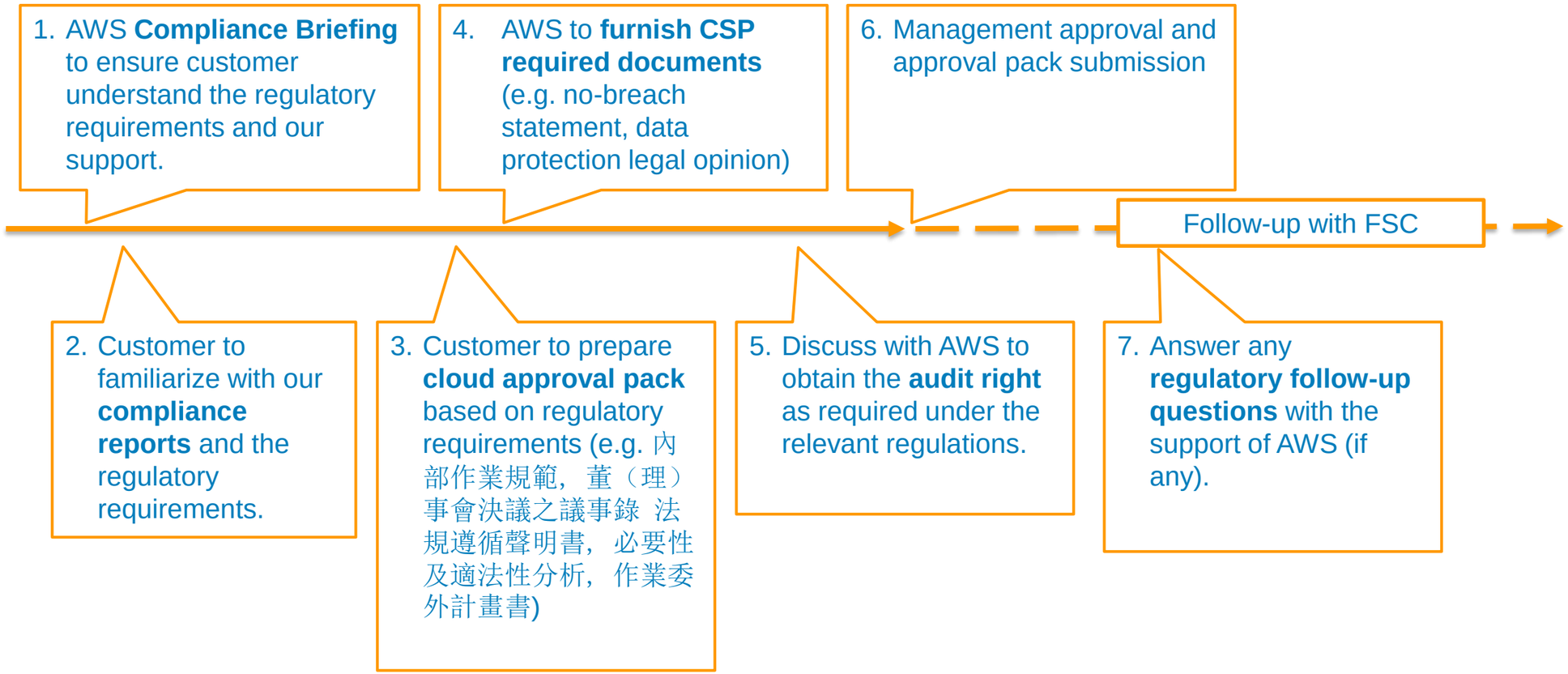
進一步閱讀 16

文件修訂歷程 16



報部流程參考時間表

FSC approval process



AWS將於今年度辦理首次金融聯合查核

- ✓ 銀行局金融機構作業委託他人處理內部作業制度及程序辦法(第 19- 1 條)
  - ✓ “金融機構將作業委託他人處理涉及使用雲端服務，應確保作業風險控管，充分評估受託機構處理之風險，採取適當風險管控措施，確保作業委外處理之品質”
  - ✓ “金融機構得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核”
- ✓ 金融機構運用新興科技作業規範 (2020/04/17版本)
  - ✓ 第八條: 得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核，並應符合下列規定：
    - ✓ (一) 確認其查核範圍涵蓋雲端服務業者處理作業相關之重要系統及控制環節。
    - ✓ (二) 應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。
    - ✓ (三) 應針對金融機構所指定作業範圍進行查核並出具報告。

- ✓ 為何聯合查核?
  - ✓ 聯合查核是指不同的金融機構委託同一獨立第三方，在同一時段和範圍下進行查核。
  - ✓ 好處: 不同的金融機構可以攤分費用，減低合規成本。

感謝您今天的與會

Queena, Financial Business Development Manager
tsaiwan@amazon.com

© 2022, Amazon Web Services, Inc. or its Affiliates.