

CYBERSEC 2023

金融資安論壇

金融業雲端轉型三部曲之挑戰與突破

國泰金控 顏勝豪 Otto Yen



顏勝豪 Otto



現在

- 國泰金控 數數發 雲端技術架構師
- 負責執行集團雲端轉型計劃，擬定集團上雲策略

過去

- 10年以上的軟體專案開發經驗
- 歷經紮實的養成訓練，由程式設計師→系統設計師→系統分析師→技術經理
- 帶領專案開發部門承接多種領域之
 - ✓ 外商銀行交易系統、商業智慧分析
 - ✓ 警政情資整合分析平台、大數據分析平台架構設計與建置

A decorative graphic on the left side of the slide, consisting of a 7x3 grid of squares. The squares are colored in shades of blue, gray, and white, arranged in a repeating pattern.

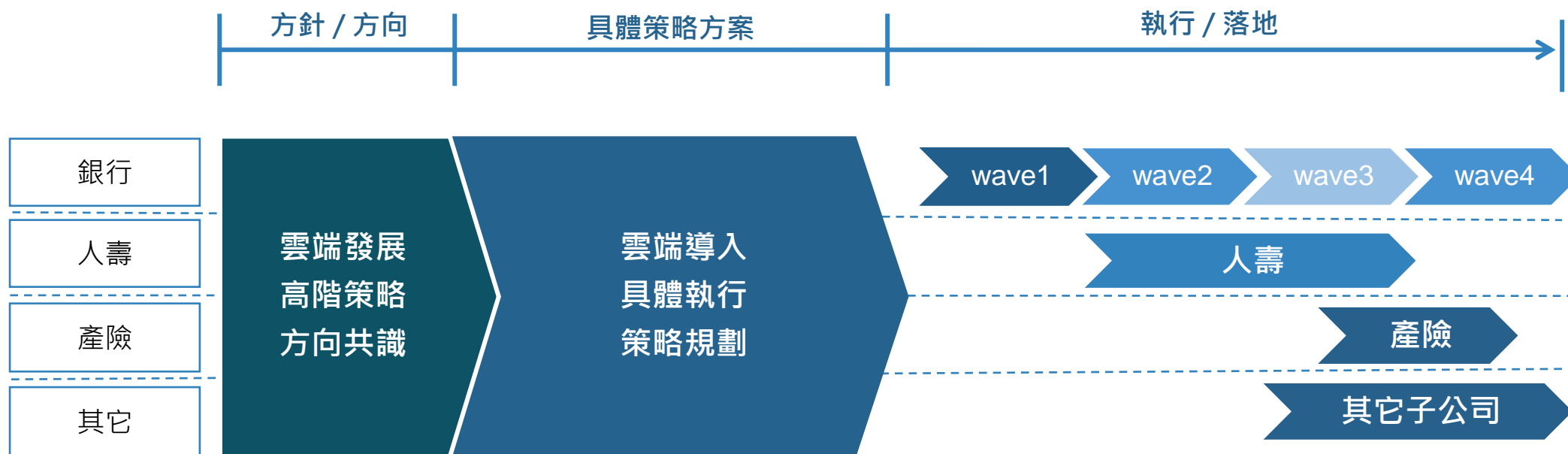
AGENDA

- 進入回顧前，先說明這一切是怎麼開始
- 2021 混合雲架構下應用系統之上雲策略
- 2022 雲端轉型過程中應用系統大規模上雲策略
- 2023 雲端轉型第三年面對的新挑戰

三年雲端轉型是與資安的血淚史合作史



在進入回顧前，先說明這一切是怎麼開始的...



共識

- 談方針
 - 方向
 - 遠景
 - 效益
 - 發展
- 提出 Cloud Ready 規劃
 - Infrastructure
 - Application
 - Organization
 - Management / Governance
 - 規劃導入的方法
- 進行 AP 詳細分析
 - 可行性評估
 - 各上雲的方案
 - AD 時程及執行計畫
 - 實際執行

目前金管會將依照雲端作業委外的重大性與否，區分為「核准制」 以及「備查制」

內部作業委託

金融機構對於**涉及營業執照所載業務項目或客戶資訊**之相關作業委外，金融機構應依主管機關規定方式，確實申報有關作業委外項目、內容及範圍等資料。



境外

將資料處理委託至境外辦理、資料儲存地位於境外
(資料處理：包括資訊系統之資料登錄、處理、輸出，資訊系統之開發、監控、維護，及辦理業務涉及資料處理之後勤作業。)

核准



境內



具重大性之作業

綜合評估是否為重大性作業

(1)對金融機構影響：

- ①委外作業對金融機構之營收與獲利之貢獻度、
- ②對盈餘、償付能力、流動性、籌資能力、資本、風險之影響、
- ③作業委託雲端業者之總曝險
- ④如無法提供服務或有資安問題，對金融機構聲譽、營運目標與策略、成本及內控制度之影響、
- ⑤對金融交易對手及對金融市場之影響程度、
- ⑥委外作業成本佔總營運成本之比例、
- ⑦委外作業失敗造成金融機構將作業移回或找其他替代者之成本，及該成本佔總營運成本之比例。

(2)對客戶影響：

- ①作業委外對客戶之影響程度、
- ②委外作業涉及客戶個人資料之數量多寡。



非重大性之作業

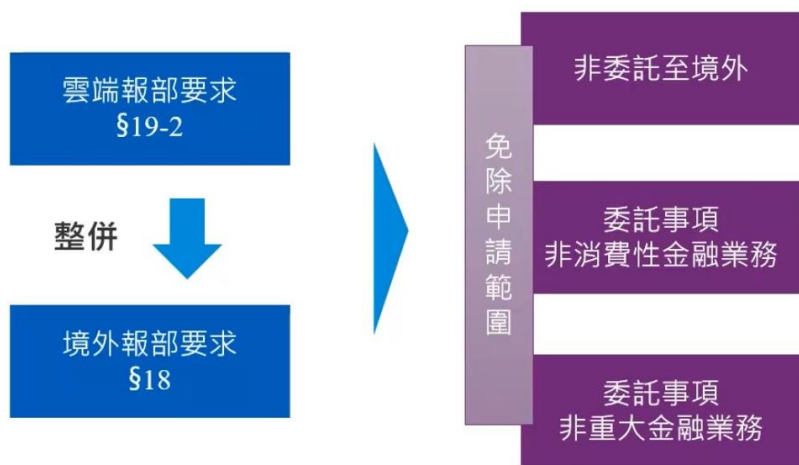
備查



今年將迎來金融業上雲最大變革

金融機構雲端服務報部之變革

金管會於2023/3/8預告修正「金融機構作業委託他人處理內部作業制度及程序辦法」草案(金管銀外字第11202705872號)



iThome 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT EXPLAINED 搜尋

企業加速 綠色轉型 全新系列【數位轉型攻略 IV：戰略新 IT】 揭曉最大資安會議熱門議題

新聞

金融業開放上雲將有重大鬆綁！未來境外公雲不是重大消金應用免申請

金管會宣布金融業委外上雲辦法將有重大修正，放寬了對於境內外雲端委外作業規定，還大幅簡化申請核准的程序，有首案申請通過核定後，其他金融業者之後要用免重申請，讓金融業很多上雲採用更容易。

文/ 余至浩 | 2023-03-08 發表 讚 51 分享

修法前後之委外申請程序比較

作業項目	現行制度	修正草案
■ 一般委外事項	免申請核准 §4	免申請核准 §4
■ 其他經主管機關核定得委外之作業項目	應申請核准 §5	首案經本會核定後，其他金融機構得逕行辦理 §5
■ 信用卡發卡及消費性貸款之行銷	應申請核准 §11	免申請核准 §11
■ 應收債權催收作業	應申請核准 §12	免申請核准 §12
■ 跨境委外	應申請核准 §18	重大性消費金融業務資訊系統委託至境外處理，應申請核准 §18
■ 使用雲端服務	應申請核准或備查 §19-2	

圖片來源: 金管會

iThome IT EXPLAINED WEBINAR
數位轉型攻略

2023 全新系列 V
即將登場!!

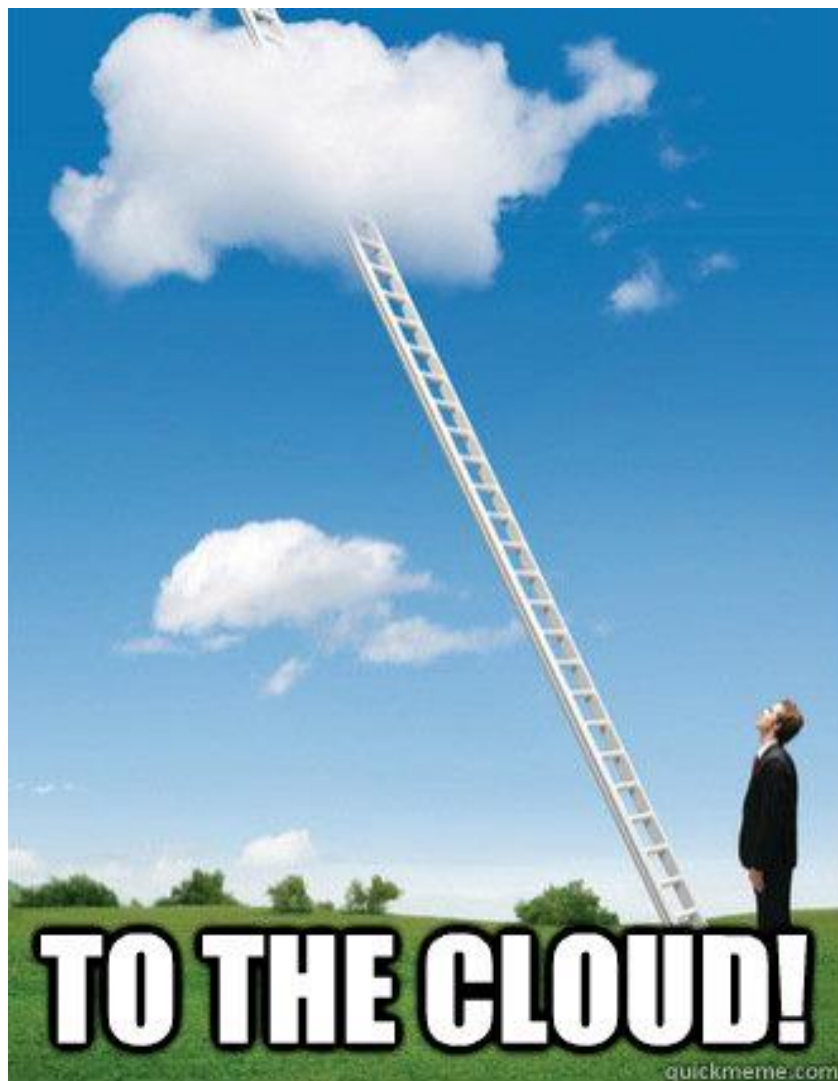
後疫關鍵議題探討
深入解析 IT 新趨勢
精彩豐富戰略講座

回憶模式

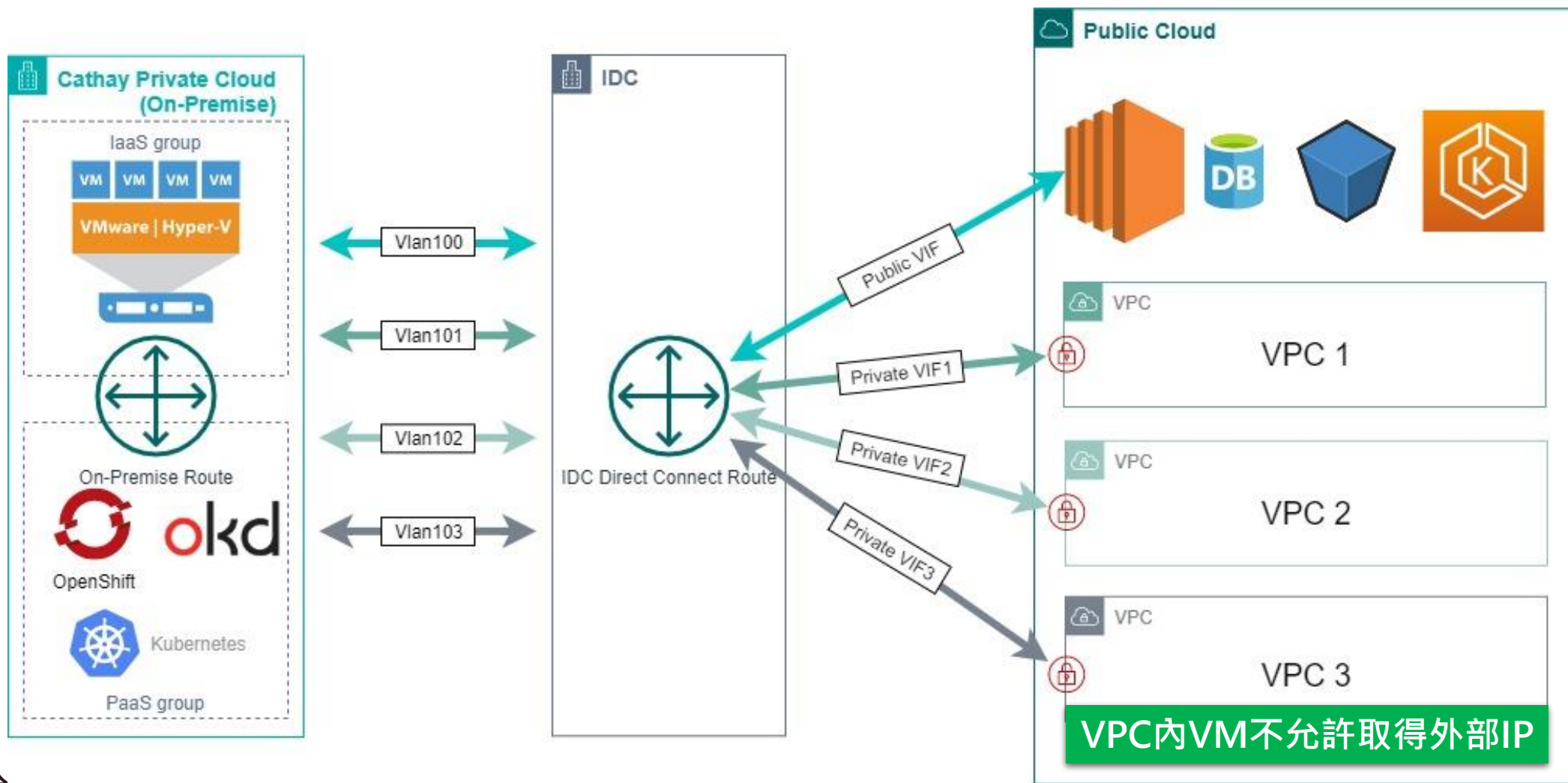
2025
2024
2023
2022
2021

金融業於混合雲架構下應用系統之上雲策略
國泰金控 Otto 顏勝豪

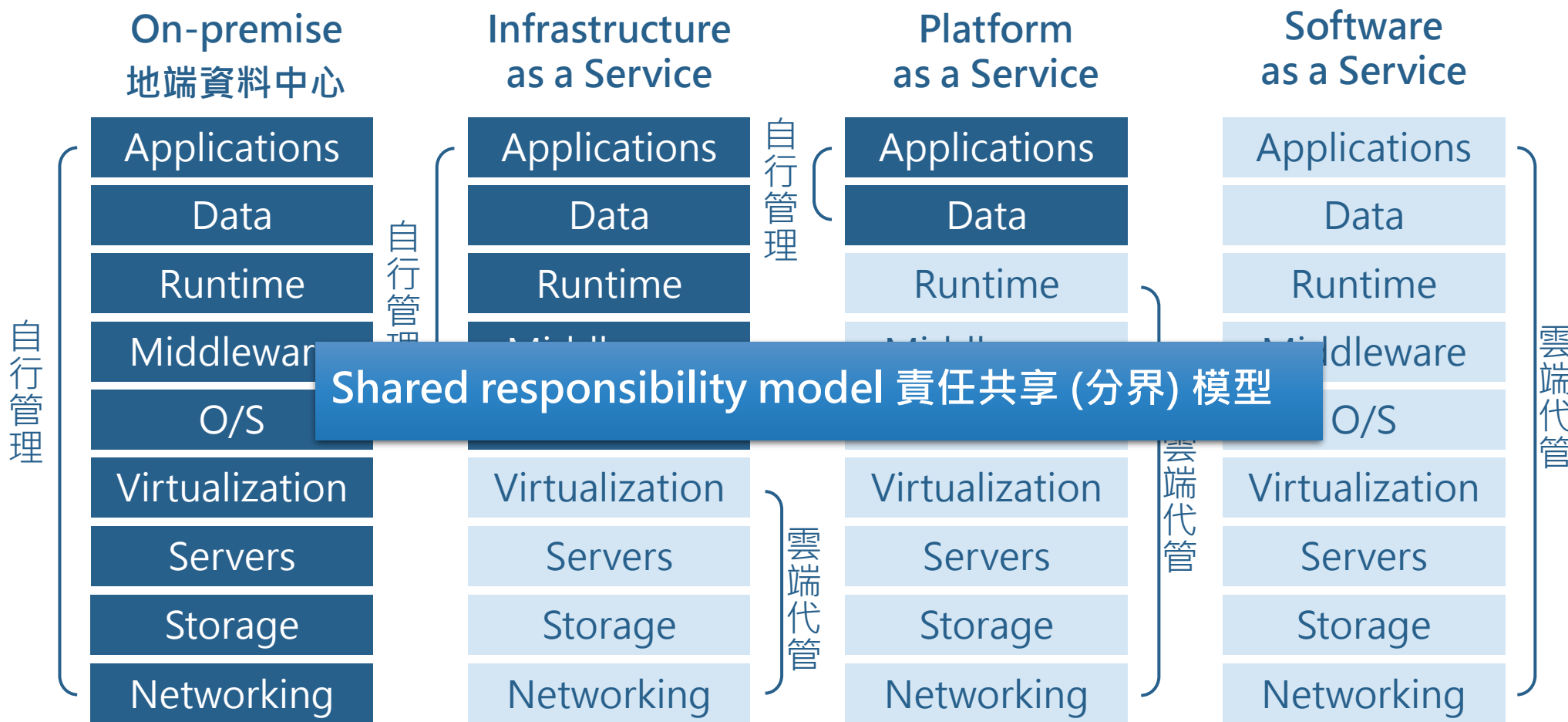
上雲不就是就在雲端上開個虛擬機再把程式放上去就好了



下圖混合雲架構中VPC設計是內網的延伸或外網？



雲端服務有IaaS、PaaS、SaaS不同模式 如何保證CSP不會偷拿你的資料？



雲端轉型初期將面臨三大挑戰

金融業上雲安全合規性

上雲將面臨外規規範

目前金管會將依照雲端作業委外的重大性與否，區分為「核准制」以及「備查制」，系統上雲相關資料加密、金鑰管理、緊急應變計畫、退場機制、系統日誌集中管控、雲端服務控管機制。

組織運作機制

尚未建立雲端組織

雲端對金融業來說屬於陌生領域，若沒有團隊負責規劃及推動進程，雲端轉型易陷於停滯不前的狀態，同時也需要補足人員雲端專業技能才能應付未來的轉型需求。

系統上雲策略與方法論

系統上雲策略規劃難度高

有大量多元且複雜的資訊系統，其中如何有效盤點、評估，為各系統安排優先順系及上雲方式成為困難課題。

Cloud Ready 專案透過5個Track因應三大挑戰

金融業上雲安全合規性

組織運作機制

系統上雲策略與方法論

Track 1 雲端安全評估

雲端安全發展藍圖

- 資安評估表
- 了解地端現有作法
- 訪談會議

Track 2 雲端安全框架

雲端安全合規作業

- 國際雲端資安框架介紹 (ISO 27017 / CCM)
- 雲端安全管理辦法範本說明

Track 3 雲端組織與技術培訓

雲端技術種子團隊

- 雲端技術人才招聘
- 外部培訓
 - Google Cloud 培訓與線上支援
- 內部培訓
 - Workshop / Onsite 輔導 / 技術支援

Track 4 應用系統評估

上雲策略與遷移計畫

- 使用國泰雲端遷移評估平台 CCMA¹
- 訪談會議

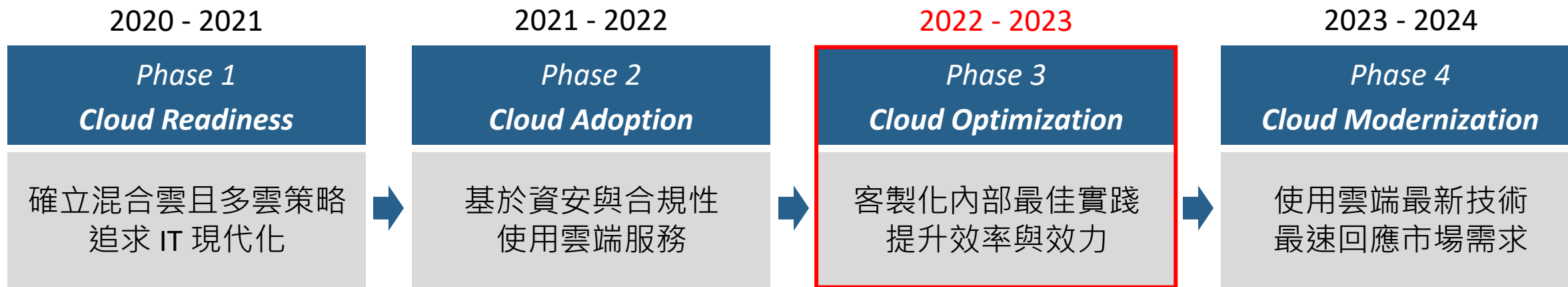
Track 5 MVC 設計與建置

示範性系統 + 雲端基礎設施

- Infrastructure : VPC 網路、IAM 權限管理、CI/CD 維運部署、IaC 管理、資安服務
- Application Architecture : PaaS、SaaS



我們開啟集團四階段的雲端轉型旅程



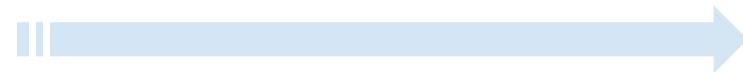
證券啟動雲端發展 Phase 1



已完成雲端發展 Phase 1



已完成雲端發展 Phase 1



回憶模式

2025
2024
2023
2022

金融業於雲端轉型過程中應用系統大規模上雲策略
國泰金控 Otto 顏勝豪

從1套系統上雲到100套系統大規模上雲

Cloud Ready

1 套系統

資安框架面

系統遷移面

環境基礎面

- 雲端運用場景下針對集團雲端採用做扎實基礎規劃與設計
- 涵蓋雲端技術架構、國際資安框架 CSA CCM
- 國內事務所協助依照法遵需求檢視文件內容適切性，確保相關程序符合 CSA CCM、雲端資安標準 ISO27017 和國內主管機關雲端安全相關條文

大規模上雲

Cloud Adoption

上 100 套系統

大規模遷移

雲端成本面

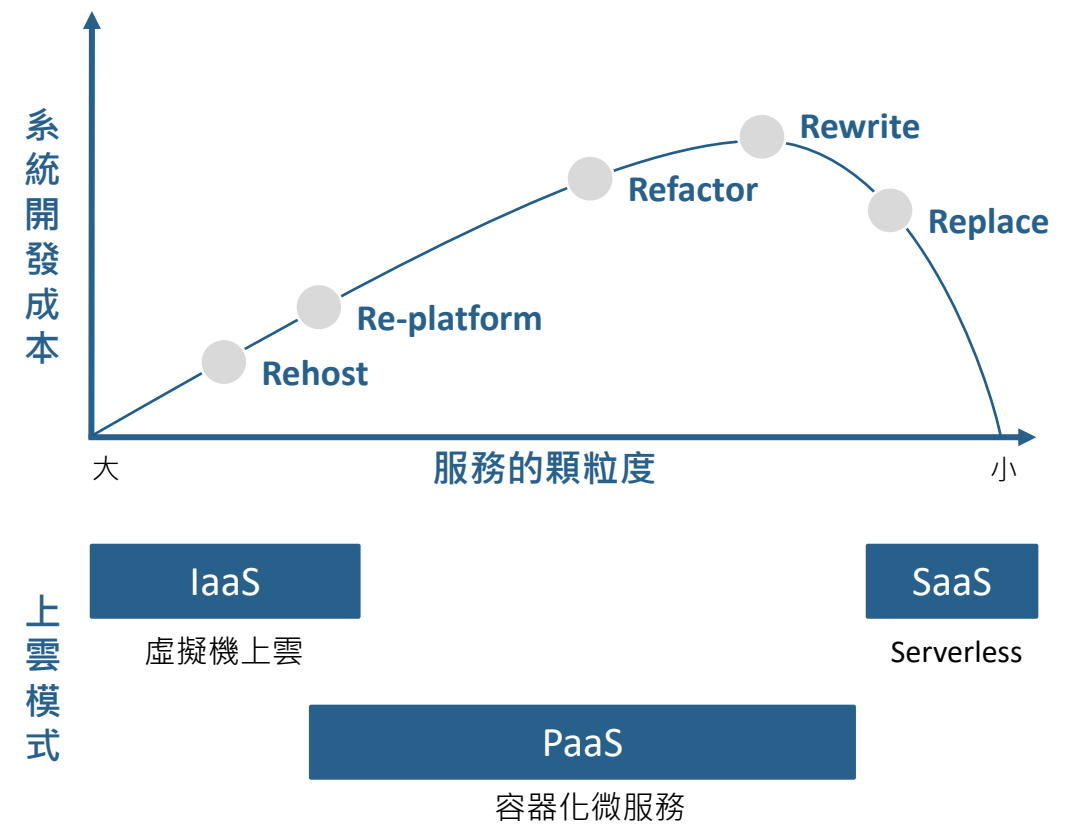
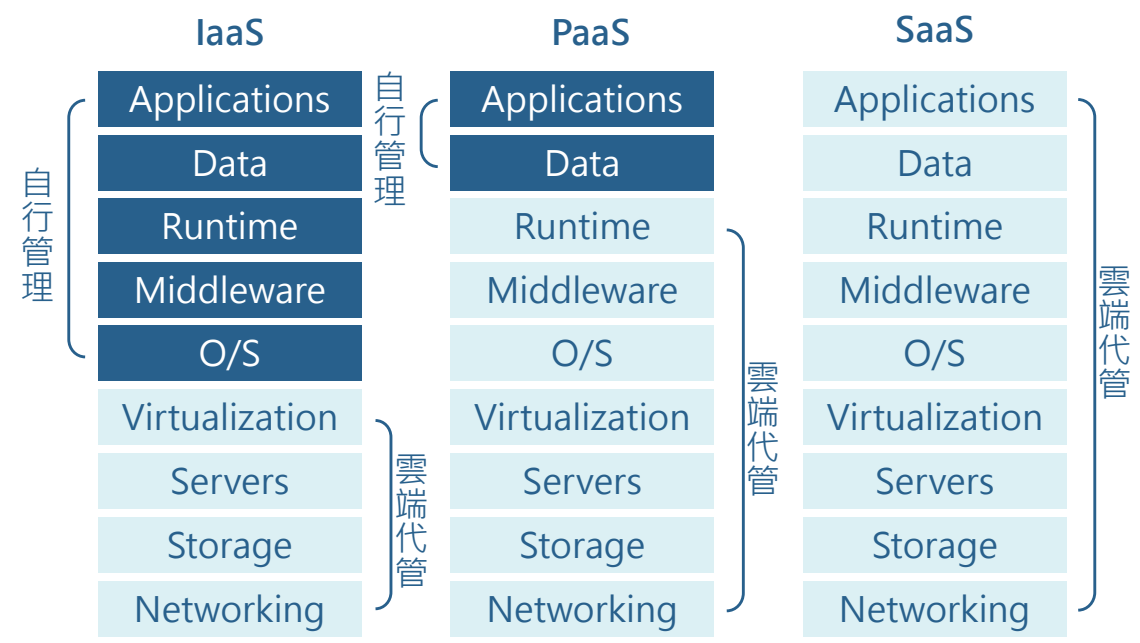
維運流程面

- 集團各子公司進入「雲端大量使用階段」，將**雲端維運管理**和**鉅額成本控制**議題納入關鍵考量
- **雲端架構標準**和**技術運作流程**成熟度需提升，多公有雲使用相比現階段單一雲使用更複雜，更需確保資訊安全
- 建立完整且成熟之雲端治理模型滿足以上關鍵點，雲端發展更穩健且更謹慎，**降低重大資安風險**



突破

集團一致 6R 系統遷移方式與雲端架構設計



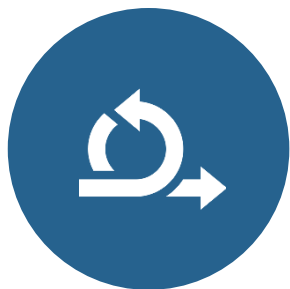
- 雲端遷移模式將透過系統訪談，依據所收集到之資訊，產出該系統初步評估建議
- 評估項目：技術、風險、業務衝擊...等面向

用一句直白的話說明 Cathay 6R 策略

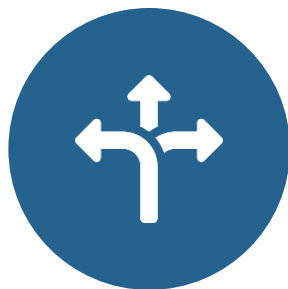


應用系統從容器化到Serverless

用一句直白的話說明Cathay 6R策略：「消滅虛擬機」



比市場快半步



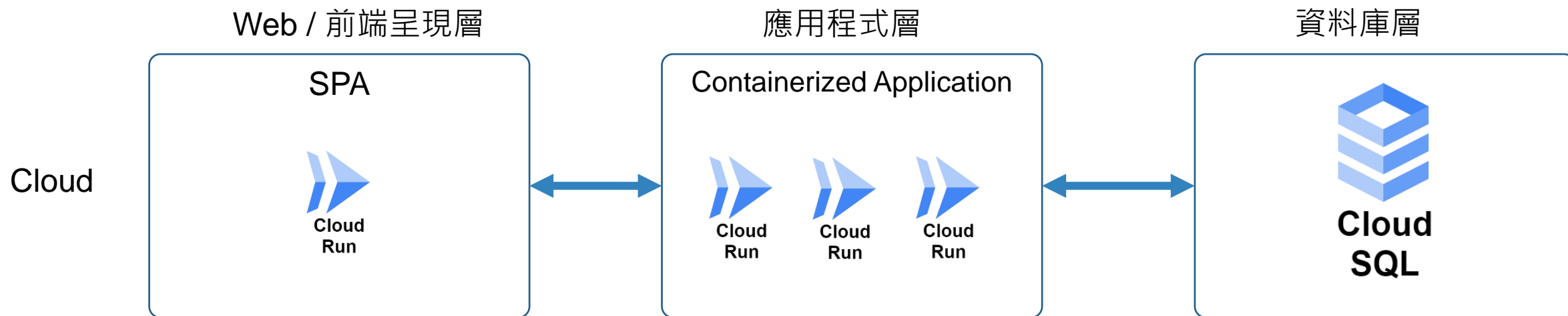
資源彈性伸縮



省錢



天然高可用



國泰集團上雲策略

- 戰略 (目標) : 消滅虛擬機
- 戰術 (方法) : Cathay 6R 雲端遷移方法論
- 戰鬥 (執行) : 敏捷技術架構

國泰金控 CATHAY FINANCIAL HOLDINGS

活動資訊 精彩議程 活動好禮 加入無限大 防疫聲明 活動結束

Session 2 雲端部署加速應用落地

14:45
|
15:05

專題演講
雲的多重宇宙 開創跨界新格局

- ◆ 上雲的思維轉變
- ◆ 上雲的技術轉變
- ◆ 上雲的行動轉變

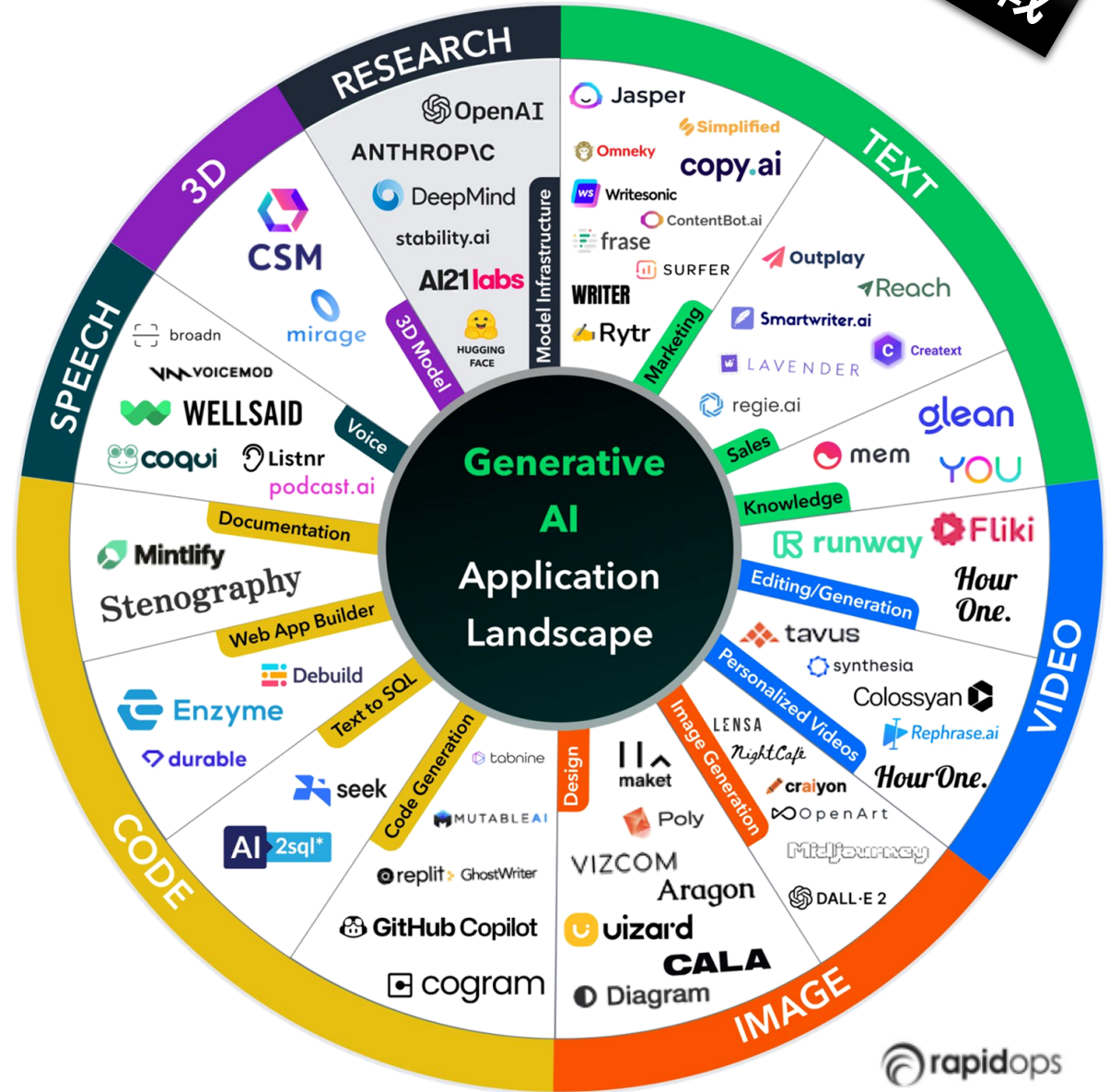
主講人：
國泰金控數數發中心數位架構發展部專案經理 | 顏勝豪 Otto Yen



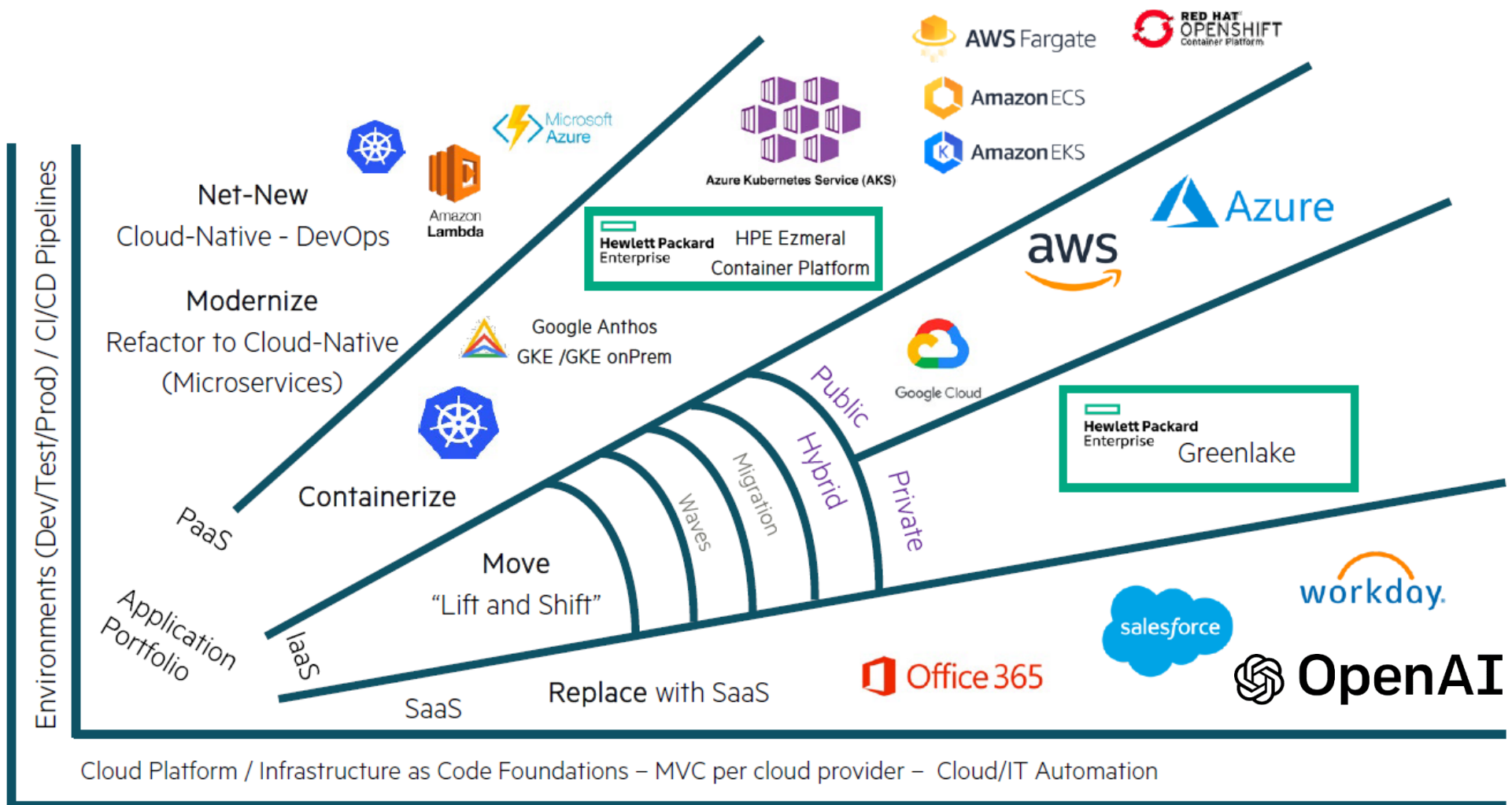
金融業雲端轉型回顧完，今年的挑戰是...

GAI生成式AI大爆發的一年

挑戰



我們使用的服務的關注，由IaaS到SaaS



OpenAI 實際資安事件：個資外洩、機敏資料外洩



AIGC 最佳實務：Gartner 建議企業使用雲端廠商提供之 AIGC 服務

Operational Best Practices

Start With Cloud APIs

Largest Model Isn't Always the Best Fit

Use Pretrained Models

Fine Tune & Optimize Your Models



以ChatGPT為例，我們既不使用網頁版也不使用API版

OT 根據 <https://www.ithome.com.tw/news/152373>
幫我產生十個問與答

好的，以下是基於該新聞產生的十個問題和答案：

1. 什麼是金控業？
答：金控業是金融控股公司的簡稱，包括銀行、保險、證券、投資等金融業務。
2. 金控業為什麼要將系統遷移至雲端？
答：將系統遷移至雲端可以提高系統的可靠性、彈性、安全性和效率，並節省成本。
3. 這次金控業將遷移哪些系統至雲端？
答：根據新聞，金控業將遷移包括核心系統、資料庫、應用程式等在內的大量系統至雲端。
4. 為什麼金控業要選擇Google Cloud作為合作夥伴？
答：金控業選擇Google Cloud作為合作夥伴，是因為Google Cloud具有全球性的服務能力、豐富的技術經驗、安全性高以及對金融業的專業性。
5. 金控業的系統遷移至雲端需要注意哪些風險？
答：金控業的系統遷移至雲端需要注意數據安全風險、系統可靠性風險、用戶體驗風險等。
6. 遷移至雲端後，金控業的系統可靠性是否會提高？
答：是的，遷移至雲端後，金控業的系統可靠性會提高，因為雲端具有高可用性、可擴展性和彈性。
7. 遷移至雲端後，金控業的系統安全性是否會提高？
答：是的，遷移至雲端後，金控業的系統安全性會提高，因為雲端擁有更高的安全性保障和監控能力。
8. 遷移至雲端後，金控業需要擔心的費用是哪些？
答：遷移至雲端後，金控業需要擔心的費用包括雲端服務費用、數據傳輸費用、購買新硬體設備等費用。
9. 金控業遷移至雲端後，如何確

Send a message.

ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 3 Version](#)

Example request

curl

```
1 curl https://api.openai.com/v1/models \  
2 -H "Authorization: Bearer $OPENAI_API_KEY"
```

Response

```
1 {  
2   "data": [  
3     {  
4       "id": "model-id-0",  
5       "object": "model",  
6       "owned_by": "organization-owner",  
7       "permission": [...]  
8     },  
9     {  
10      "id": "model-id-1",  
11      "object": "model",  
12      "owned_by": "organization-owner",  
13      "permission": [...]  
14    },  
15    {  
16      "id": "model-id-2",  
17      "object": "model",  
18      "owned_by": "openai",  
19      "permission": [...]  
20    },  
21  ],  
22  "object": "list"  
23 }
```



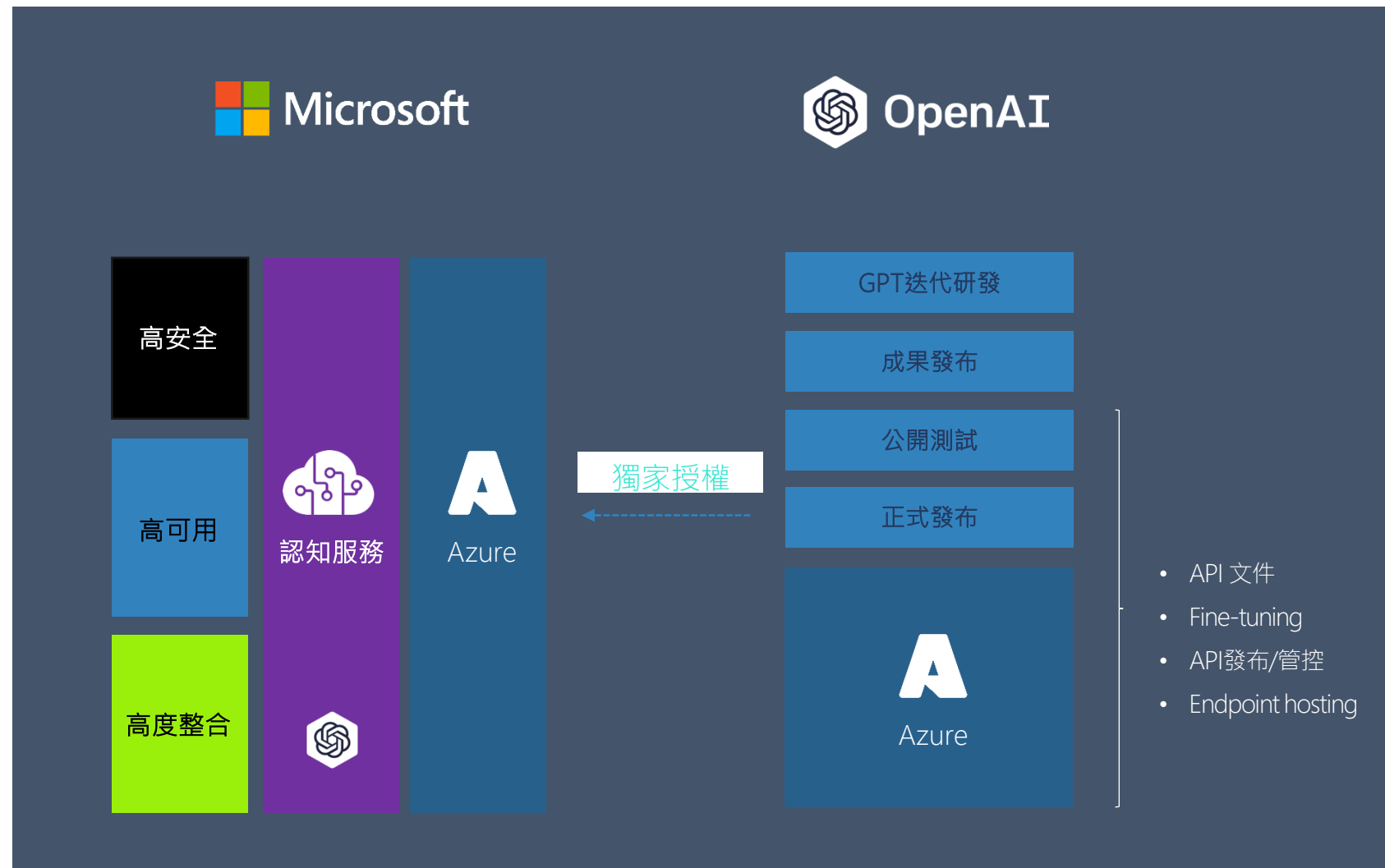
國泰金控

Cathay Financial Holdings

“Azure” Open AI 是一套 AIGC SaaS 服務

Azure OpenAI 是微軟與 OpenAI 合作推出的人工智慧平台。

Azure OpenAI 將 OpenAI 的技術和平台集成到 Azure 平台中，為開發者提供一個強大的人工智慧開發平台，並使開發者能夠使用這些技術來創建更智能的應用程序，藉由 Azure 的資安防護機制確保數據應用及環境更加安全。



三大雲端廠商皆有推出 AIGC SaaS 服務

突破



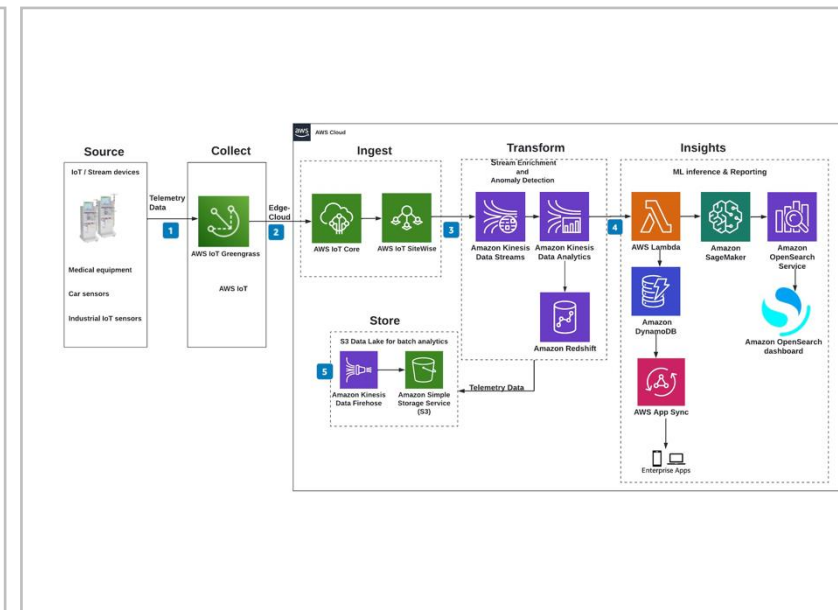
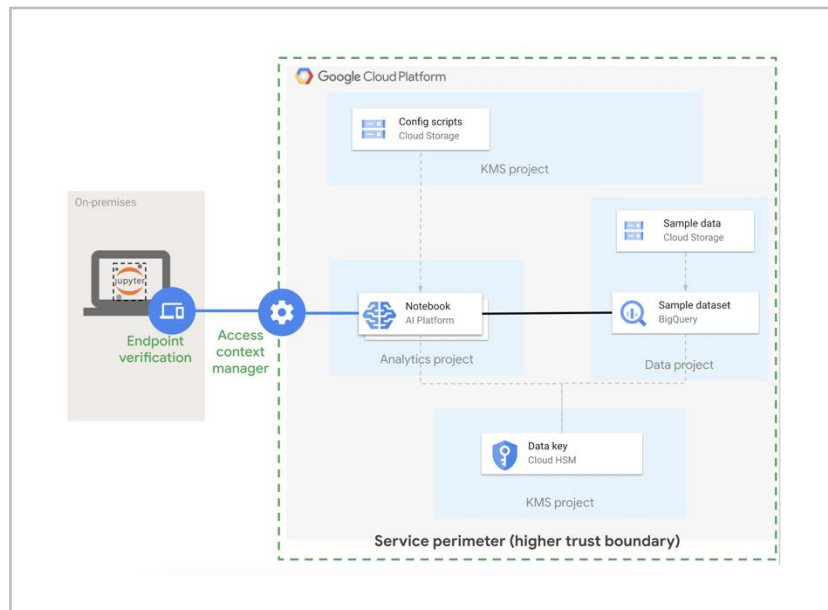
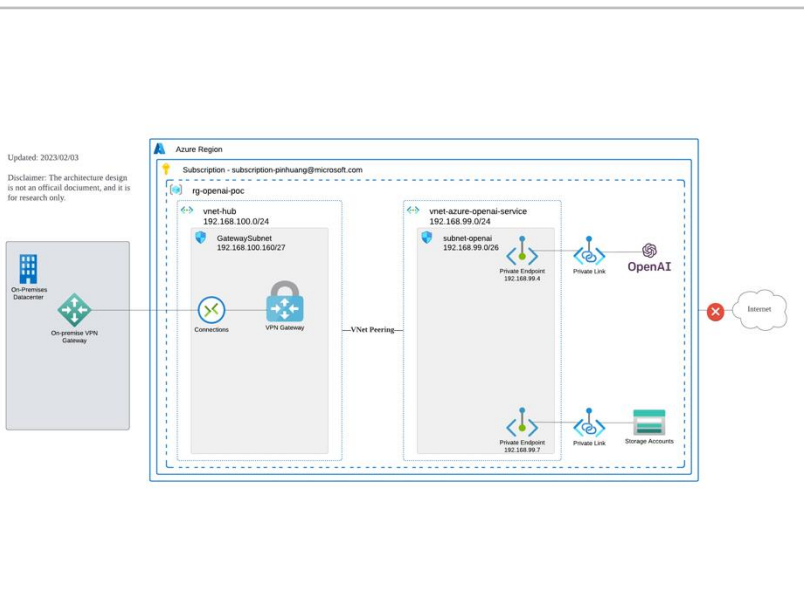
Azure OpenAI



GCP Vertex AI



AWS Bedrock



三大雲端廠商提供之 AIGC SaaS 皆為封閉式環境，並搭載其雲原生之資安配套，系統安全性如同一般 SaaS 服務。

雲端廠商於 SaaS 資安管理之關注面向：高可用、安全、監控、擴增性

Reliability & Scalability

- 多區域可用
- 保證SLA 99.9%
- 更高Rate Limit (TPM/QPM)
- 企業級有償Support

Management

- Endpoint 部署管理和監控
- Token 監控
- 整合資源監控 (Monitor / Log Analytics)
- 更好的 Error & debug 支持

Security

- 企業合規 (SOC2 , HIPAA , ISO , GDPR Data Privacy etc.)
- 私有網路 (vNet) , Private Endpoint/Link
- 企業倫理審查 (Responsible AI)
- AD集成, RBAC/IAM 權限管理
- 托管身份 (Managed ID)

Extensibility

- Custom Domain
- API 擴充
- 整合現有Cognitive Service的服務架構
- 整合自動化 (Automation Task , ARM部署)

SaaS 三大管理面向：環境資料管理、平台供應商管理、合規性管理

- 選擇合適的 SaaS 平台
- 確認可提供的服務級別協議 (SLA)
- 管理 SaaS 供應商
- 成本效益



- SaaS 平台國際標準合規認證
- 契約規範
- 資訊安全風險評估
- 金融交易和風險管理
- 法律和合規要求

- 是否為核心業務作業場域
- 是否有個資處理
- 是否有機敏資訊
- 是否串接內部系統

SaaS 環境資料管理：分層分權管理

	Lab		Production	
環境說明	非核心業務作業場域 無個資處理、無機敏資訊 無串接內部系統		核心業務作業場域 涉及個資處理、涉及機敏資訊 串接內部系統	
管理方式	自行管理	可帳號控管 可稽核管理 集中管理	可帳號控管 可稽核管理 集中管理	無管理機制
審查	需資安審視且符合規範		需資安審視且符合規範	需資安審視且符合規範 例外管理
SaaS 平台	ChatGPT Miro Figma KKTIX TwSMS	Azure OpenAI Google Workspace SendGrid SurveyCake Adobe	Azure OpenAI Google Workspace SendGrid SurveyCake Adobe	 ChatGPT Miro Figma KKTIX TwSMS

SaaS 平台合規性管理：確保平台是否符合監管要求

管理方法	管理要點
SaaS 平台國際標準合規認證	SaaS 平台應該符合相關的法律法規和標準，以及市場國際標準要求，如 PCI DSS、ISO 27001 等。
契約規範	確定 SaaS 供應商的服務契約中是否涵蓋了所需的服務內容，是否具備足夠的賠償條款，以及是否符合企業的風險管理和合規要求。
資訊安全風險評估	確定所選擇的 SaaS 供應商是否具備足夠的資訊安全防護措施，以及是否能夠保護機密資訊不受外部威脅。
金融交易和風險管理	對 SaaS 進行詳細的交易和風險管理，以確保 SaaS 平台能夠快速處理大量的金融交易，並且可以根據風險管理策略進行風險評估和控制。
法律和合規要求	確定所選擇的 SaaS 供應商是否符合所在國家和地區的相關法律法規和監管要求。

金融業雲端轉型三年，回顧每個階段的挑戰與突破

2023

Optimize & Review
金融業雲端轉型三部曲之
挑戰與突破

03

AI數據上雲



2022

Cloud Adoption
金融業於雲端轉型過程中
應用系統大規模上雲策略

02

OA上雲



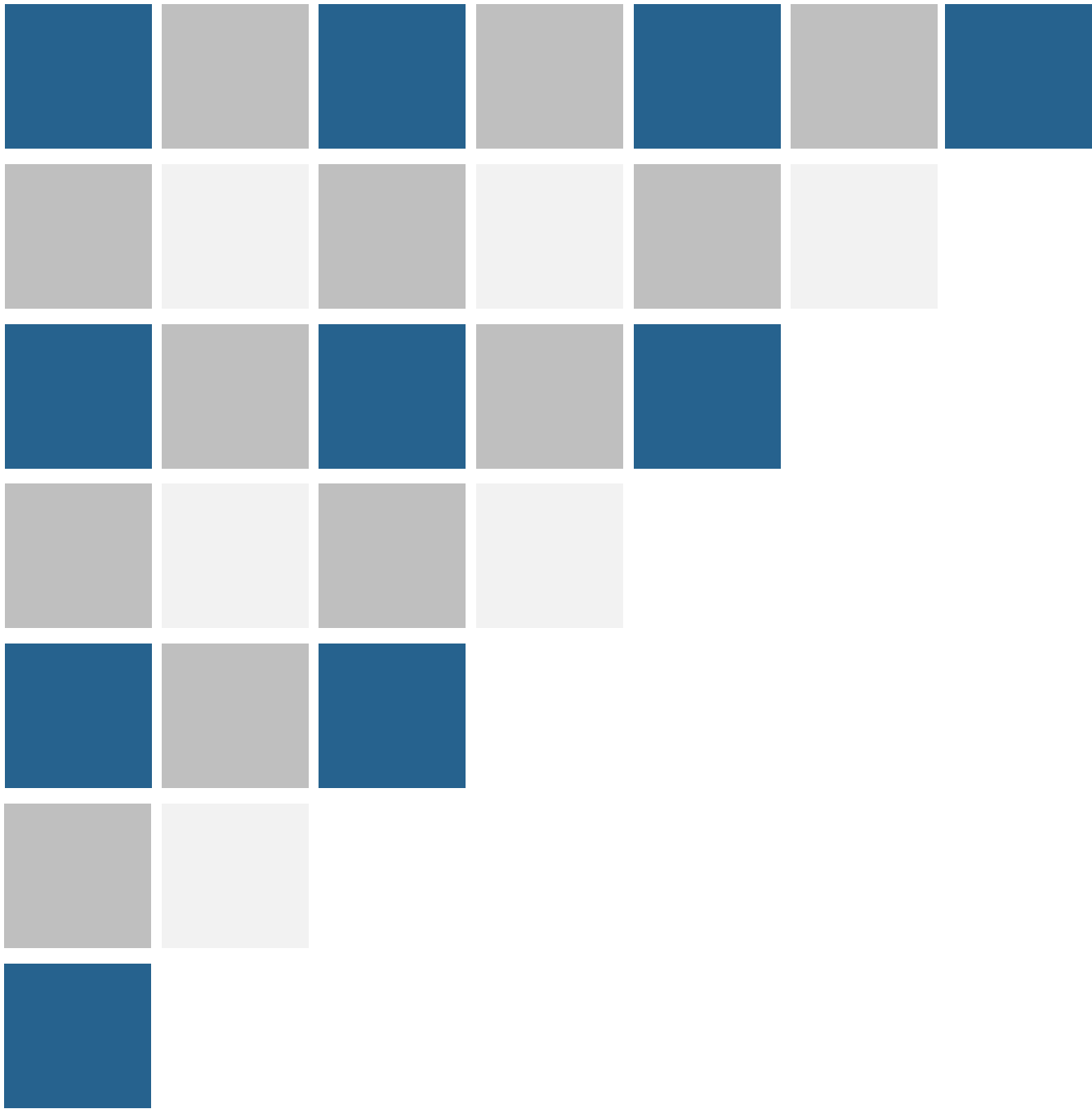
2021

Cloud Ready
金融業於混合雲架構下應
用系統之上雲策略

01

應用系統上雲





Thank you.