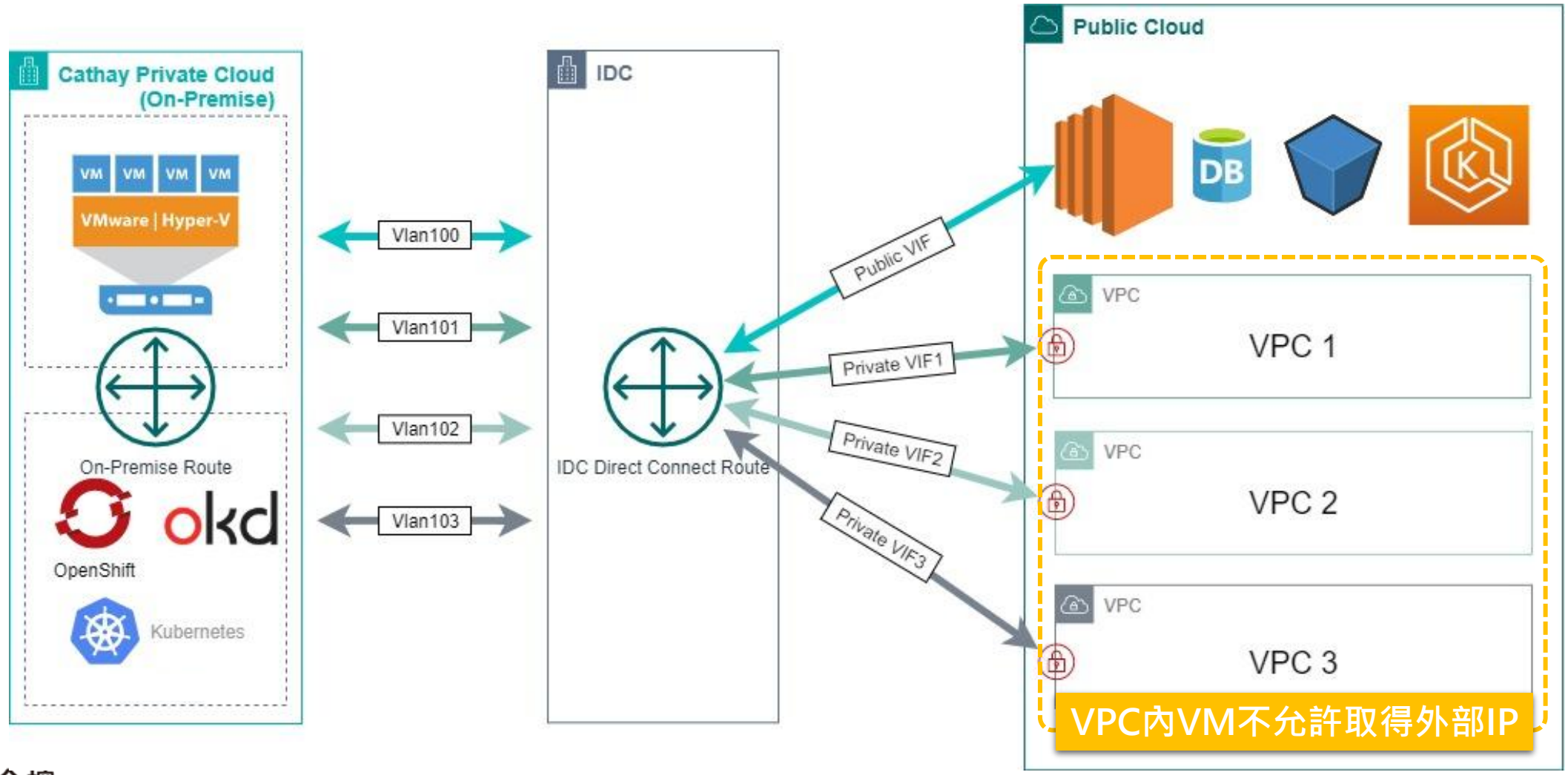
金融業於混合雲架構下應用系統之上雲策略

國泰金控 Otto 顏勝豪

Agenda

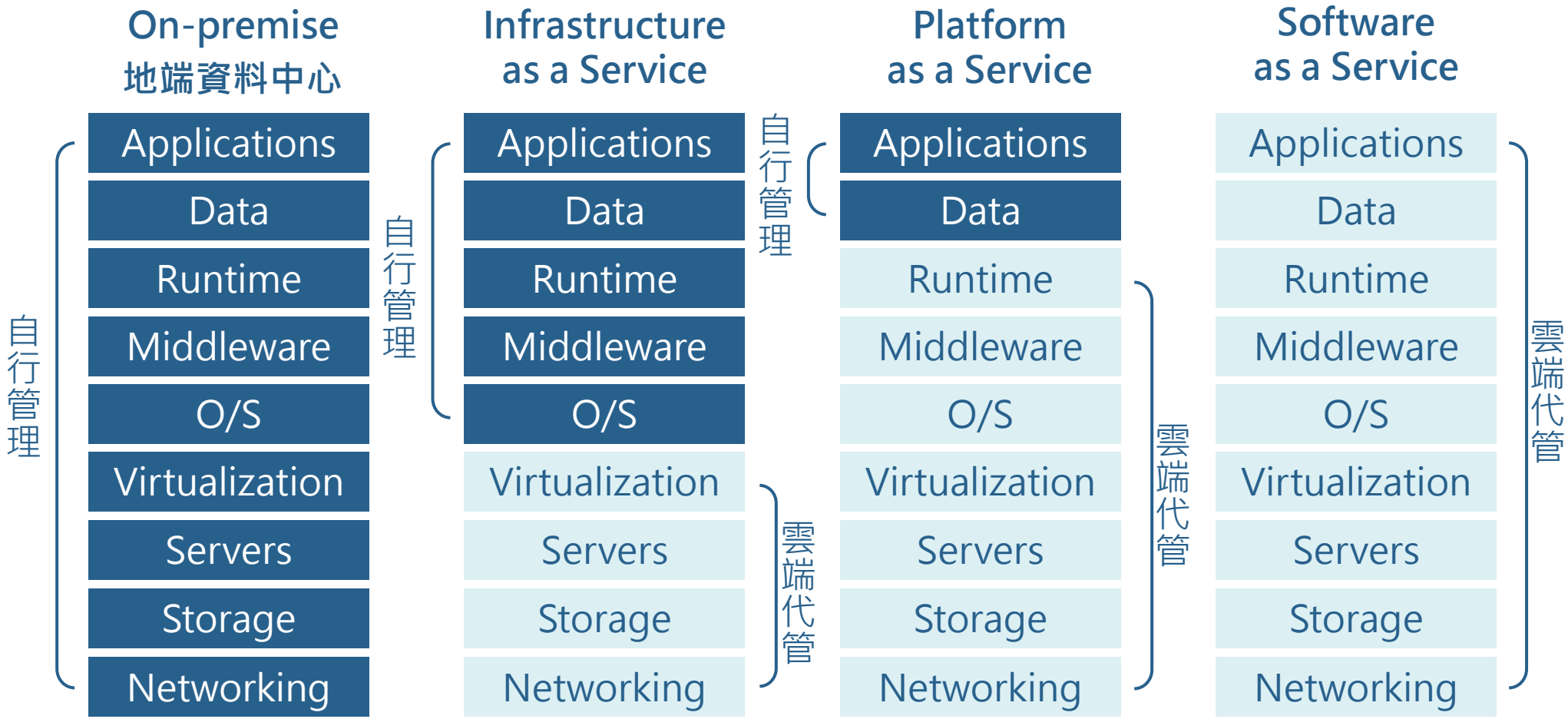
- 雲端技術趨動數位轉型
- 金融業上雲資安與合規性
- 雲端運算服務模式
- 混合雲架構中應用系統上雲策略
- 應用系統雲端遷移方法論介紹
- 在混合雲架構中使用IaC雲端自動化技術
- 國泰集團轉型上雲旅程

下圖混合雲架構中VPC設計是內網的延伸或外網？



雲端運算服務模式有IaaS、PaaS、SaaS不同模式，如何保證CSP不會偷拿你的資料？

Shared responsibility model 責任共享 (分界) 模型



2020年疫情大爆發時在國外流行的故事 (true story)

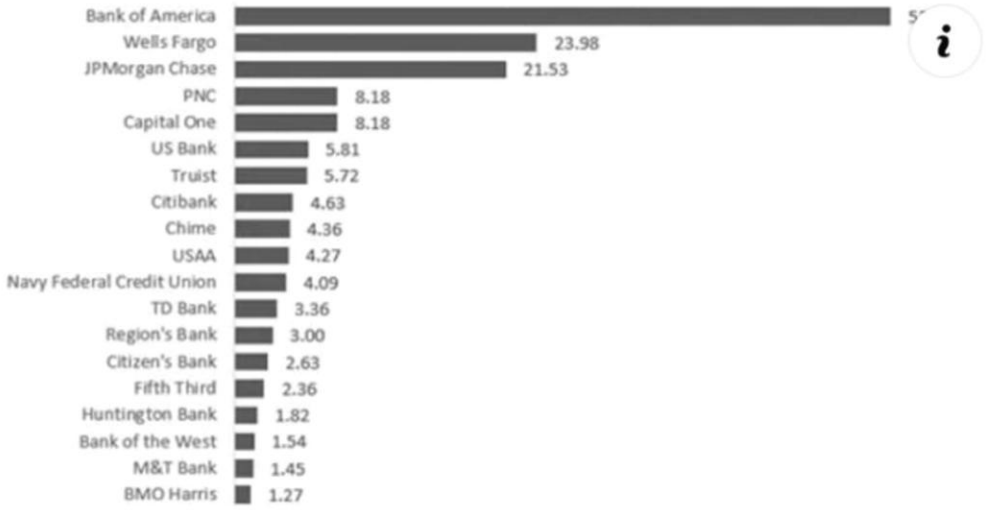
Fintech 金融科技趨勢分享

Aug 2 ·

🗣2020年美國純網銀業者的逆襲

新冠肺炎危機迫使美國消費者必須依靠數位通路，才能與他們現有的銀行交易和互動，如果這些銀行做不到，消費者只能琵琶別抱、別無他法。

從純網銀的逆襲來看，讓美國消費者意識到兩點：1）他們真的可以不需要實體分支機構，並且2）社區銀行和信用合作社的數位產品有缺點，無法滿足用戶需求。



60

covid-19

iThome

Zoom首季財報出爐，營收成長169%，客戶大增3倍

iThome

Amazon今年第二季營收成長40%，締造新獲利紀錄

亞馬遜第二季獲利52.4億美元，比去年同期成長99.7%，其中AWS雲端服務的獲利貢獻度占了57%

讚 6.2 萬 按讚加入iThome粉絲團 讚 58 分享

文/ 陳曉莉 | 2020-07-31 發表

32 分享

採用雲端以加速 IT 現代化已成國際趨勢

全球監管最嚴格的金融企業越來越多地採用來自 AWS, Azure 和 GCP 等公有雲服務

Significant Drivers to make a move from On Premise Infrastructure to Cloud Platform

敏捷性 | 成本效益 | 現代化安全

MetLife

提升營運效率
改善客戶體驗
節省 45-55% Infra 支出
利用公有雲 / 容器 / 微服務

ZURICH

建置現代化 PaaS
40% 應用系統上雲
降低成本達 30%
新程式上線縮短至 48 小時

BNP PARIBAS

提升營運效率
加速客戶服務
80% 服務流程自動化

Allianz

簡化保險流程
提升客戶體驗
導入全面 DevOps 加速開發

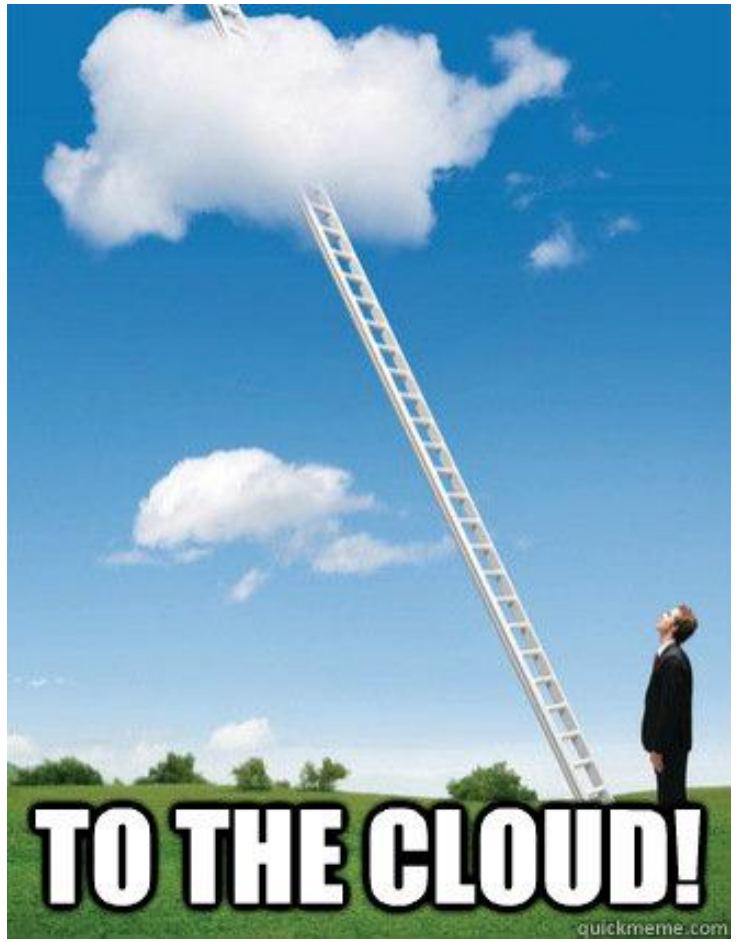
AXA

提升敏捷性
加速新服務推出
完成 1,000 多個應用系統上雲
最終目標：6,000 – 6,500 個 (Global)

UNIONINSURANCE

改善客戶體驗
即時創新產品推出

應用系統上雲？不就是就在雲端上開個虛擬機再把程式放上去就好了



未考慮資安與合規，就別談金融業上雲

產物保險股份有限公司管理電子商務系統，核有違反保險法相關規定，爰依保險法第171條之1第4項規定核處罰鍰新臺幣(以下同)120萬元整，並依同法第149條第1項規定予以2項糾正

2021-06-09

一、裁罰時間：110年6月9日
二、受裁罰之對象：　　產物保險股份有限公司
三、裁罰之法令依據：保險法第149條第1項、第171條之1第4項
四、違反事實理由：
(一)該公司107年8月於資訊部門下增設資安專責單位，依法應配置適當人力資源及設備，負責規劃、監控及執行資訊安全管理作業，然當時僅配有1名資安人力，直至109年1月起始增加為2人，檢查發現系統弱點修補管控欠妥，防火牆規則設定審核欠落實，以及未建立重要日誌監控及告警機制等資安防護作業欠妥事項，顯示資安專責單位未能妥適行使職權及有效發揮監督功能，核有未落實執行保險法第148條之3第1項授權訂定之「保險業內部控制及稽核制度實施辦法」第6條之1規定情事，依保險法第171條之1第4項規定，核處罰鍰新臺幣(下同)60萬元。
(二)該公司107年4月16日租用雲端基礎設施(IAAS)，運用Platform(　)，以雲端架構建置「　　投保系統」，查有未妥善訂定資料加密金鑰管理程序、未訂定妥適之緊急應變計畫及退場機制等情事，又辦理　　投保系統」之開發及維護作業，未受公司網路保護機制管控，主機系統日誌未納入資訊部門集中管控，與公司所訂內部規定不符。該公司雲端服務控管機制欠妥，未落實「保險業作業委託他人處理應注意事項」第7點規定，不利資訊安全及客戶權益之保護，核有違反保險法第148條之3第1項授權訂定之「保險業內部控制及稽核制度實施辦法」第5條第1項第14款規定情事，爰依保險法第171條之1第4項規定，核處罰鍰60萬元。
(三)有關資安管理部分，有提報董事會之資安整體執行報告欠完整、對廠商交付之報告未確實檢核、未訂定重要性主機監控管理規範及系統修補程序、對主機帳號密碼管理欠妥、弱點掃描範圍欠完整等缺失，不利資訊安全防護，經核有礙健全經營之虞。
(四)辦理委外廠商管理部分，所訂委外開發人事系統合約，同意廠商遠端連線辦理維護，未妥為評估必要性及資安風險；另相關委外作業服務未訂定緊急應變計畫且辦理實地查核作業有欠確實等情事，經核有礙健全經營之虞。
五、裁罰結果：核處罰鍰120萬元整及2項糾正。
六、其他說明事項：保險業辦理電子商務，應確實建置或完備電子商務系統資訊安全管理規範及標準作業程序、配置適當人力並落實執行，俾利確保有效發揮資安維護管控功能。另委外作業應確實評估資安風險並妥為訂定緊急應變計畫，以維資訊安全及消費者權益之保護。

關鍵字：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...

雲端運算四大優勢

為什麼使用雲端運算技術？

敏捷性

雲端可讓您輕鬆存取各種技術，方便您更快地進行創新，並建立幾乎任何您能想像到的事物，這樣您便可以**自由地進行試驗、測試新構思，讓新型態業務快速發佈到市場上**

彈性

使用雲端運算，您不必為了因應未來的業務高峰，預先佈建過多的資源。相反地，您只需佈建實際所需的資源量。您可以擴展和縮減這些資源，**以便在業務需求改變時立即擴大或縮小容量**

變動成本

雲端可將**資本費用 (資料中心、實體伺服器等) 轉變成變動費用，讓您僅針對所使用的 IT 付費**。此外，由於規模經濟，變動費用遠比您自行完成的費用更低

快速進行全球部署

利用雲端，您可以在幾分鐘內擴展到新的地理區域並進行全球部署。例如，AWS、Azure及GCP 的基礎架構遍及全球，因此只要按幾下滑鼠，就能在多個實體位置部署應用程式。**將應用程式放在更接近最終使用者的地方**，以減少延遲並改善他們的體驗，另外**藉由多區域多機房架構，快速提供DR、HA機制**

雲端轉型關鍵元素

雲端運算543：3種服務模式

End Users

SaaS 軟體即服務

按需訂閱、隨訂隨用

Application Developers

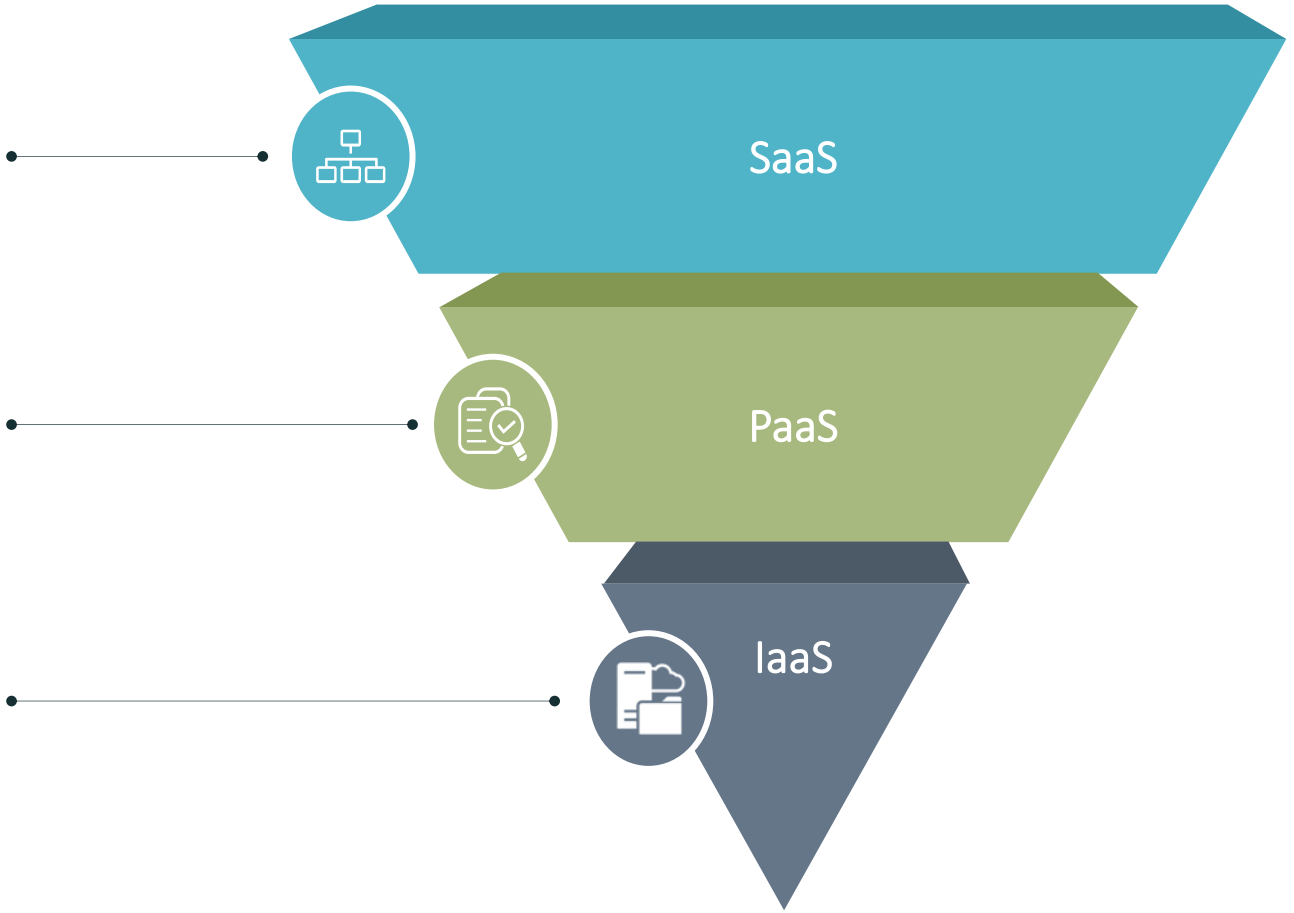
PaaS 平台即服務

服務快速開發、快速佈署

System Administrators

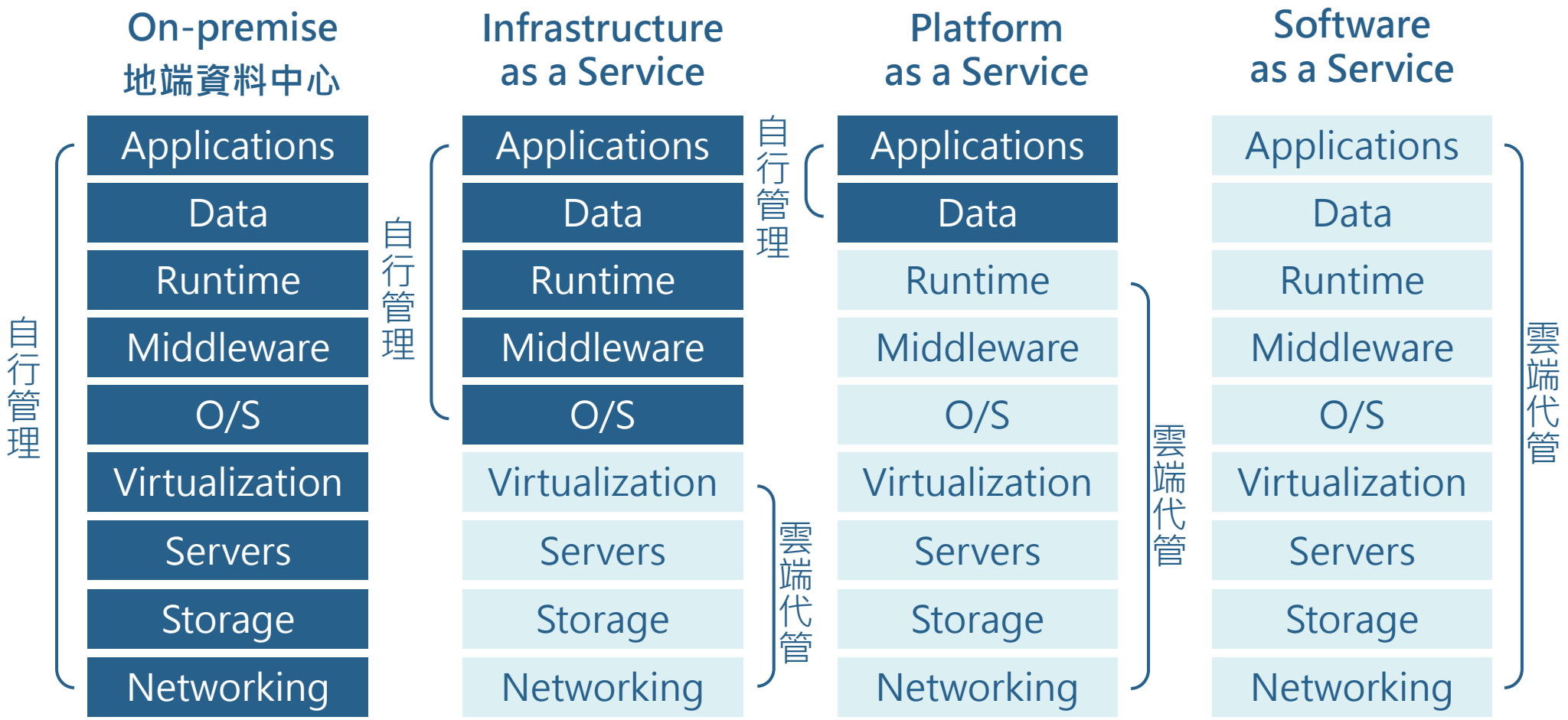
IaaS 基礎建設即服務

軟硬體資源彈性擴充



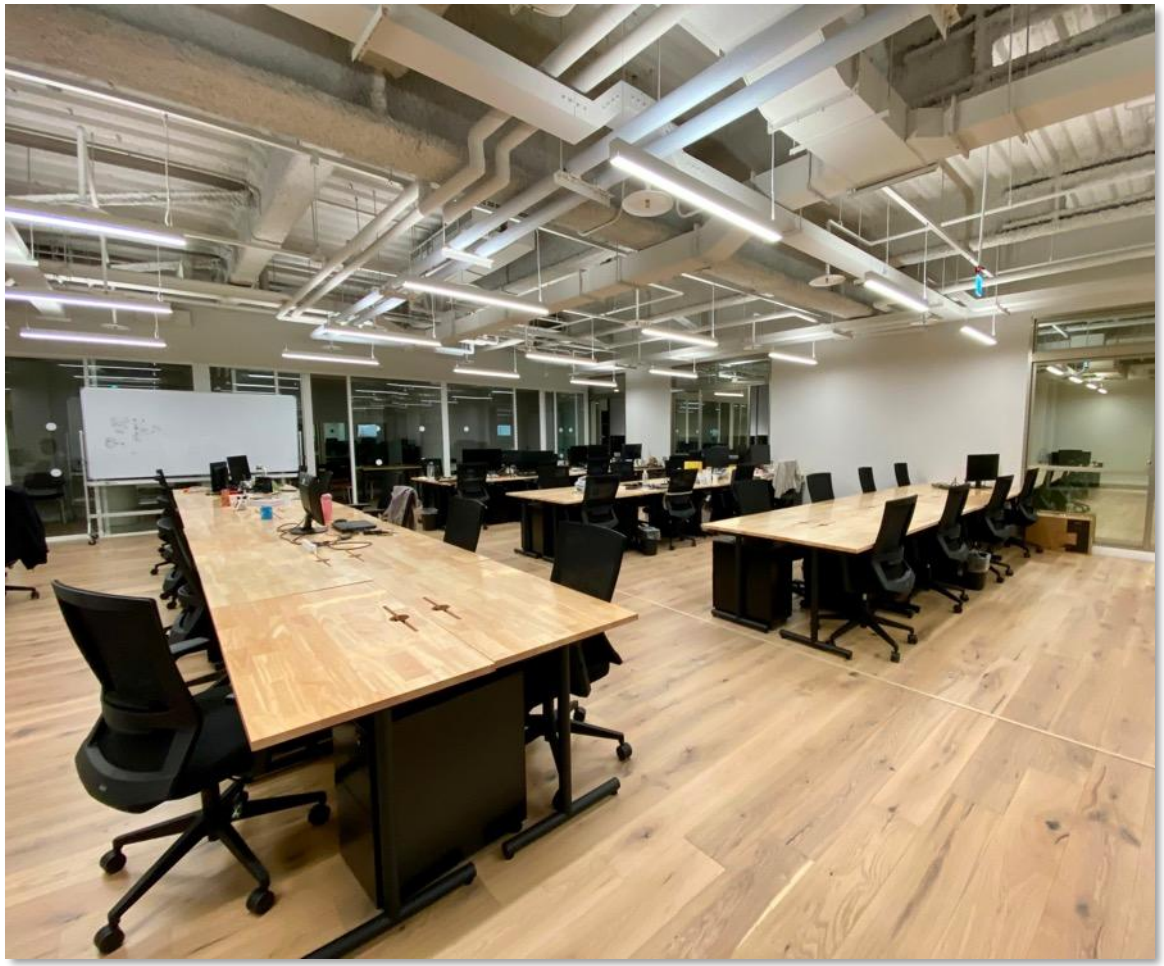
雲端運算服務模式 IaaS、PaaS、SaaS

每一種雲端運算服務模式提供不同等級的控制、靈活性和管理



猜一猜這是什麼服務模式？IaaS？SaaS？PaaS？

猜一猜這是什麼服務模式？IaaS？SaaS？PaaS？



猜一猜這是什麼服務模式？IaaS？SaaS？PaaS？

基於不同雲端服務模式討論雲端服務使用與管理方式

雲端服務模式		On-Prem	AWS	Azure	GCP
SaaS	企業依據其業務需求 選用SaaS服務		SegaMaker	Cognitive Services	Auto ML MK API ML Engine BigQuery
PaaS	Container Management	Kubernetes OpenShift	EKS	AKS	GKE
	Micro Services App Development Platform	Knative、Dapr	AWS Lambda	Azure Function	Google Function
	Object Storage	NAS	AWS S3	Azure Storage	Cloud Storage
	In-Memory Data Store	Redis	ElastiCache	RedisCache	MemoryStore
	SQL	Oracle PostgreSQL DB2	Amazon RDS	Azure SQL	Cloud SQL
	NoSQL	HBase	DynamoDB	HDInight	Big Table
IaaS	Virtual Server	VMWare HyperV	EC2	Virtual Machine	Compute Engine
	Virtual network	LAN	VPC	VNet	VPC

系統上雲後對組織與管理的影響

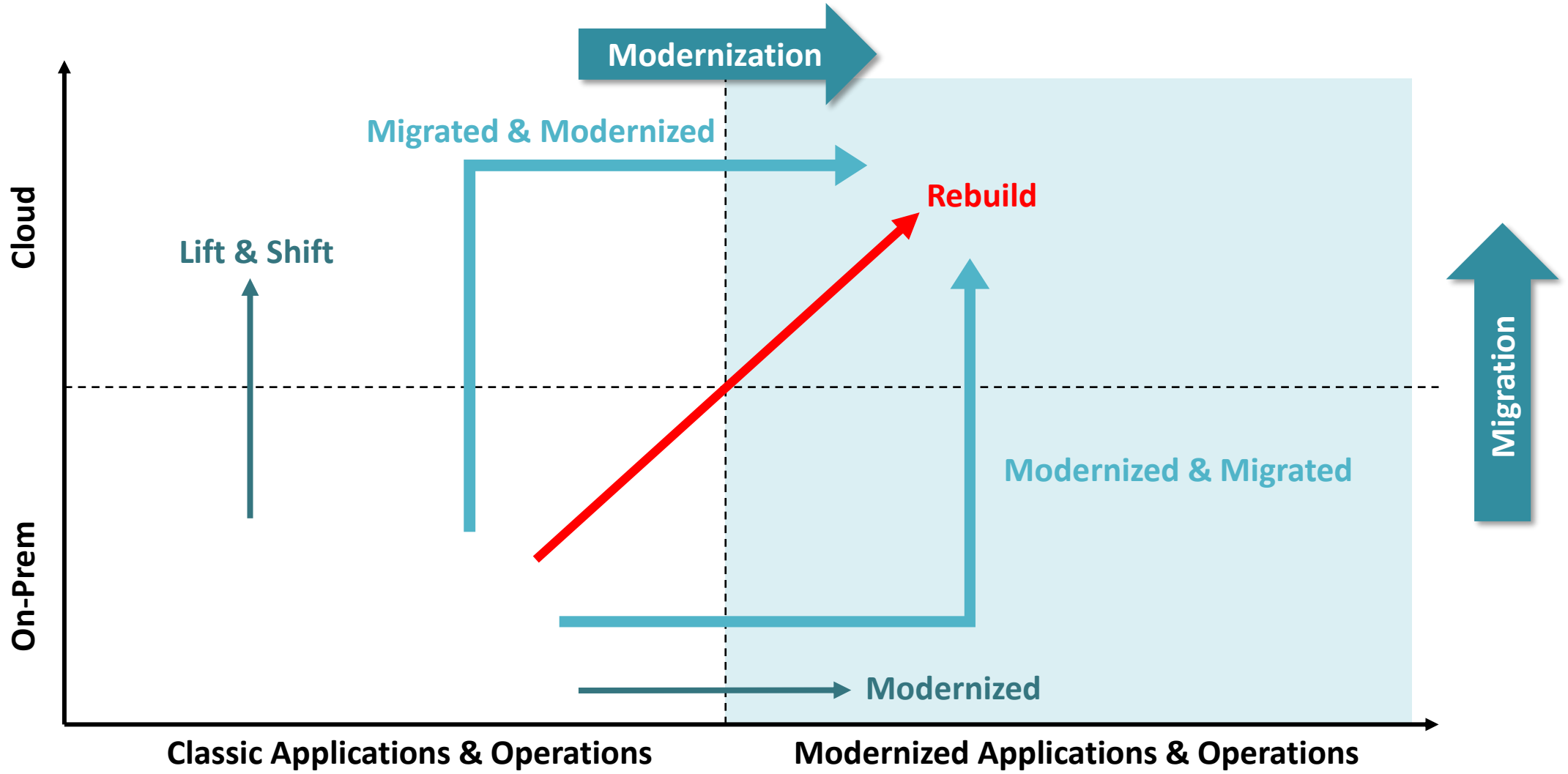
在混合雲架構中，每個應用系統依其特性採用不同上雲策略

我們藉由分析各用系統各種維度特性，決定其上雲策略

Domain-based	Tier	System	Criticality	Generation
Non-core	Frontend	Open	Non-critical	New
Core	Backend	Closed	Critical	Old

Environment-based	Operational State	Workload Demand	Data Access	Data Classification
Test & Dev	Disaster Recovery	Burst	Back-up	Non-sensitive
Production	Business as Usual	Normal	Operational	Sensitive

傳統應用系統上雲可採不同途徑上雲



應用系統雲端遷移方法論介紹

Cloud APs Migration

從三大面向評估分析系統現況，提供各應用系統雲端遷移模式建議，協助選定適合的 MVC 先導上雲系統

- 技術面
- 商業面
- 風險面

目標

系統上雲建議

提供專業諮詢，使諮詢對象有更佳的雲端遷移策略

方法論 & 工具

設計評估問項評分標準以及圖表判讀方法

預期成效

- 選出適合上雲的系統
- 排定上雲優先順序
- 幫助諮詢對象能夠創造最大效益

諮詢對象

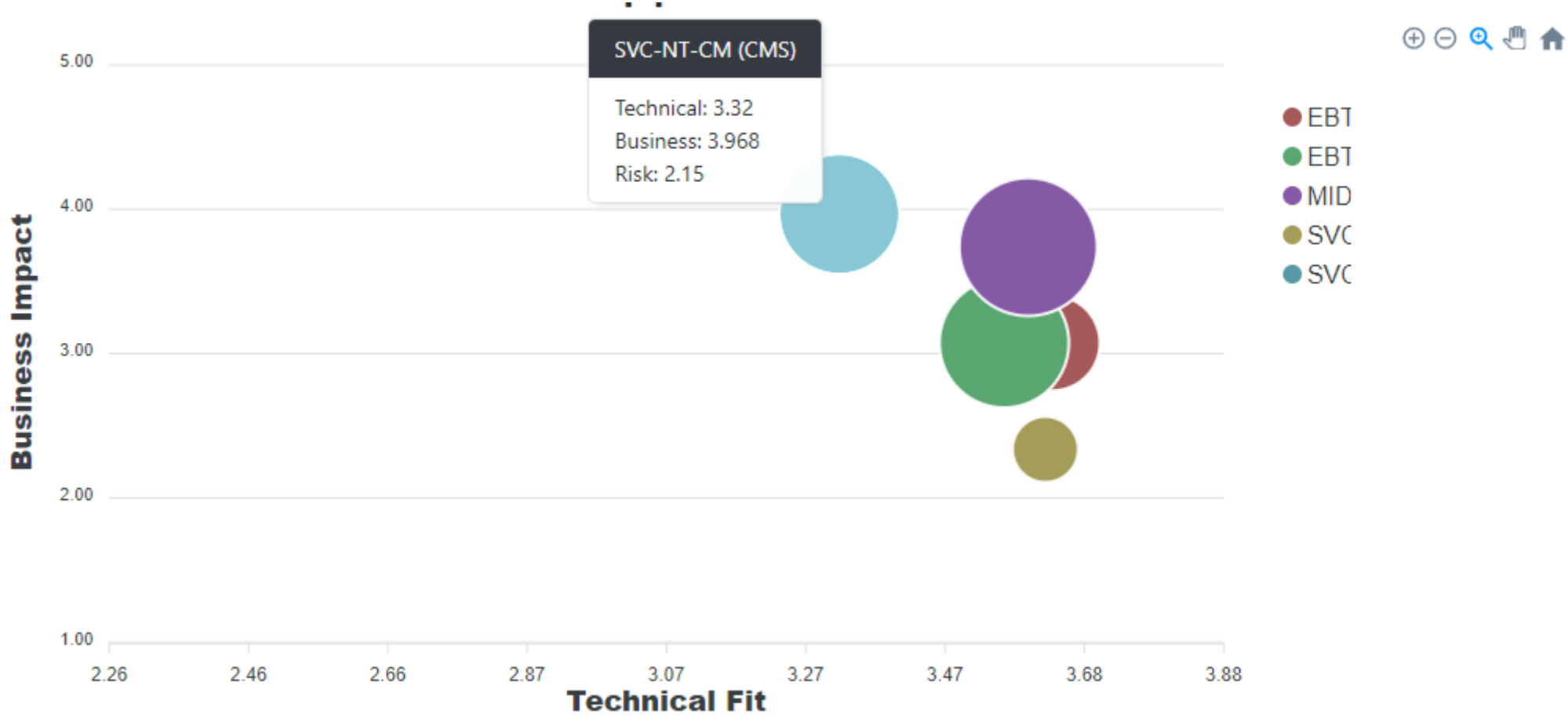
以子公司為單位進行諮詢

- 國泰產險 Cathay Century Insurance
- 國泰人壽 Cathay Life Insurance
- 國泰世華銀行 Cathay United Bank
- 國泰綜合證券 Cathay Securities Corporation

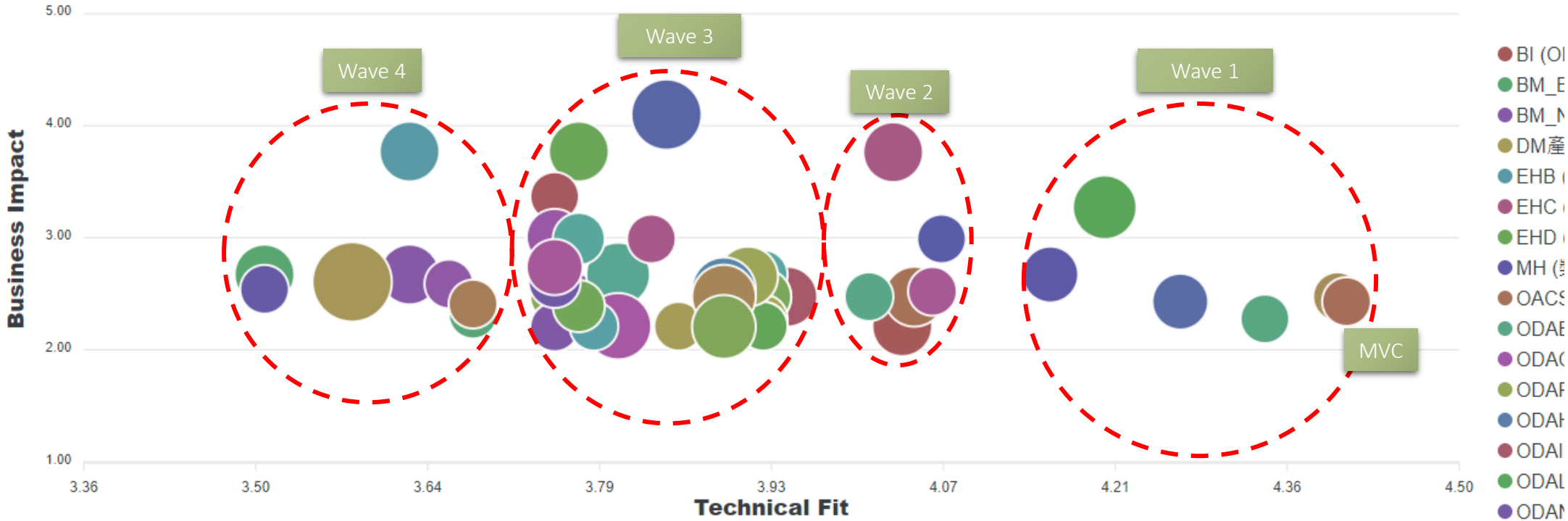
評估流程

系統評估 > 圖表呈現 > 排定順序

5個應用系統上雲評估

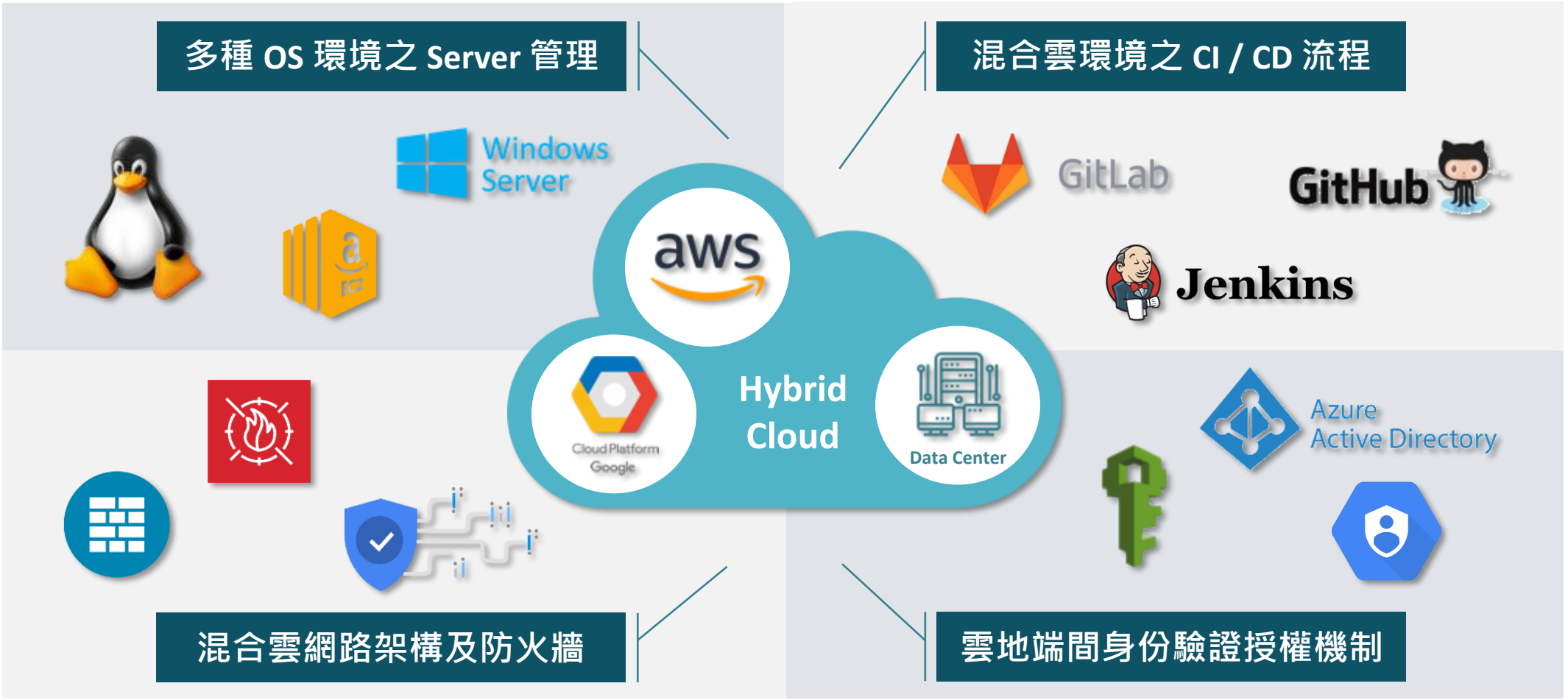

SVC-NT-CM (CMS)
Technical: 3.32
Business: 3.968
Risk: 2.15
Business Impact
5.00
4.00
3.00
2.00
1.00
2.26
2.46
2.66
2.87
3.07
3.27
3.47
3.68
3.88
Technical Fit
EBT
EBT
MID
SVC
SVC

50個應用系統上雲評估 → 500個應用系統上雲評估

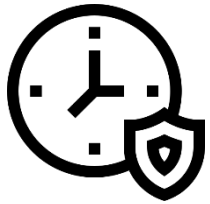


同時在基礎建設、雲端環境及週邊網路環境也要符合雲端發展策略條件

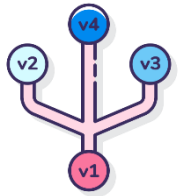
在基礎建設方面，由於我們採混合雲架構，對網路架構設計更為重要



在混合雲架構中使用IaC雲端自動化技術，有助於資安、合規、管理、治理等要求

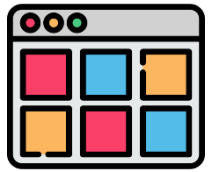


速度與安全性



可版本管理

環境一致



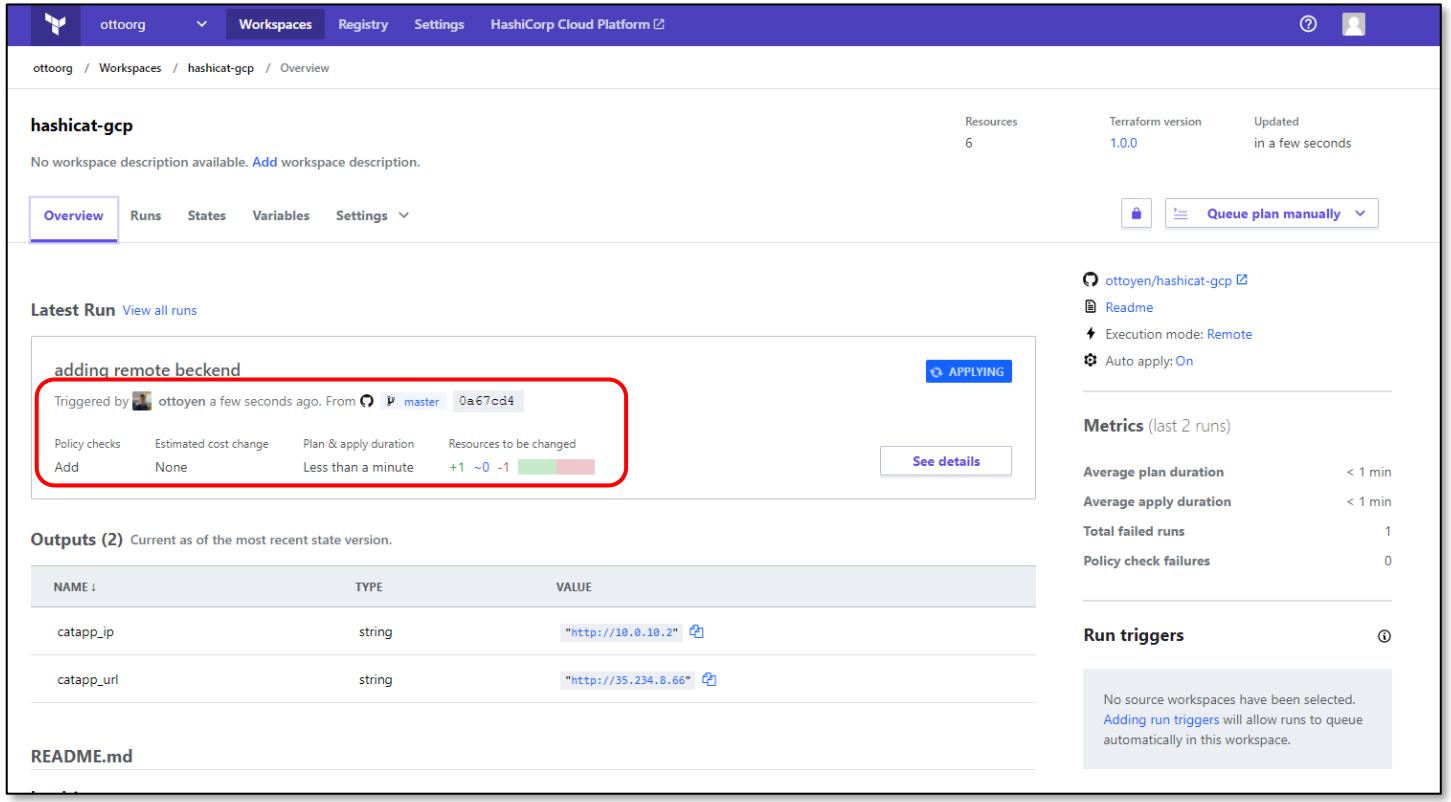
檢核作業面合規性

容易追蹤問題

稽核與軌跡

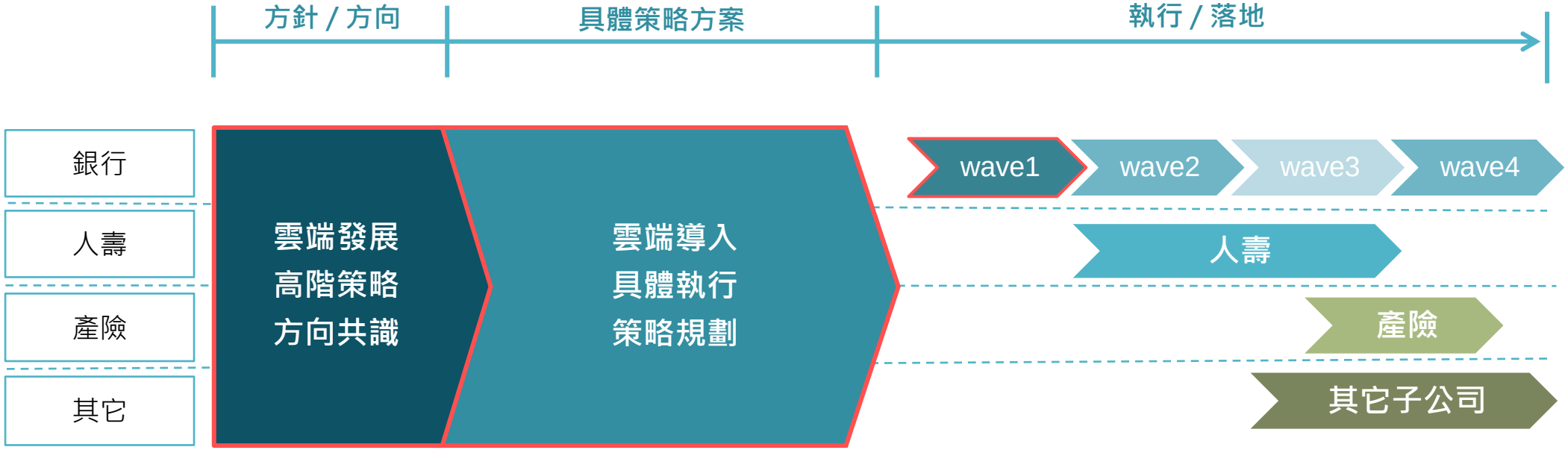
藉由IaC技術達到Policy、Compliance、Security、Cost Control as Code

- Policy
  - Limit region
  - Naming rule
- Security
  - Can’t assign public IP
  - Firewall source range
- Compliance
  - CIS benchmark
  - PCI DSS
- Cost limit
  - Limit machine type
  - Limit disk size



國泰集團轉型上雲旅程

發展目標將著重在集團雲端發展策略及銀行端的導入



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