Track 2 | Session 2

電商平台的資安維運與成本管理

Annie Lin

Territory Business Development Manager

Amazon Web Services

Rick Hwang

Senior Technical Manager

91APP

aws SUMMIT ONLINE

Agenda

What is cost optimization?

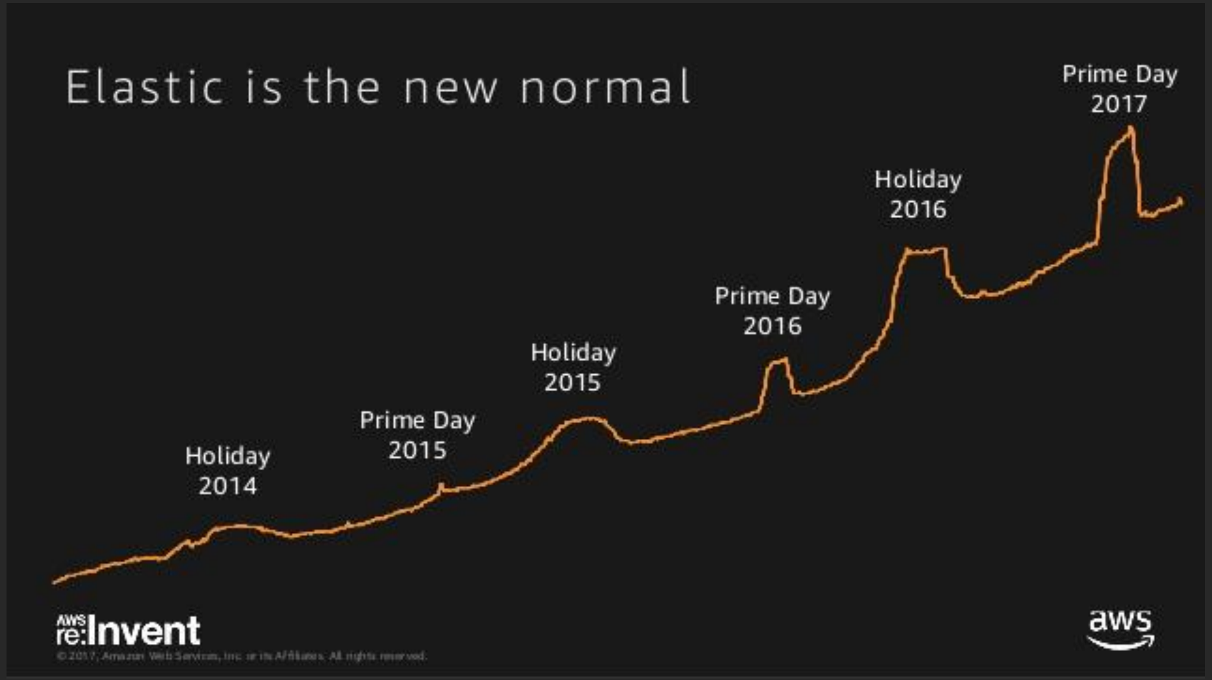
Financial management

Operation efficiency with security

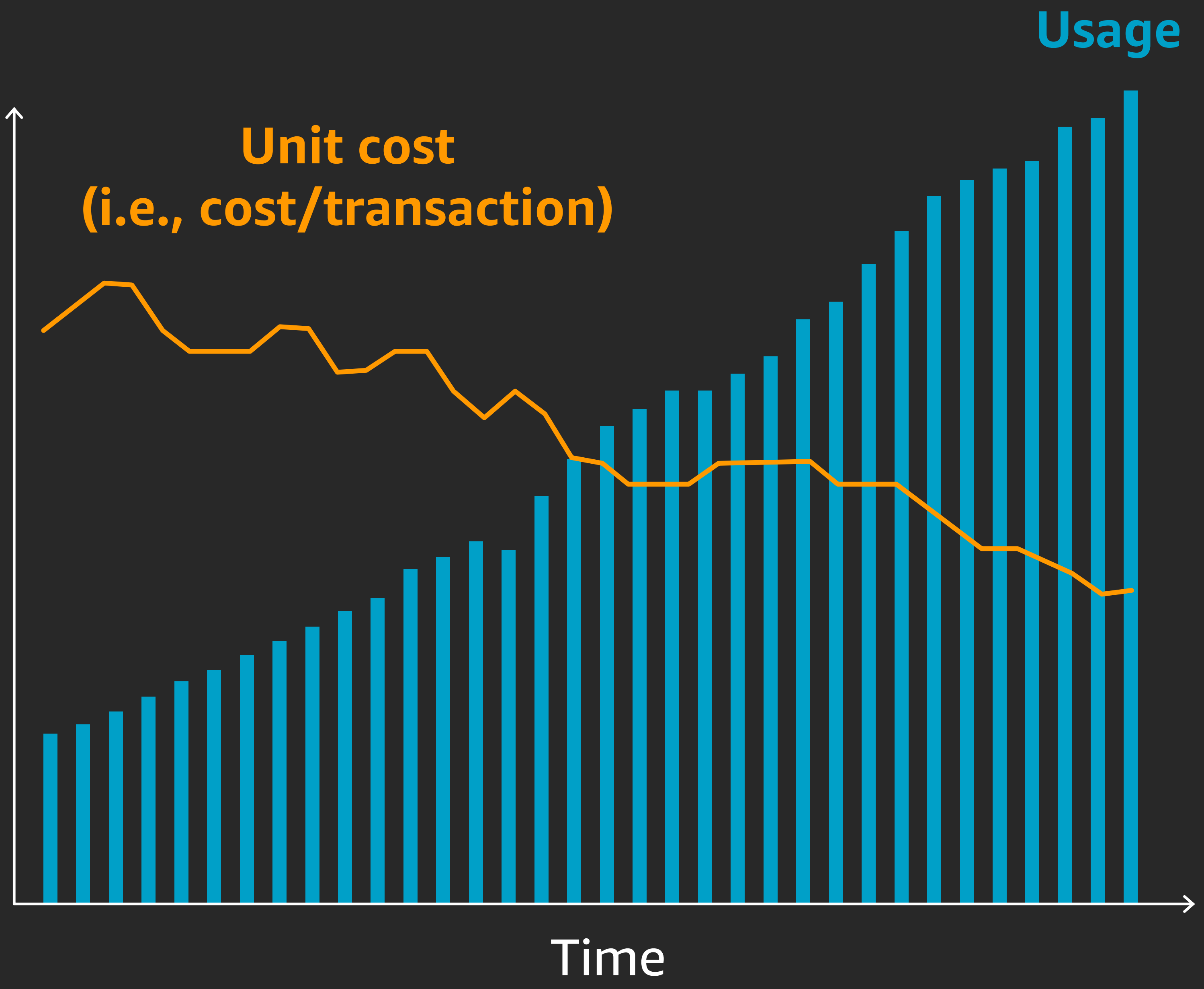
Get real-time guidance from AWS

What is cost optimization?

Ecommerce: it’s hard (and it’s getting harder)



Elastic is the new normal



Large events, sustained growth

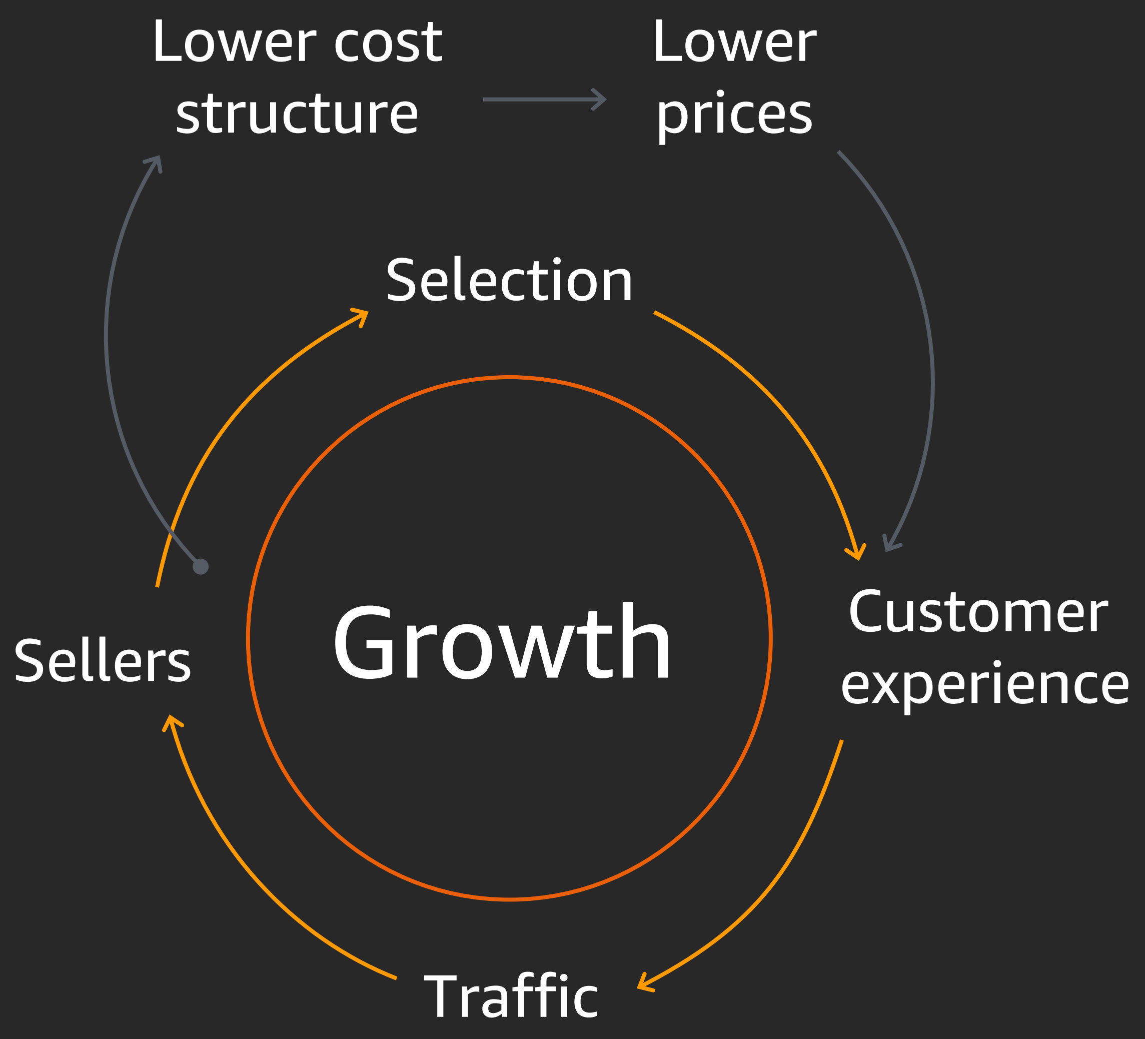
For example, Black Friday and Prime Day at *Amazon.com*

What is cost optimization?

The ability to run systems to
deliver **business value**
at the lowest **price point**

Financial management

AWS lowers prices over time



80

price reductions since 2006

(as of February 6, 2020)

Savings Plans: flexibility and management costs

Highest discount
up to 72%

High discount
up to 66%

Standard RI

Regional RI
(AZ)

Size flex (AWS Linux)
(AZ, size)

Convertible RI
(AZ, size, family, OS, tenancy)

EC2 Instance Savings Plans
(AZ, size, OS, tenancy)

Compute Savings Plans
(AZ, size, family, OS, tenancy, region, service)

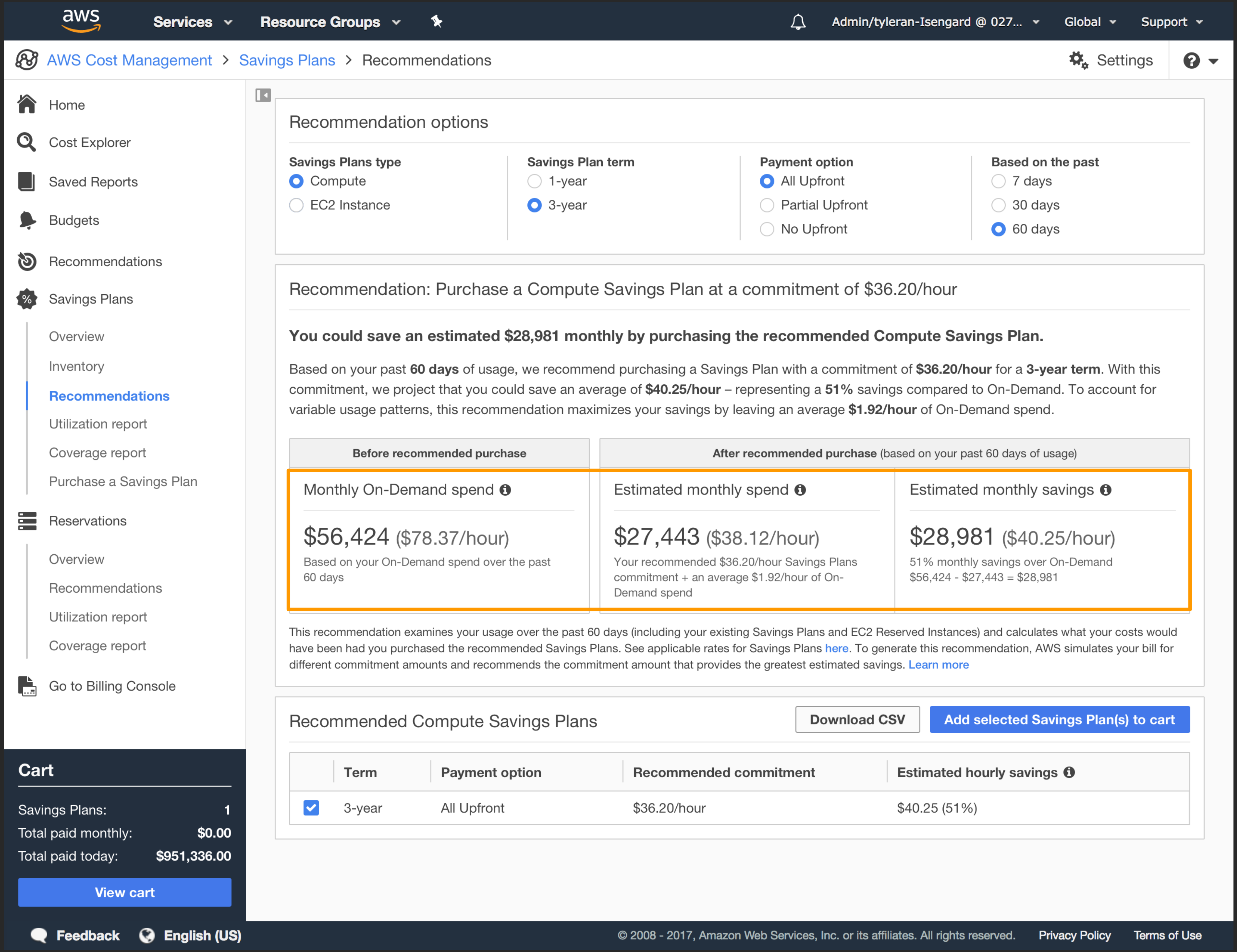
FLEXIBLE ACROSS

- ✓ Size: E.g. move from m5.xl to m5.4xl
- ✓ OS: E.g. change from m5.xl Windows to m5.xl Linux
- ✓ Tenancy: E.g. modify m5.xl Dedicated to m5.xl Default tenancy

FLEXIBLE ACROSS

- ✓ Instance family: E.g. Move from C5 to M5
- ✓ Region: E.g. change from EU (Ireland) to EU (London)
- ✓ OS: E.g. Windows to Linux
- ✓ Tenancy: E.g. switch Dedicated tenancy to Default tenancy
- ✓ Compute options: E.g. move from EC2 to Fargate or Lambda

Simplified purchasing experience via AWS Cost Explorer



Cart

Savings Plans:	1
Total paid monthly:	$0.00
Total paid today:	$951,336.00

View cart

Recommendation options

Savings Plans type
● Compute
○ EC2 Instance

Savings Plan term
○ 1-year
● 3-year

Payment option
● All Upfront
○ Partial Upfront
○ No Upfront

Based on the past
○ 7 days
○ 30 days
● 60 days

Recommendation: Purchase a Compute Savings Plan at a commitment of $36.20/hour

You could save an estimated $28,981 monthly by purchasing the recommended Compute Savings Plan.

Based on your past **60 days** of usage, we recommend purchasing a Savings Plan with a commitment of **$36.20/hour** for a **3-year term**. With this commitment, we project that you could save an average of **$40.25/hour** – representing a **51%** savings compared to On-Demand. To account for variable usage patterns, this recommendation maximizes your savings by leaving an average **$1.92/hour** of On-Demand spend.

Before recommended purchase	**After recommended purchase** (based on your past 60 days of usage)	
Monthly On-Demand spend	Estimated monthly spend	Estimated monthly savings
$56,424 ($78.37/hour) Based on your On-Demand spend over the past 60 days	$27,443 ($38.12/hour) Your recommended $36.20/hour Savings Plans commitment + an average $1.92/hour of On-Demand spend	$28,981 ($40.25/hour) 51% monthly savings over On-Demand $56,424 - $27,443 = $28,981

This recommendation examines your usage over the past 60 days (including your existing Savings Plans and EC2 Reserved Instances) and calculates what your costs would have been had you purchased the recommended Savings Plans. See applicable rates for Savings Plans here. To generate this recommendation, AWS simulates your bill for different commitment amounts and recommends the commitment amount that provides the greatest estimated savings. Learn more

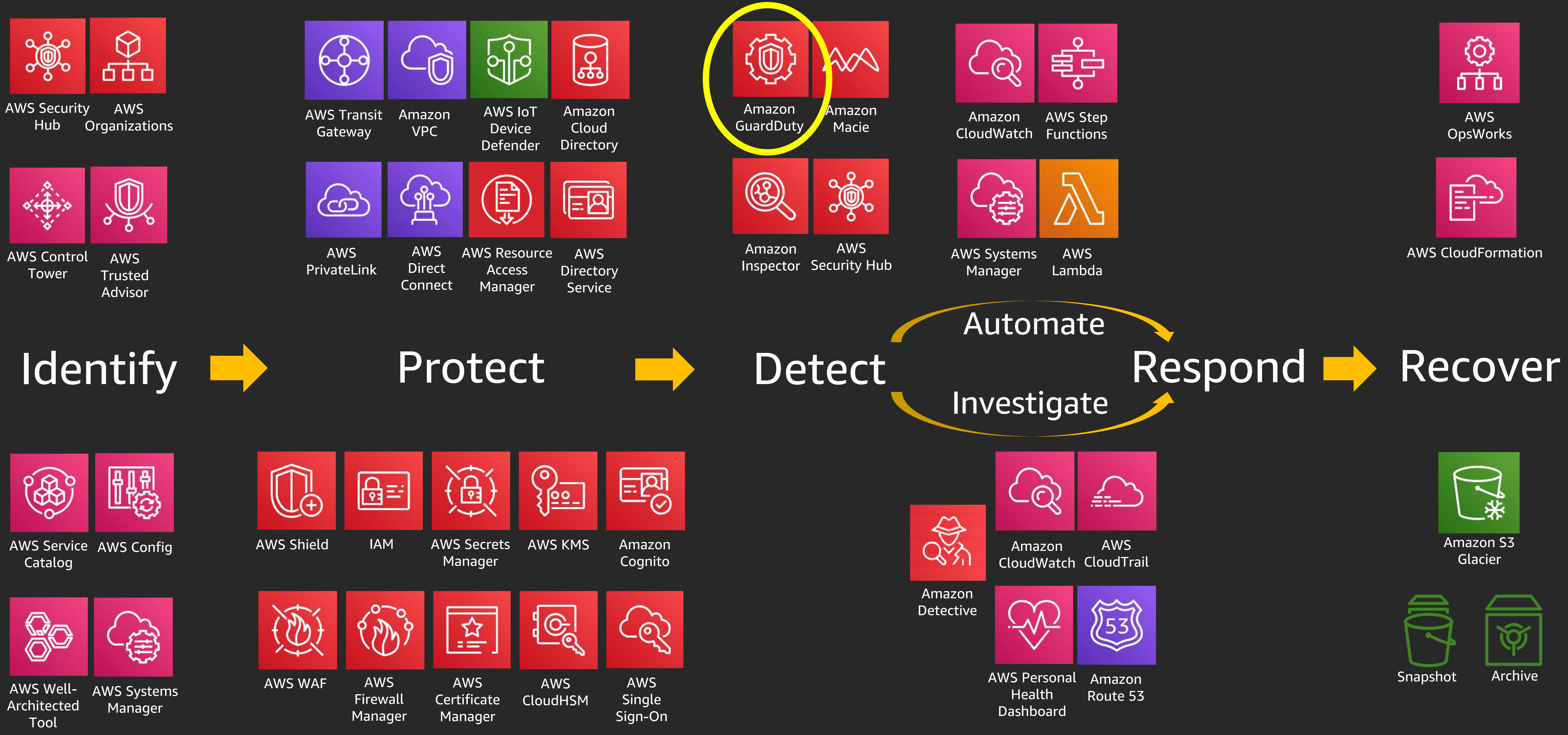
Recommended Compute Savings Plans

Download CSV | Add selected Savings Plan(s) to cart

	Term	Payment option	Recommended commitment	Estimated hourly savings
☑	3-year	All Upfront	$36.20/hour	$40.25 (51%)

Operation efficiency with security

AWS foundational and layered security services



AWS Security Hub

AWS Organizations

AWS Control Tower

AWS Trusted Advisor

Identify

AWS Service Catalog

AWS Config

AWS Well-Architected Tool

AWS Systems Manager

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

AWS PrivateLink

AWS Direct Connect

AWS Resource Access Manager

AWS Directory Service

Protect

AWS Shield

IAM

AWS Secrets Manager

AWS KMS

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Detect

Automate

Investigate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Respond

Amazon Detective

Amazon CloudWatch

AWS CloudTrail

AWS Personal Health Dashboard

Amazon Route 53

AWS OpsWorks

AWS CloudFormation

Recover

Amazon S3 Glacier

Snapshot

Archive

GuardDuty: key features

Managed threat detection service

One-click activation with no architectural or performance impact

Continuous monitoring of your AWS accounts and resources

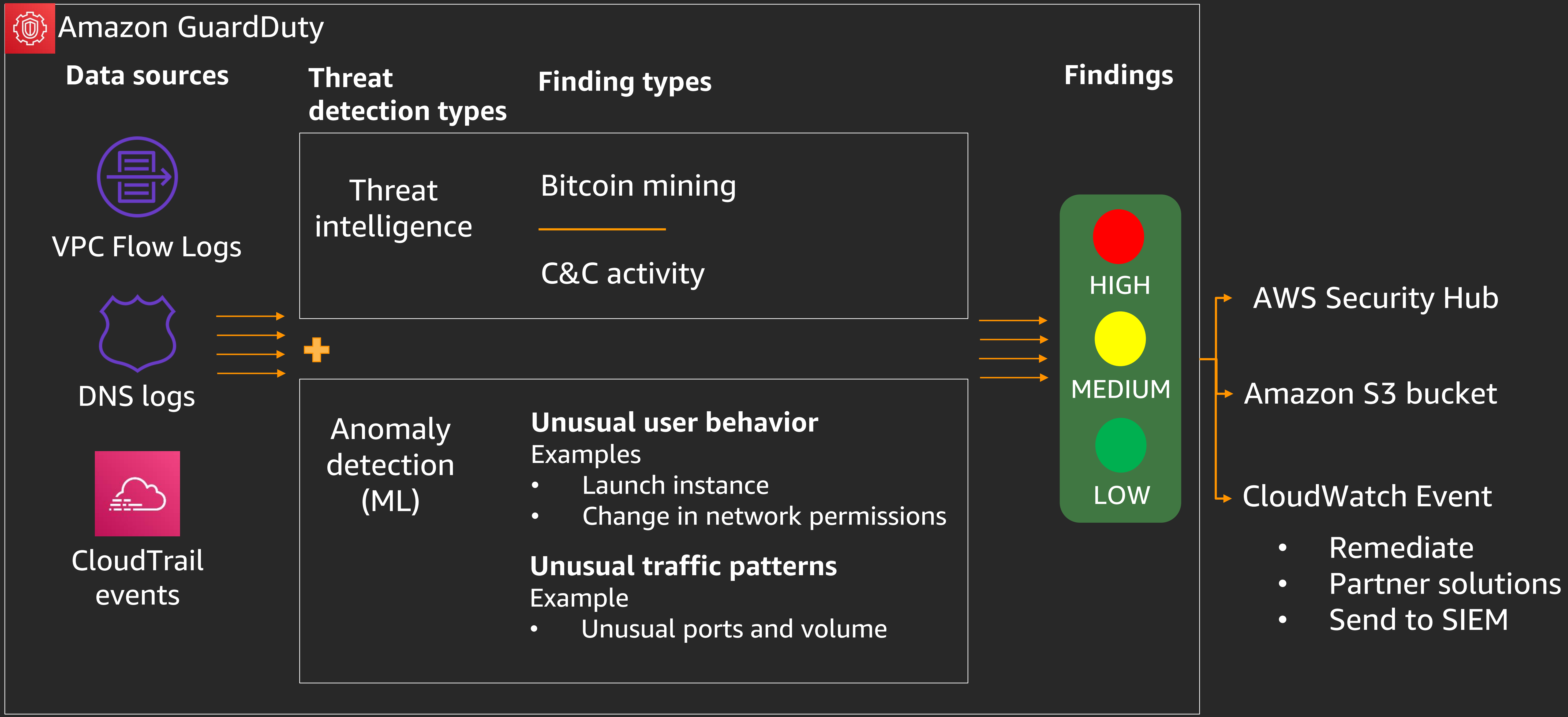
Global coverage with regional results

Detects known threats (threat intel–based)

Detects unknown threats (behavior-based)

Enterprise-wide consolidation and management

How Amazon GuardDuty works



Amazon GuardDuty

Data sources

VPC Flow Logs

DNS logs

CloudTrail events

Threat detection types

Finding types

Threat intelligence

Bitcoin mining

C&C activity

Anomaly detection (ML)

Unusual user behavior
Examples

- Launch instance
- Change in network permissions

Unusual traffic patterns
Example

- Unusual ports and volume

Findings

HIGH

MEDIUM

LOW

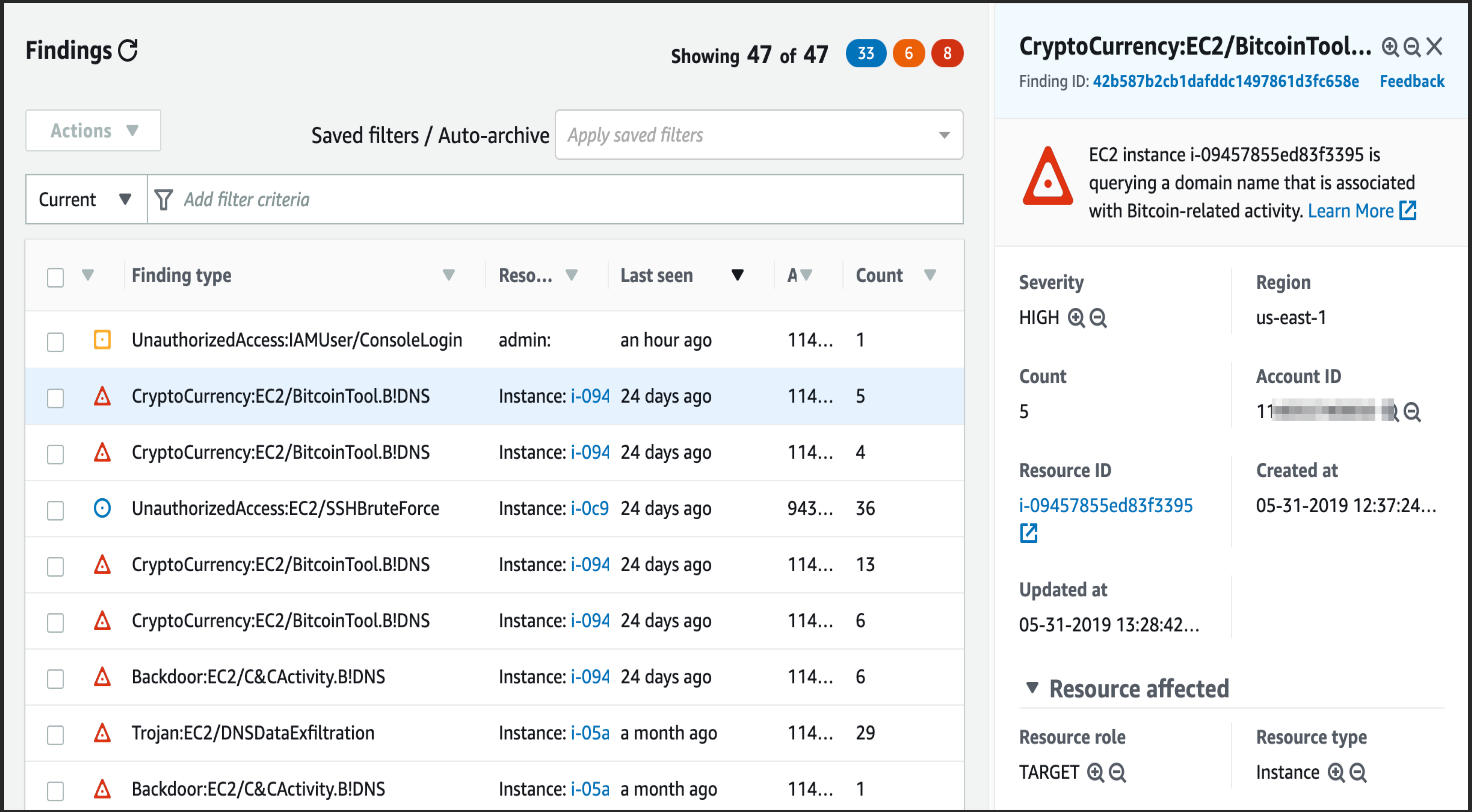
AWS Security Hub

Amazon S3 bucket

CloudWatch Event

- Remediate
- Partner solutions
- Send to SIEM

Reviewing findings



Findings ↻

Showing 47 of 47 33 6 8

Actions ▼ Saved filters / Auto-archive *Apply saved filters*

Current ▼ *Add filter criteria*

□		Finding type	Reso...	Last seen	A	Count
□	□	UnauthorizedAccess:IAMUser/ConsoleLogin	admin:	an hour ago	114...	1
□	△	CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	5
□	△	CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	4
□	○	UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-0c9	24 days ago	943...	36
□	△	CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	13
□	△	CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	6
□	△	Backdoor:EC2/C&CActivity.B!DNS	Instance: i-094	24 days ago	114...	6
□	△	Trojan:EC2/DNSDataExfiltration	Instance: i-05a	a month ago	114...	29
□	△	Backdoor:EC2/C&CActivity.B!DNS	Instance: i-05a	a month ago	114...	1

CryptoCurrency:EC2/BitcoinTool...

Finding ID: 42b587b2cb1dafddc1497861d3fc658e Feedback

EC2 instance i-09457855ed83f3395 is querying a domain name that is associated with Bitcoin-related activity. Learn More

Severity HIGH	**Region** us-east-1
Count 5	**Account ID** 11[redacted]
Resource ID i-09457855ed83f3395	**Created at** 05-31-2019 12:37:24...
Updated at 05-31-2019 13:28:42...	

▼ **Resource affected**

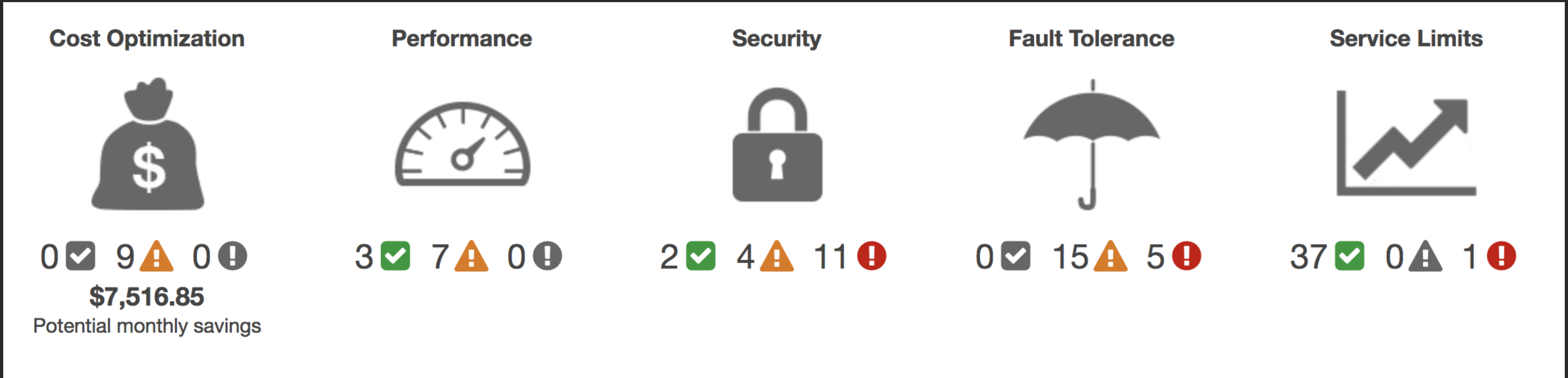
Resource role TARGET	**Resource type** Instance

Threat information

- Severity
- Region
- Count/Frequency
- Threat type
- Affected resource
- Source information
- Viewable via Amazon CloudWatch Events

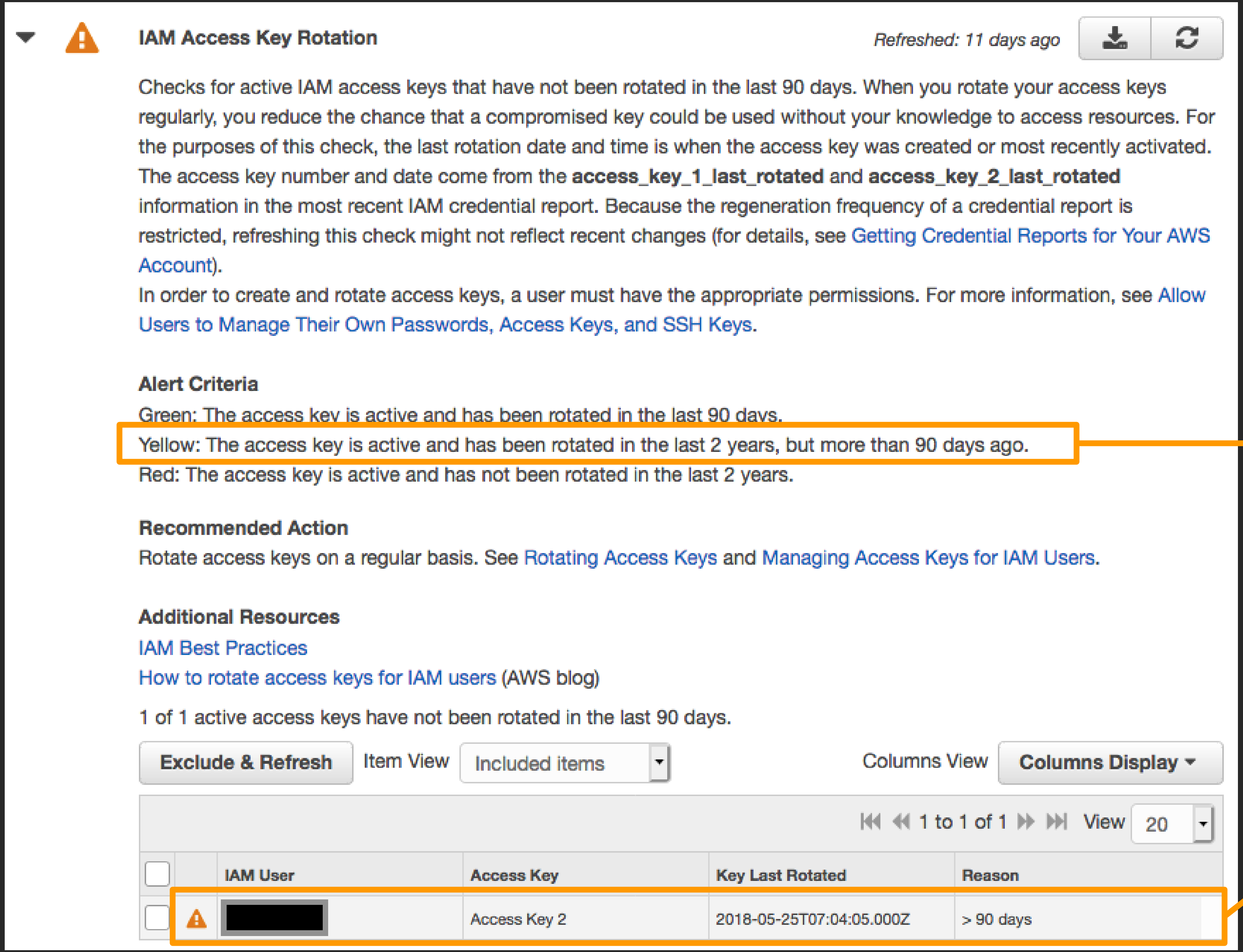
Get real-time guidance from AWS

AWS Trusted Advisor



Cost Optimization	Performance	Security	Fault Tolerance	Service Limits
0 ✓ 9 ⚠ 0 ❗	3 ✓ 7 ⚠ 0 ❗	2 ✓ 4 ⚠ 11 ❗	0 ✓ 15 ⚠ 5 ❗	37 ✓ 0 ⚠ 1 ❗
$7,516.85 Potential monthly savings				

Remediation sample: security



⚠ **IAM Access Key Rotation**

Refreshed: 11 days ago

Checks for active IAM access keys that have not been rotated in the last 90 days. When you rotate your access keys regularly, you reduce the chance that a compromised key could be used without your knowledge to access resources. For the purposes of this check, the last rotation date and time is when the access key was created or most recently activated. The access key number and date come from the **access_key_1_last_rotated** and **access_key_2_last_rotated** information in the most recent IAM credential report. Because the regeneration frequency of a credential report is restricted, refreshing this check might not reflect recent changes (for details, see Getting Credential Reports for Your AWS Account).
In order to create and rotate access keys, a user must have the appropriate permissions. For more information, see Allow Users to Manage Their Own Passwords, Access Keys, and SSH Keys.

Alert Criteria
Green: The access key is active and has been rotated in the last 90 days.
Yellow: The access key is active and has been rotated in the last 2 years, but more than 90 days ago.
Red: The access key is active and has not been rotated in the last 2 years.

Recommended Action
Rotate access keys on a regular basis. See Rotating Access Keys and Managing Access Keys for IAM Users.

Additional Resources
IAM Best Practices
How to rotate access keys for IAM users (AWS blog)

1 of 1 active access keys have not been rotated in the last 90 days.

☐		IAM User	Access Key	Key Last Rotated	Reason
☐	⚠	[redacted]	Access Key 2	2018-05-25T07:04:05.000Z	> 90 days

Reason for the alert

Resource causing the alert

Summary: state of cost optimization

Do you have a cost optimization team or function?

Do you have an operations team or function?

Do you have a security team or function?

Billing → Value and efficiency

在矩陣型組織裡，如何有效管理 AWS 的成本結構與系統架構

Rick Hwang

Senior Technical Manager
91APP

aws SUMMIT ONLINE

Agenda

91APP 公司簡介

背景與現象

目標與方向

嘗試與改變

總結與摘要

91APP 公司簡介

91APP

品牌新零售
虛實融合OMO最佳夥伴

公司介紹

虛實融合OMO最佳夥伴

台灣最大 & 成長最快
品牌新零售解決方案公司

- 為零售企業打造線上電商&門市OMO循環
- 2013年成立，前Yahoo!、興奇科技經營團隊創辦
- 總部在台北，馬來西亞/香港分公司
- 公司同仁逾400人
- 連續四年榮獲「創新商務獎/最佳商業模式」
- 獲選「勤業眾信亞太區高科技高成長前500強」

(Ranked 152th,Deloitte Technology Fast 500 Asia Pacific)

品牌客戶超過10,000家

獲國內外大型實體零售品牌肯定，91APP 協助多家企業成功推動 OMO 變革轉型

Dior
MAKE UP FOR EVER PROFESSIONAL - PARIS
GUERLAIN PARIS
3INA
全聯福利中心
FamilyMart
康是美 COSMED
PHILIPS

AIGLE DEPUIS 1853
RIVER WOODS Est. 59
.st TAIWAN
STRIPE CLUB TAIWAN
Levi's®
SKECHERS
Keds
Dickies

Crate&Barrel
乾唐軒 ACERA
王德傳 Wang De Chuan Fine Chinese Tea Since 1862
Columbia
BLUE WAY
Triumph
Wacoal
Mode Marie 曼黛瑪璉

Timberland
THE NORTH FACE
kipling
HILLTOP EST.1984
歐都納 ATUNAS
LA NEW
SO NICE
伊蕾名店 NEW FASHION COLLECTION

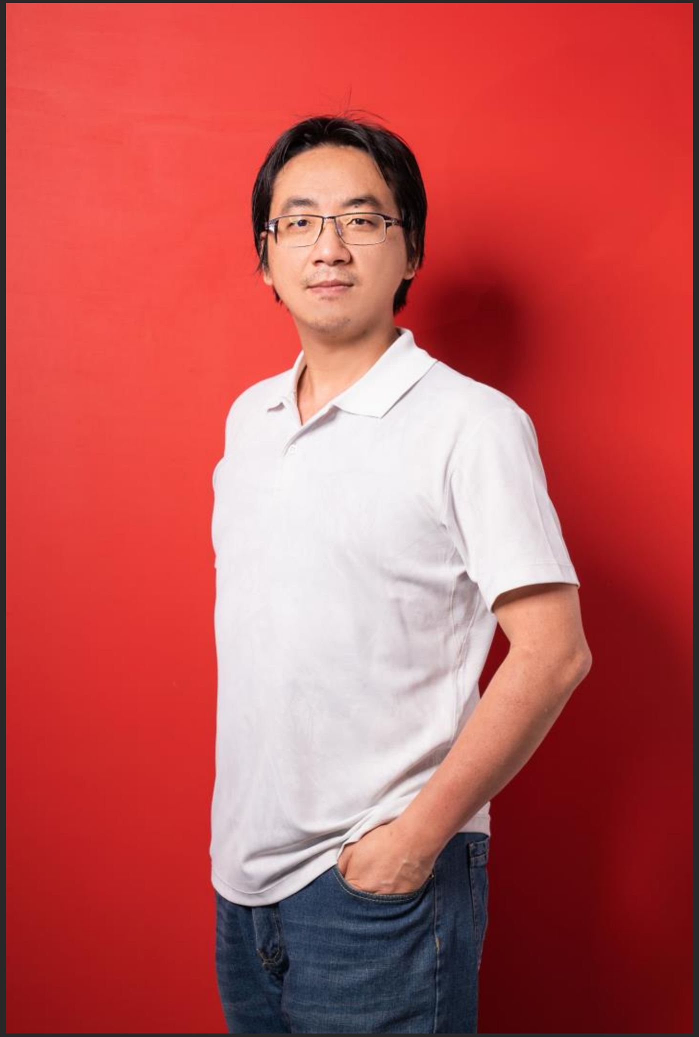
台塑生醫 FORMOSA BIOMEDICAL
THEFACESHOP NATURAL STORY
小三美日 make ∞ beauty
ISPO 伊仕柏
METROASIS OUTDOORS 城市綠洲 戶外生活館
STAY REAL
NATURALLY JOJO
蜜雪兒 MYSHEROS

講者背景: Rick Hwang

- Sr. Manager @ 91APP

- 經營管理
- Cloud / AWS
- DevOps / SRE
- Distributed Systems

- 音樂 吉他 鍵盤 編曲
- 哲學 科幻 金庸 喇賽



91APP

- Complete Think、喝咖啡聊音樂、譯著：分散式系統設計

背景與現象

背景：矩陣型組織與敏捷開發模式

數十個功能型部門 (Functional Teams)，200+ 人的團隊

- PM、PO、HD
- Backend、DBA
- Frontend、Mobile
- QA、QE
- Infra、Security、Data
- Architect

數個團隊 (Mission Teams)，數個產品線別

- OMO
- E-Commerce
- User Experience Optimization
- Enterprise Service
- CRM
- Globalization Team
- … etc

背景：產品系統與系統架構

5 / 個

產品線

6 / 個

業務市場

10+ / 個

Accounts

20+ / 個

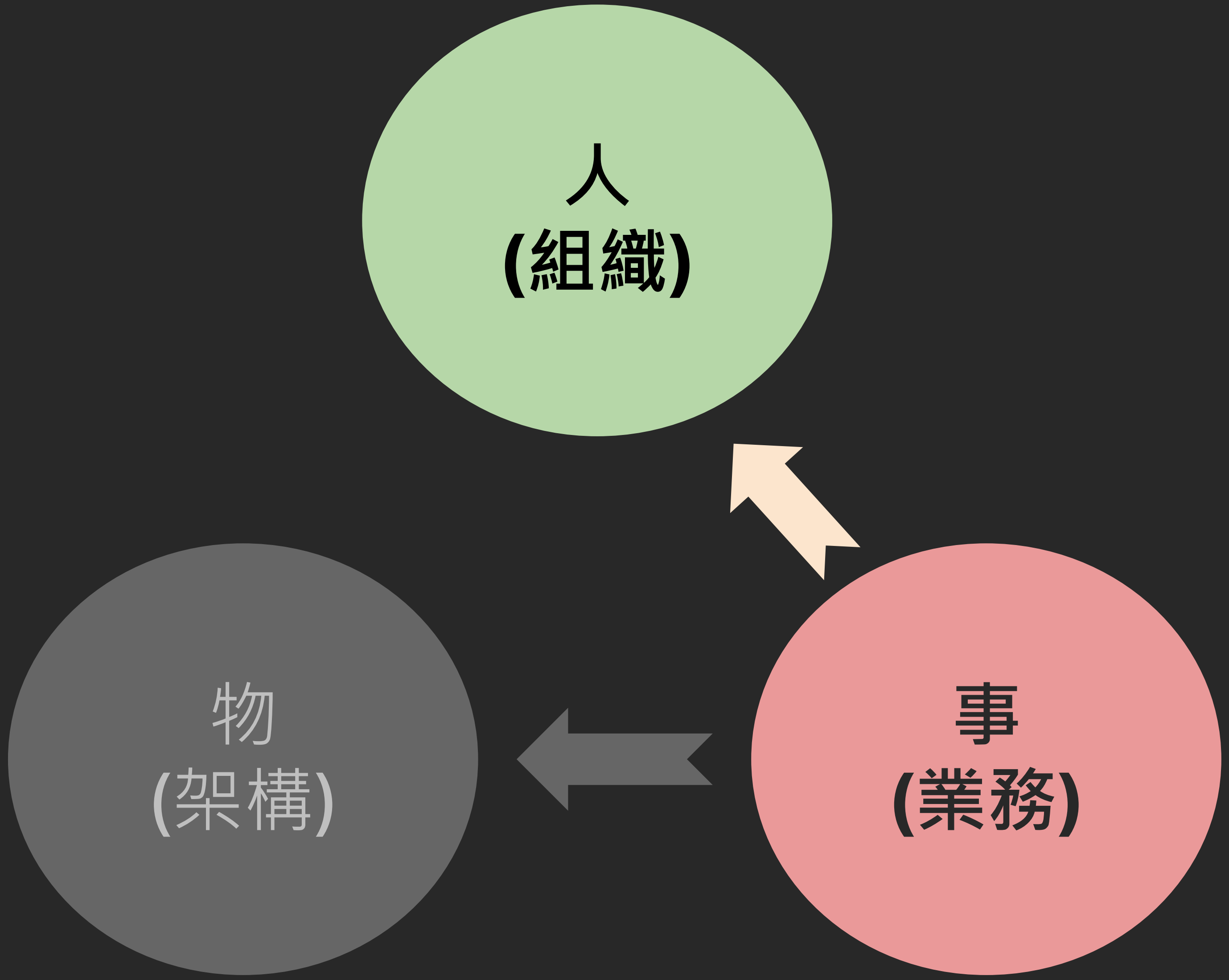
VPCs

40+ / 個

Services

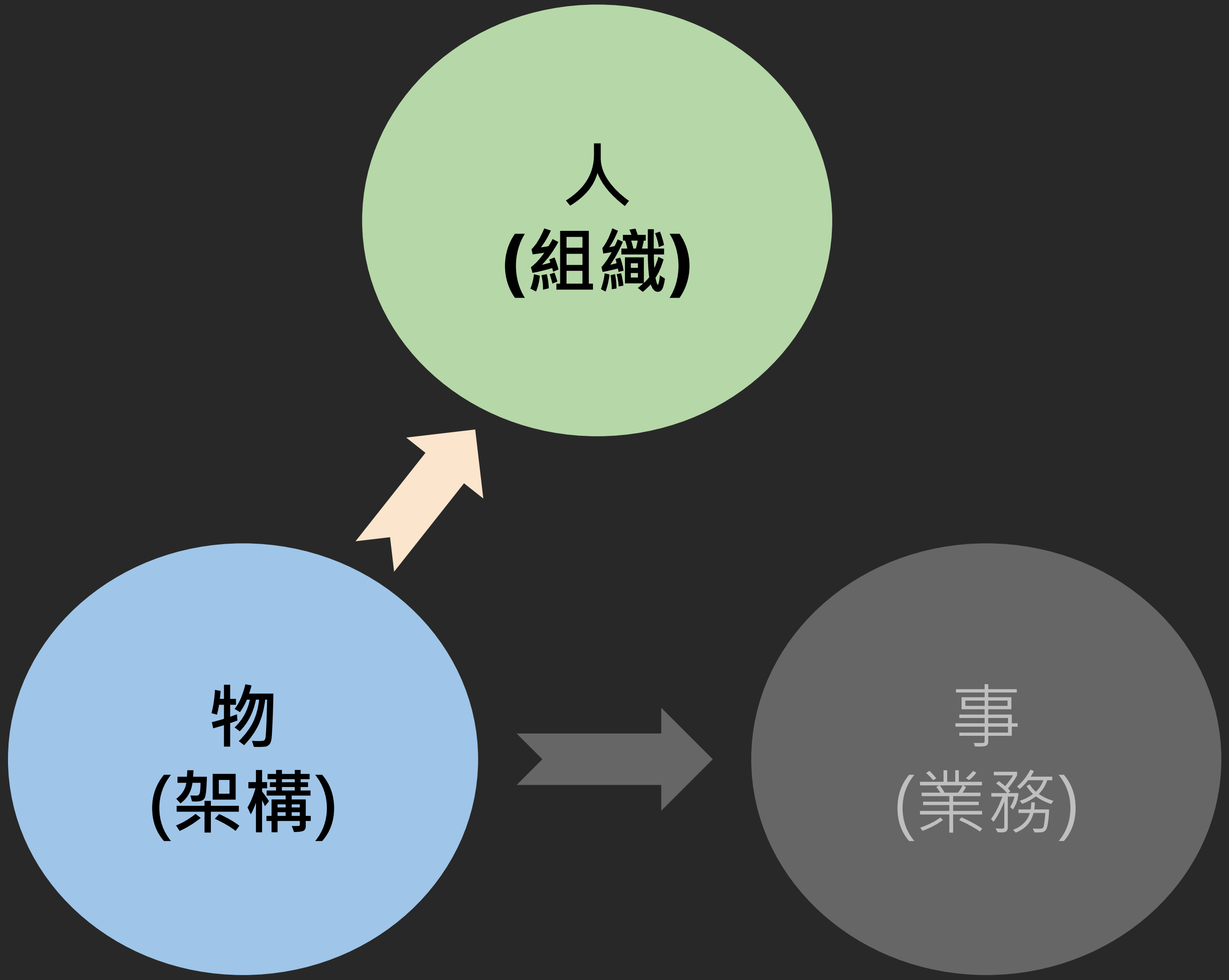
現象一：業務的驅動

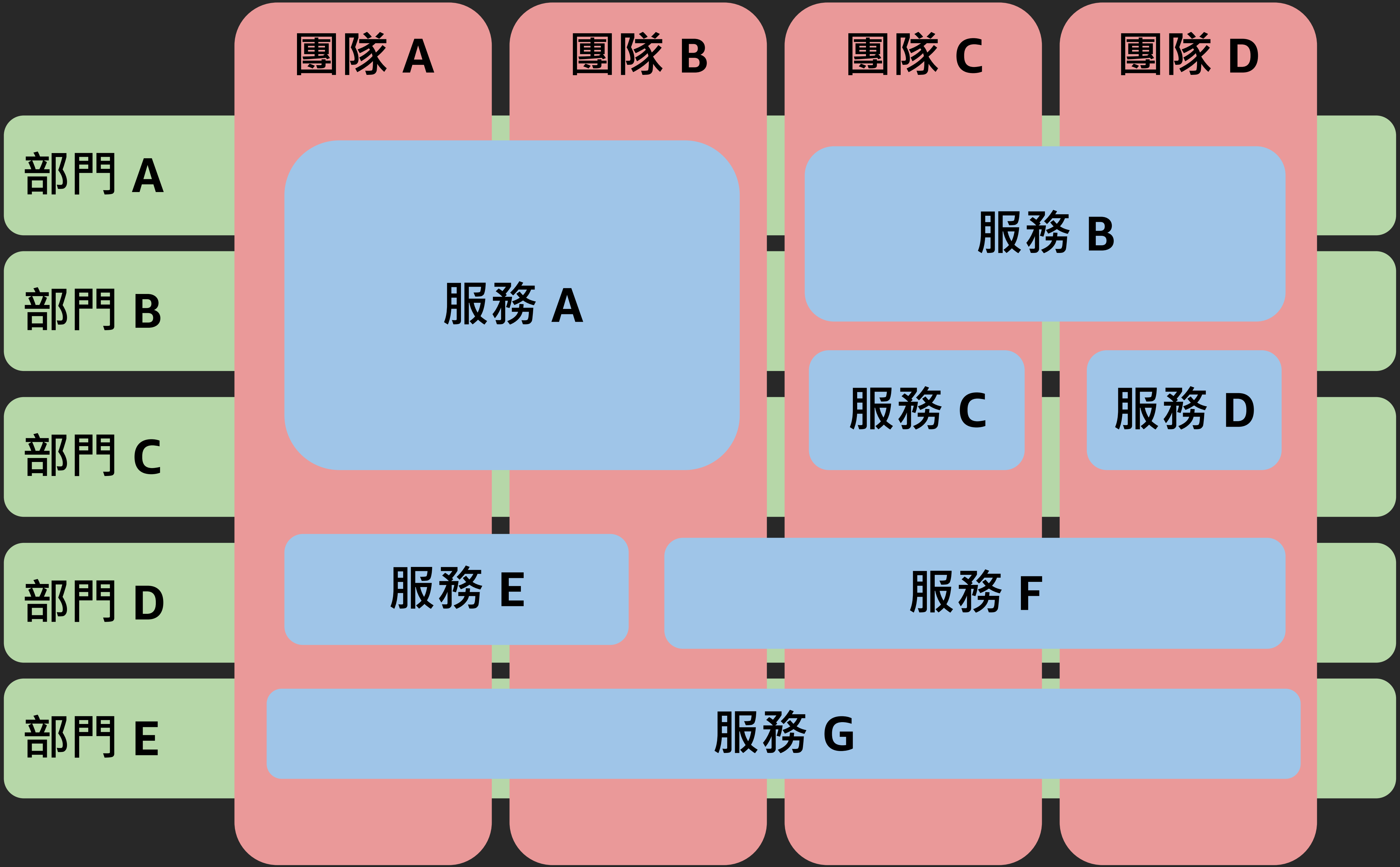
- 市場變了，調整業務方向
- 調整團隊的組織架構，但與系統關係卻已脫勾
- 已經在運行的**系統服務**不易改變
- 業務驅動，屬於外在顯性需求



現象二：與系統的連結

- 內部增加基礎服務，部署多環境，像是導入 EKS、Service Mesh、KMS、EFS，技術架構複雜。
- 系統架構與業務脫鉤，收入與支出不對稱
- 技術驅動，屬於內在隱性需求





團隊 A

團隊 B

團隊 C

團隊 D

部門 A

部門 B

部門 C

部門 D

部門 E

服務 A

服務 B

服務 C

服務 D

服務 E

服務 F

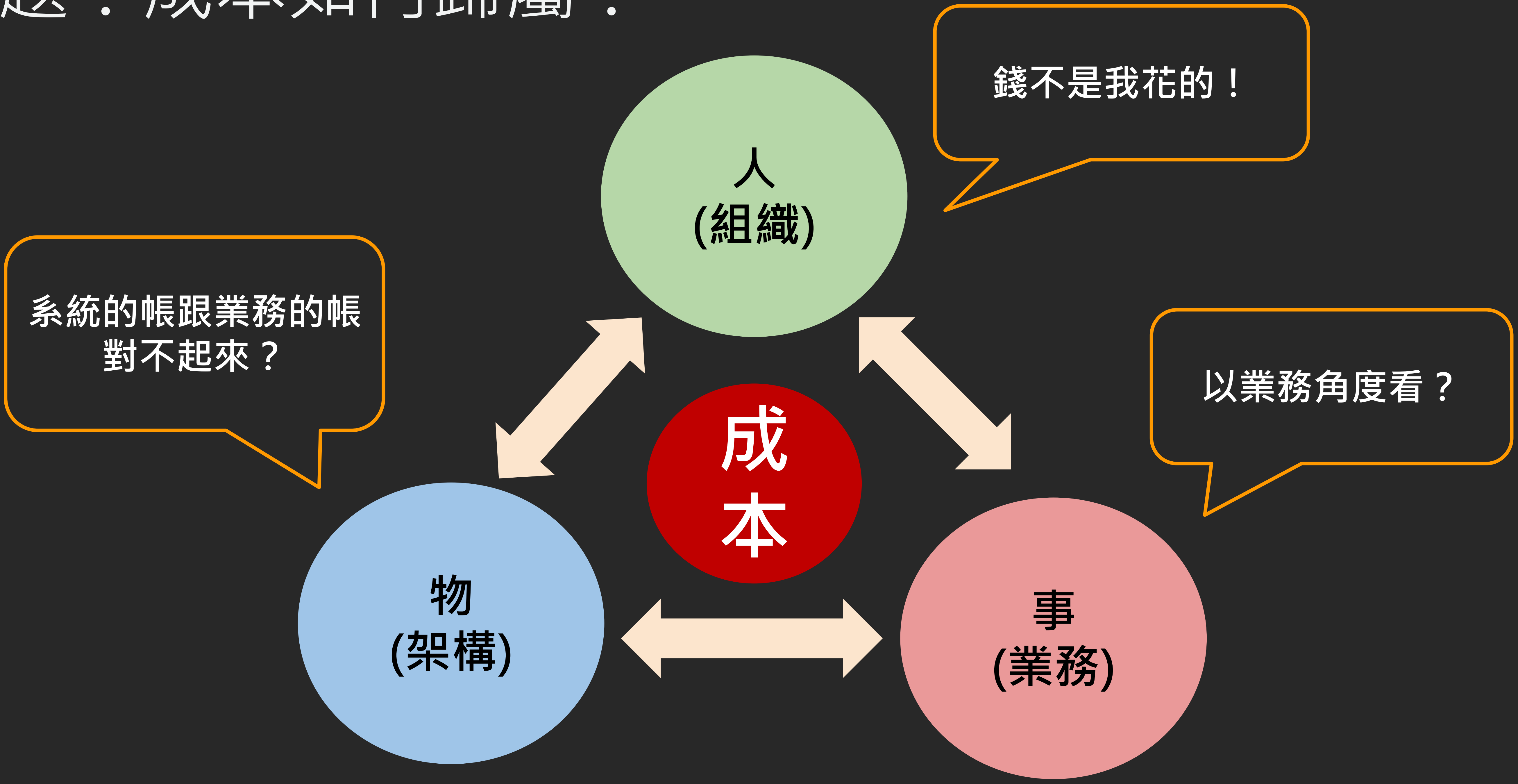
服務 G

🟩 組織 (人) → 部門

🟥 業務 (事) → 團隊

🟦 系統 (物) → 服務

問題：成本如何歸屬？

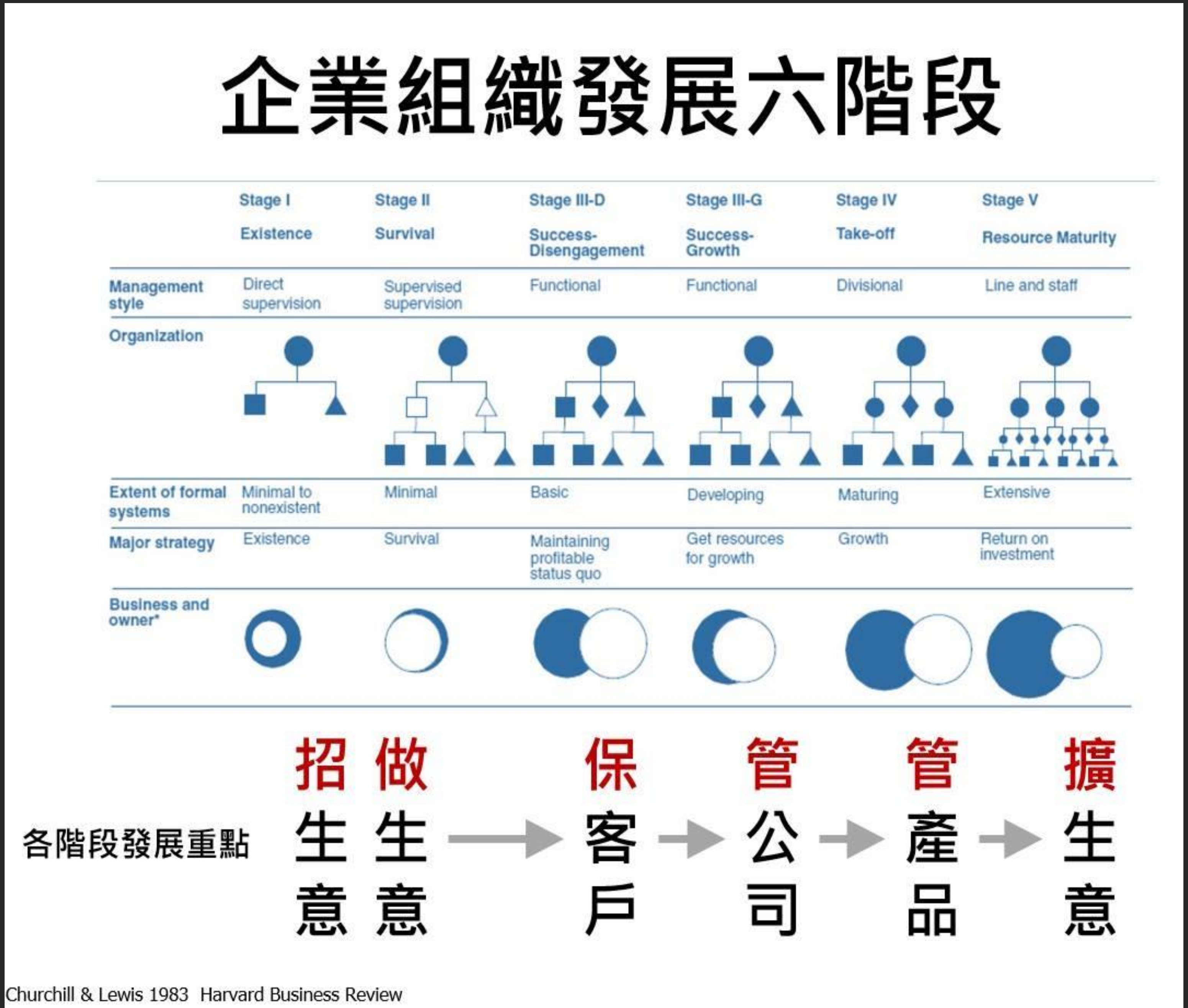


目標與方向

公司進入快速成長、擴展業務階段

即保客戶、管公司。

開源與節流並重。



企業組織發展六階段

	Stage I Existence	Stage II Survival	Stage III-D Success-Disengagement	Stage III-G Success-Growth	Stage IV Take-off	Stage V Resource Maturity
Management style	Direct supervision	Supervised supervision	Functional	Functional	Divisional	Line and staff
Organization						
Extent of formal systems	Minimal to nonexistent	Minimal	Basic	Developing	Maturing	Extensive
Major strategy	Existence	Survival	Maintaining profitable status quo	Get resources for growth	Growth	Return on investment
Business and owner*						

各階段發展重點　招生意　做生意 → 保客戶 → 管公司 → 管產品 → 擴生意

Churchill & Lewis 1983 Harvard Business Review

https://hbr.org/1983/05/the-five-stages-of-small-business-growth

目標一：讓業務可以規模化

- 網路基礎架構
- 組織權限管理策略
- 配置管理
- 產出物管理
- CI / CD 規模化

微服務的基礎建設 - Service Discovery - Andrew Wu

從零開始的 Configuration Management - Levi Chen

談產出物管理 (Artifacts Management) - Rick Hwang

目標二：成本可管可控

- 資源使用率
- 資源管理策略
- 資源歸屬
- 成本結構與分析

“If You Can’t Measure It,

You Can’t Improve It.”

Peter Drucker

嘗試與改變

嘗試一：定義 AWS Resource Tag 規範

了解**成本結構**與**歸屬**，定義 Tag 規範，依照三個維度圈：

1. By Mission Teams (團隊)
2. By Departments (部門)
3. By Services (服務)

- Tagging Best Practices - Implement an Effective AWS Resource Tagging Strategy
- Tagging AWS resources

問題

結構問題：

1. 團隊隨業務改變而調整 ⊗
2. 部門與業務連結太弱 ⊗
3. 服務與業務跟團隊有關係 ⚠

技術問題：

1. 資源數量多，標記 Tag 需要人工判斷
2. 有些 AWS 服務的 Tag 是隱藏的，像是 CloudWatch Log
3. 有些成本無法標記 Tag，像是資料傳輸

得到的結論

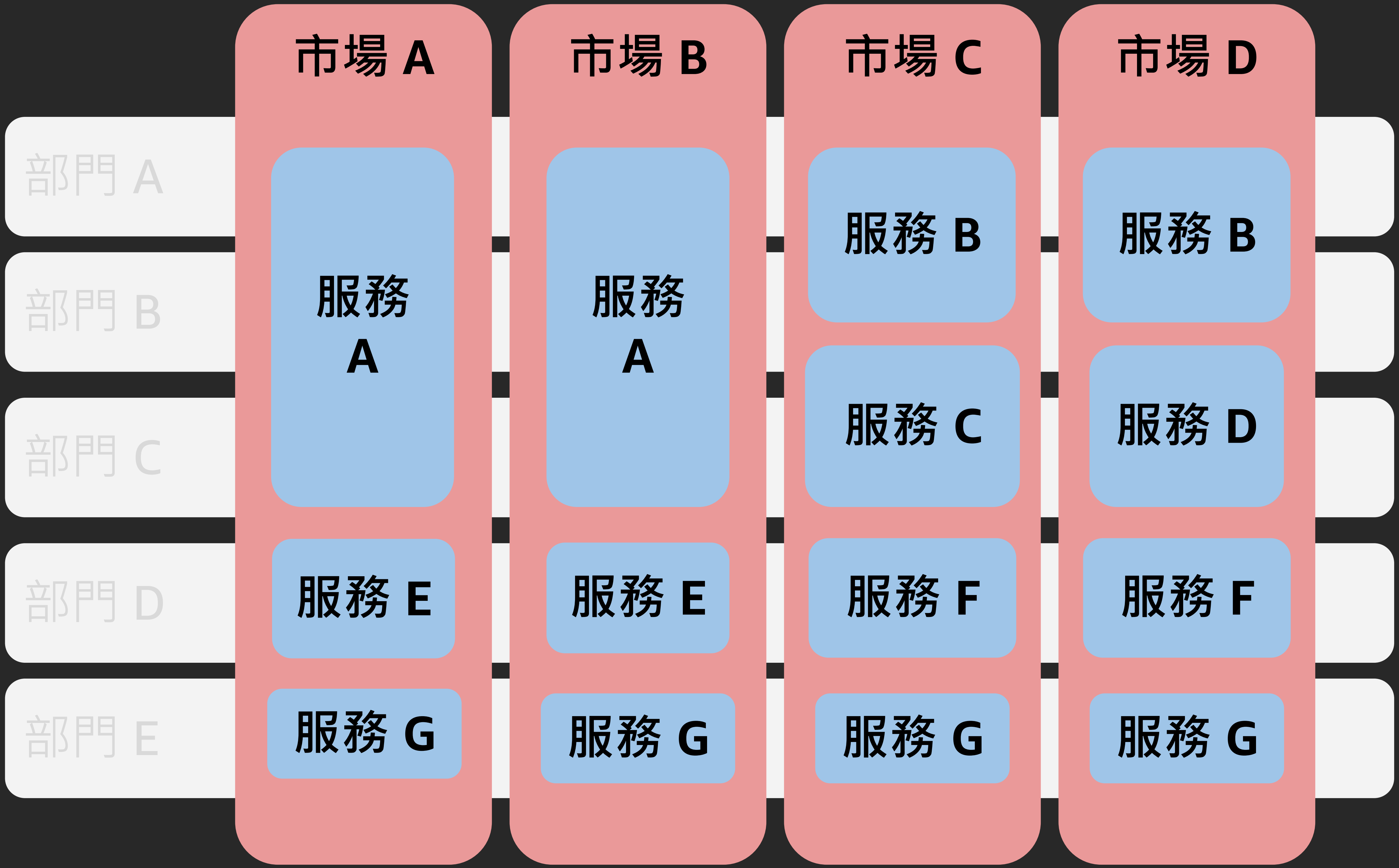
企業的組織結構與系統架構之間

有著難分難捨的關係

(康威定律)

調整：市場 + 服務 (系統)

弱化用組織分帳



市場 A

服務 A

服務 E

服務 G

市場 B

服務 A

服務 E

服務 G

市場 C

服務 B

服務 C

服務 F

服務 G

市場 D

服務 B

服務 D

服務 F

服務 G

部門 A

部門 B

部門 C

部門 D

部門 E

組織 (人) → 部門

市場 (事) → 團隊

系統 (物) → 服務

實際執行

制定 Resource Tag 規範

某服務比上個月少了多少錢！

資源歸屬 = 成本報表

依服務歸屬，規範制度化

大家開始主動注意成本結構問題

嘗試二：人員管理

5 / 個

產品線

10+ / 個

Accounts

200+ / 個

產品研發團隊

6 / 個

業務市場

40+ / 個

Services

問題

公司變大了，人變多了，有那麼多 AWS 帳號與 IAM 。

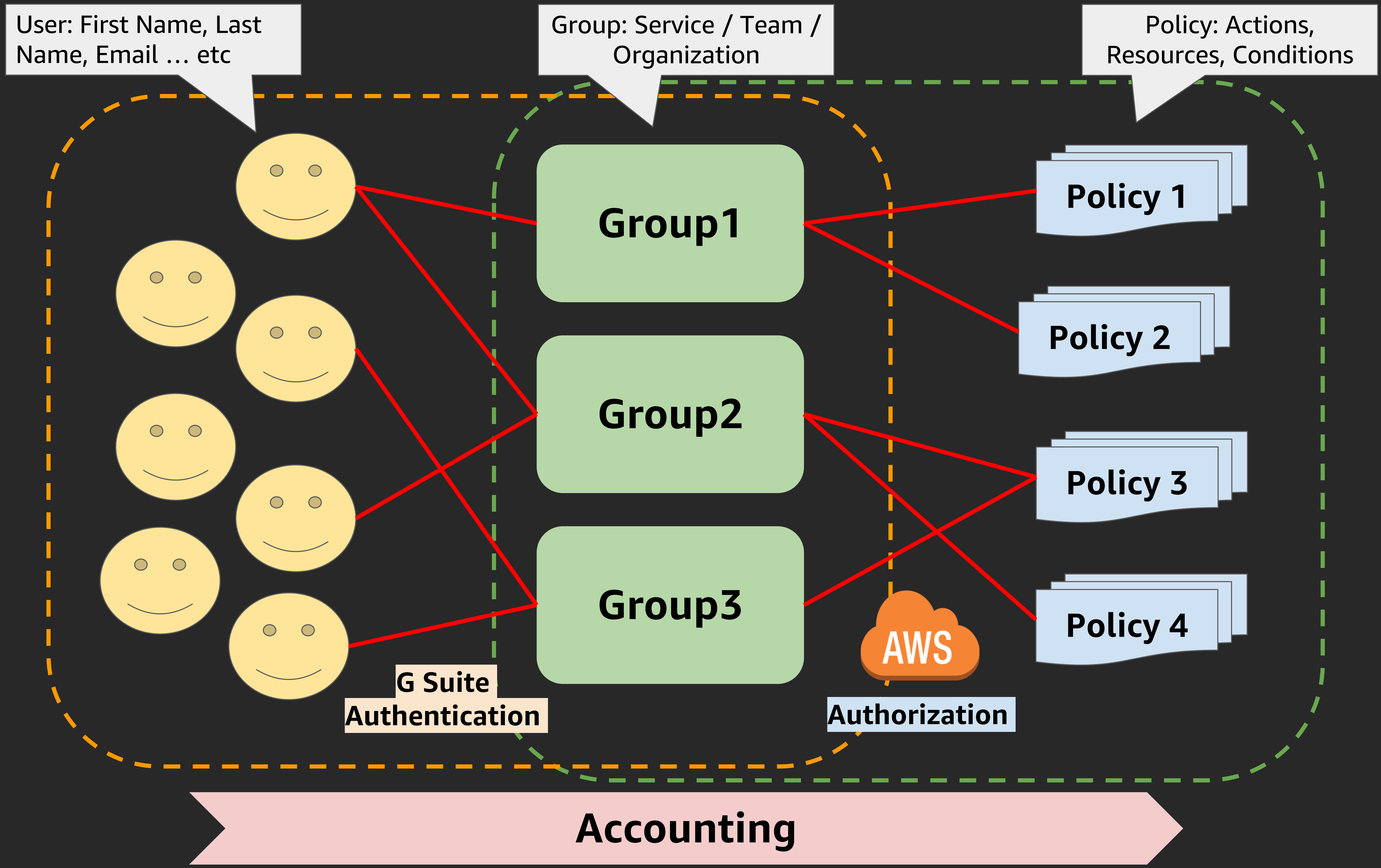
這麼多人，有人進來，也有人出去，怎麼確保人員異動時，

權限都能夠快速地增加、**乾淨地移除**？

技術解

AWS + G Suite

[Federated Single Sign-On to AWS Using Google Suite]


User: First Name, Last Name, Email … etc
Group: Service / Team / Organization
Policy: Actions, Resources, Conditions
Group1
Group2
Group3
Policy 1
Policy 2
Policy 3
Policy 4
AWS
G Suite Authentication
Authorization
Accounting

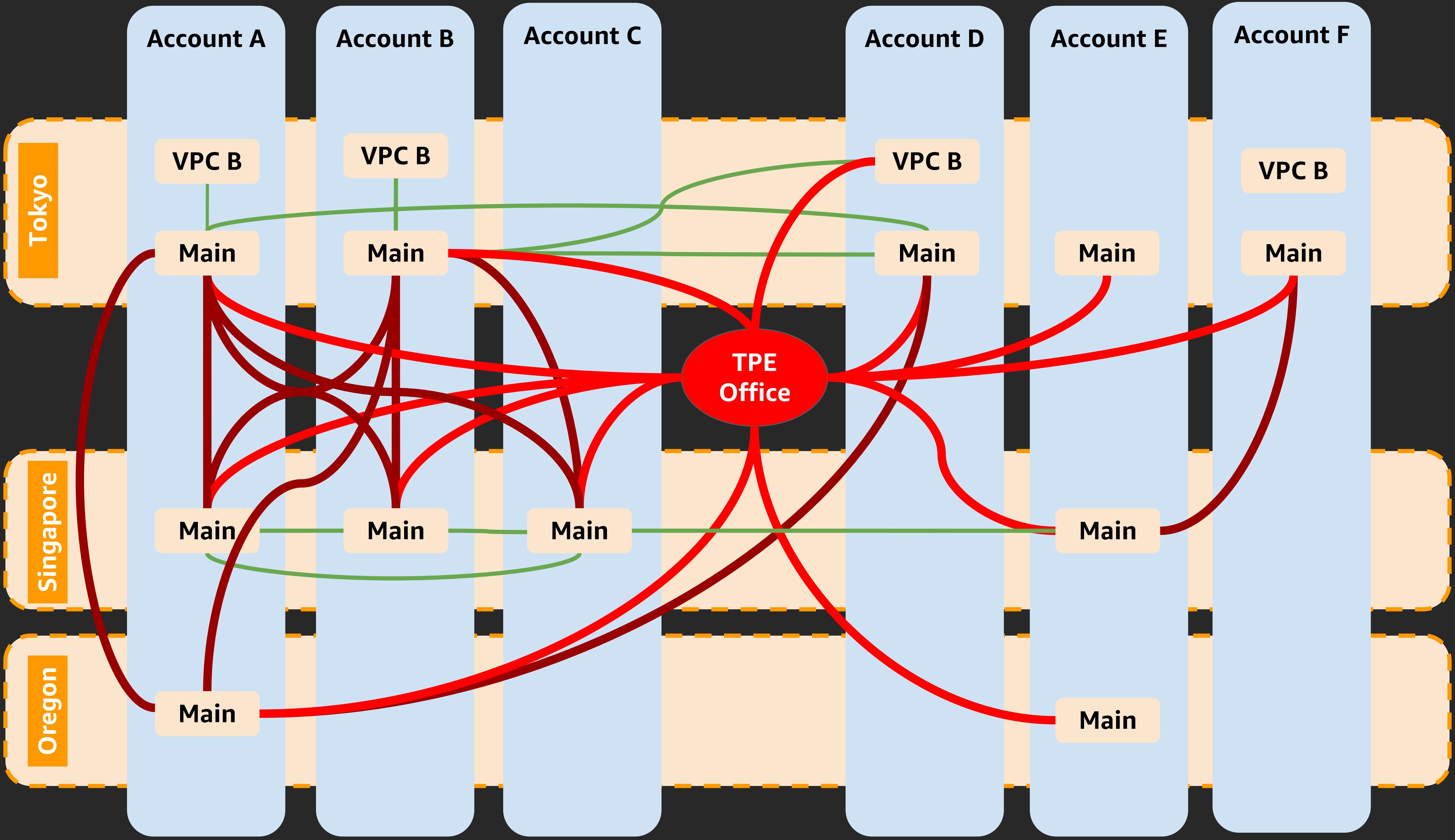
評估與成果

- ✓ 可否支援多 AWS 帳號？
- ✓ 如何綁定 G Suite User 與 IAM Role @ AWS Account 的綁定？
- ✓ 如何管理綁定的權限與授權？
- ⚠ 如何大量異動與調整？
- ⚠ 可否針對 G Suite 的使用者群組設定？
- ✓ 使用者登入後的 Session 時間？
- ⚠ 支援 IAM Programmatic User？

嘗試三：可擴展的基礎網路架構

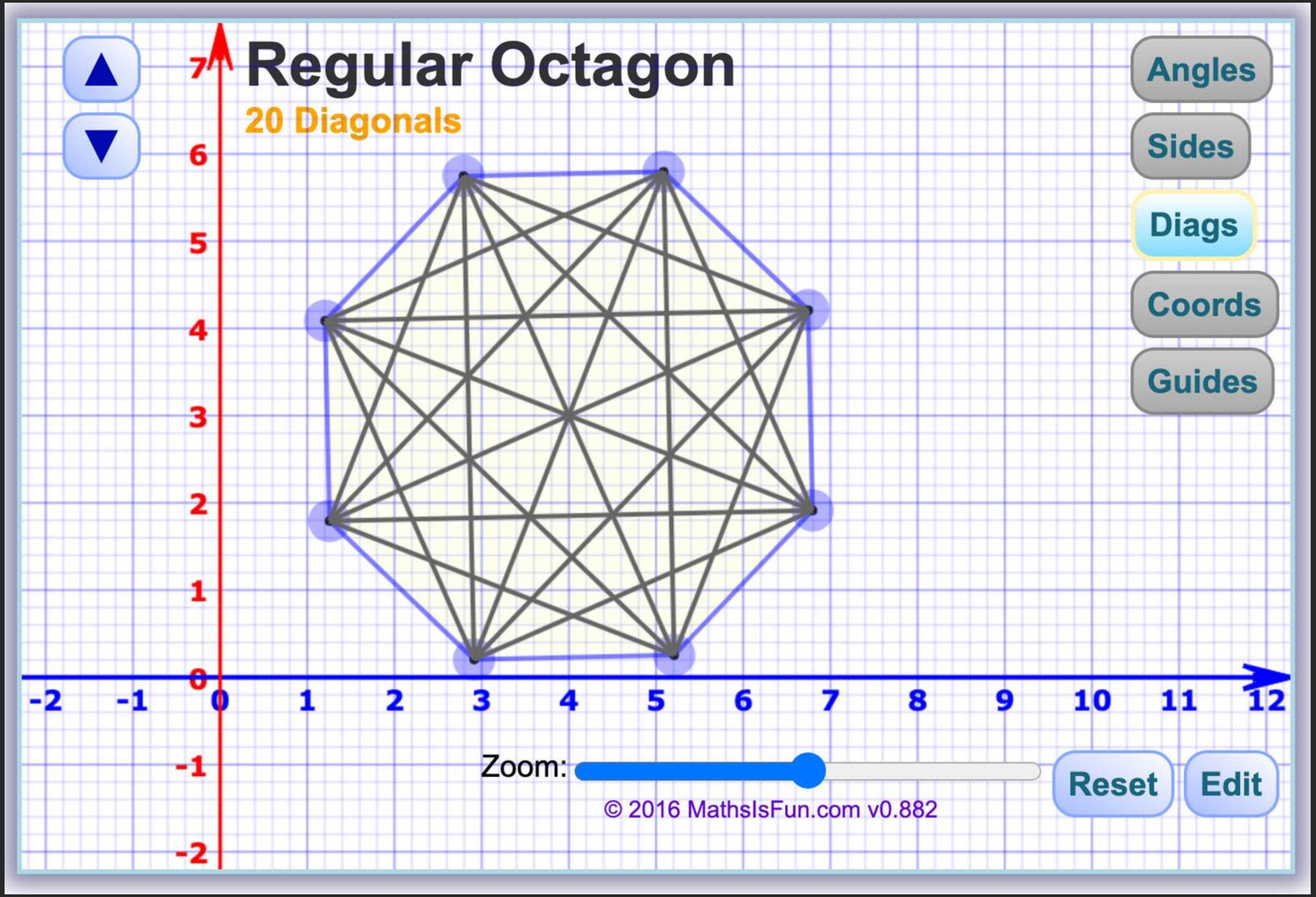
資料交換範圍廣大的服務，需要一個良好的網路架構來支持，像是：

- 資料分析平台
- 使用者認證服務 (SSO、Auth)
- 內部持續交付流水線
- 內部配置管理服務


Account A
Account B
Account C
Account D
Account E
Account F
Tokyo
Singapore
Oregon
VPC B
VPC B
VPC B
VPC B
Main
Main
Main
Main
Main
TPE
Office
Main
Main
Main
Main
Main
Main

多邊形對角線

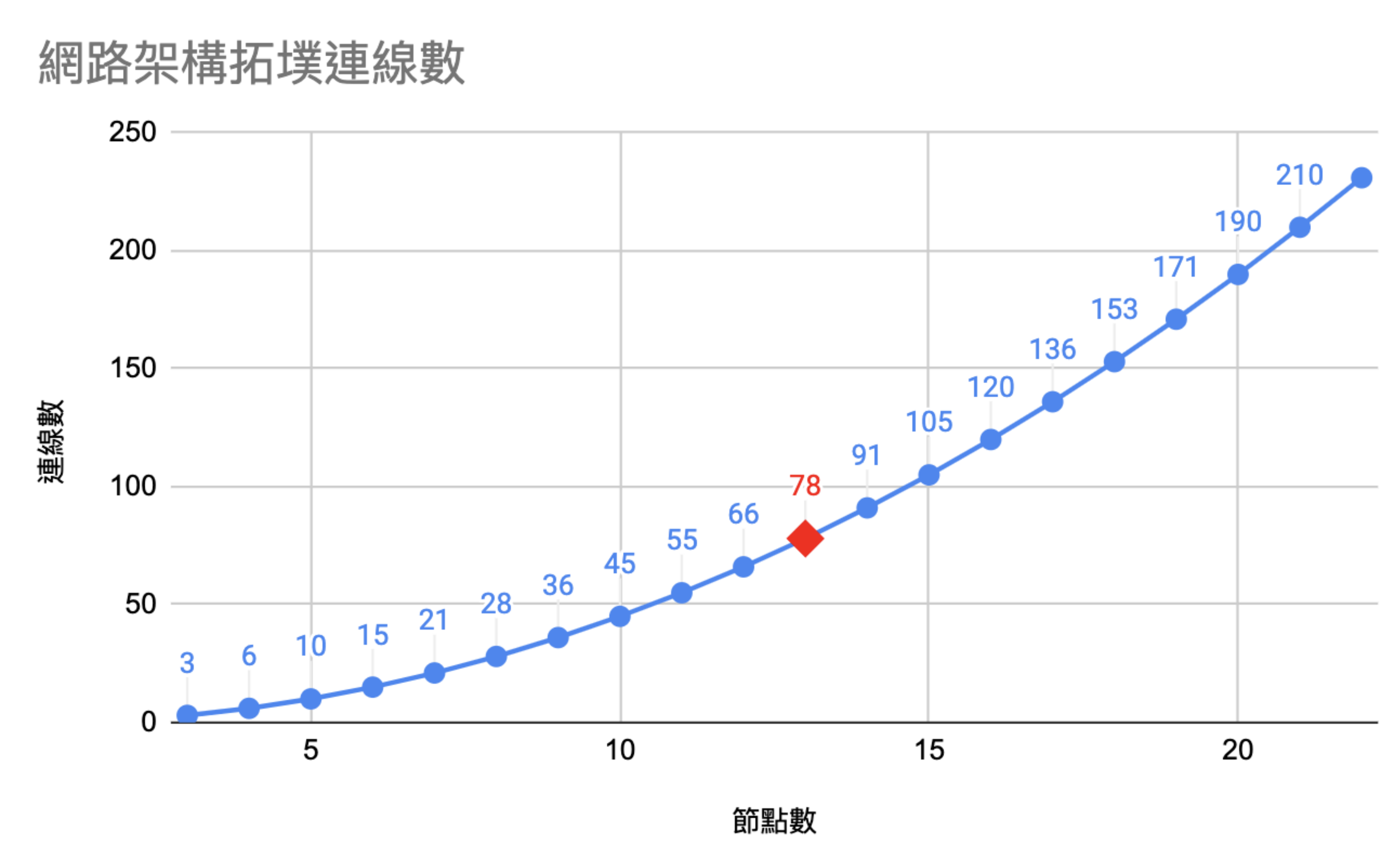
連線數 = n * (n-3) / 2



https://www.shuxuele.com/geometry/polygons-diagonals.html

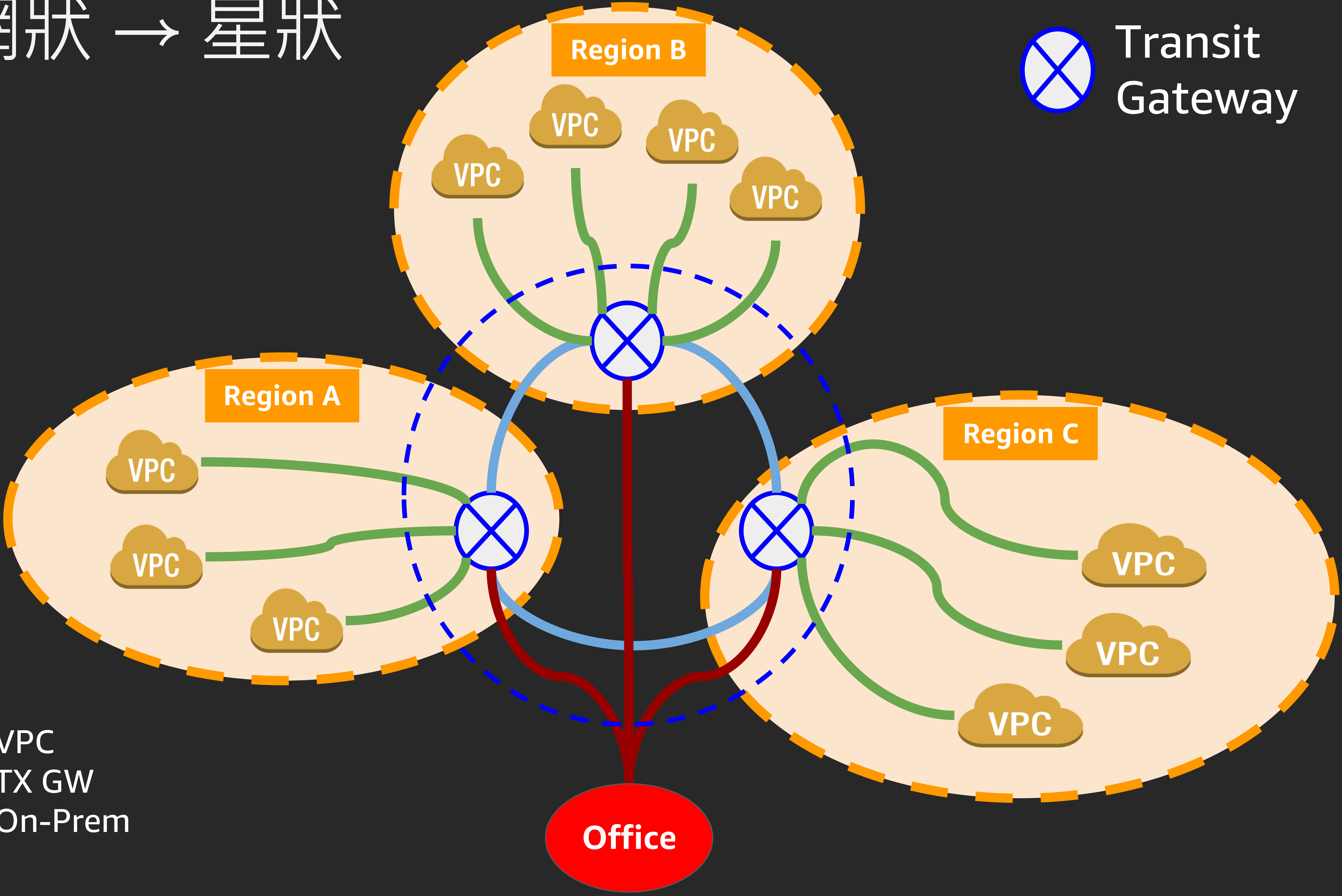
問題

- 網路拓墣複雜度變高，造成管理與溝通成本很高
  - 不易清楚現況，釐清現況費時
  - 管理複雜度高，造成溝通成本



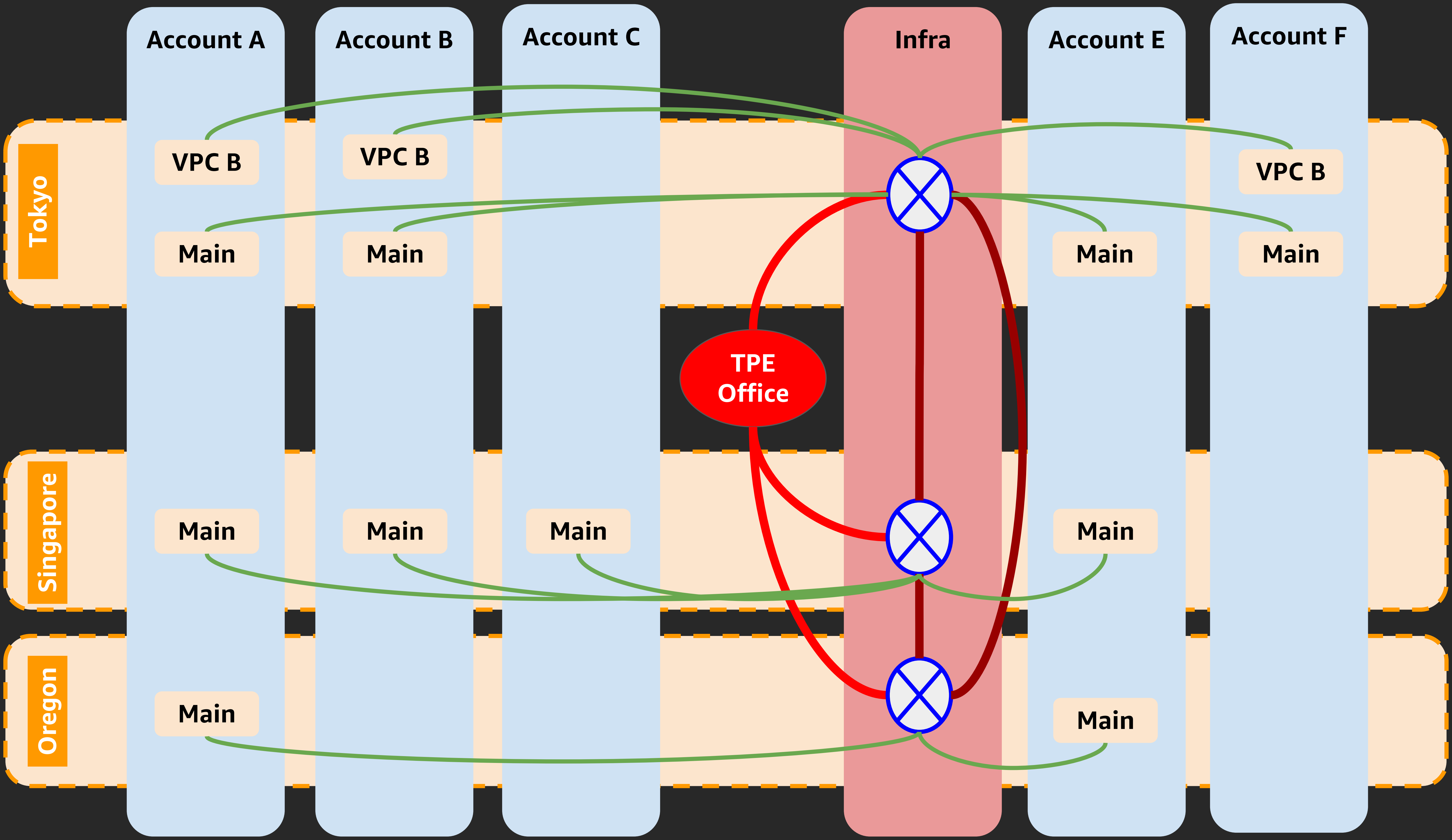
- 資料中心節點數 = n
- 連線數 (含邊線) = n * (n-3) / 2 + n
- 假設資料中心節點數 = 13
- 理論值最大的拓墣連線 = 78

目標：網狀 → 星狀



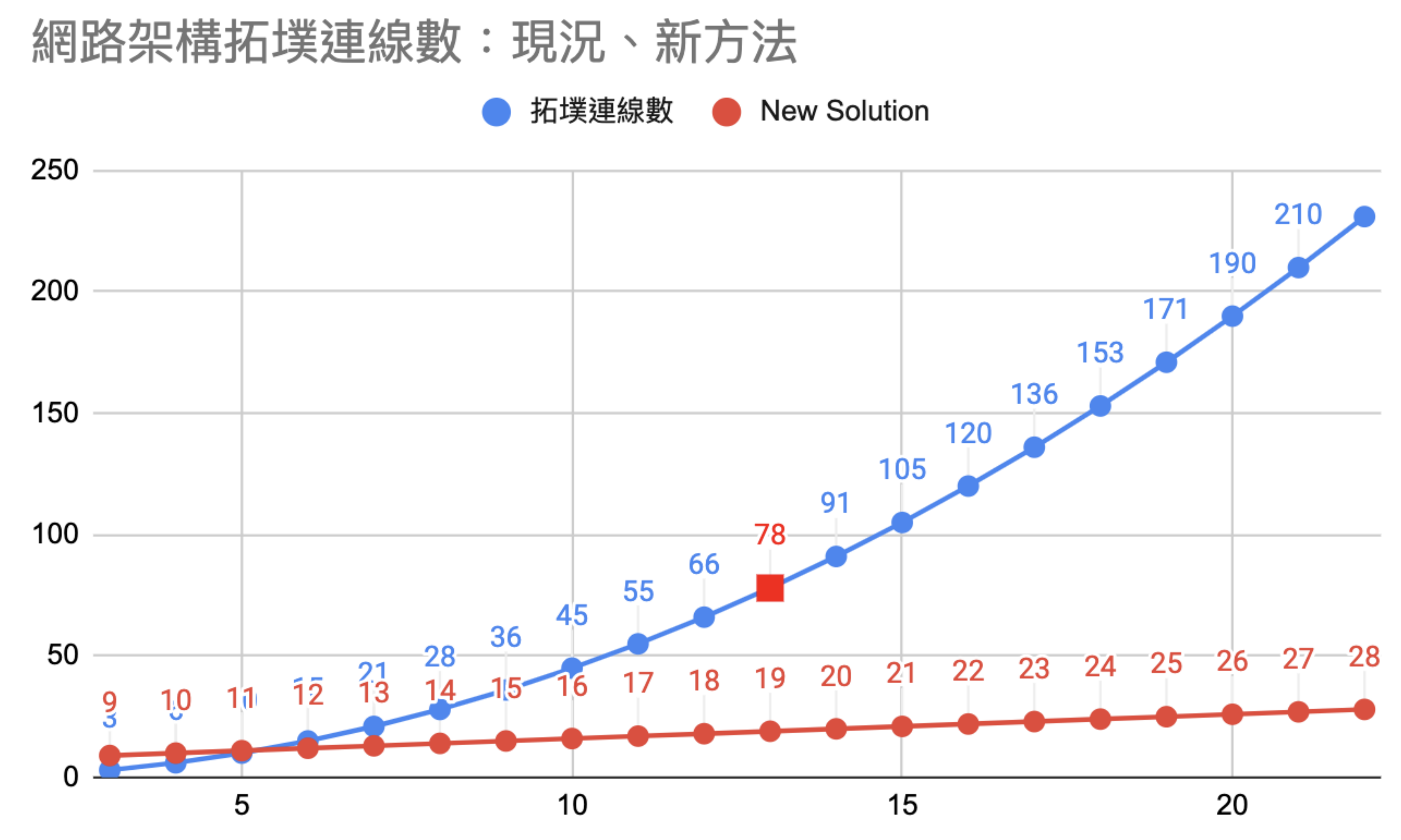
⨂ Transit Gateway

星狀：TX GW → VPC
網狀：TX GW → TX GW
星狀：TX GW → On-Prem


Account A
Account B
Account C
Infra
Account E
Account F
Tokyo
VPC B
VPC B
VPC B
Main
Main
Main
Main
TPE
Office
Singapore
Main
Main
Main
Main
Oregon
Main
Main

解法

1. 透過 Transit Gateway 簡化網路拓墣結構，降低複雜度，提高可管理、可控性
2. 提高網路架構擴展性



網路架構拓墣連線數：現況、新方法

總結與摘要

組織與成本結構的歸屬

制定 Resource Tag 規範

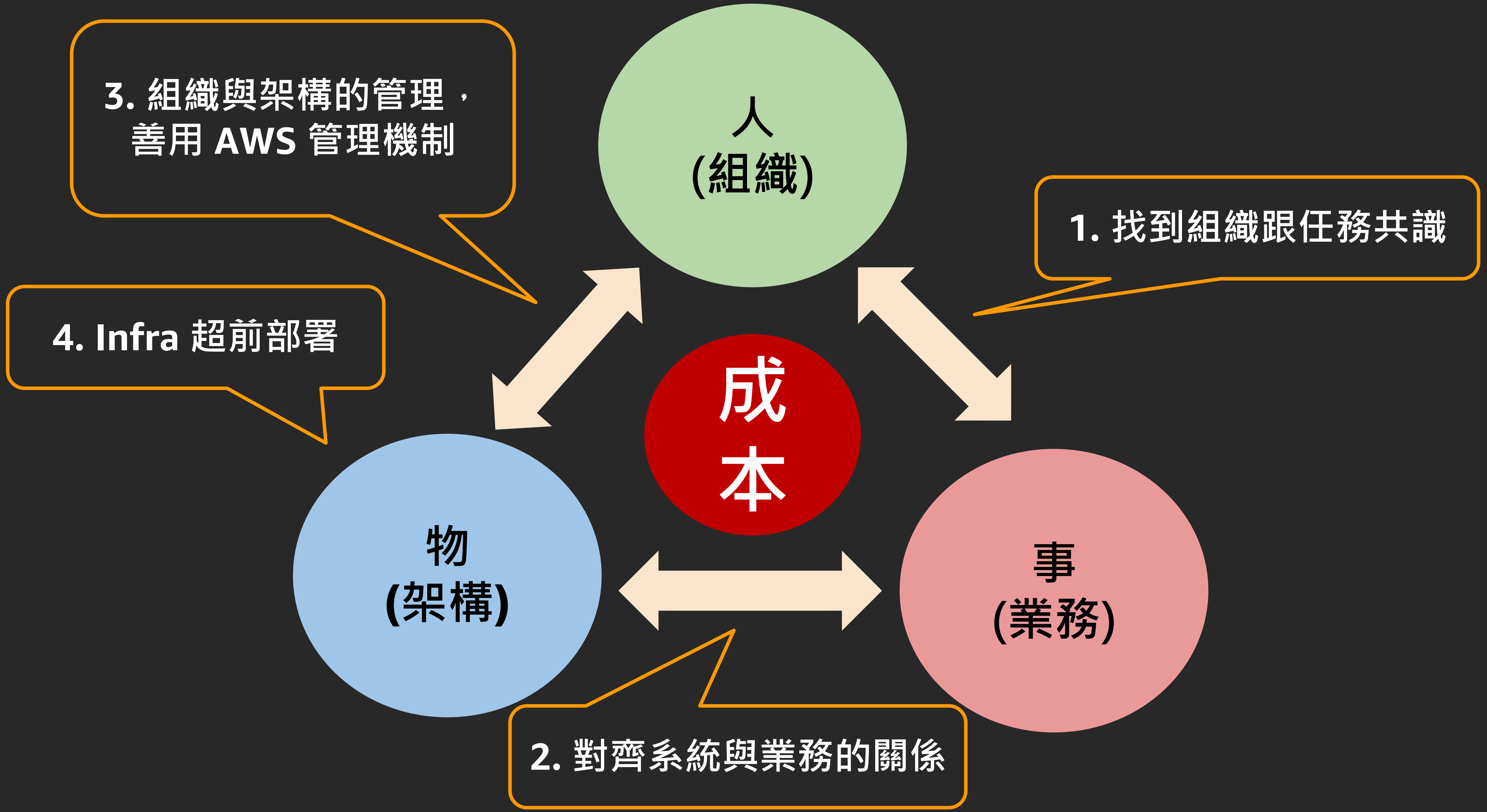
某服務比上個月少了多少錢！

資源歸屬 = 成本報表

依服務歸屬，規範制度化

大家開始主動注意成本結構問題

發展中的企業：成本管理策略



歸納：網路架構規劃的四個原則

可擴展
(Scalable)

可控制
(Controllable)

可管理
(Manageable)

可治理
(Governanceable)

相關資訊

- Building a Scalable and Secure Multi-VPC AWS Network Infrastructure
- Tagging Best Practices - Implement an Effective AWS Resource Tagging Strategy
- 微服務的基礎建設 - Service Discovery
- 從零開始的 Configuration Management
- 談產出物管理 (Artifacts Management)

Thank you!

Annie Lin
annian@amazon.com

Rick Hwang
rickhwang@nine-yi.com

aws SUMMIT ONLINE