雲端安全及管控

網際網路演化進程

PC 為主的網路

Wave 1 : WWW
~350M PCs annually

Connecting PCs

手機/雲端服務為主的網路

Wave 2 : Mobile/Cloud
2.3B annually

Connecting People

Source : Harvard University

不同的看法of Cloud

- 未來的趨勢
- 新瓶裝舊酒
- 不 安全

雲端運算定義

- 雲端運算是一種具備大量且可擴充之IT相關能力的運算方式，透過網際網路技術並以服務形式(provided as a service)提供給外部的使用者---Gartner
- 雲端運算是一個具有高度彈性及延展性的運算中心，可以提供使用者所需要的應用程式，並可依據資源使用的多寡來收費---IDC
- 雲端運算是一種及時的IT能力運算網路平台，可透過網際網路被申請、供應、傳遞與消費---Forrester
- 雲端運算 = 所需要的應用軟體與資源都在網際網路中，可以透過任何裝置上的瀏覽器取得---Google
- 雲端運算是一種運算方式，運算資源是動態易擴充且虛擬的，往往透過網際網路提供，使用者不需要了解“雲端”中基礎建設的細節，不需具備相對應的專業知識，也無需直接進行控制---IBM

雲端運算定義

- 雲端運算是基於網際網路的運算方式，透過網際網路為個人使用者或企業使用者提供按需求取用的服務。

- 雲端運算服務通常提供能夠透過瀏覽器存取的商業應用，使用者需要雲端運算的計算平臺或資訊技術（IT）基礎設施，並在這些平臺與設施中運行應用。

- （NIST）最具權威，其雲端定義為：「雲端運算是一種模式，能方便且隨需求應變地透過連網存取廣大的共享運算資源（如網路、伺服器、儲存、應用程式、服務等），並可透過最少的管理工作及服務供應者互動，快速提供各項服務。」。

NIST提出的定義

- 雲端運算五項重要特徵、四種佈署模式、三類服務模式以及一般特性，其整體架構如下圖：

NIST提出的定義


服務模式
軟體即服務 (SaaS)
平台即服務 (PaaS)
架構即服務 (IaaS)
一般特徵
大規模
彈性運算
同質性
分散地理位置
虛擬化
服務導向
低成本的軟體
進階安全性

軟體即服務

- 是一種以提供軟體服務為觀念的服務基礎，軟體服務供應商，以租賃的概念提供客戶服務，而非購買。
- 比較常見的模式是提供一組帳號密碼。此服務軟體是安裝於集中式的網絡伺服器並確保在網際網路或者區網內執行其功能。
- 因為具備高靈活性、卓越的服務、強大的可擴展性和較低的維護成本。為目前最流行的雲端運算類型。
- Google Apps、Saleforce.com、MS Office 365、Microsoft Azure

平台即服務

- 平台即服務提供使用者能將雲端基礎設施部署與建立至用戶端，或者藉此獲得使用程式語言、程式庫與服務。使用者不需要管理與控制雲端基礎設施，包含網路、伺服器、作業系統或儲存，但需要控制上層的應用程式部署與應用代管的環境。
- PaaS將軟體研發的平台做為一種服務，以軟體即服務（SaaS）的模式交付給使用者。因此，PaaS 也是 SaaS 模式的一種應用。但是，PaaS 的出現可以加快 SaaS 的發展，尤其是加快 SaaS 應用的開發速度。

基礎設施即服務

- 客戶端無須購買伺服器、軟體等網路設備，即可任意部署和運行處理、存儲、網路和其它基本的計算資源，不能控管或控制底層的基礎設施，但是可以控制作業系統、儲存裝置、已部署的應用程式，有時也可以有限度地控制特定的網路元件
- 商業模式屬於“使用才付費”的模式，確保用戶僅需支付他們使用的服務。服務商會利用虛擬化技術，提供幾乎無限的客戶端服務，使承載的硬體效益更高IBM、Amazon.com、Microsoft Azure

Services Platform and Applications

雲提供使用者服務

Microsoft Forefront
Silverlight
Live Search Maps
Office Live WorkSpaces
Windows Live Hotmail
Windows Live Spaces
Windows Live
Live Search
Microsoft Dynamics CRM Online
Microsoft Exchange Online
Microsoft SharePoint Online
Microsoft HealthVault
Microsoft Online Services
Windows Live Messenger
msn adCenter
msn
XBOX LIVE

Software + Services

雲的運算平台

Live Services
Microsoft .NET Services
Microsoft SQL Services
Microsoft SharePoint Services
Microsoft Dynamics CRM Services
Windows Azure

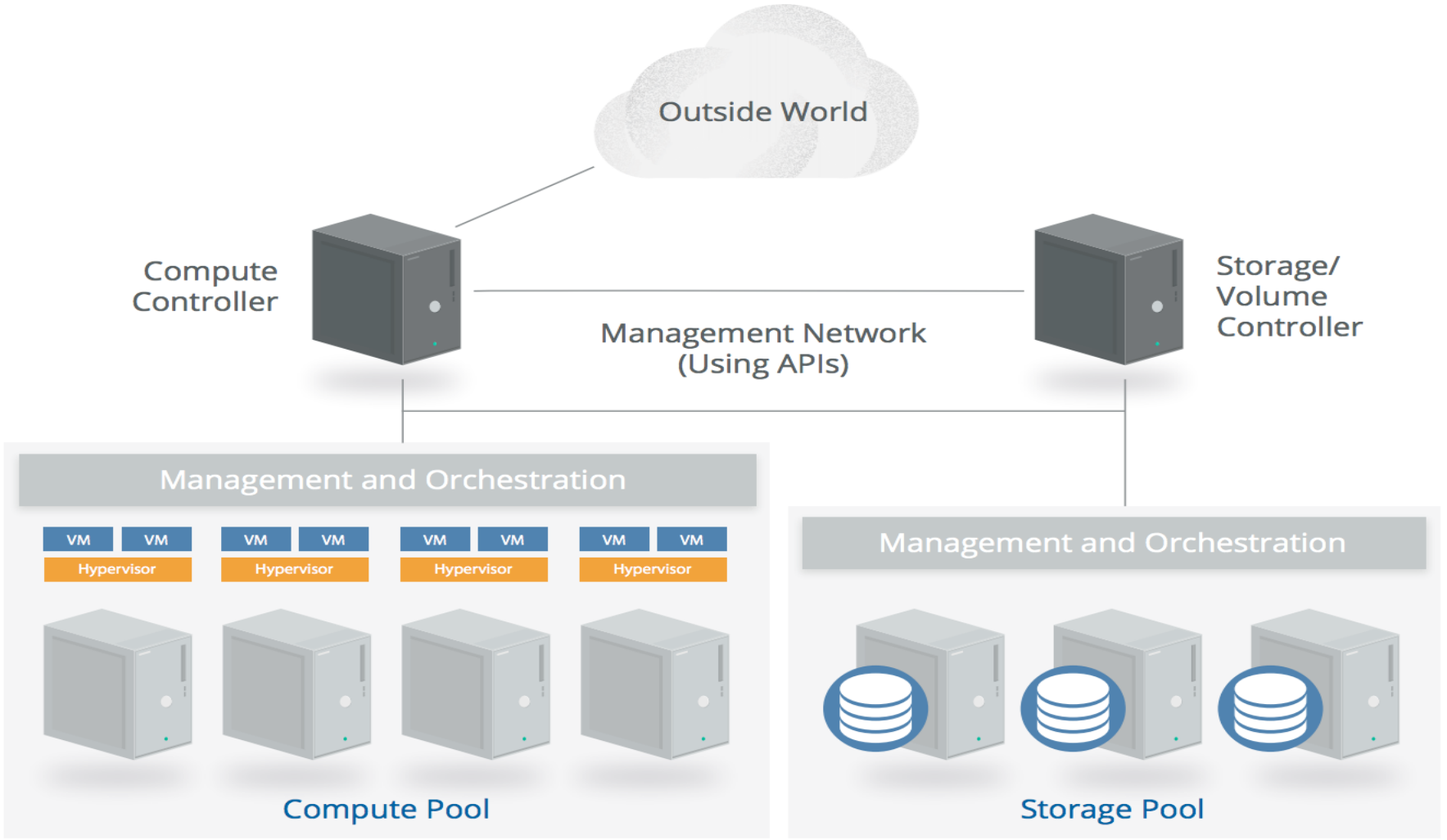
Platform as a Service

基礎服務

INFRASTRUCTURE SERVICES
ONLINE SECURITY
GLOBAL DELIVERY
ENVIRONMENTAL FOCUS

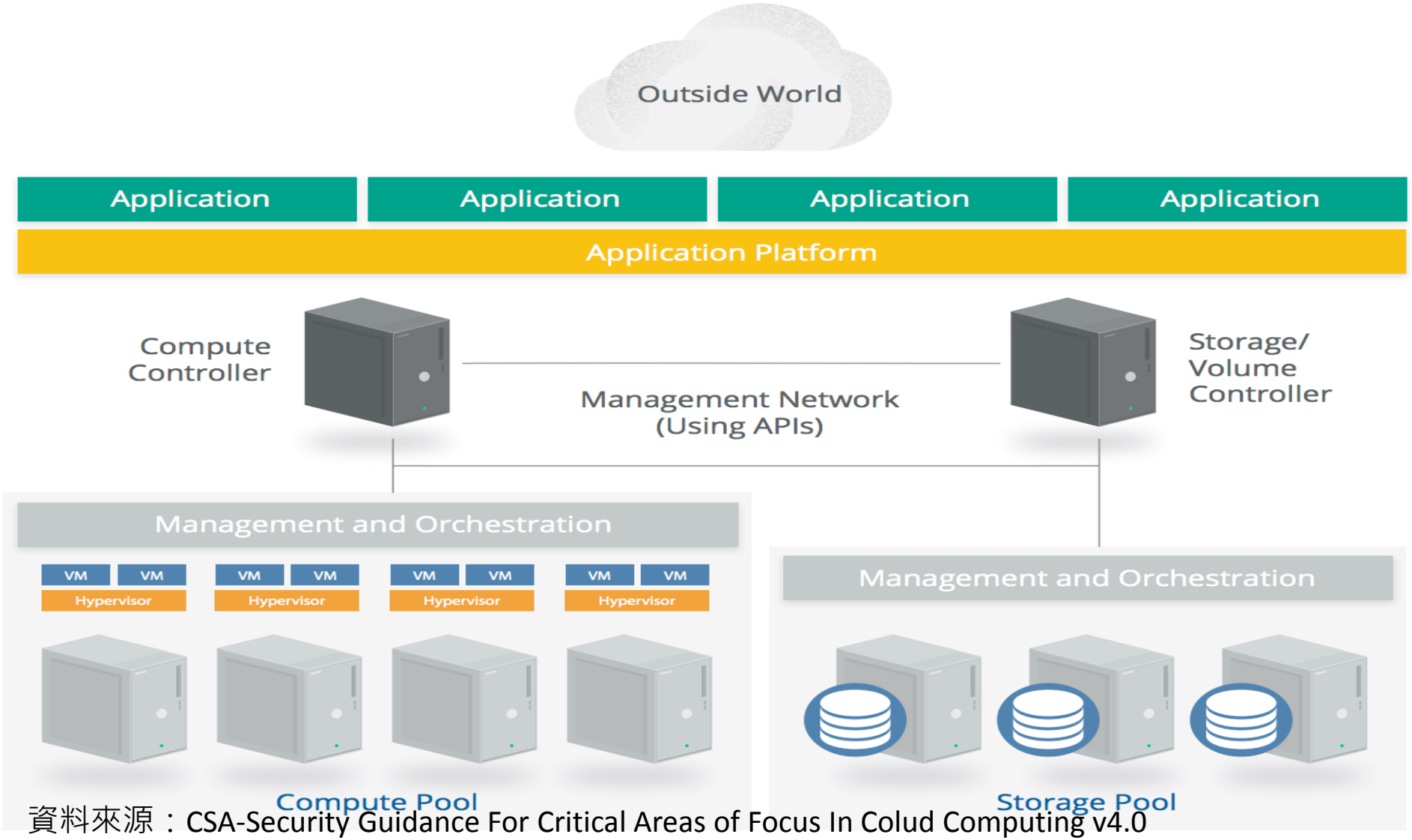
Infrastructure as a Service

IaaS



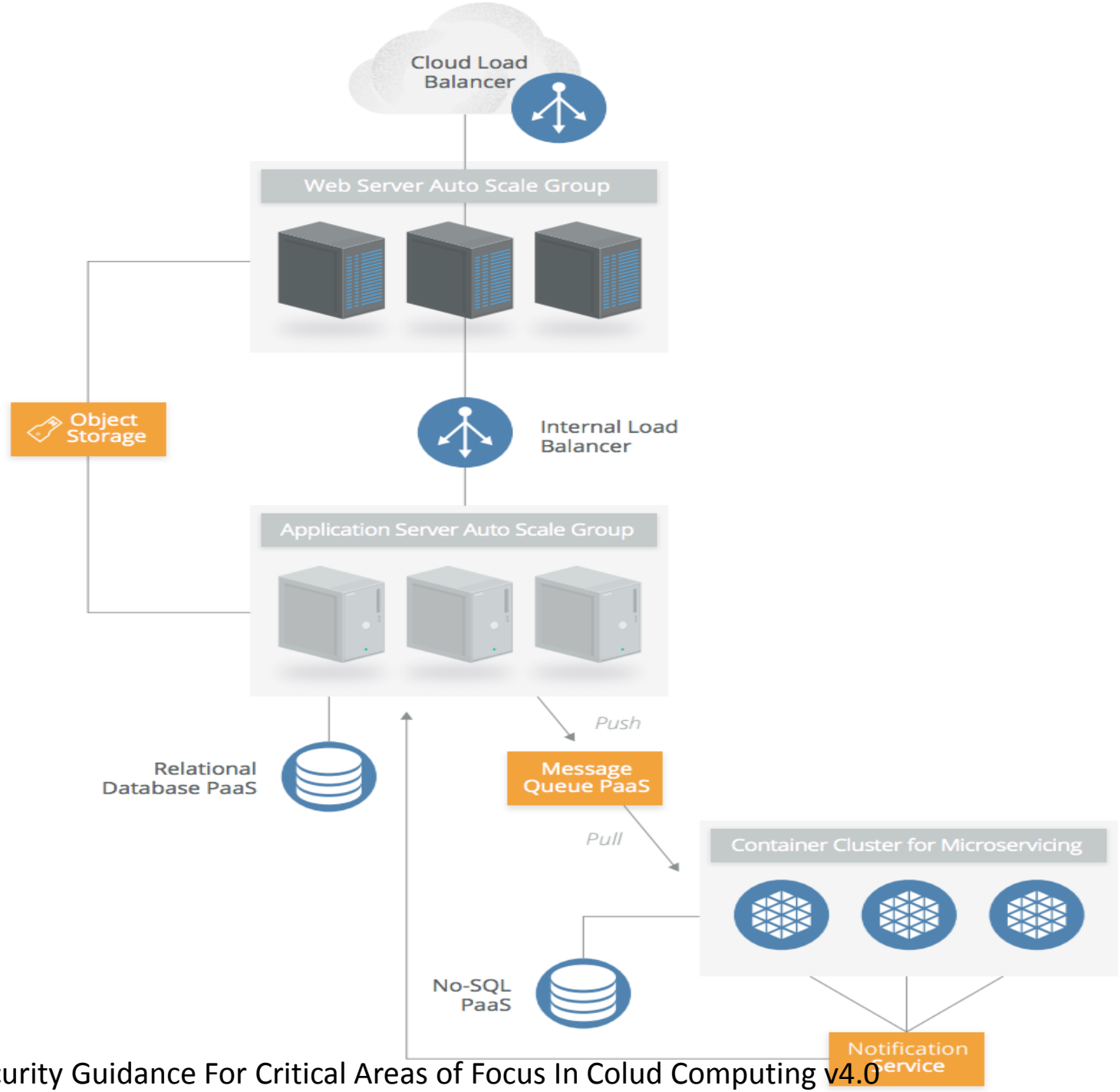
資料來源：CSA-Security Guidance For Critical Areas of Focus In Colud Computing v4.0

PaaS

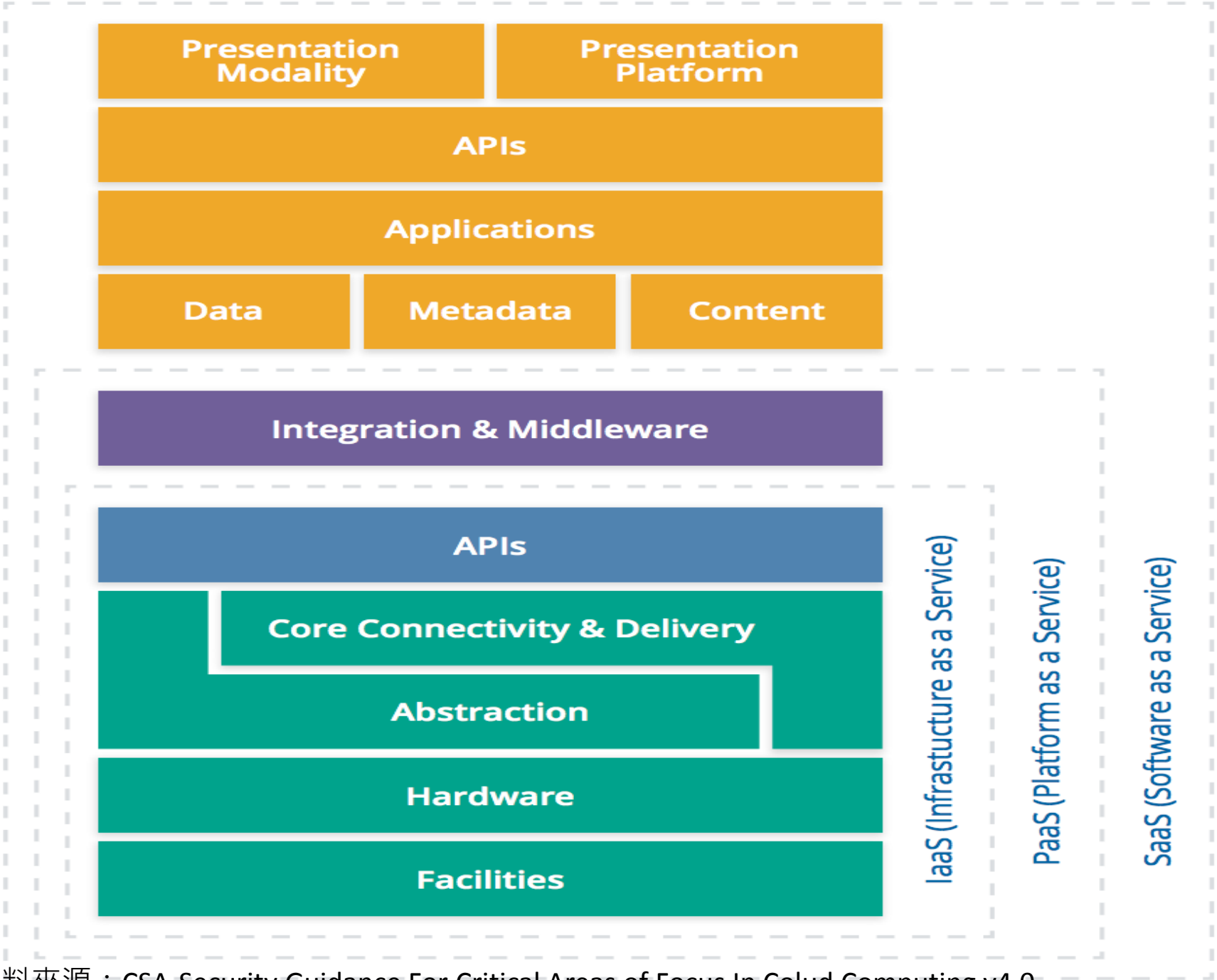


資料來源：CSA-Security Guidance For Critical Areas of Focus In Colud Computing v4.0

SaaS



資料來源：CSA-Security Guidance For Critical Areas of Focus In Colud Computing v4.0



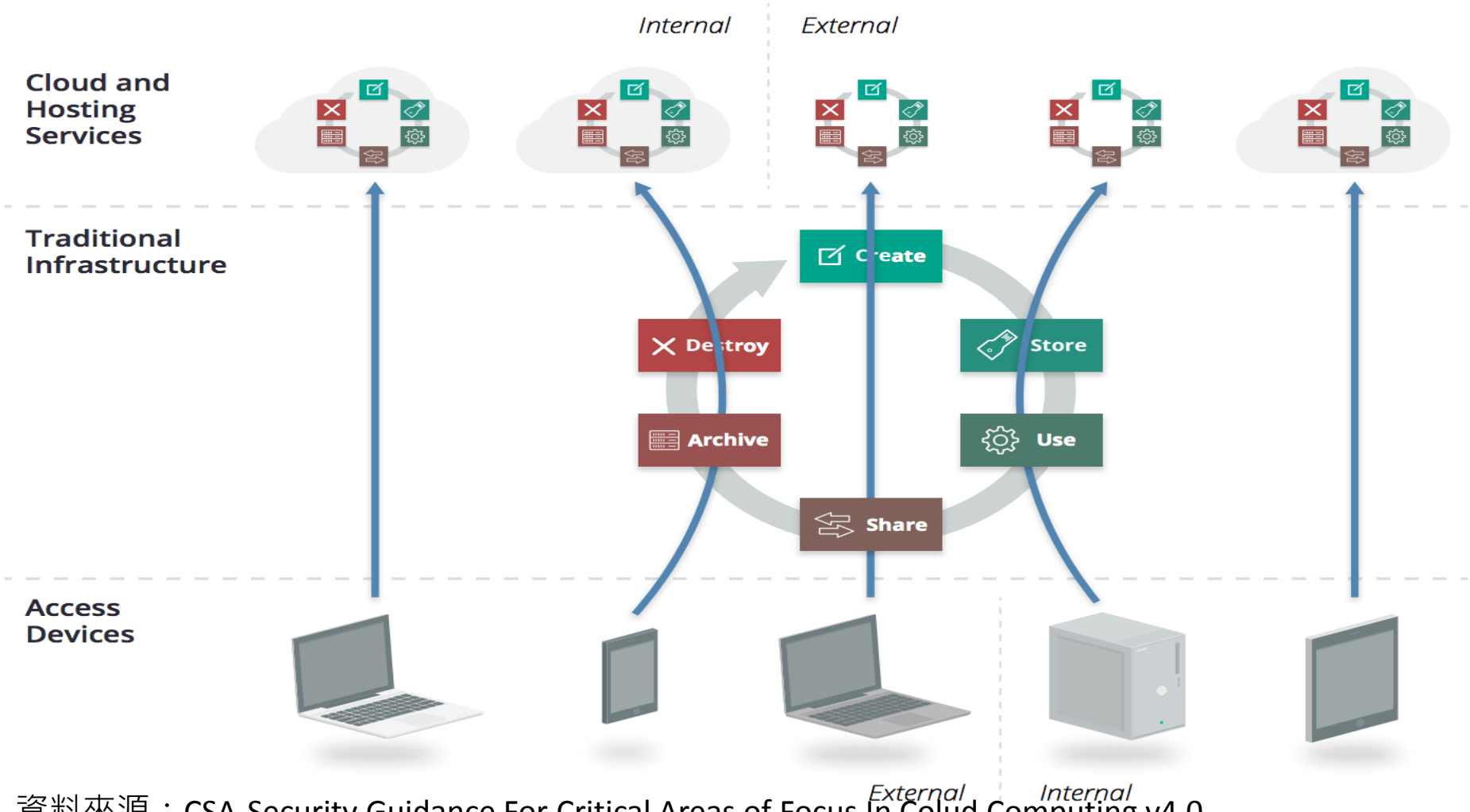
資料來源：CSA-Security Guidance For Critical Areas of Focus In Colud Computing v4.0

雲端9大威脅

- 資料外洩（Data Breaches）
- 資料遺失（Data Loss）
- 帳號被駭（Account Hijacking）
- 不安全的APIs程式（Insecure APIs）
- 拒絕服務（Denial of Service）
- 惡意的內部人員（Malicious Insiders）
- 濫用雲端服務（Abuse of Cloud Services）
- 審慎評鑑不足（Insufficient Due Diligence）
- 共享環境所造成難以避免的議題（Shared Technology Issues）

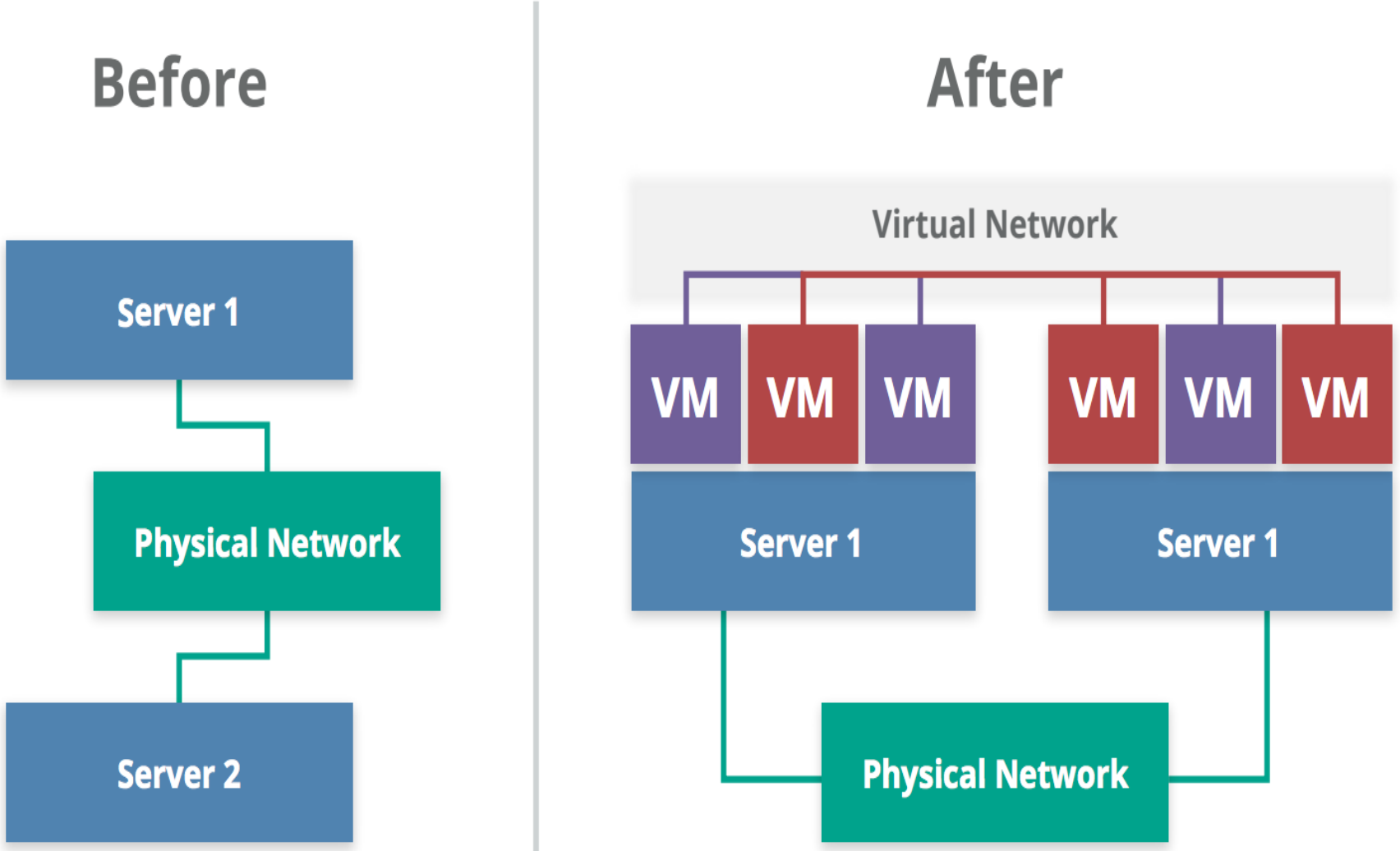
資料來源：CSA-The Notorious Nine:Cloud computing Top Threats in 2013

Issue1
Locations and Entitlements



資料來源：CSA-Security Guidance For Critical Areas of Focus In Colud Computing v4.0

Issue2
Network different



資料來源：CSA-Security Guidance For Critical Areas of Focus In Colud Computing v4.0

虛擬化主機安全建議

- 識別虛擬化技術
- 確保VM具備安全機制
- 留意VM Image的安全
- 透過加密機制管控
- 隔離、更新後再啟動

雲端安全認證

目前雲端安全認證概況

- ISO27001:2013
- Cloud Security Alliance（ CSA ）
- EuroCloud Star Audit (ECSA)
- ISO27017
- ISO27018

CSA

- 雲端安全聯盟(CSA, Cloud Security Alliance)成立於RSA Conference 2009，為全球性的非營利組織
- 致力於在雲端運算環境下提供最佳的安全方案。自其成立起，雲端安全聯盟發佈的雲端安全指南及其開發成為雲端運算領域令人矚目的重要文件。
- 雲端安全聯盟CSA的宗旨：
  - 提供用戶和供應商對雲端運算必要的安全需求與資安認知。
  - 促進對雲端運算安全最佳做法的獨立研究
  - 發起正確使用雲端運算和雲端安全解決方案的宣傳和教育計畫
  - 創建有關雲端安全保證的問題和方針的明細表

資料來源：CSA

雲端安全開放認證架構

▲OCF採取三層式的認證架構。（圖片來源：CSA Open Certification Framework）

稽核內容
CCM 16個Domain
(CCM3.01) -133 Controls

AIS	Application & Interface Security 應用系統與介面安全
AAC	Audit Assurance & Compliance 稽核確保與符合性
BCR	Business Continuity Management & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Management
DCS	Datacenter Security 資料中心安全
EKM	Encryption & Key Management 密碼學與金鑰管理
GRM	Governance & Risk Management 治理與風險管理
HRS	Human Resource Security 人力資源安全
IAM	Identity & Access Management 識別與存取管理
IVS	Infrastructure & Virtualization Security 架構與虛擬化安全
IPY	Interoperability & Portability相互運作與可移植性
MOS	Mobile Security 行動安全
SEF	Sec. Incident Management & E-Disc & Cloud Forensics
STA	Supply Chain Management, Transparency & Accountability
TVM	Threat & Vulnerability Management 威脅與弱點管理

資料來源：CSA

開放認證架構的評鑑方式

- 第一層：STAR自我評鑑
  - 自我評估問卷(Consensus Assessments Initiative Questionnaire;CAIQ)，描述各項已符合安全要求的作法與因應措施，傳送至CSA註冊管理單位(STAR Registry)進行審查(STAR:Trust & Assurance Registry)
  - 針對CAIQ安全問題，填寫(Yes or No)並提出描述說明
  - 每年需定期重新自我評鑑(週期最多不得超過18年月)

開放認證架構的評鑑方式

- 第二層：STAR認證-第三方獨立評鑑
  - 結合ISO 27001和雲端控制矩陣的安全控制措施要求，透過第三方驗證單位進行獨立的安全查核
  - 第三方驗證單位(BSI)將對16個Domain進行評分
  - 等級「無」、「銅」、「銀」、「金」
- 第三層：基於證證的持續監控
  - 此一階段的實施做法，目前還在發展中

參考資料：
https://cloudsecurityalliance.org/star/#_registry
http://www.netadmin.com.tw/article_content.aspx?sn=1306130001&jump=1
http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=14&aid=7653

EuroCloud Star Audit (ECSA)

- 1. ECSA是一套專門用來評鑑雲服務的驗證機制
- 2. 自2011年成立以來，歐洲雲服務聯盟即運用ECSA驗證機制之要求內容來評估雲服務，該服務涵蓋特定供應鏈所牽涉之所有參與成員
- 3.雲服務商無法協商或選擇性決定驗證哪些領域，涵蓋所有重要的控制領域且均為必要，包含：
  - provider‘s profile 服務商相關基本資訊
  - contract and compliance including data privacy protection against local law 合約及當地法規要求之資料隱私保護符合性
  - Security 資訊安全
  - Operations 服務維運作業
  - Environment and technical infrastructure基礎設施之環境與技術構面
  - Processes 流程
  - Relevant parts of the application and implementation 應用系統導入牽涉之
  - Interoperability and data portability互通性與轉移性

資料來源：ECSA

EuroCloud Star Audit (ECSA)

- 4. ECSA驗證過程係結合生態體系內相關合作夥伴共同完成，其驗證內容以模組化的結構，分三個星級，去評鑑特定服務在不同控制領域的管理狀況，不但適用於大型雲服務商，即使中小型雲服務商也有機會通過評鑑
- 5. 若某特定雲服務符合ECSA機制下的驗證準則，即可通過評鑑而獲得ECSA星級證書
- 6. 證書有效期為二年，前提是該服務之供應鏈下包商或雲服務本身在各評鑑的控制領域沒有重大變更
- 7. ECSA驗證機制對於雲服務客戶而言，當他想要值得信賴的雲服務時，是一種有意義的篩選工具，也可降低其個別進行驗證所需之成本

資料來源：ECSA

EuroCloud Star Audit (ECSA)

- 8. The EuroCloud Star Audit is a joined activity performed by the ECSA partners within an eco-system.
- 9. With the ECSA EuroCloud Europe delivers a valuable instrument with a high level of transparency and guidance for customers and providers alike.

資料來源：ECSA

稽核內容

- Profile（服務商描述）
  - General Information服務商一般資訊
  - Physical Data Location Customer Data儲存客戶資料之實體數據中心地點
  - Service Management服務管裡
  - Extended Company Profile延伸性之公司資訊
  - Reference Information about the Cloud Service合約所載雲服務之參考資訊
  - Certifications獲證資訊
- Contract and compliance合約與符合性
  - Adeaquate contract terms適當之合約條款
  - Rules for Data Management資料管理之規則
  - Contractual Data Privacy requirements資料隱私保護之合約需求
  - Service Level Agreements服務水準協議內容
  - Terms in case of bancrupcy服務商破產倒閉之處理條款
  - Terms for pricing and cost allocation有關服務計價與成本配置之條款

資料來源：ECSA

稽核內容

- Security and Data Privacy安全與資料隱私
  - Security Management安全管理
  - Technical Security安全技術
  - Techncial data privacy measures資料隱私保護之技術性措施
  - Data integrity資料完整性界定
  - Auditability可被稽核性

- Operations and infrastructure維運與基礎設施
  - General DC assessment數據中心之一般評估
  - Access control存取控制
  - Area and environment assessment環境安全評估
  - Resilience回覆彈性
  - DC Operations數據中心維運作業

資料來源：ECSA

稽核內容

- Operations processes維運作業流程
  - Customer Support客戶支援
  - Service Management服務管理
  - Data backup processes資料備份流程
  - Quality assurance品質保證

- Service Type specifc assessment特定服務類別之評估
  - IaaS基礎設施即服務
  - PaaS平台即服務
  - SaaS軟體即服務

資料來源：ECSA

稽核內容（範例）

Are the procedures for digital signatures of data objects in accordance with national law?	
Excellent	ISAE3402 attestation
Good	Attestation by appropriate auditors
Sufficient	A compliance statement by the provider if applicable

資料來源：ECSA

ISO 27017與 ISO27001比較

- 主要的差異在於 Access Control例如:

- 9.2.1 User registration and deregistration ---使用者註冊與註銷
- 9.2.2 User access provisioning ---使用者存取權限之配置
- 9.2.3 Management of privileged access rights ---具特殊存取權限之管
- 9.4.1 Information access restriction ---資訊存取限制
- 9.4.4 Use of privileged utility programs ---具特殊權限公用程式之使用

ISO27017:2015

- ISO 27017 建議七個新增的安全控制，分別列舉如下：
- 這些都是基於雲端服務的基本安全要求
- 3.1 Shared roles and responsibilities within a cloud computing environment ---雲計算環境中的共同角色和責任
- 1.5 Removal of cloud service customer assets ---刪除雲服務客戶資產
- 5.1 Segregation in virtual computing environments ---虛擬計算環境中的分離
- 5.2 Virtual machine hardening ---虛擬機強化
- 1.5 Administrator’s operational security ---管理者的操作安全
- 4.5 Monitoring of cloud services ---雲服務監控
- 1.4 Alignment of security management for virtual and physical networks ---虛擬和物理網路的安全管理對齊

ISO 27017 雲端服務之風險評鑑

- 但雲端服務建置或使用後，組織無法得知下列資訊：
  - 哪些資訊資產為我所用?
  - 是否與他人共用資訊資產? 又與哪些組織共用?
  - 資訊機房坐落何方?
  - 網路管控機制為何? 等…
- 任何參與雲端運算服務的組織，都有可能因為任何資訊交換或虛擬資產(virtual asset)的影響，導致產生風險。因此各個組織應建立風險溝通共用衡量機制，並將風險評估資訊傳遞給直接依賴此服務及虛擬資產的使用者
- 建議可採用ISO 31000標準之架構，建立風險溝通通用衡量機制

ISO 27017 雲端服務之風險評鑑

- 雲端服務使用者進行風險評鑑時，要應考量下列因素：
  - 雲端服務使用者無法直接觸及資訊安全管理、風險增加、或是有困難進行風險評估
  - 使用雲端運算服務後，會導致組織資訊設施及資訊系統的改變
  - 雲端服務提供者所揭露的資訊過於侷限
  - 雲端服務提供者所揭露的資訊安全、弱點及風險，會影響到所有使用此雲端服務的使用者(基於雲端服務共享的特性)
  - 各國各地區法令規範的不同與衝突之風險議題

ISO 27018與 ISO27001比較

- 主要在於 Operation Security，也就是雲端服務的維運
- 12.1.4 Separation of development, testing and operational environments (when personal data is used for testing) ---開發，測試和操作環境的分離（當個人資料用於測試時）
- 12.3.1 Information backup (multiple copies of data; procedures for the backup, recovery and erasure; providing information to the customer) ---資訊備份（數據的多個副本;備份，恢復和擦除的過程;向客戶提供資訊）
- 12.4.1 Event logging (process for reviewing logs; recording changed privacy information; providing information to the customer) ---事件日誌（查看日誌的過程;記錄更改的隱私資訊;向客戶提供資訊）

ISO 27018對於個人隱私資料安全控制

- Rights of the customer to access and delete the data ---客戶存取和刪除數據的權限
- Processing the data only for the purpose for which the customer has provided this data ---僅為客戶提供此數據的目的處理數據
- Not using the data for marketing and advertising ---不使用數據進行營銷和廣告
- Deletion of temporary files ---刪除臨時文件
- Notification to the customer in case of a request for data disclosure ---在請求數據披露的情況下通知客戶
- Recording all the disclosures of personal data ---記錄個人數據的所有披露
- Disclosing the information about all the sub-contractors used for processing the personal data ---披露關於用於處理個人數據的所有分包商的信息

ISO 27018對於個人隱私資料安全控制

- Notification to the customer in case of a data breach ---在資料洩露的情況下通知客戶
- Document management for cloud policies and procedures ---雲政策和程序的文件管理
- Policy for return, transfer and disposal of personal data ---個人資料的退回，轉讓和處置政策
- Confidentiality agreements for individuals who can access personal data ---可以存取個人資料的個人的保密協議
- Restriction of printing the personal data ---列印個人資料的限制
- Procedure for data restoration ---資料復原步驟
- Authorization for taking the physical media off-site ---異地存放實體媒體置的授權
- Restriction of usage of media that does not have encryption capability ---限制不具有加密功能的媒體的使用
- Encrypting data that is transmitted over public networks ---透過公共網路傳輸的加密數據

ISO 27018對於個人隱私資料安全控制

- Destruction of printed media with personal data ---使用個人資料列印媒體的銷毀
- Usage of unique IDs for cloud customers ---雲客戶的唯一ID的使用
- Records of user access to the cloud ---用戶對雲的存取記錄
- Disabling the usage of expired user IDs ---禁止使用過期用戶帳號
- Specifying the minimum security controls in contracts with customers and subcontractors ---與客戶和分包商簽訂的合同中設定最低安全控制
- Deletion of data in storage assigned to other customers ---刪除分配給其他客戶存儲中的資料
- Disclosing to the cloud customer in which countries will the data be stored ---向雲客戶公開資料將存儲在哪些國家/地區
- Ensuring the data reaches the destination ---確保資料到達目的地

雲端安全注意事項

雲端安全注意事項

- Cloud Specific Assessment （ IaaS, PaaS, SaaS) 雲特定的評估
- Security Assessment 安全評估
- Legal Compliance Assessment 法律符合性評估
- Data Privacy Assessment 資料隱私評估
- Complete Cloud Supply Chain covered 涵蓋完整雲供應練
- ITIL, IT Service Management 資訊服務管理

CSCC *Security for Cloud Computing*

- 1. Ensure effective governance, risk and compliance processes exist ---確保存在有效的治理，風險和合規流程
- 2. Audit operational and business processes---審計業務和業務流程
- 3. Manage people, roles and identities ---管理人員，角色和身份
- 4. Ensure proper protection of data and information ---確保正確保護數據和資訊
- 5. Enforce privacy policies ---強制執行隱私政策
- 6. Assess the security provisions for cloud applications ---評估雲應用的安全規定
- 7. Ensure cloud networks and connections are secure ---確保雲網路和連接安全
- 8. Evaluate security controls on physical infrastructure and facilities ---評估有形基礎設施和設施的安全控制
- 9. Manage security terms in the cloud service agreement ---管理雲服務協議中的安全術語
- 10. Understand the security requirements of the exit process ---了解退出過程的安全要求

資料來源：Cloud Standards Customer Council

Thank You
Question?