



Choosing a Secure Cloud Service Provider

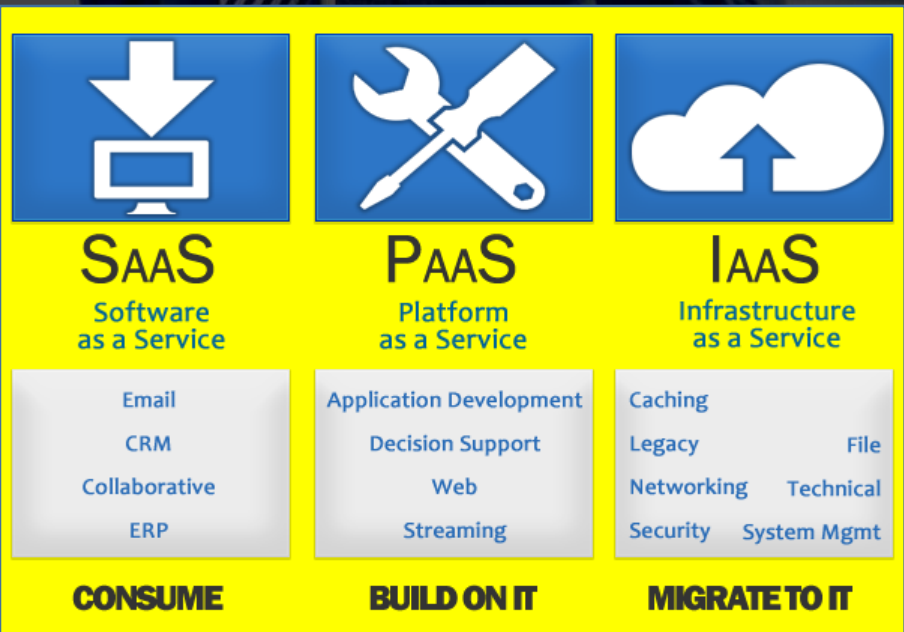
Dr. Ricci IEONG, CISSP, CISA, CISM, CCSK, CCSP, CEH, GPEN, GIAC Advisory Board, ISSAP, ISSMP, F.ISFS

Vice President – Professional Development

Cloud Security Alliance (HK&M) Chapter

CLOUD SERVICES

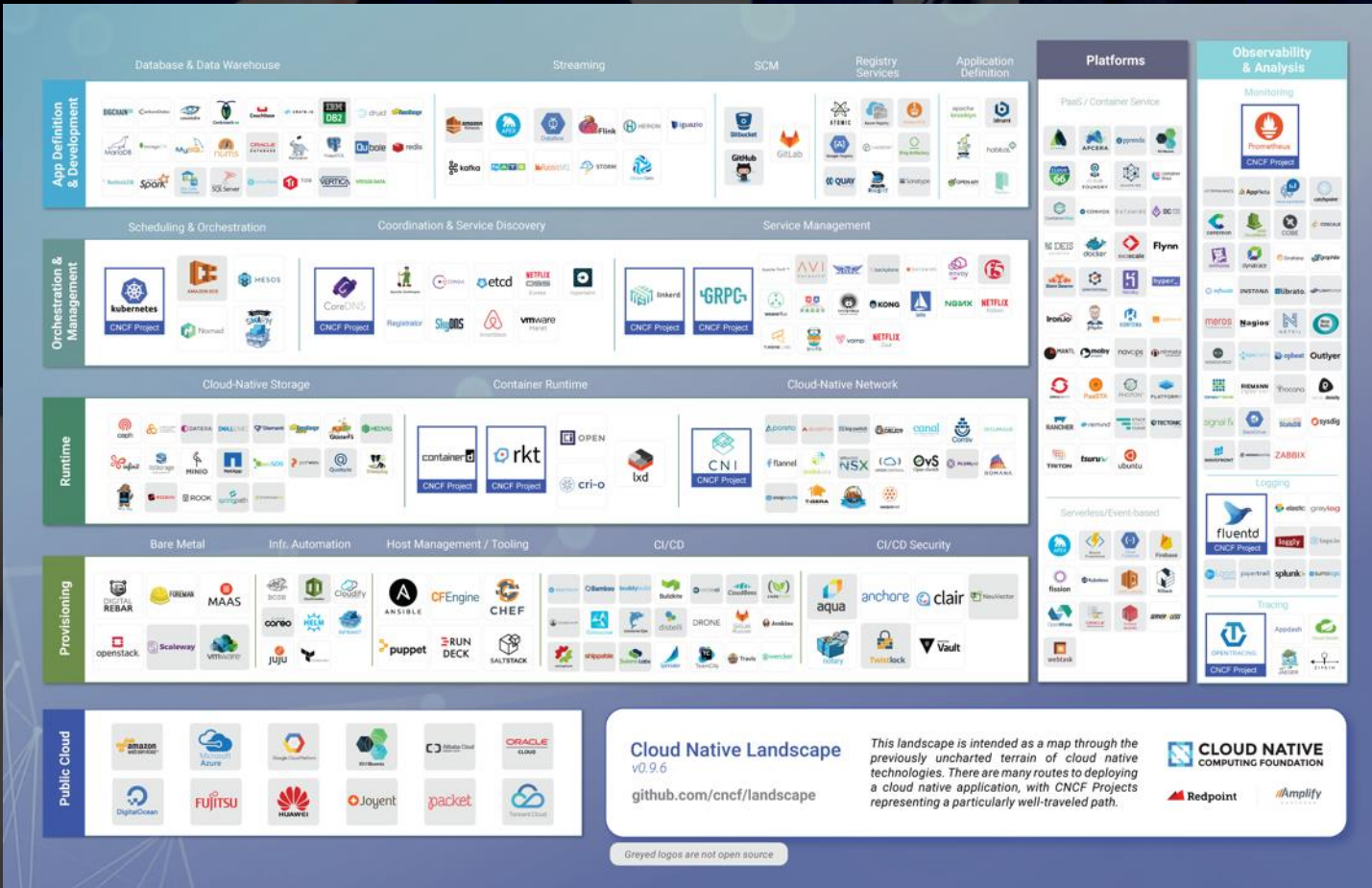
- *Software as a Service (SaaS)*
- *Platform as a Service (PaaS)*
- *Infrastructure as a Service (IaaS)*



Multiple Cloud Services Providers



Cloud Native Landscape 2017



Trend of Cloud Adoption (2017)

Just 23% of organizations today completely **trust** public clouds to keep their data secure. (McAfee, Intel 2017)

Fully integrated (50%) and unified security solutions (47%) are enabling organizations to increase their **trust** in the security of public clouds

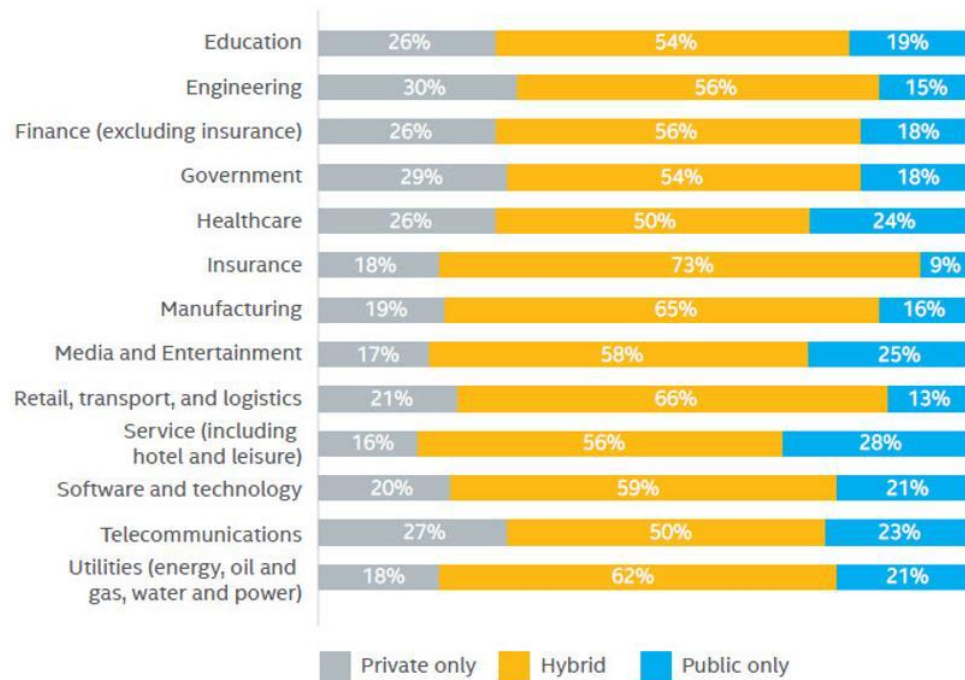
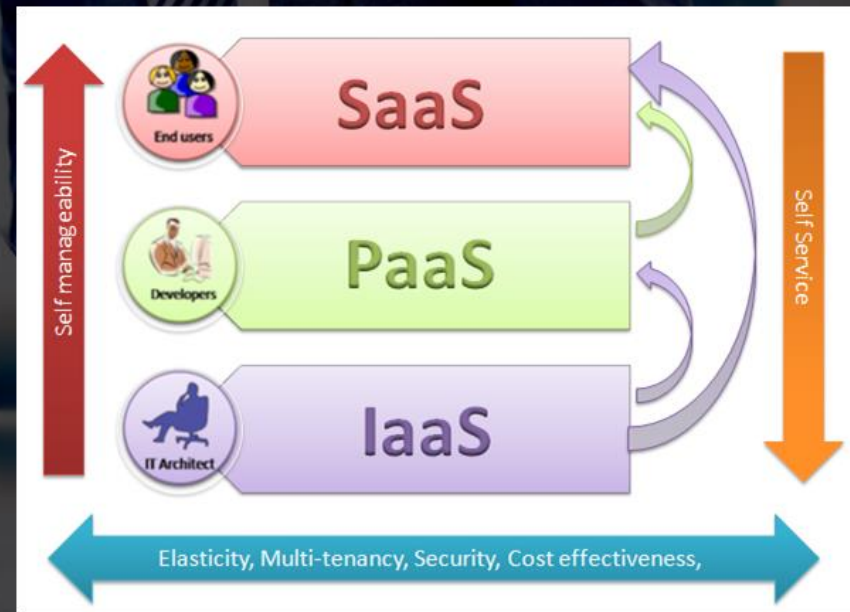


Figure 7. Which type of cloud architecture is your organization currently using? (grouped by industry)

BENEFITS OF USING CLOUD SERVICES

- Less startup or license costs
- Pay-for-usage models that can be scaled up or down
- No long-term contracts
- No capital outlays for servers and other infrastructure to run the applications
- Reduced administrative efforts on applications updates, monitoring, fixes and enhancements
- Accessible from any device, anywhere



EVALUATE A CLOUD SERVICE PROVIDER

- The cost
 - Usually based on a per-use utility model but also variations.
- The Features
- The physical location of the servers
 - Especially for sensitive data.
- Reliability
 - If the data must be accessible.
- Service-level agreement (SLA)
 - Uptime (outages)
 - Resources
 - Compensation
- Security



HOW TO CHOOSE A CLOUD SERVICE PROVIDER (from CSA 2016 Talk)

Business and Operation Aspects	Technical Aspects
<u>Business health and processes</u> <ul style="list-style-type: none">• Financial health• Organization, governance, planning, and risk management• Reputation• Business knowledge and technical know-how• Compliance audit	<u>Technical capabilities and processes</u> <ul style="list-style-type: none">• Ease of deployment, management, and upgrade• Standard interfaces• Event management• Change management• Hybrid capability
<u>Administration support</u> <ul style="list-style-type: none">• Service Level Agreements (SLAs)• Performance reporting• Resource monitoring and configuration management• Billing and accounting	<u>Security practices</u> <ul style="list-style-type: none">• Security infrastructure• Security policies• Identity management / Integrity Monitoring• Data backup and retention• Physical security• Certifications



8 criteria to ensure you select the right cloud service provider to 修身齊家 治國 平天下

- Certifications & Standards
- Technologies & Service Roadmap
- Data Security, Data Governance and Business policies
- Service Dependencies & Partnerships
- Contracts, Commercials & SLAs
- Reliability & Performance
- Migration Support, Vendor Lock in & Exit Planning
- Business health & Company profile

<https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider>

Certifications & Standards

Standards organisations & frameworks – examples;

Cloud



Security



Operations



Is Cloud Secure?

Date	Incident
February 2017	A vulnerability in Slack was discovered which had the potential to expose the data of the company's reported four million daily active users..
February 2017	CloudFlare, a content delivery network, leaked sensitive customer data stored by millions of websites powered by the company.
March 2017	Wikileaks CIA Vault 7 exposed 8,761 documents on alleged agency hacking operations
June 2017	Deep Root Analytics, a conservative data firm, misconfigured an Amazon S3 Server that housed information on 198 million U.S. voters.
July 2017	Verizon had the same issue and announced a misconfigured Amazon S3 data repository at a third-party vendor that exposed the data of more than 14 million U.S. customers.



Technologies & Service Roadmap

Depending on your particular cloud strategy, you may also want to evaluate the overall portfolio of services that providers can offer.

Technologies

Make sure the provider's platform and preferred technologies align with your current environment and/or **support your cloud objectives**.

Does the provider's cloud architectures, **standards and services** suit your workloads and management preferences?

Assess how much **re-coding or customisation** you may have to do to make your workloads suitable for their platforms.

Service roadmap

Ask about the provider's **roadmap of service development** – How do they plan to continue to innovate and grow over time? Does their roadmap fit your needs in the long term?



Data Governance and security

Define Data Governance

Define a data classification scheme in place that defines types of data according to sensitivity and/or policies on data residency.

Protect data in transit through encryption of data moving to or within the cloud.

Data Breach Management

With data loss and breach notification processes and then ensure they are aligned with your organisation's risk appetite and legal or regulatory obligations.

The provider's information security controls should be demonstrably risk-based and clearly support your own security policies and processes.

Data Security

Ensure user access and activity is auditable via all routes and get clarity on security roles and responsibilities as laid out in the contacts or business policies documentation.



Service Dependencies & Partnerships

Vendor relationships

Service providers may have **multiple vendor relationships** that are important to understand.

Assessing the provider's relationship with key vendors, their accreditation levels, technical capabilities and staff certifications, is a worthwhile exercise.

Subcontractors and service dependencies

The Code of Practice requires **explicit clarification of service dependencies** and the implications on SLAs, accountability and responsibility.

Contracts, Commercials & SLAs

Identifying the important factors to help clarify risk and suitability

Service Delivery

- Service definition
- Roles and responsibilities
- Service management
- Service availability
- DR and Service continuity



Business Terms

- Insurance
- Business policies (x14)
- Fees and commercial terms
- Publicity
- Operational reviews



Data Assurance

- Data management
- Data security
- Ownership and use rights
- Data conversion



Legal Protections

- Indemnification
- Intellectual property
- Limitation of liability
- Warranties





Contracts, Commercials & SLAs

Service level agreements (SLA) should contain 3 major components:

- Service level objectives

- Remediation policies and penalties/incentives related to these objectives

- Exclusions and caveats

specify how issues should be identified and resolved, by who and in what time period.

Service level objectives (SLOs) typically cover:

- accessibility,

- service availability (usually uptime as a percentage),

- service capacity (what is the upper limit in terms of users, connections, resources, etc.),

- response time and

- elasticity (or how quickly changes can be accommodated).

Verify through providing them same imaginary downtime scenario for comparison

Cloud Commercials

Bundle of services and pricing models

Cloud Commercials



Consumption Period

	CSP - A	CSP - B	CSP - C
Minutes	✓	✓	✗
Hours	✗	✓	✗
Months	✗	✓	✓
Years	✓	✗	✓



Packaged

	Tier 1	Tier 2	Tier 3
Core	1	2	3
RAM	512MB	1GB	4GB
Storage	20GB	30GB	40GB
Network	3TB	6TB	9TB



Configurable





Reliability & Performance

Ensure Performance

Check the performance of the service provider against their SLAs for the last 6-12 months

Ensure Reliability

Ensure your chosen provider has established, documented and proven processes for dealing with planned and unplanned downtime.

Look to understand the provider's disaster recovery provisions, processes and their ability to support your data preservation expectations (inc. recovery time objectives).

DR plan should include criticalness of data, data sources, scheduling, backup, restore, integrity checks, etc.

Assign Responsibilities

Roles and responsibilities, escalation processes and who has the burden of proof, all must be clearly documented in the service agreement.

Transfer Risk

Consider purchasing additional risk insurance if the costs associated with recovery are not covered by the provider's umbrella terms and conditions.

Migration Support, Vendor Lock in & Exit Planning

Portability and Lock-in

Cloud services that rely heavily on bespoke or unique proprietary components may impact your portability to other providers or in-house operations.

Avoid the risk of vendor lock in by ensuring your chosen provider has minimal use of proprietary technology or you minimise the use of services that limit your ability to migrate or transition away.



Vendor Lock-in

Examples of vendor lock-in candidates

- CSP compatible application architecture
- Proprietary cloud management tools
- Customised geographic diversity
- Proprietary cloud APIs
- Customised cloud Web services (e.g. Database)
- Premium configurations
- Custom configurations
- Data controls and access
- Data formats (not standardised)
- Service density with one provider




Migration Support, Vendor Lock in & Exit Planning

Exit provisions

Similarly, ensure you have a clear exit strategy in place at the start of your relationship. Moving away from a CSP's service isn't always an easy or smooth transition, so it's worth finding out about their processes before signing a contract.

Furthermore, consider how you'll access your data, what state it will be in and for how long the provider will keep it.

A background image showing two men in business suits. The man on the left is looking down at a document, and the man on the right is looking at the same document. They appear to be in a meeting or collaborative work environment.

Business health & Company profile

Company Financial Status

Assessing the technical and operational capabilities of a potential supplier is obviously important, but take time to consider the financial health and profile of your shortlisted providers.

As Microsoft say in their short guide on provider selection: “The provider should have a track record of stability and be in a healthy financial position with sufficient capital to operate successfully over the long term”.

Try and establish if the organisation has had any past legal issues, has been, or is being sued and how they respond to legal challenges - ask directly or do your own research.



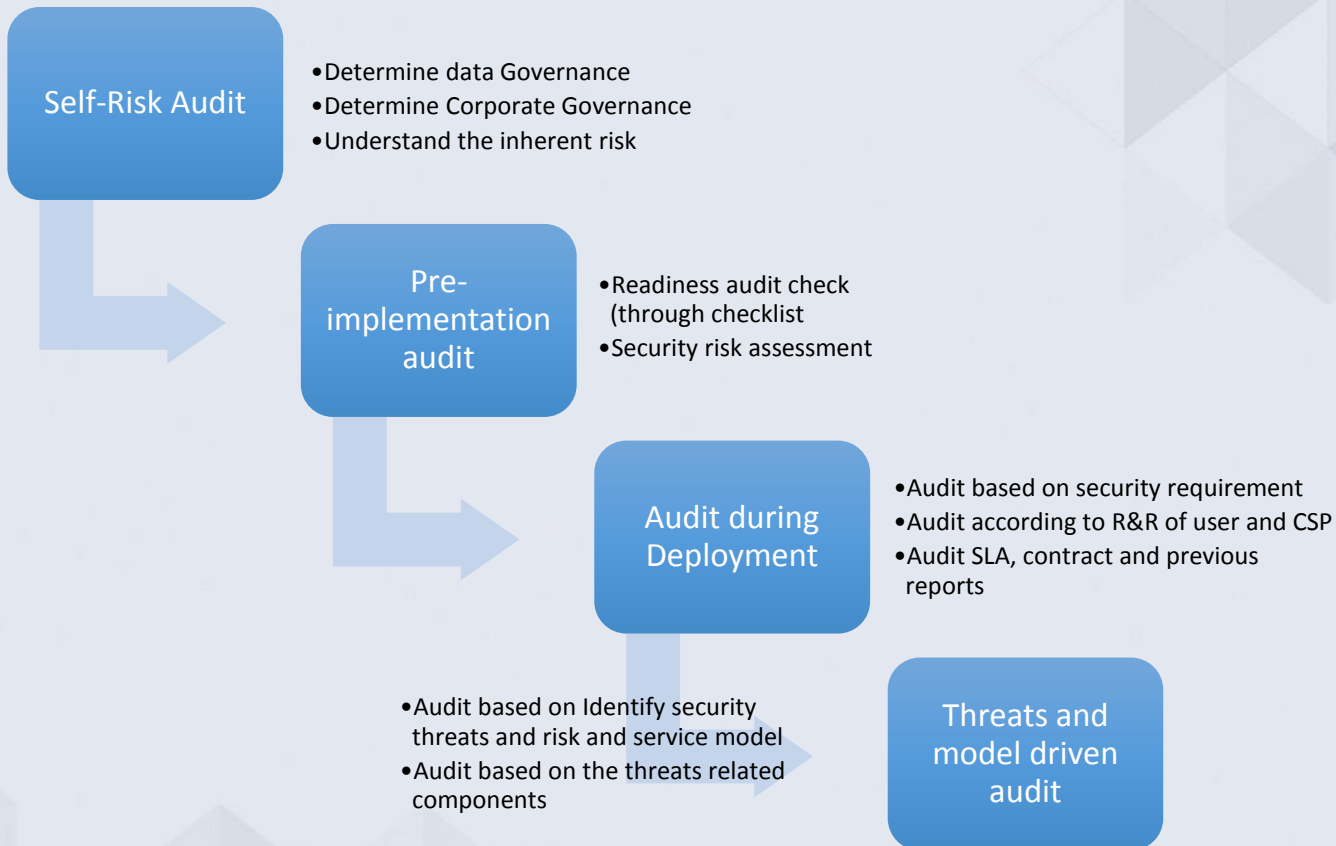
Code of Practice Framework

Define certification framework

Code of Practice certified cloud service providers have declared and committed to providing good quality services that adhere to **the guidelines and best practices** set out in the COP.

The COP is a **comprehensive framework** that enables service providers to benchmark their operations against standards developed by their peers and in many ways is a checklist for best practice in the provision of cloud services.

Overall methodology



Pre-implementation audit

Readiness audit check
(Modified from Security
Considerations for Cloud
Computing ISACA)

Security risk assessment

Pre-Cloud implementation or engagement checklist

Background information about the nature of application (to be answered by Cloud User)

Questions	Descriptions
1-1. Functions and nature of the application	
1-2. Business Owner	
1-3. Data Owner	
1-4. List of User group(s)	
1-5. Application to be migrated to the cloud?	
1-6. Application data to be transferred to the cloud?	
1-7. Have a list of potential cloud provider candidates and perform a sanity check on them (financial situation, references, authenticity, etc.) been prepared?	
1-8. Has business case and evaluation of cost/benefits for migration to cloud been provided?	
1-9. Have infrastructure, design and requirements of application candidates to be moved to cloud been evaluated	

Background information about the business operations of application (to be answered by Cloud User)

Questions	Descriptions
2-1. Service Model to be selected?	IaaS / PaaS / SaaS
2-2. Deployment Model to be selected?	Private / Public / Hybrid / Community
2-3. Which team will be responsible for handling the internal operations / support requirement?	

2-4. System Availability requirement

2-5. What is the requirement

2-6. What is the requirement

Background information about the security requirement of application (to be answered by Cloud User)

Questions	Descriptions
3-1. Data Classification Level	

Cloud Service Provider Provided Document Check (To be requested by Cloud User)

Document List	Descriptions	IaaS	PaaS	SaaS	✓
4-1	Services Level Agreement	M	M	M	
4-2	Contract	M	M	M	
4-3	Security Risk Assessment Report (ISO 27001, 27017, 27018, SOC2, SOC3 report, etc)	M	M	M	
4-4	Privacy Level Agreement	O	O	M	
4-5	IT Security Policies, IT Policies	O	O	O	
4-6	BCP/DRP	M	M	M	
4-7	Backup plan and arrangement/options	M	M	M	
4-8	Change Management arrangement/options	O	M	M	
4-9	Security Monitoring and Detection	M	O	O	



Thank You.

Cloud Security Alliance Hong Kong & Macau Chapter
csahkm.org