INSTITUTIONAL AND PROCUREMENT PRACTICE NOTE ON CLOUD COMPUTING

8TH ADB APPEN
EGP CONFERENCE 2022

WORLD BANK GROUP
Governance

Hunt La Cascia
Senor Procurement Specialist
World Bank
hlacascia@worldbank.org

December 2, 2022

Agenda

1. Benefits of Cloud Computing?
2. Cloud Service Models
3. Cloud Deployment Models
4. Cloud Security Accreditations and Certifications
5. Lesson Learned through Case Studies
6. Pillar 1: Institutional Coordination Mechanisms
7. Pillar 2: Data Classification and Security Framework
8. Pillar 3: Procurement Arrangements

WORLD BANK GROUP

Benefits of cloud computing?

- Identified risks of moving to cloud computing:
  - Will their data be safe?
  - Will they have sovereign control over access to data stored offshore?
  - Will privacy be protected?

- "G-Cloud" or "GovCloud"
  - Due to an inadequate assessment framework to identify and assess these risks, the typical response of most client governments is to develop a government's cloud (i.e., "G-Cloud" or "GovCloud").
  - Logical for more sensitive or mission-critical data.

- Adopting a hybrid cloud model,
  - Which leverages the cloud services from the private sector to work in conjunction with the G-Cloud can offer immense opportunities to save costs, improve security, enhance performance, and strengthen resilience.

Definition of Cloud Computing

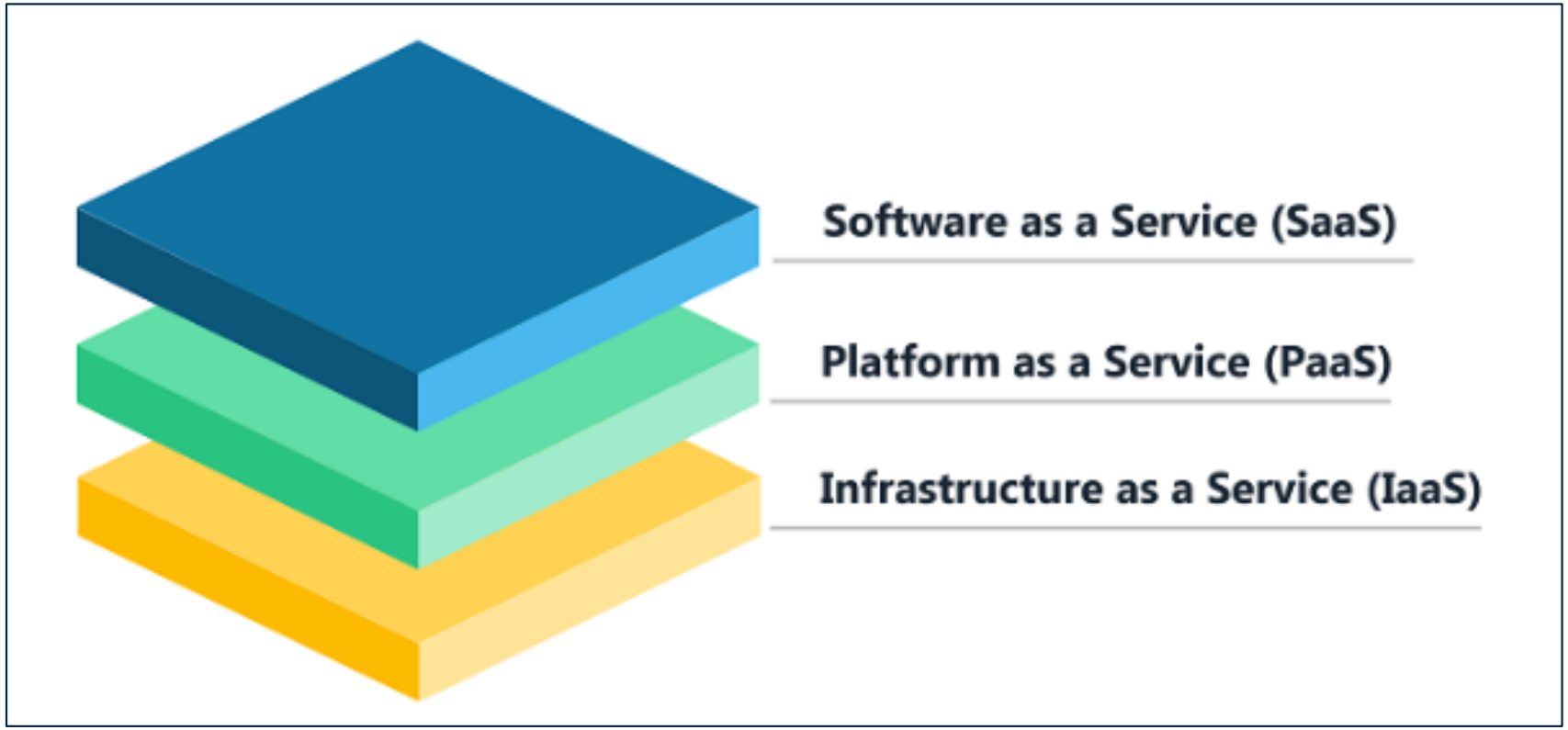
"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

By US government's National Institute of Standards and Technology (NIST)

WORLD BANK GROUP

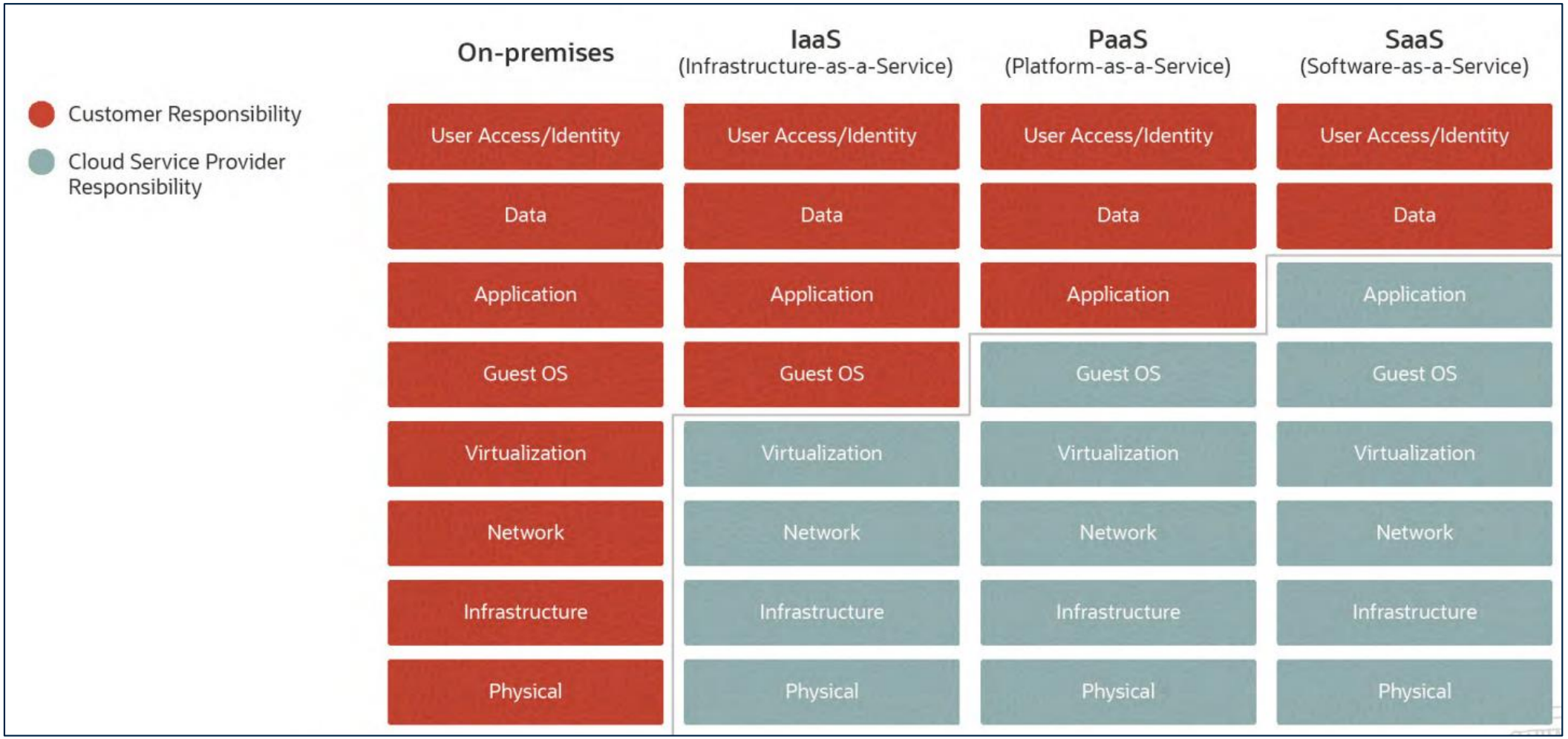
Cloud Service Models

The term "cloud services" refers to a broad range of services offerings, which can be categorized as either Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).



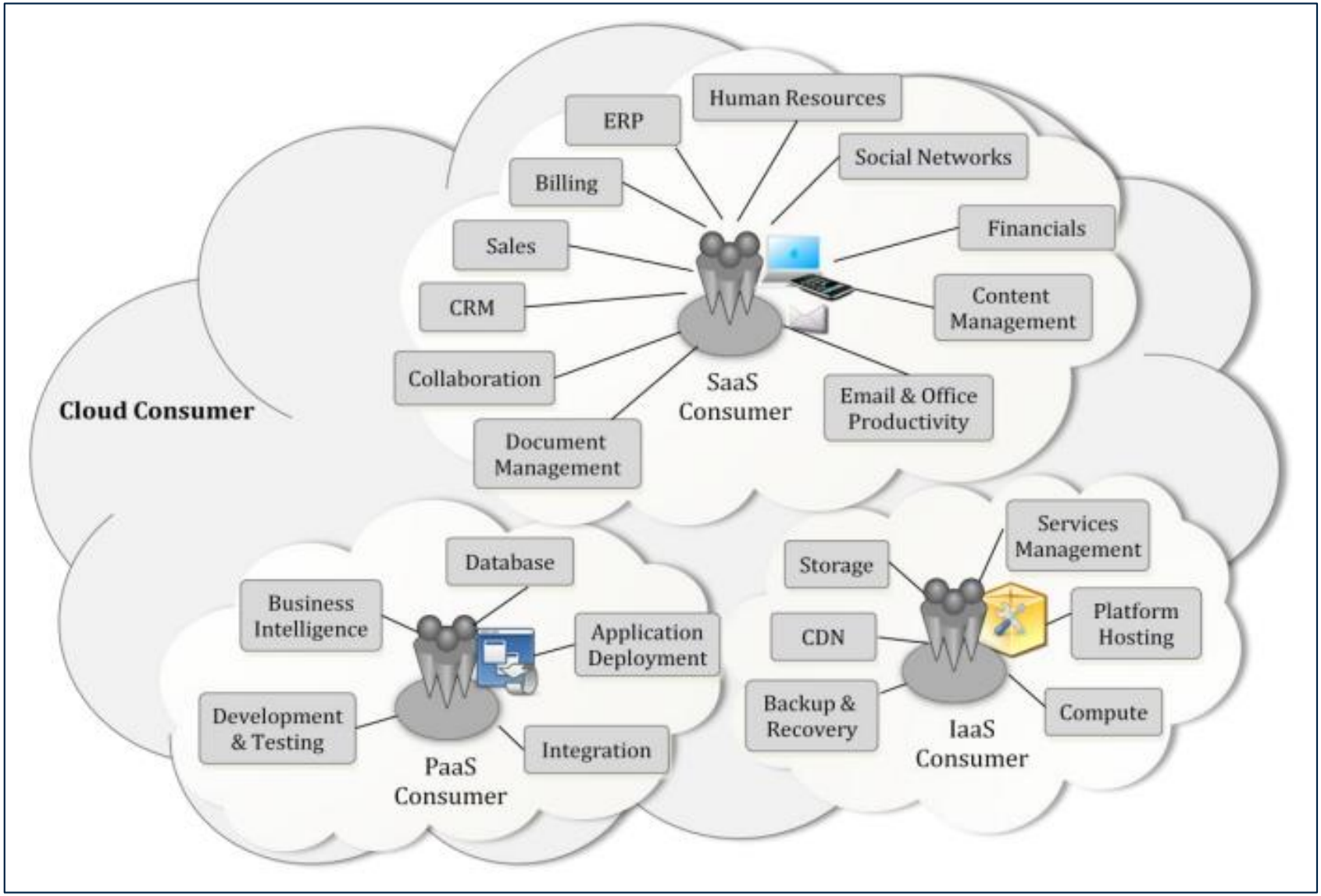
WORLD BANK GROUP

Shared Responsibility between Consumer and CSP



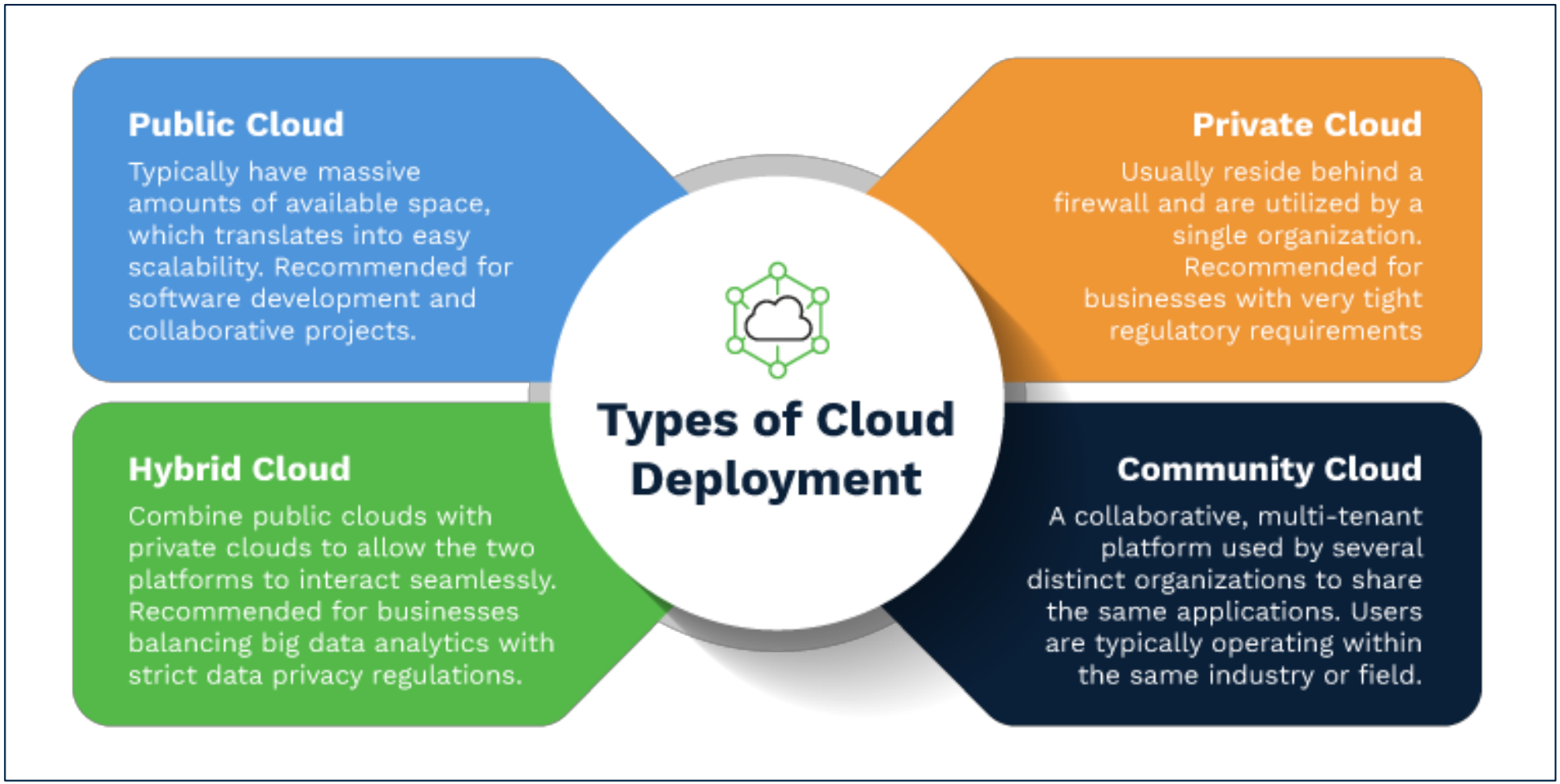
WORLD BANK GROUP

Example Services Available to a Cloud Consumer



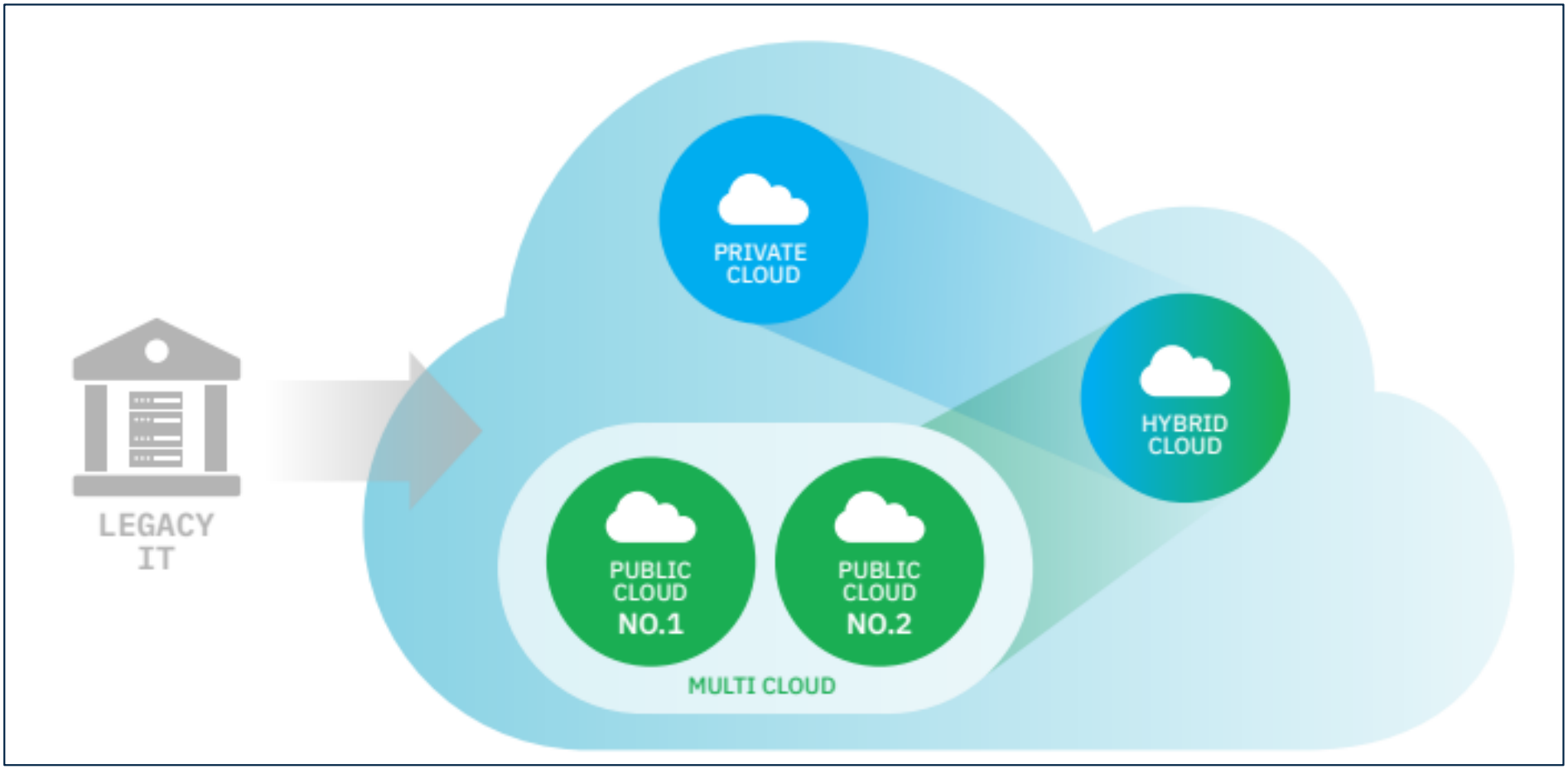
WORLD BANK GROUP

Cloud Deployment Models



WORLD BANK GROUP

Cloud Deployments Fit Needs



WORLD BANK GROUP

Cloud Security Accreditations and Certifications

CSPs may also demonstrate their cybersecurity credentials through an accredited certification body (also called a third-party assessor). Some key terms for this process include:

- Accreditation
- Certification
- Conformity Assessment Activity

A Comparative Analysis of Case Studies

The experiences of the five case studies provide insights into "good practices" for institutional coordination mechanisms and procurement arrangements for integrating cloud services into public entity operations

- Japan
- Australia
- UK
- South Africa
- UAE*

Lesson Learned through Case Studies

Key similarities and differences between these case studies, divided into three pillars:

- Pillar 1: Institutional Coordination Mechanisms
- Pillar 2: Data Classification and Security Framework
- Pillar 3: Procurement Arrangements

Pillar 1: Institutional Coordination Mechanisms

Pillar 1: Institutional Coordination Mechanisms provides the similarities and differences and strengths and weaknesses, of the institutional coordination mechanisms for procuring secure cloud services, including:

- "Cloud First" Principle
- Top-Level Policies and Strategies
- Institutional Framework

Pillar 1: Institutional Coordination Mechanisms

"Cloud First" Principle

- First consider potential cloud solutions before considering any other option (such as on-premises computing solutions).

- Many countries also require procuring agencies to consider public cloud solutions before any other cloud deployment model if that public cloud provides appropriate security controls for the data to be handled.

- In four of the five case studies, cloud first principles are articulated within top-level government policies and strategies that pertain to the whole-of-government. For example: Japan, Australia, UK and Dubai.

Pillar 1: Institutional Coordination Mechanisms

Top-Level Policies and Strategies

- The "top-down" policy approach encourages consistent implementation of pre-approval and procurement processes by public organizations seeking to procure public cloud solutions.
- The use of standardized frameworks and processes can also allow for streamlining of CSP and cloud service approvals across procuring agencies.
- In four of the five case studies, cloud first principles are articulated within top-level government policies and strategies that pertain to the whole-of-government. For example: Japan, Australia, UK and Dubai.
- South Africa has not yet finalized its top-level policy on cloud computing. Its National Policy on Data and Cloud remains in draft form. However, in its current draft form, the National Policy does not articulate a "cloud first" principle.

Pillar 1: Institutional Coordination Mechanisms

Institutional Frameworks

Major differences in the institutional frameworks to advance cloud pre-approval and procurement. These differences can be categorized into three models: Centralized, Decentralized, and Hybrid.

CENTRALIZED MODEL: A centralized approach that puts the responsibility upon Ministerial of ICT, in collaboration with third-party assessors, to pre-approve cloud services that are then added to its Cloud Service List. In turn, procuring agencies may issue Tenders for cloud services on the Cloud Services List, without the need to conduct their own security assessment of the cloud service.

DECENTRALIZED MODEL: Centralized Public Service and Administrations offers guidance on how procuring agencies should approach the cloud service procurement process, including business and security aspects of cloud procurement. Procuring agencies are responsible for finding, assessing and approving, and procuring cloud services.

HYBRID MODEL: Under the Hybrid approach, each procuring agency is ultimately responsible for assessing the security of cloud services against its own security needs (sometimes with the assistance of third-party assessors).

Summary of Institutional Framework

Summary of Institutional Frameworks of the Case Studies			
Case Study	Model	Strengths	Weaknesses
Japan	Centralized	• Streamlines security responsibilities within one organization facilitating the pre-approval of cloud services and listing the pre-approved cloud services. • Eases the security assessment process for procuring agencies.	• Available pre-approved cloud offerings may be limited compared to other models. • Centralized system could create bottlenecks.
South Africa	Decentralized	• Standardized procurement guidance provides for flexibility in agency-level cloud assessment and approval process. • Empowers agencies to tailor their assessment, approval, and procurement activities to its unique circumstances.	• No centralized listing of cloud services available. • Lack of centralized apparatus risks non-uniformity in security of procured cloud services.
Australia **UK** **Dubai**	Hybrid	• Streamlines security responsibilities within one organization approving or verifying the certification of cloud services. • Centralized marketplace eases the process of selecting and assessing various cloud services.	• Multiple organizations with varied responsibilities could cause complexity and confusion.

WORLD BANK GROUP

Pillar 2: Data Classification and Security Framework

Pillar 2: Data Classification and Security Framework provides the on the strengths and weaknesses, of the data classification and security framework considerations for secure cloud services, including:

- Data Classification
- Data Residency Requirements
- Security Controls
- Security Assessments
- Continuous Monitoring

Pillar 2: Data Classification and Security Framework

Data Classification

- Each case study has its own, unique data classification system.
- Commonalities include the use the Confidentiality, Integrity, and Availability (CIA) framework when considering levels of injury in case of a security incident.
- Distinguishing between lower-priority "Sensitive" or "Protected" data versus higher-priority "Classified" or "Secret" data.
- Japan is unique in that it only pertains to one data classification level – "Confidential 2", which corresponds with the US government's FedRAMP Moderate Impact Level.

Comparison of Data Classification Levels

Japan (ISMAP)	Australia	UK	South Africa	Dubai
• Confidential 2	• Unclassified (Unofficial, Official, Official: Sensitive) • Classified (Protected, Secret, Top Secret	• Official • Secret • Top Secret	• Restricted • Confidential • Secret • Top Secret	• OPEN • SHARED-Confidential • SHARED-Sensitive • SHARED-Secret

Pillar 2: Data Classification and Security Framework

Data Residency Requirements

Required

- **South Africa**: Public cloud data must always reside within the borders of South Africa (with limited exceptions).
- **Dubai**: Dubai forbids the handling of SHARED data outside the UAE. In addition, CSPs handling SHARED data for government entities must have a minimum of two data centers within the country's geographic jurisdiction. However, there is an exemption process for procuring agencies seeking to host shared data outsides UAE, which is based on a risk assessment process.

Recommended

- **Australia**: Recommends cloud consumers use CSPs and cloud services located in Australia for handling their sensitive and security-classified information. Australia also requires CSPs handling data at or above the Official:Senstive data level to obtain a Hosting Certification Framework (HCF) certification.
- **UK**: Recommends public agencies to consider the implications of where data is hosted.
- **Japan**: Procuring agencies should strongly consider the potential risks of the handling of data that may become subject to foreign laws and regulations when selecting cloud service offerings.

Pillar 2: Data Classification and Security Framework

Security Controls

- Each case study has its own, unique regime of security controls for the pre-approval of public cloud services.
- Japan and Dubai developed their own control regimes based upon existing international standards.
- Australia bases its controls upon NIST standards. Other countries (e.g., UK and South Africa) rely more directly upon existing laws, regulations, and guidance.

Pillar 2: Data Classification and Security Framework

Security Assessments

- **Security Self-Assessment**: Are procuring agencies required to assess their own risk profiles before assessing cloud services?
- **Third-Party Assessors**: Do third-party assessors conduct a security assessment of the CSP as part of the review process?
- **Assessment Reuse**: Can CSPs share third-party assessments with multiple procuring agencies?
- **Controls Inheritance**: As part of the security assessment, do cloud services inherit the security controls of other cloud services they are built upon?
- **Reassessment Requirements**: Must approved CSPs and their cloud services be periodically re-assessed?

Pillar 2: Data Classification and Security Framework

Comparison of Security Assessment Considerations and Activities					
	Japan	Australia	UK	South Africa	Dubai
Security Self-Assessment	Yes	Yes ("Phase 2A" Report)	Yes	Yes	Yes
Third-Party Assessments	Yes ("ISMAP Assessors")	Yes ("IRAP Assessors")	No	No	Yes ("Certification Bodies")
Assessment Reuse	Yes (approved services added to Cloud Service List)	Yes	No	No	Yes
Controls Inheritance	No	Yes	Case-by-case	Case-by-case	Yes
Reassessment Requirements	Every 12 months	Every 24 months	24-month maximum G-Cloud Contract	Contracts cannot exceed 5 years	Basic reviews every 12 months and full re-certifications every 3 years

Pillar 2: Data Classification and Security Framework

Continuous Monitoring

- All case studies require procuring agencies to work with CSPs to continuously monitor the security of a cloud service.
- For example, under Japan's ISMAP, cloud services must be renewed on an annual basis by ISMAP Assessors to ensure the continued security of each offering.
- Other countries similarly engage in long-term continuous monitoring through mandatory security reassessments, incident reporting requirements, and guidance for cloud lifecycle security.

Pillar 3: Procurement Arrangements

Pillar 3: Procurement Arrangements provides the on the strengths and weaknesses, of the arrangements to procure cloud services, including:

- Finding and Selecting Cloud Services
- Managing Vendor Lock-in
- Payment Methods

Pillar 3: Procurement Arrangements

Finding Cloud Services

- Offering a centralized marketplace of cloud services. The UK, Australia, and Dubai have developed online marketplaces for cloud services for procuring agencies.

- Another mechanism is a listing of pre-approved cloud offerings. For example, Japan's ISMAP Cloud Services List provides procuring agencies with an updated list of pre-approved cloud services.

- South Africa does not currently have a centralized List or Marketplace of cloud service offerings. Instead, each procuring agency conducts its own market research or Open Tender process to begin its cloud procurement activities.

Pillar 3: Procurement Arrangements

Selecting and Contracting Cloud Services

- Marketplaces are designed to facilitate simplified, short-term contracts for cloud services.
- Security is a key consideration when selecting cloud services from the marketplaces
- Cost including total cost of ownership and other considerations may include business and operational needs, technical “fit” of the service, and service management.

Pillar 3: Procurement Arrangements

Summary of Procurement Models of the Case Studies			
Case Study	Model	Strengths	Weaknesses
Australia **UK** **Dubai**	Marketplace	• A marketplace offers a centralized location for procuring agencies to review cloud services with and without pre-approvals or certifications. • There is flexibility in how to add CSPs and their cloud services onto a marketplace, how procuring agencies can select and contract with a CSP, and how to approach pricing and payments.	• Requires advanced e-government capabilities to create and maintain an online marketplace.
Japan	Pre-Approved List	• Lists of pre-approved CSPs offers procuring agencies an easy way to locate secure cloud services. • Procuring agencies can engage in typical procurements (such as Tenders) for cloud services on the pre-approved lists.	• Procurements off the pre-approved lists are conducted on a case-by-case basis, meaning there are no standardized contract templates available.
South Africa	Top-Level Guidance	• Procuring agencies must abide by the DPSA's Determination and Directive. • This system provides flexibility in procurement methods for each agency.	• May result in discrepancies in security and service standards across the public sectors.

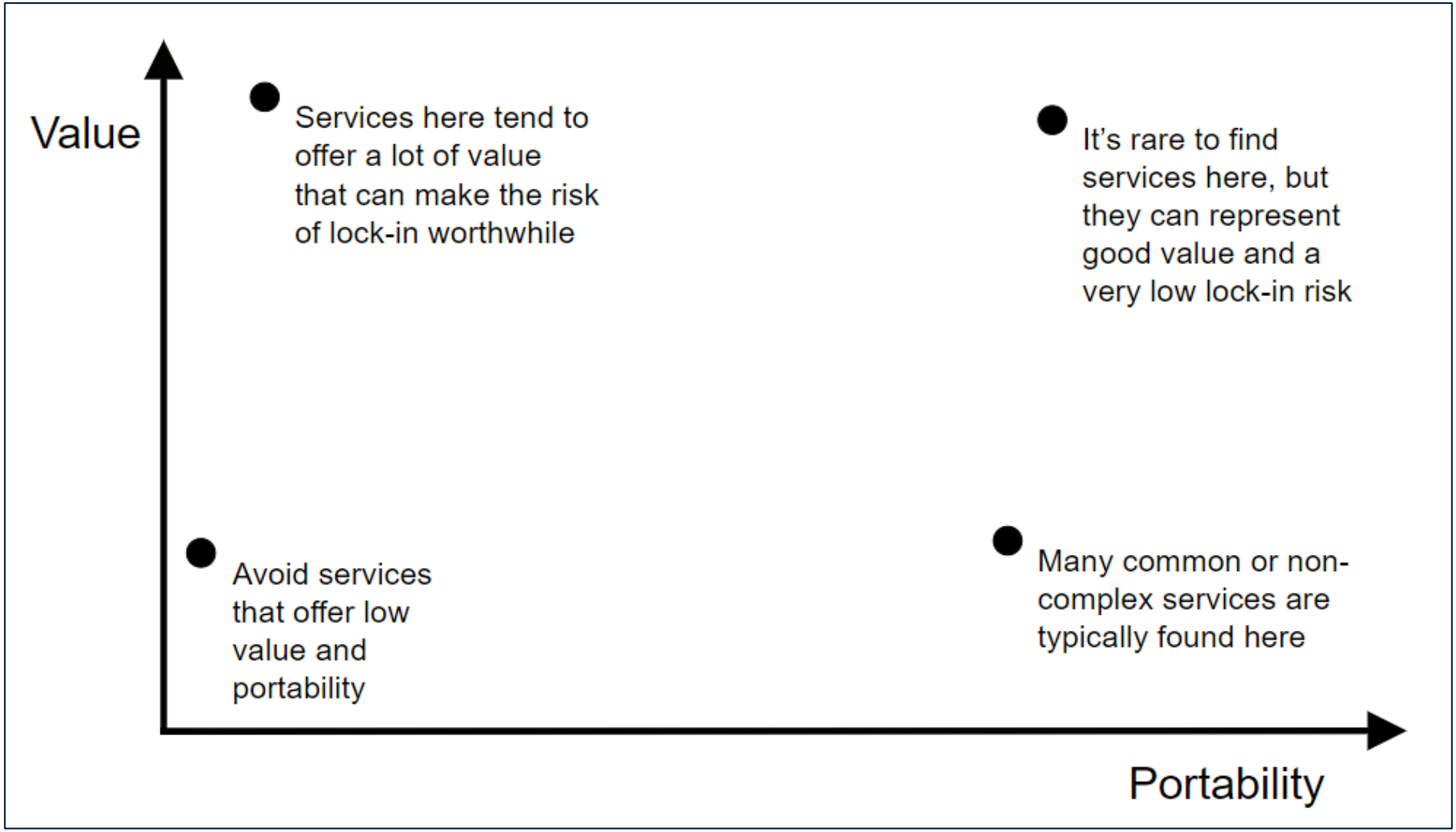
Pillar 3: Procurement Arrangements

Managing Vendor Lock-in

- Short-term cloud services contracts are one effective tool for managing the risk of lock-in.

- Procuring agencies assess CSPs to maximize both the value and portability of the services.
  - Portability refers to the ease and affordability of moving a system and data from one CSP to another.
  - More portable offerings decrease vendor lock-in risk.
  - Agencies should consider portability ease and costs as part of its cloud service procurements.

Portability and Value Considerations for Cloud Services



WORLD BANK GROUP

Pillar 3: Procurement Arrangements

Payment Methods

- **Transparency**: CSP pricing information should be available and easy to understand for procuring agencies.
- **Variable Prices**: Cloud procurement models should allow flexibility to ensure cloud prices can fluctuate based upon market pricing, taking advantage of price reductions in the cloud market.
- **Multiple Pricing Models**: CSPs should be able to offer different pricing models to enable procuring agencies to assess which model best fits its needs.
- **Pay-Per-Use Model ("Utility Style")**: Countries should develop an on-demand, pay-as-you-go (i.e., "utility style") option for procuring cloud services to help reduce costs.

Thank you!

WORLD BANK GROUP
Governance