Republic of Lebanon

OMSAR

Office of the Minister of State for Administrative Reform

Implementation of Lebanon's National Digital Transformation Strategy

Workshop 2

July 15-16, 2024

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

DAY 2: DATA HOSTING

OPENING REMARKS

OVERVIEW AND OBJECTIVES OF WORKSHOP 2

AGENDA

DAY 1: E-GOVERNMENT

- Architectural framework
- Current platforms in Lebanon
- Global insights
- Strategic implementation

DAY 2: DATA HOSTING

- Global strategic approaches
- Current practices
- Future directions for Lebanon

WHAT TO EXPECT ON DAY 2

A.

Data Hosting Strategies

9:15 - 10:05

B.

Data centers

10:05 – 10:50

C.

Overview of data hosting for Lebanon

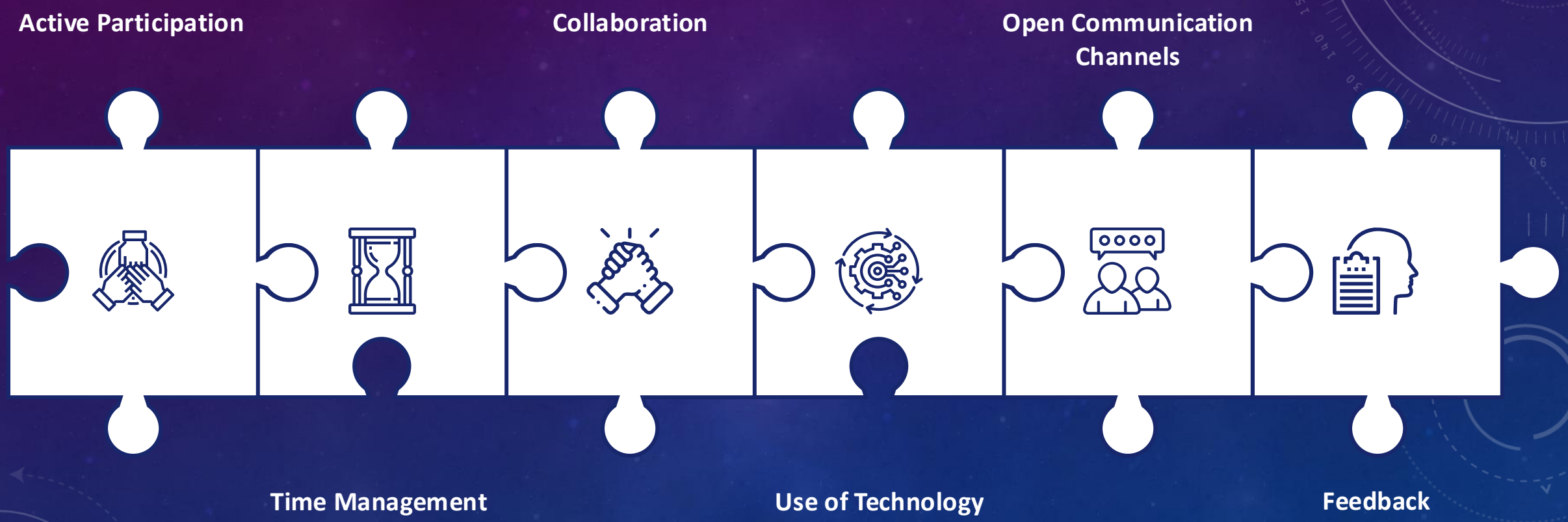
11:20 - 12:45

D.

The way forward for Lebanon

14:00 - 15:30

REMINDER OF OUR RULES OF ENGAGEMENT FOR A PRODUCTIVE WORKSHOP ENVIRONMENT



A. DATA HOSTING STRATEGIES

DATA CENTERS & CLOUD: COMPARISON

What is a data center?

Physical location that contains computing machines and related hardware

-or-

Infrastructure underlying cloud

What is the cloud?

Compute resources provisioned on demand over a network

-or-

Functionality at your fingertips

GOVERNMENTS USUALLY CLASSIFY DATA INTO 3 OR 4 LEVELS, BASED ON THE SEVERITY OF THE IMPACT IF DISCLOSED AND THE POTENTIAL THREATS INVOLVED

Benchmark of government data classifications

Preliminary

KSA
1. Public
2. Confidential
3. Secret
4. Top Secret

UAE
1. Secret
2. Sensitive
3. Confidential
4. Open

Egypt
1. Public
2. Internal
3. Sensitive
4. Confidential

Japan
1. Handle with Care
2. Confidential
3. Secret
4. Top Secret

Singapore
1. Restricted
2. Confidential
3. Secret
4. Top Secret

Jordan
1. Ordinary
2. Confidential
3. Private
4. Sensitive
5. Secret

Qatar
1. Public
2. Internal
3. Restricted
4. Secret
5. Top secret

India
1. Restricted
2. Confidential
3. Secret
4. Top Secret

China
1. Internal
2. Confidential
3. Secret
4. Top Secret

South Korea
1. General
2. For external use
3. Confidential
4. Secret
5. Top Secret

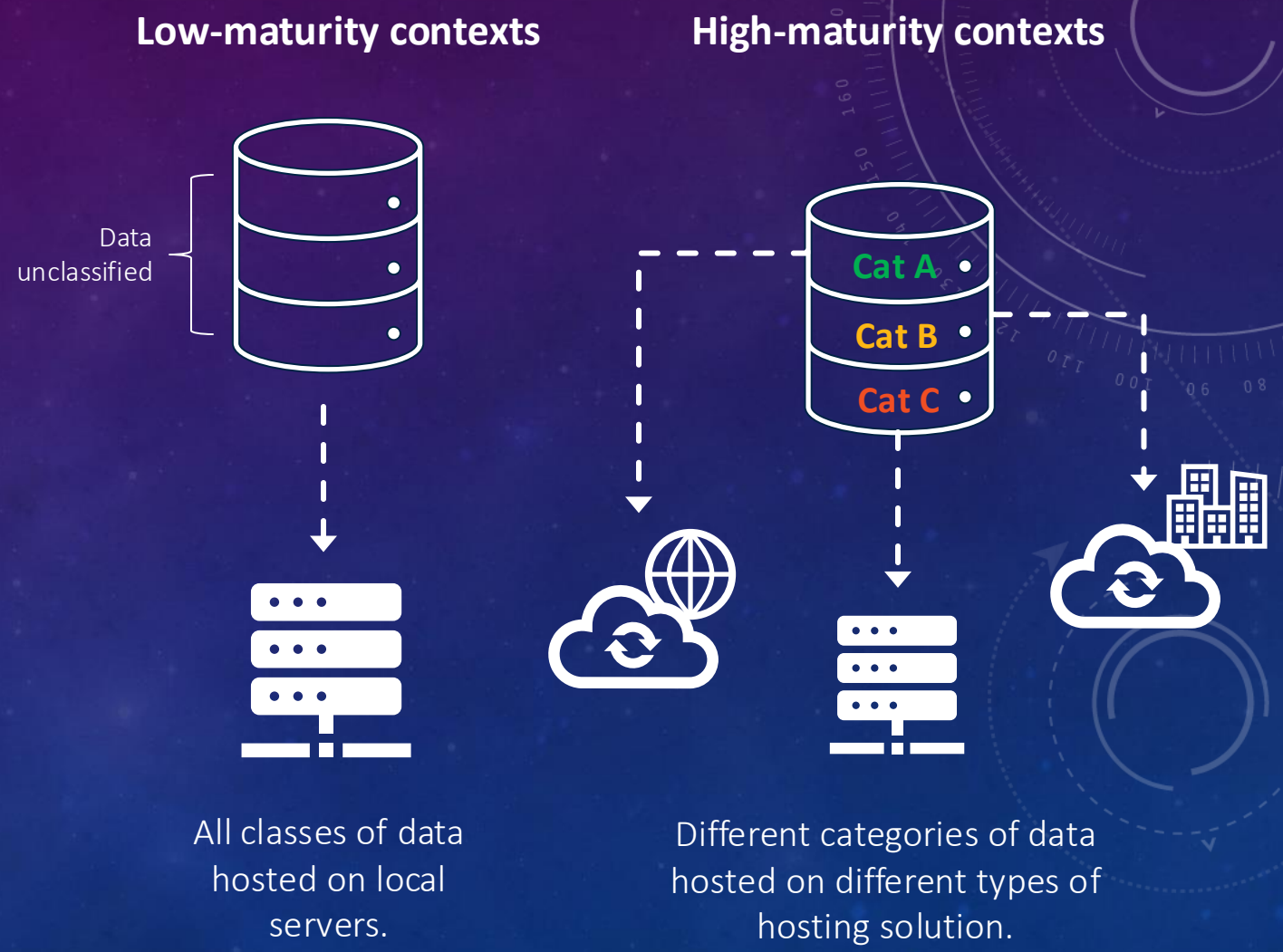
1 Sensitivity level (from lowest to highest)

Source: Desk Research, Roland Berger

DATA CLASSIFICATION: KEY ENABLER OF MATURE E-GOVERNMENT

- ✓ **National data governance framework** includes data classification
- ✓ Data classification framework should consider **requirements** for each type of data – such as confidentiality, availability, and integrity.

No one-size-fits-all solution: different data → different hosting needs.



CLOUD HAS THREE PRIMARY DEPLOYMENT MODELS, WHICH DIFFER MAINLY IN THE LEVEL OF CONTROL AND OWNERSHIP BETWEEN THE CLOUD SERVICE PROVIDER (CSP) AND THE USER

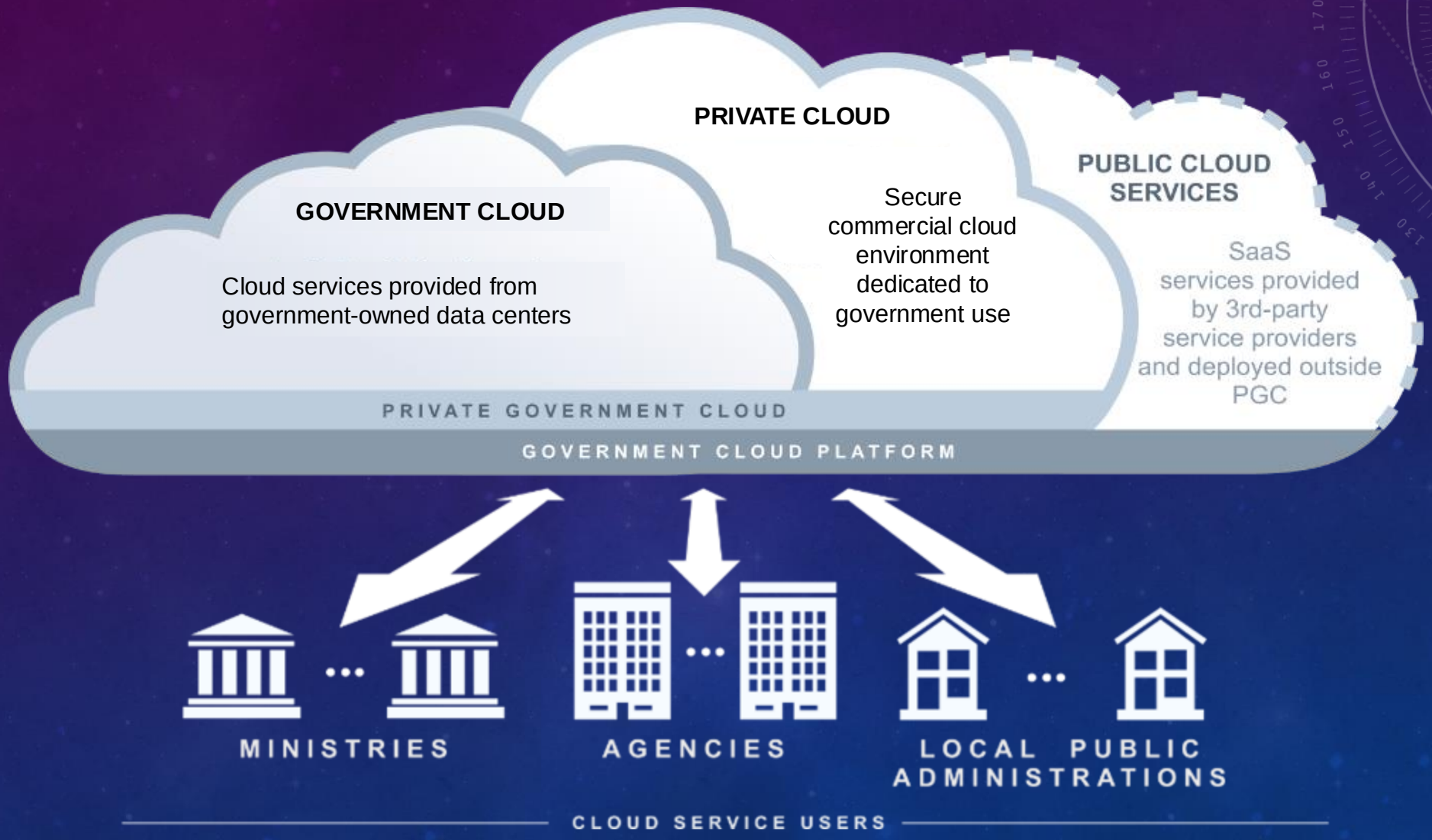
Overview of cloud deployment models

	Private Cloud	Community Cloud (Goverment-owned)	Public Cloud
Users	**Single organization** (ministry)	Used by **community of consumers** (e.g., government ministries)	**General public**
Operating model	**Owned & operated by the org. itself, 3rd party, or combination**	One or more organizations or third party	Owned and operated by a cloud provider
Location	**On or off** premises	**On or off** premises	**On** premises of cloud provider
Deployment Speed	**Longer timelines**, due to deployment & testing	**Faster timelines**, plug and play model	**Faster timelines**, plug and play model
Example	Private cloud **US Dept. Of Defense**	**KSA**'s National Information Center, **Singapore**'s Gov-Cloud	**KSA** allows commercial CSP to host government data

Hybrid Cloud - Combination of the three models above

Source: MCIT, Roland Berger

HYBRID CLOUD PARADIGM



A CLOUD FIRST POLICY IS A STRATEGIC APPROACH ADOPTED BY GOVERNMENTS WHERE PRIORITY IS GIVEN TO CLOUD COMPUTING SOLUTIONS OVER TRADITIONAL ON-PREMISES IT SYSTEMS

Introduction to Cloud first policy

Definition

Strategic approach adopted by organizations or governments where **priority is given to cloud computing solutions over traditional on-premises IT systems** when new projects or services are being planned and implemented

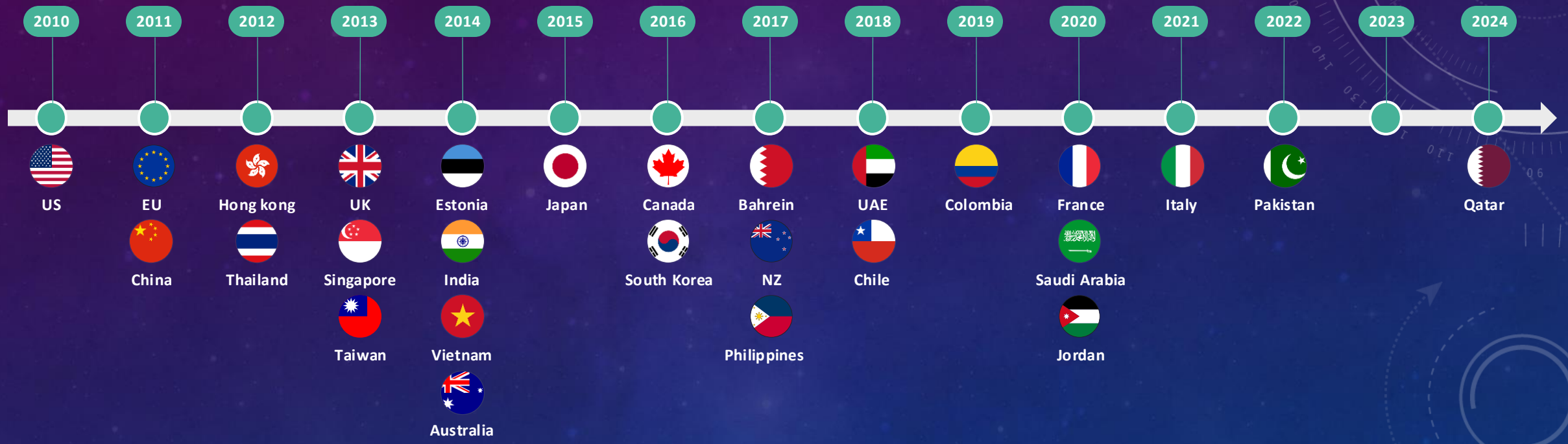
Cloud benefits for governments

- **Cost efficiency**
- **Scalability and Flexibility**
- **Innovation**
- **Enhanced Security and Compliance**
- **Improved accessibility**

Sources: Roland Berger

AN INCREASING NUMBER OF COUNTRIES HAVE IMPLEMENTED CLOUD FIRST POLICIES OVER THE PAST 15 YEARS

Overview of cloud first policies in the world



45+ countries have a cloud first policy in place

Sources: AWS, Roland Berger

WITH THE ADOPTION OF PUBLIC CLOUD, IT HAS BECOME COMMON FOR DATA TO BE STORED AND PROCESSED OUTSIDE OF A COUNTRY'S TERRITORY

Government data localization regulations

Countries enabling data to be stored and processed overseas

Strictly restricted → **Permissive depending on data classification**

- KSA
- Jordan
- UK
- NZ
- Qatar

Quotes from policies

"All data in both the Government Cloud and the Commercial Governmental Cloud should be **located geographically inside the borders of Saudi Arabia**"
- KSA Cloud fist policy

Data classified as ordinary or private **"can be inside or outside the Kingdom"**
- Cloud Policy

"Only store data classified as RESTRICTED or below in a public cloud service, **whether it's hosted onshore or offshore**"
- Government Cloud First Policy

"[...] it is **no longer necessary for data to be "on premise" or "locally"** [...] measures setting up an **elevated protection** [...] are **more efficient than localization requirements**"
- Cloud Policy Framework

"Enable teams to **use Cloud services provided overseas or globally**"
- Government Cloud First Policy

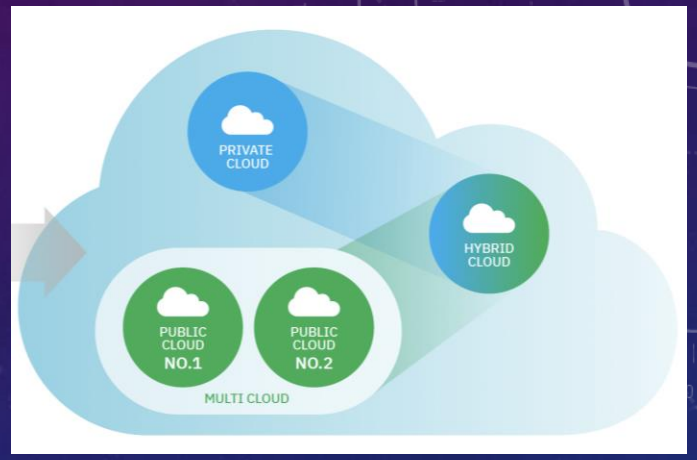
BENEFITS OF HYBRID CLOUD FOR THE PUBLIC SECTOR

Hybrid cloud offers multiple advantages over legacy systems and enables transformative applications:

Hosting silos

- ✓ **Compatible with data localization requirements**
- × **High cost**
- × **Poor physical security of data centers**
- × **Highly vulnerable to cyberattacks**
- × **Limited performance & ability to integrate cutting-edge solutions**
- × **Poor scalability and flexibility**
- × **Requires significant internal technical expertise**
- × **Difficult to be green or sustainable at such a small scale**

Hybrid cloud



- ✓ **Cost-efficient** (low cost option for less sensitive data)
- ✓ **Improved physical security**
- ✓ **Access to cutting-edge cybersecurity incident monitoring**
- ✓ **Improved resilience and availability**
- ✓ **Increased performance and access to cutting-edge solutions**
- ✓ **Highly flexible and scalable**
- ✓ **Reduced need for internal technical expertise**
- ✓ **More environmentally sustainable, using renewable energy**
- ✓ **Multi-provider solution: reduce risk of lock-in**
- ✓ **Data localization of sensitive data**
- × **Initial transition from hosting silos can be challenging**
- × **Procurement expertise needed to assure appropriate SLAs**

CLOUD POLICY: CLARIFY HOW GOVERNMENTS MOVE TOWARDS CLOUD

- **Cloud policies and guidelines** (Cloud First, Cloud Smart, Cloud Preferred, Guidelines on Use of Cloud…) guide institutions in migrating public systems to the cloud.
- Policy must take **a risk-based approach** balancing competing priorities (e.g. security, cost, availability).
- Some **variance in approach**: some countries strongly promote **public cloud by default** (e.g., UK) whereas others simply provide **guidelines** (e.g., Denmark).
- To succeed, cloud policies need to be accompanied by:
  - ✓ **Enabling regulations** (e.g., allowing public data to be hosted on cloud)
  - ✓ Facilitate **cloud procurement** (frameworks, marketplaces, standard contracts, SLAs, etc.)
  - ✓ **Systems readiness** (e.g. cloud-native architecture)
  - ✓ Necessary **digital skills**, including technical and procurement teams
  - ✓ **Enforcement mechanisms**

THE UK HAS IMPLEMENTED A GOVERNMENT CLOUD FIRST POLICY, INTRODUCING KEY PRINCIPLES THAT APPLY TO ALL PUBLIC BODIES WHEN PROCURING NEW OR EXISTING SERVICES

UK Government Cloud First policy

Date: 2013

Scope: approach mandatory for **central government** entities & strongly **recommended to wider public sector**

Objective: Balance between delivering technology quickly, cost and resource required, and reducing risk

Default to Public Cloud, through a UK government purchasing framework

If private cloud or colocation required, use Crown Hosting (Joint Venture between UK government and ARK Data Centers)

Enable teams to use cloud services provided by European Economic Area countries

Services not servers: default for using higher-level cloud services, not colocation

Sources: Roland Berger

THE GOVERNMENT CLOUD FIRST POLICY RECOMMENDS TO DEFAULT TO THE PUBLIC CLOUD AS MUCH AS POSSIBLE BECAUSE OF ITS ELASTICITY, SECURITY, AND FLEXIBLE PRICING MODEL

UK Government Cloud First policy – Fundamental principles

"Default to public cloud" principles

- Organizations default to Public Cloud first
- Community, hybrid or private models accepted (SECRET or TOP SECRET)
- Organizations not in Public Cloud should evidence the value for money

Rationale for prioritizing public cloud

- **Elasticity and resilience:** public cloud helps scale more efficiently
- **Best of breed security:** public cloud services have a $1 billion+ budgets per year to mitigate many common risks
- **Pay-as-you-go pricing:** cloud services are usually billed based on consumption, down to a very low level of granularity

Sources: Roland Berger

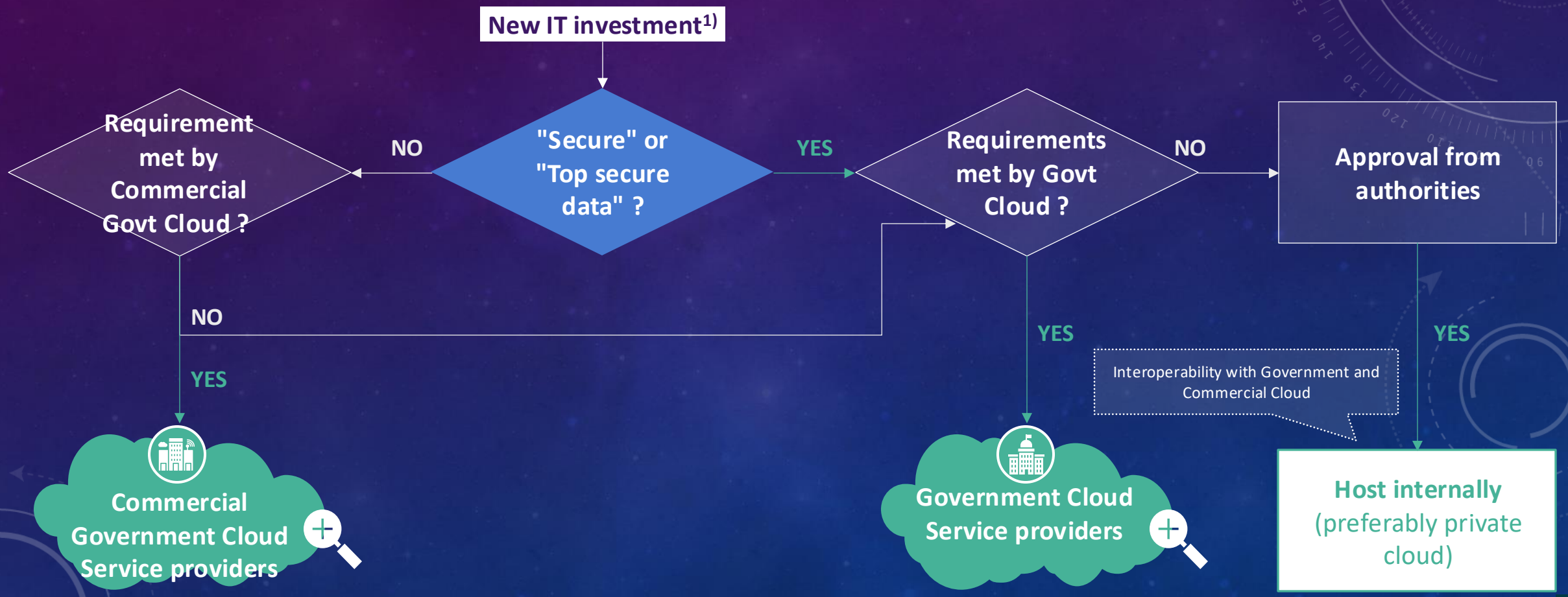
SINGAPORE COMMERCIAL CLOUD FIRST POLICY: 70% OF GOVERNMENT SYSTEMS IN PUBLIC CLOUD

- ✓ Context: Needed to **scale** gov't digital transformation while promoting local cloud **market development**.
- ✓ Singapore launched its Commercial Cloud First Policy in 2018, with the goal of **migrating 70% of government systems to commercial public cloud** by 2023.
- ✓ Rationale: achieve **cost savings** (reported 50%) and **operational efficiencies** while ensuring **cybersecurity** and **data protection**
- ✓ Hybrid solution: **interoperability with G-cloud** for data classified as unsuitable for public cloud
- ✓ G-cloud implemented in **partnership with private** providers

Singapore Government Tech Stack

KSA HAS INTRODUCED A CLOUD-FIRST POLICY FOR ALL GOVERNMENT ENTITIES, EXCEPT THOSE RESPONSIBLE FOR NATIONAL SECURITY, PRIORITIZING THE USE OF CLOUD SOLUTIONS

KSA's cloud first policy



1) procurement of new hardware and software, renewal of hardware and renewal of present software licenses

Sources: Ministry of Communications and Information Technology Roland Berger

KSA JUSTIFIES ITS EMPHASIS ON CLOUD COMPUTING BASED ON EFFICIENCY, AGILITY, RELIABILITY, SECURITY, AND CAPACITY FOR INNOVATION

Cloud computing benefits according to KSA Cloud First Policy

Dimension	Rationale
Efficiency	•Increased utilization of assets optimizing the current state and reducing the need for future capacity expansions, •Translates into cost effectiveness (~30% savings in total cost of ownership)
Agility & reliability	•Possibility for users to scale up and scale down depending on demand •Improve overall time to market with a “plug and play” approach
Security	•Cloud services typically offer a high level of cybersecurity difficult to attain by government entities, with best-in-class protocols applied
Innovation	•Enabler to transform the way government entities deploy services (e.g., taxi or food order companies)

Sources: Ministry of Communications and Information Technology Roland Berger

KSA HAS ESTABLISHED TWO PRIMARY CATEGORIES FOR CLOUD PROVIDERS BASED ON CYBERSECURITY STANDARDS, ALLOWING THEM TO HOST VARYING LEVELS OF SENSITIVE GOVERNMENT DATA

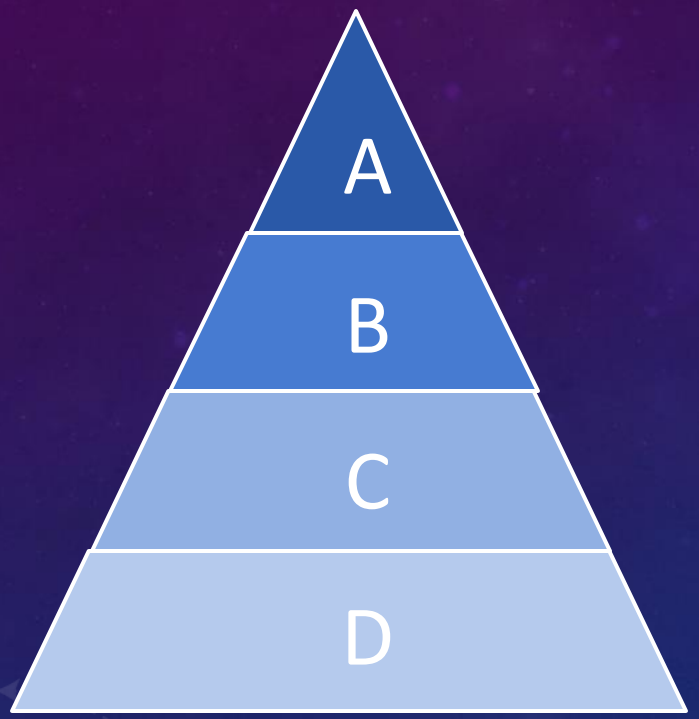
	Government Cloud Service provider	Commercial Governmental Cloud Service provider
Definition	a) Government-owned community cloud (NIC) or b) Any commercial cloud provider meeting NCA's cybersecurity requirements (for all 4 levels of data classification)	• Any commercial cloud provider meeting the NCA's cybersecurity requirements to host: – Only Open and Restricted data classifications – Only Open data classifications
List of service providers	stc, SITE, موبايلي mobily, زين zain, edaratgroup, DETASAD, GO Telecom, DEEM, سلام salam, virtual vision, Safe Decision, zaintech, Tamkeen Technologies, SAP, NOURNET, HUAWEI CLOUD, Google Cloud, Alibaba Cloud, ORACLE	Class (B): BIOS Business Integrated Operating Systems Branch فرع بيزينس انتجريتد اوبيريتنج سيستمز Class (A): Naseej نسيج, صحارى نت Sahara Net, wafai cloud, kalaam, Skyband, TOPNET, iNet

All data in both the Government Cloud and the Commercial Governmental Cloud should be located geographically inside the borders of Saudi Arabia.

Sources: Ministry of Communications and Information Technology, Communication, Space & Technology Commission, Roland Berger

JORDAN AUTHORIZES DATA CLASSIFIED AS ORDINARY OR PRIVATE TO BE PRESERVED AND PROCESSED OUTSIDE ITS TERRITORY BY PRIVATE OPERATORS

Overview of Jordan Cloud policy – Data localization

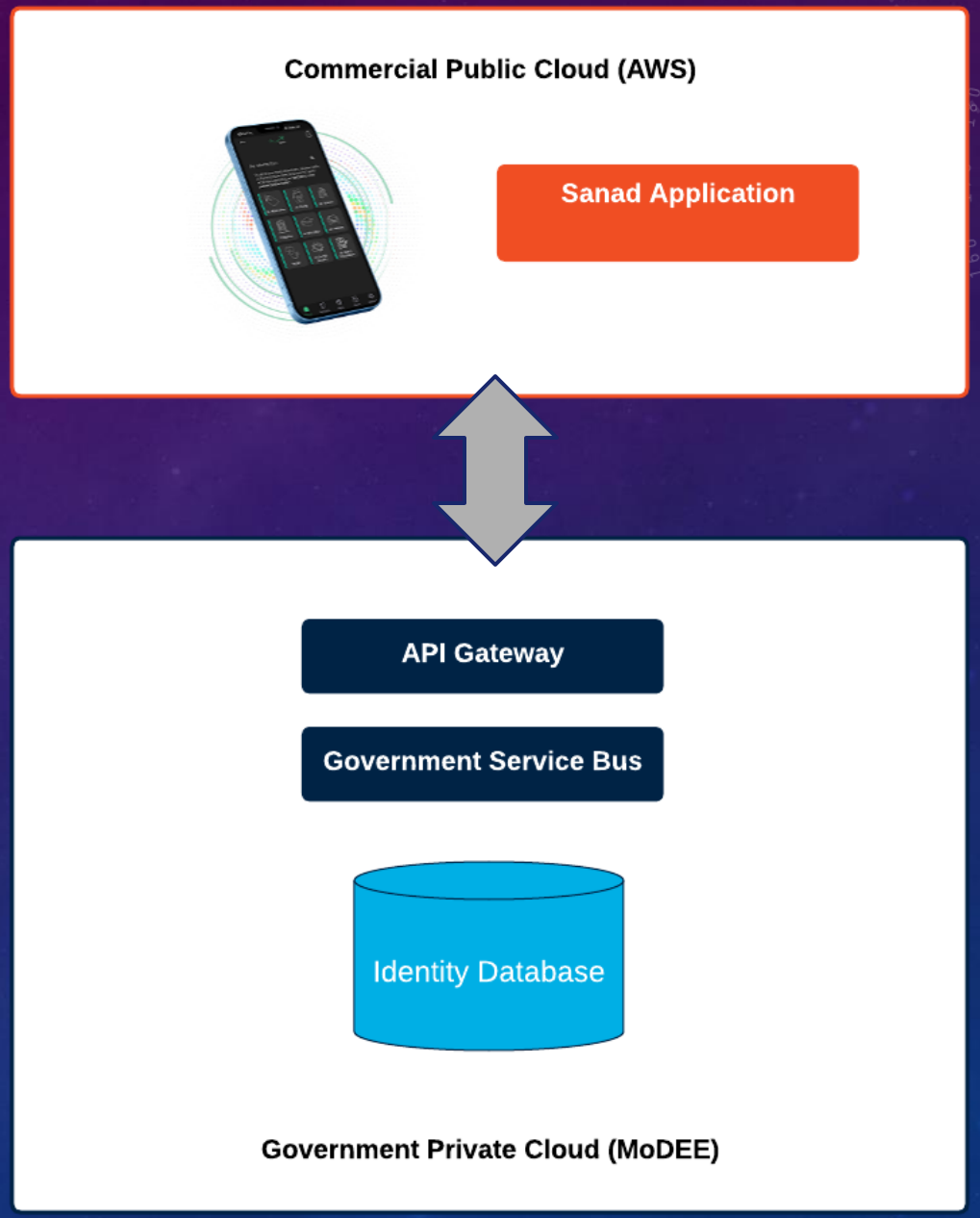


Classification level	Authorized place of preservation & processing	Authorized data center types
Secret	Limited **within the Kingdom**	**Government** data centers
Sensitive	Limited **within the Kingdom**	**Government and private** data centers
Private	**Inside or outside** the Kingdom	**Government and private** data centers
Ordinary	**Inside or outside** the Kingdom	**Government and private** data centers

Only countries with compliant privacy and personal data protection legislation can host Jordan government data

Sources: Roland Berger

JORDAN SANAD APPLICATION CLOUD ARCHITECTURE



ADEQUACY

Means of enabling cross-border data flows to a set of trusted countries

Unilateral sovereign decision: Just up to who you trust!

European Union

GDPR adequacy of 15 jurisdictions incl:

- Argentina
- Japan
- South Korea
- New Zealand
- Switzerland
- United Kingdom
- Uruguay

Formal rigorous procedure

Philippines

- Trusted Singapore due to extradition agreement
- Enabled use of AWS (Singapore region) for national ID system (application layer)

DISASTER RECOVERY SITES ARE FACILITIES DESIGNED TO REPLICATE & RESTORE THE OPERATIONS OF A PRIMARY DC IN THE EVENT OF A DISASTER – GEOGRAPHICAL DISPERSION IS KEY

Definition

- Secondary facility to **replicate and restore the operations** in the event of a **disaster**
- With redundant systems, backup power supplies, and other critical infrastructure to **ensure that data & applications remain accessible and operational during unforeseen disruptions**

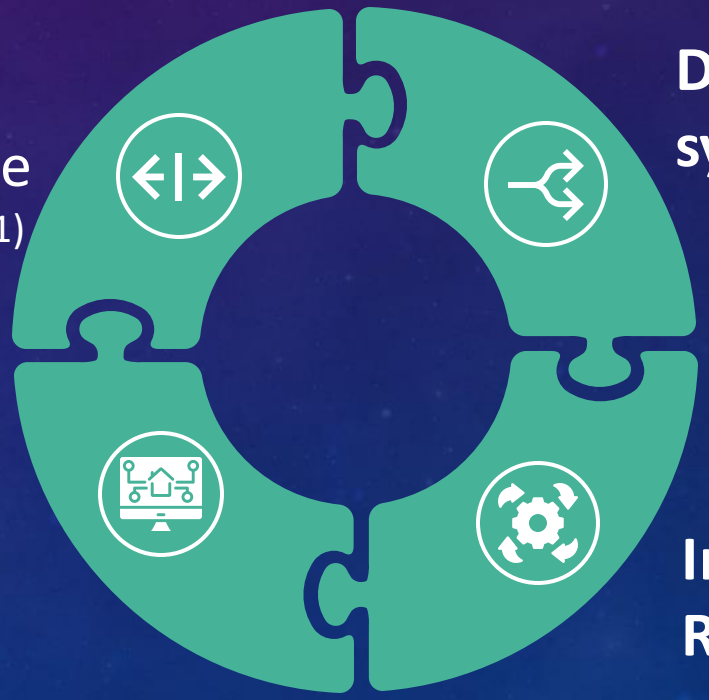
Disaster recovery for a Data Center key features

Geographical Dispersion
Generally, a distance of at least ~160 km[1)]

Data synchronization

Testing and maintenance

Infrastructure Readiness



1) Common industry guideline - U.S. federal regulators have even recommended distances of up to 320 km to ensure resilience in the event of a disaster (Enterprise Systems) for financial services

Sources: Roland Berger

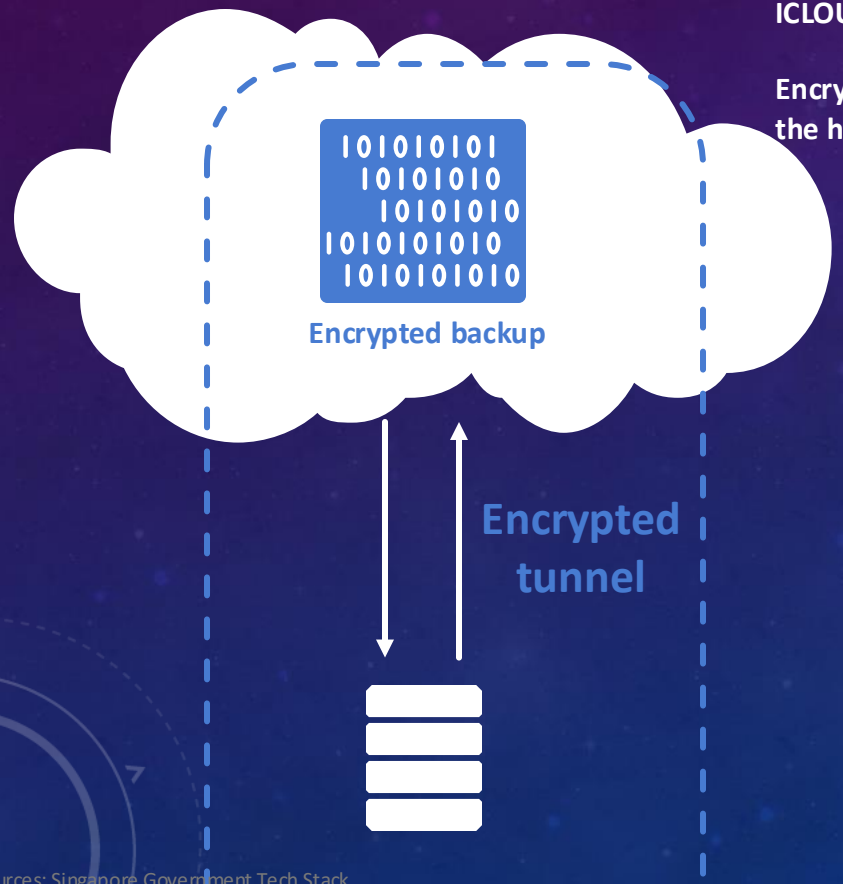
CROSS-BORDER FLOWS AS AN INGREDIENT OF NATIONAL DISASTER RECOVERY STRATEGY

Focus on cross-border flows

Minimal risk: encrypted data at both ends

ICLOUD MECHANISMS

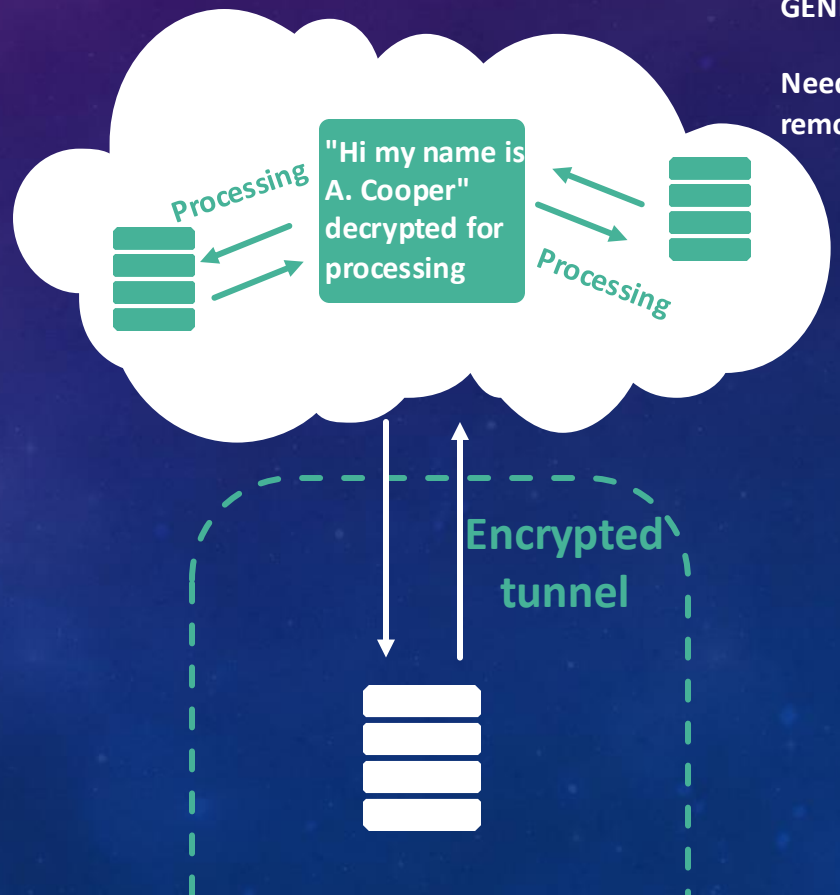
Encryption is never on the host server



Some risk: data stored unencrypted

GENERAL MODEL

Needed is processed by remote servers



Sources: Singapore Government Tech Stack

UKRAINE'S RAPID ADAPTATION DURING THE RUSSIAN INVASION PROOVED LEVERAGING CLOUD SOLUTIONS FOR DATA REDUNDANCY CAN PROVE CRITICAL TO MAINTAIN RESILIENCE

Ukrainian case

Centralized data storage can be a vulnerability

Ukraine initially enacted a law requiring all e-government data to be hosted within the country, aiming to secure sensitive information within national borders.

Flexibility and adaptability are key

With the onset of the Russian invasion in early 2022, Ukraine quickly changed its law to allow data hosting on international cloud services like AWS. This enabled the duplication of critical data outside the conflict zone.

Implementing redundancy through cloud

The primary data center in Ukraine was damaged due to the war, but the data remained secure and accessible because it had been duplicated to cloud services.

Sources: Roland Berger

B. DATA CENTERS

THE QUALITY OF A DATA CENTER DEPENDS ON ENERGY SUPPLY, CONNECTIVITY, LOCATION, PHYSICAL SECURITY, CYBERSECURITY, AND STAFFING

Components of a data center

Real estate

- Dedicated facility
- Located outside risk areas
- State-of-the-art physical security

Staff

- Highly skilled personnel
- 24/7 rotation

Energy and connectivity

- Dual electric grid supplies
- Battery and generator backups
- Multiple fiber connections

Information Security

- Sophisticated cybersecurity solutions

Source: Roland Berger

DATA CENTERS ARE CLASSIFIED FROM TIER I TO IV BY AN INDEPENDENT BODY BASED ON UPTIME GUARANTEES, FAULT TOLERANCE, AND SERVICE COSTS

Data center tier ranking: overview and comparison

Tier ranking overview

Accreditation body: Uptime Institute

Classification methodology kept confidential, but key metrics include:

- Uptime guarantees
- Fault tolerance
- Service cost

	I	II	III	IV
Uptime guarantee	−			+
Component redundancy	✗	✓	✓	✓
Price	−			+
Staffing	✗	1 shift	1+ shift	24/7/365

Source: phoenixNAP, Roland Berger

STRINGENT STANDARDS DEFINE A TIER IV DATA CENTER, ENSURING MAXIMUM SECURITY, RELIABILITY, AND PERFORMANCE

Key success factors of data centers

Physical - dedicated facility, ideally located, with high security standards

- Purpose-built, dedicated facility in an owned building
- 60MW facility, expandable to 120MW+
- Located within an Availability Zone for 99.999% uptime to users

Fit out - Fault tolerant -- high-quality energy supply and connectivity

- Two physically diverse electrical power supplies, backed by PPAs
- Carrier neutral with 20+ independent fiber providers
- Cold aisle containment and Dual Power Distribution Unit (PDU)
- Cloud on-ramps

Information Security - with high quality standards

- $1 billion per year cyber budget
- HIPAA, ISO, and SSAE certifications
- Firewalls, intrusion detection and prevention systems, and VPNs

Illustration

Sources: Roland Berger

ENERGY ACCOUNTS FOR MOST OF THE COST INVOLVED IN RUNNING A LARGE DATA CENTER

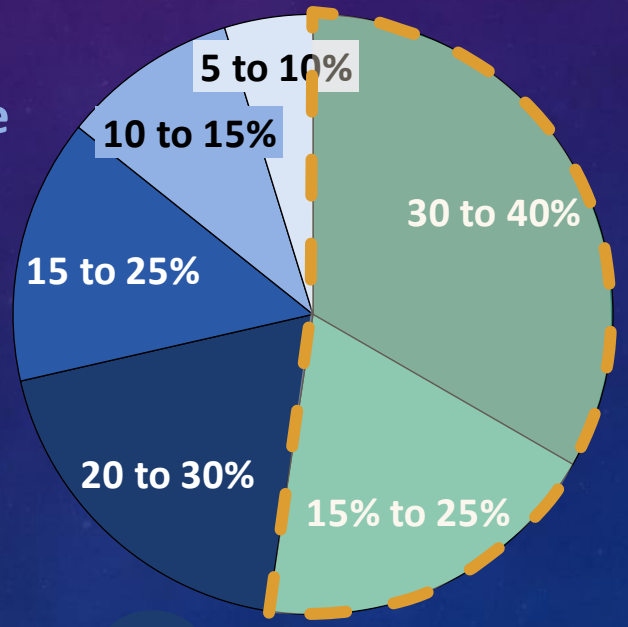
Breakdown of annual data center costs

Lease or depreciation of infrastructure

Equipment maintenance and security

Licenses, connectivity and security

Personnel



Energy = 45 to 65%

Energy to power servers

Energy consumed by cooling network

Source: Roland Berger

DIESEL COSTS DRIVE UP ENERGY PRICES FOR LEBANESE DATA CENTERS COMPARED WITH OTHER MENA COUNTRIES

Analysis of electricity costs for a data center in Lebanon and selected countries [Sept-2023; USD/MWh_e]

Electricity issues in Lebanon

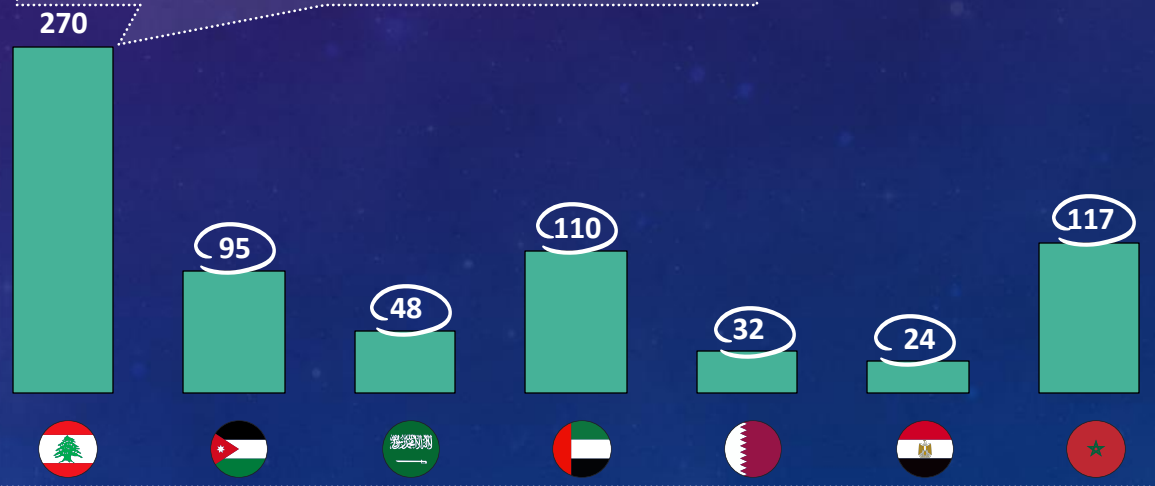
Intermittency and instability of electricity network (avg 3 hours/day) leads to significant supply fluctuations and interruption

Supply instability necessitates use of diesel generators, creating dependency on diesel fuel supplies

Supply instability results in high cost of electricity, higher than in other countries in the region

Cost of electricity for a data center in a selection of countries[1)]

Weighted average based on the proportion of each power source in the Lebanese electricity mix



Energy prices are subject to **significant variations from one period to the next** and can vary depending on the **point of measurement** (e.g., residential vs. industrial)

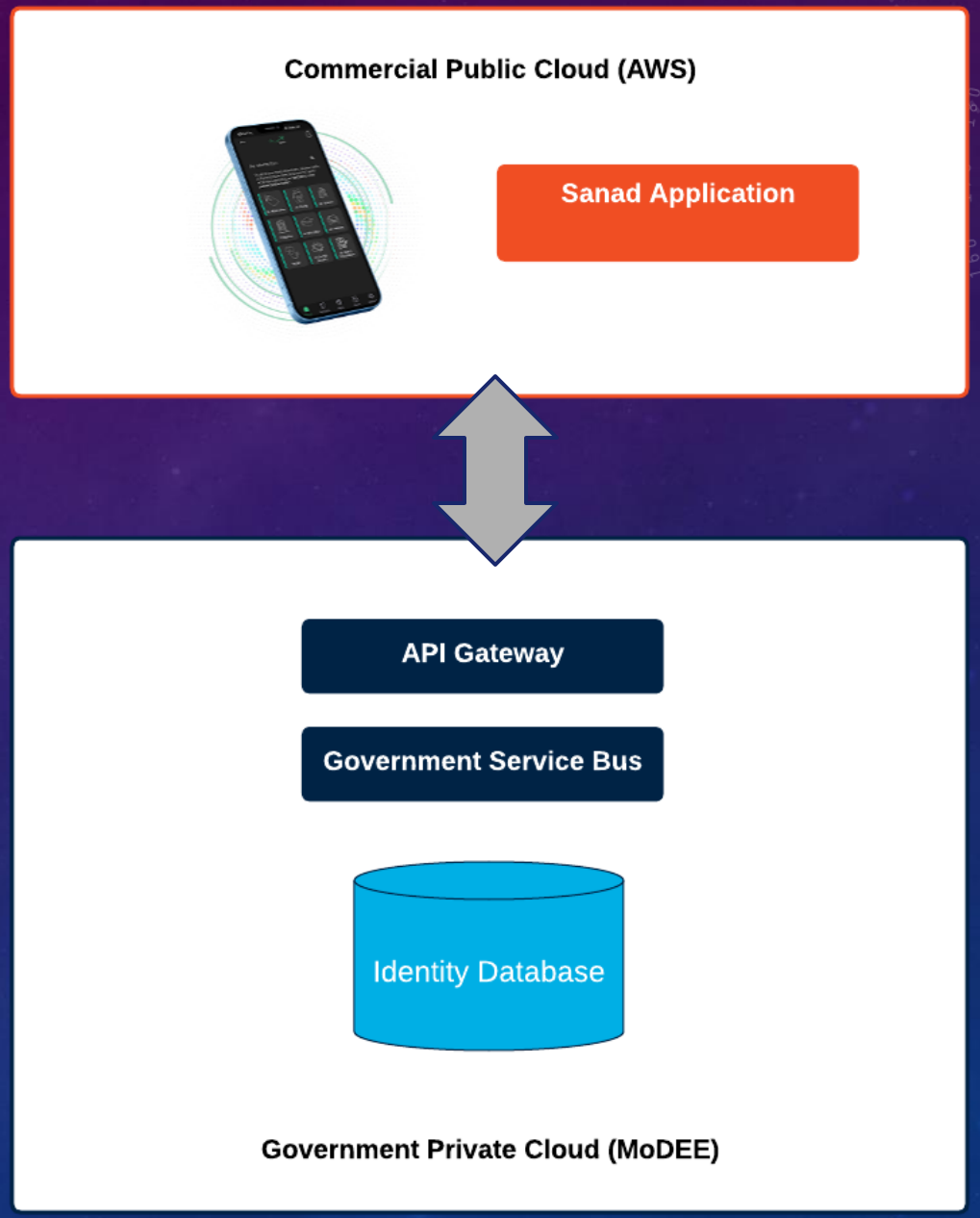
Source: IPT, GlobalPetrolPrices.com, Roland Berger

C. OVERVIEW OF DATA HOSTING IN LEBANON

PANEL WITH USERS OF CLOUD SERVICES

PANEL WITH DATA CENTER OPERATORS

JORDAN SANAD APPLICATION CLOUD ARCHITECTURE



D. THE WAY FORWARD FOR LEBANON

THE WAY FORWARD FOR LEBANON

KEY COMPONENTS OF DATA HOSTING MODEL

Breakout session objectives and agenda

Objective: discuss and define the way forward for data hosting in Lebanon

20 minutes

Step 1: Round table discussions

Discuss the key components of an ideal data hosting model for Lebanon.

Input a **summary of the table's** discussions and key findings using Mentimeter

10 minute for question 1

5 minutes each for questions 2 & 3

20 minutes

Step 2: Group reporting

One person from each table recaps the discussion in **2 minutes**

10 minutes

Step 3: Comments and Q&A

Elaborate and seek clarifications

Q&A

INTERACTIVE SESSION: OPINIONS ON COST DRIVERS AND SOLUTIONS

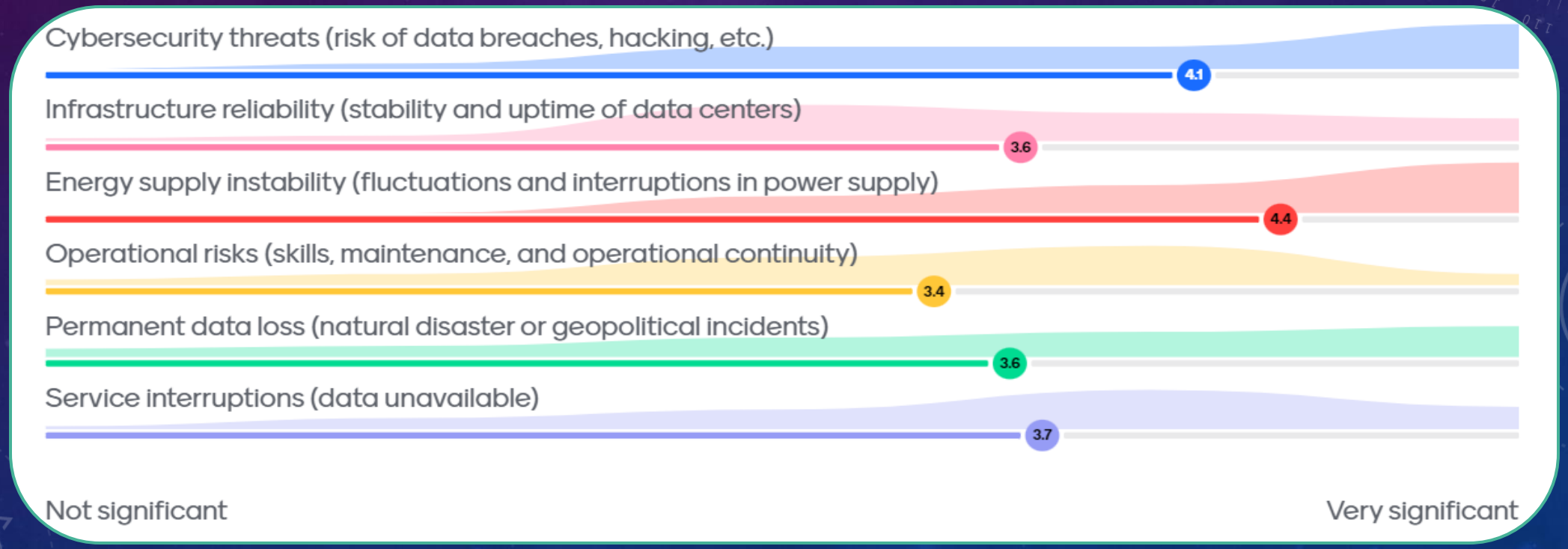
30 responses

On a scale of 1 to 5, how significant do you consider each of the following cost drivers for data centers in Lebanon?

INTERACTIVE SESSION: OPINIONS ON COST DRIVERS AND SOLUTIONS

30 responses

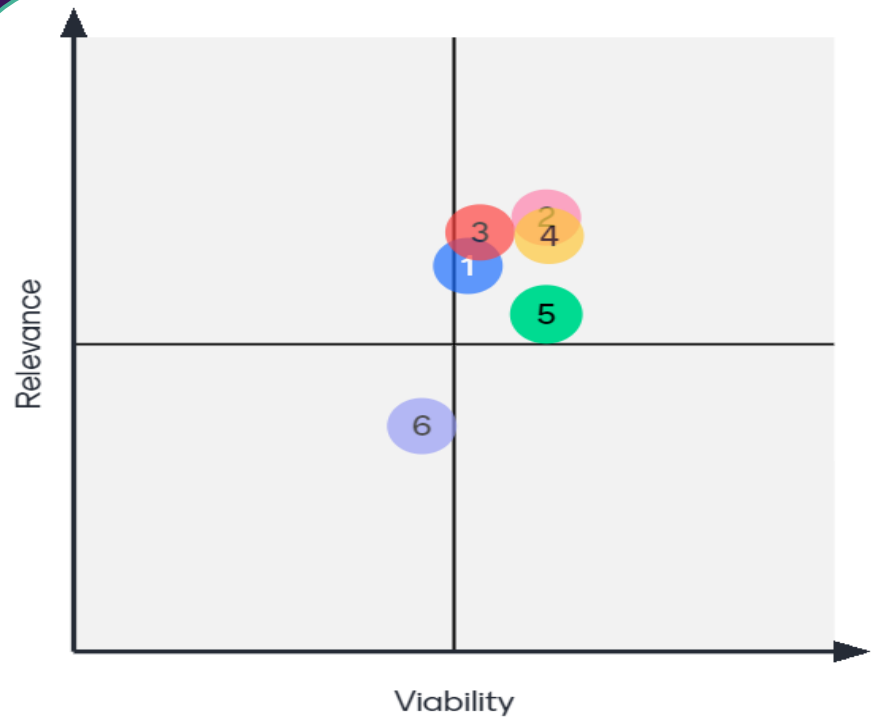
On a scale of 1 to 5, how significant do you consider each of the following risk factors for data centers in Lebanon?



INTERACTIVE SESSION: OPINIONS ON COST DRIVERS AND SOLUTIONS

30 responses

For each solution, rate viability and relevance for Lebanese e-government?



1 Cloud first policy

2 Hybrid cloud approach

3 Private cloud for government

4 Public-private partnerships for data center operations

5 Local commercial cloud providers

6 International commercial cloud providers

CONCLUSION & NEXT STEPS

WORKSHOP FEEDBACK

Scan the QR code and participate

https://ntgt.de/a/s.aspx?s=499777X109320729X91282

CLOSING REMARKS

Thank you

Lebanon Digital Transformation Strategy

2020 - 2030