IAPP UK Intensive 2026

Privacy | AI governance | Cybersecurity law

Training 23-24 February

Workshops 24 February

Conference 25-26 February

LONDON

#IAPPIntensive26

Digital Trust in Action: UK–Asia Synergies for a Resilient Future

WELCOME AND INTRODUCTIONS

Joe Jones

Director of Research & Insights,

IAPP

Abhishek Tiwari

FIP, CIPP/A, CIPP/E, CIPM, AIGP

Associate Director,
PWC India

Charmian Aw,

FIP, CIPP/A, CIPP/E, CIPP/US, CIPM, AIGP

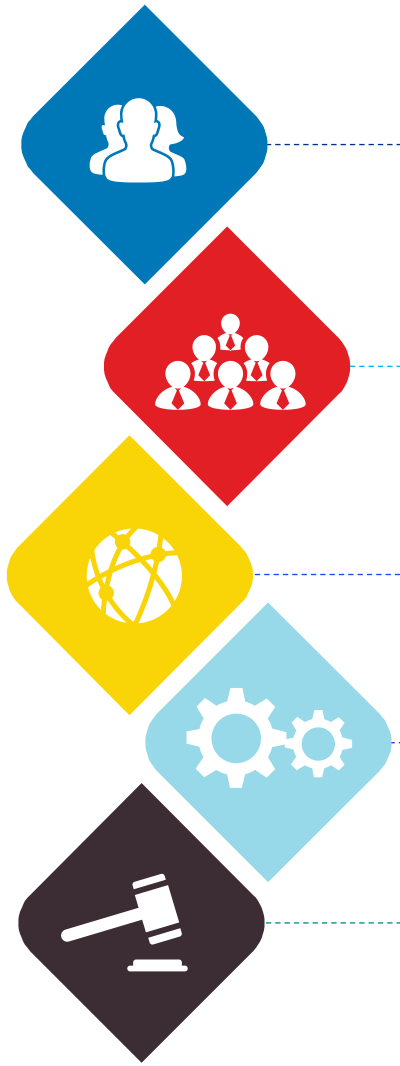
Partner,
Hogan Lovells

Christopher Chew,

FIP, AIGP, CIPP/A, CIPM,

Technical Leader, Security & Digital Trust - Office of the CTO, Cisco Singapore

Key Learnings from the session



- Understanding Digital Trust and Its Global Importance
- Comparative Frameworks and Lessons Learned
- India: Modernizing Data Protection with the DPDPA
- Singapore: A Mature, Innovation-Forward Framework
- Cross-Jurisdictional Implications

Understanding Digital Trust and Its Global Importance

Definition & Importance

Digital trust is the confidence in security, privacy, and reliability of digital systems, vital for innovation and trade

Challenges in Digital Trust

Cyberattacks, misinformation, and fragmented regulations threaten digital trust, requiring resilience and collaboration

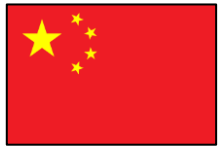
UK and Asia Collaboration

UK and Asia align pro-innovation regulation and digital transformation to overcome challenges and foster growth

Frameworks for Trust

Initiatives like OECD guidelines and CBPR Forum promote international standards and interoperability for digital trust

Comparative Frameworks and Lessons Learned

	Key Regulations	Focus Area
	Digital Operational Resilience Act (DORA) General Data Protection Regulation (GDPR)	Operational resilience, cybersecurity
	Digital Personal Data Protection Act (DPDPA)	Consent-based data processing, cross-border transfers
	Personal Data Protection Act (PDPA)	Data protection, compliance
	Personal Information Protection Law (PIPL)	Personal information security

India: Modernizing Data Protection with the DPDPA

India's Digital Personal Data Protection Act (DPDPA) marks a **major shift in its privacy landscape**. It introduces

01 **Consent-based processing**

02 **Cross-border transfer rules**

03 **Obligations for Data Fiduciaries**

Relevance for UK–Asia Digital Trust

India can draw from **UK GDPR's risk-based approach** and **EU/UK accountability frameworks** to strengthen enforcement

India's model still balances **national security + digital economy growth**, which differs from the EU's more rights-centric stance

These measures align India more closely with global frameworks, though the regulatory ecosystem remains fragmented across sectors

Singapore: A Mature, Innovation-Forward Framework

Singapore is recognized for its **progressive, business-friendly data governance model** under the Personal Data Protection Act (PDPA)

01 A strong emphasis on **accountability, Breach Notification, Data Portability**, and **AI governance guidance**

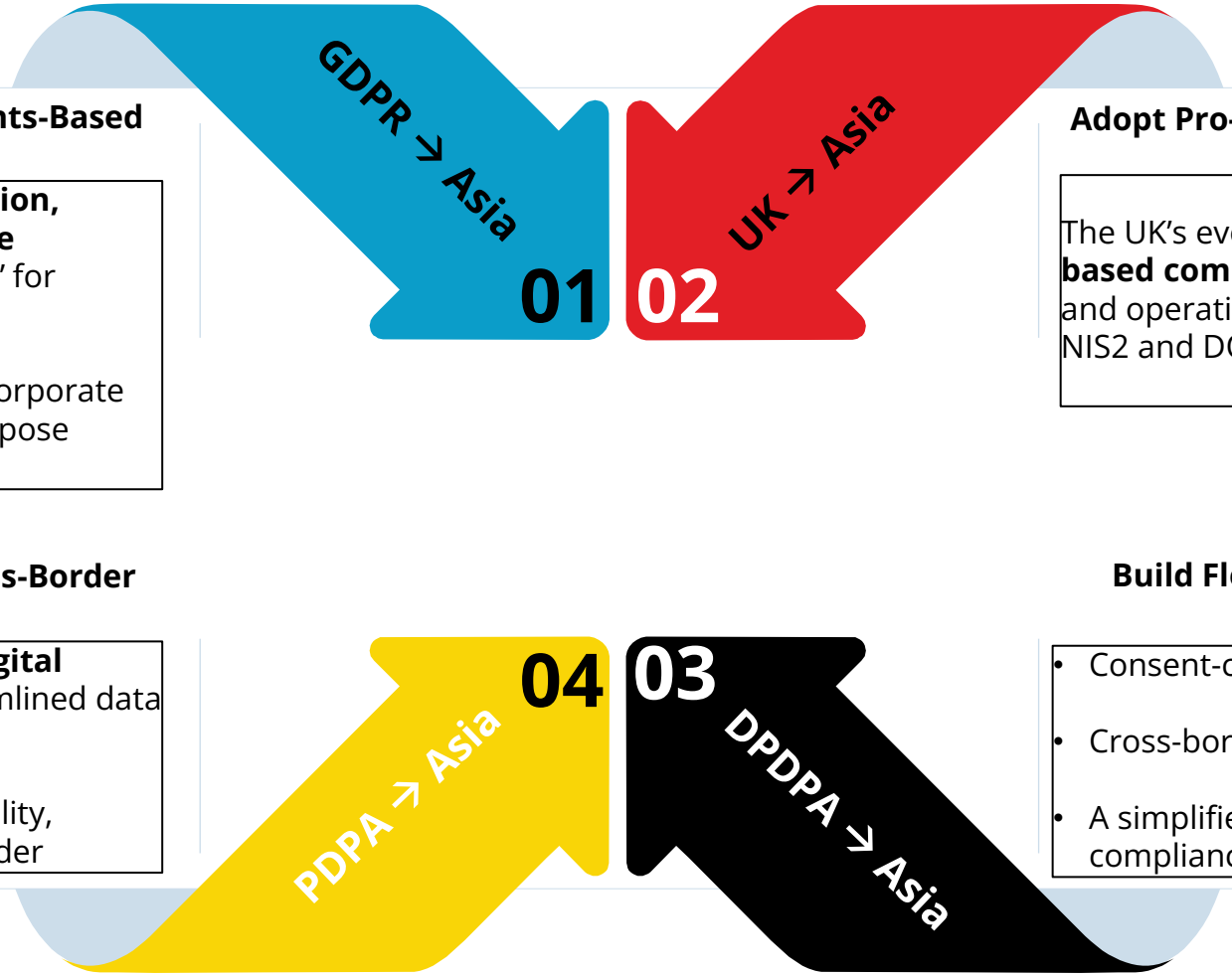
02 The UK–Singapore **Digital Economy Agreement (UKSDEA)** sets **best-in-class standards** for digital trade, interoperability, and cybersecurity cooperation

Relevance for UK–Asia Digital Trust

Singapore's frameworks emphasize **regulatory coherence**, a major challenge across Asia

Its "**trusted data flows**" model aligns strongly with UK aspirations for safe, innovation-friendly data mobility

Lessons from GDPR, UK Frameworks, Singapore PDPA & India DPDPA for Asia



Strengthen Accountability & Rights-Based Governance

- GDPR's emphasis on **documentation, transparency, and demonstrable compliance** sets a "gold standard" for governance
- Asian frameworks increasingly incorporate GDPR-like obligations, such as purpose limitation and breach notification

Adopt Pro-Innovation, Risk-Based Regulation

The UK's evolving frameworks emphasize **risk-based compliance**, pragmatic AI governance, and operational resilience (inspired partly by EU NIS2 and DORA)

Prioritize Interoperability & Cross-Border Trust

- Singapore's approach supports **digital economy agreements** and streamlined data mobility.
- It promotes clarity on data portability, breach notification, and cross-border transfer rules

Build Flexible, Sector-Friendly Privacy Frameworks

- Consent-centric processing
- Cross-border transfer mechanisms
- A simplified, business-friendly digital compliance philosophy

Cross-Jurisdictional Implications

1 Fragmentation remains a major barrier

Different regulatory philosophies across Asia (e.g., India vs. Singapore vs. China) create complexity for multinational operations

Companies must maintain multi-framework compliance across privacy, cybersecurity, and AI governance

2 Need for integrated cyber + data protection strategies

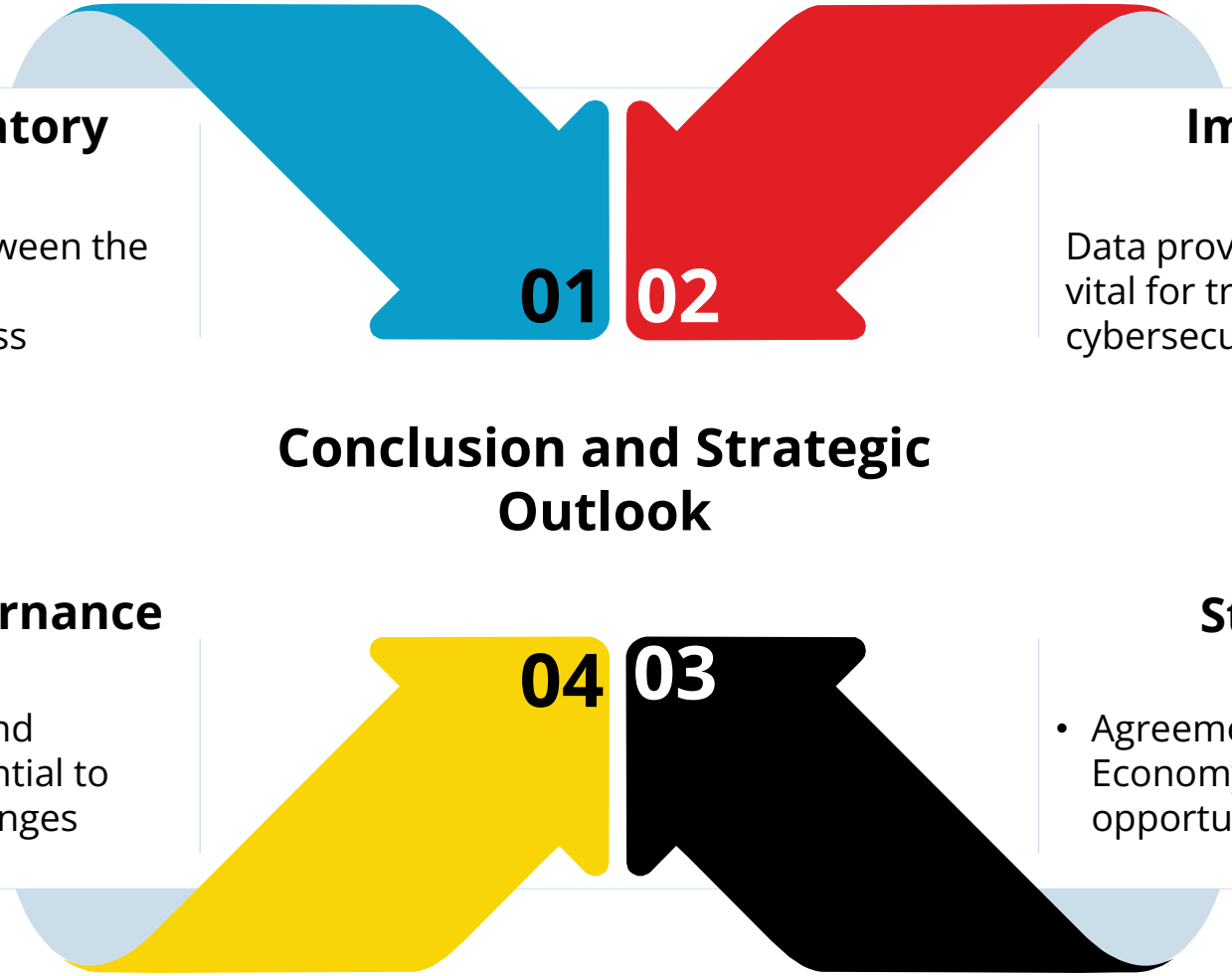
For UK–Asia collaboration, this means:

- Harmonizing resilience standards
- Joint AI safety protocols
- Cloud & operational
- Resilience alignment

3 Interoperability is the new competitive advantage

Companies increasingly realize that compliance cannot be isolated → **integrated governance across data privacy, cybersecurity, and AI** is essential

Building a Resilient Future Through Collaboration



Collaborative Regulatory Frameworks

- Harmonizing regulations between the UK and Asia fosters trust and streamlines compliance across borders

Importance of Data Transparency

Data provenance and transparency are vital for trust in AI-driven decisions and cybersecurity resilience

Conclusion and Strategic Outlook

Cross-Disciplinary Governance Models

- Integrating legal, technical, and operational expertise is essential to tackle emerging digital challenges effectively

Strategic Bilateral Partnerships

- Agreements like the UK-Singapore Digital Economy Agreement unlock economic opportunities and protect digital integrity

The Way Forward

EU Digital Laws

Across the EU's digital rulebook, figuring out who the rules apply to and what they mean for organizations is no small feat. Providing a high-level overview of the EU Digital Laws Report, this infographic summarizes key details around the Data Governance Act, Data Act, Digital Markets Act, Digital Services Act, Artificial Intelligence Act and NIS2 Directive.

	Data Governance Act	Data Act	Digital Markets Act	Digital Services Act	Artificial Intelligence Act	NIS2 Directive
Scope	Data intermediation services providers, data altruism organizations and public sector-bodies	Holders of connected device data, providers of data processing services and device users	Designated gatekeepers and core platform services	Online platforms and designated very large online platforms, online search engines and designated very large online search engines, online marketplaces, hosting services, caching services and mere conduits	Operators, e.g., providers, deployers of high-risk AI systems, AI systems and general-purpose AI models	Essential or important entities, e.g., those in energy, banking, health care, digital infrastructure, etc.
Purpose	To facilitate trustworthy mechanisms for data sharing across sectors and member states	To encourage fair access to and use of data across the internal market with a focus on enabling access to data generated by connected devices and related services	To ensure fair competition and contestability in the digital goods and services sector	To ensure a safe, transparent online environment and prevent illegal and harmful online activities and the spread of disinformation	To manage risks around the use of artificial intelligence	To further improve the resilience of public and private entities against cybersecurity threats and disruptions of IT systems and networks

**IAPP EU Digital Laws Report*

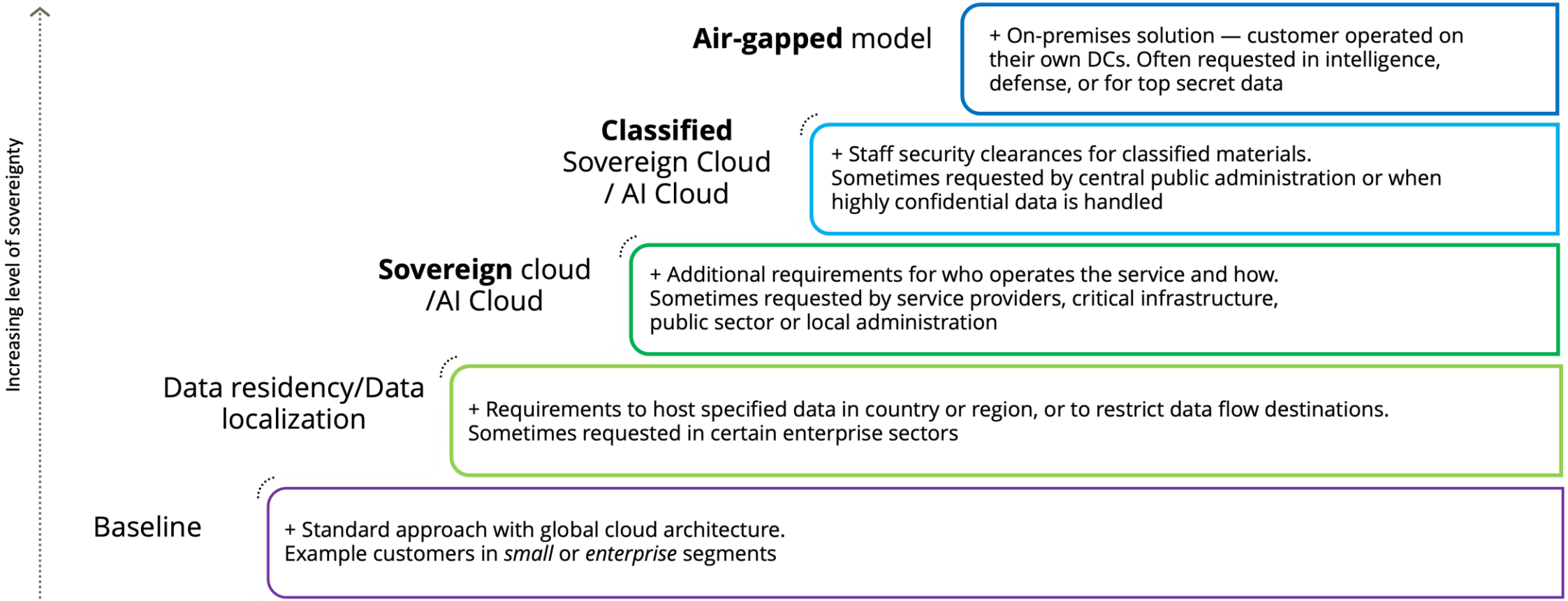
	Data Governance Act	Data Act	Digital Markets Act	Digital Services Act	Artificial Intelligence Act	NIS2 Directive
Key requirements	Fiduciary-like responsibilities, public registration, data sharing, information provision and security measures	Data accessibility, data portability, confidentiality, transparency, fair data use and security	Interoperability, data access, data use and prohibitions on anticompetitive practices	Tiered requirements including transparency, content moderation, notice and takedown procedures, redress mechanisms, provisions of non-deceitful online interfaces, security, safety and privacy for minors and risk assessments	Establishment of risk management systems, data governance, technical documentation, record keeping, transparency, human oversight, accuracy, robustness and cybersecurity and AI literacy registration	Strengthens established and introduces new requirements for cybersecurity risk management and incident reporting
Date of applicability	September 2023	September 2025	May 2023	February 2024	Some provisions are applicable as of February 2025, while others will be applicable as of August 2026 and August 2027.	The deadline for member states to transpose the NIS2 Directive into their national law was October 2024.
Penalties	Member states are to set penalties that are "effective, proportionate and dissuasive."	Supervisory authorities under the EU General Data Protection Regulation may impose fines of up to 20,000,000 euros (USD22,985,800) or 4% of global annual revenue, whichever is higher. The European Data Protection Supervisor may impose fines of up to 50,000 euros (USD57,468) per infringement to a maximum of 500,000 euros (USD574,677) per year.	Gatekeepers can be fined up to 10% of global annual revenue or up to 20% for repeated infringements.	VLOPs/VLOSEs can be fined up to 6% of global annual revenue.	Prohibited AI practices (Article 5) can garner fines of up to 35,000,000 euros (USD40,227,425) or 7% of global annual revenue, whichever is higher. Other violations can garner fines of up to 15,000,000 euros (USD17,240,700) or 3% of global annual revenue, whichever is higher.	An essential entity can garner fines of up to 10,000,000 euros (USD11,493,800) or 2% of global annual revenue, whichever is higher; an important entity can garner 7,000,000 euros (USD8,045,660) or 1.4%, whichever is higher.

**IAPP EU Digital Laws Report*

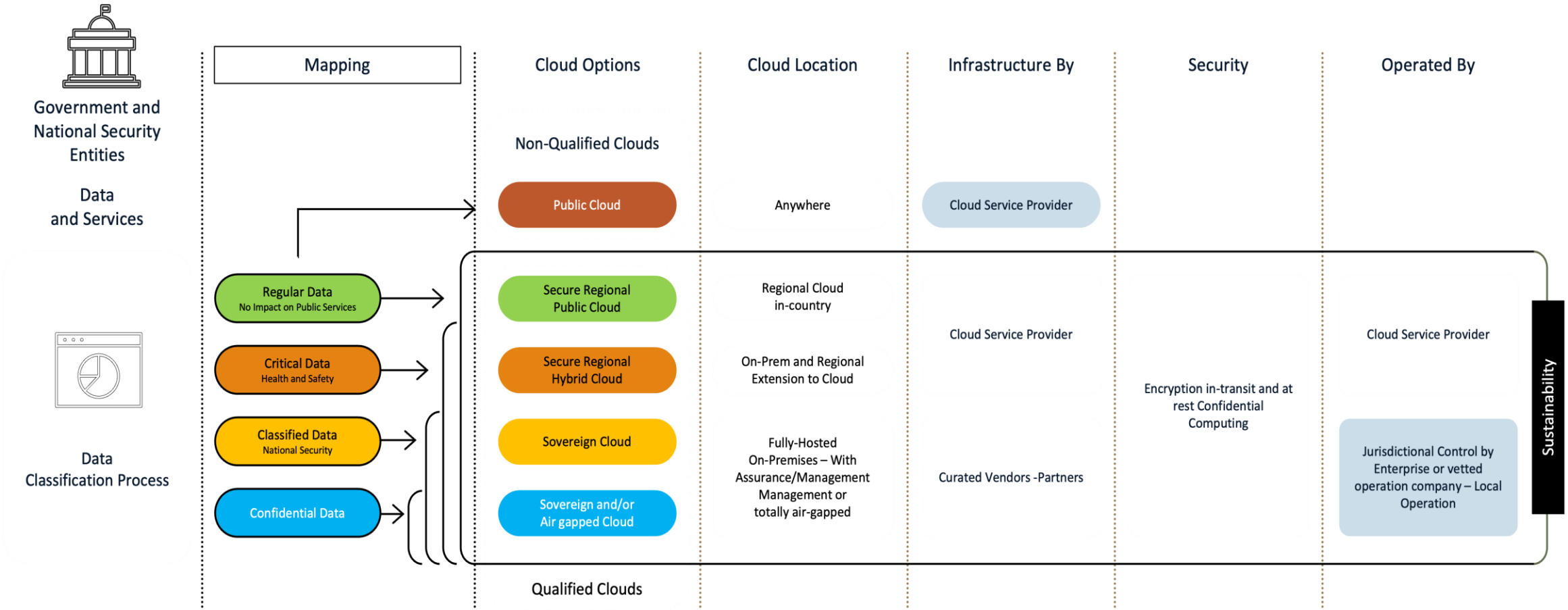
"Digital sovereignty refers to the ability to have control over your own **digital destiny – the data, hardware and software** that you rely on and create"

WORLD ECONOMIC FORUM

Sovereignty as a Spectrum
Local Residency and Operations

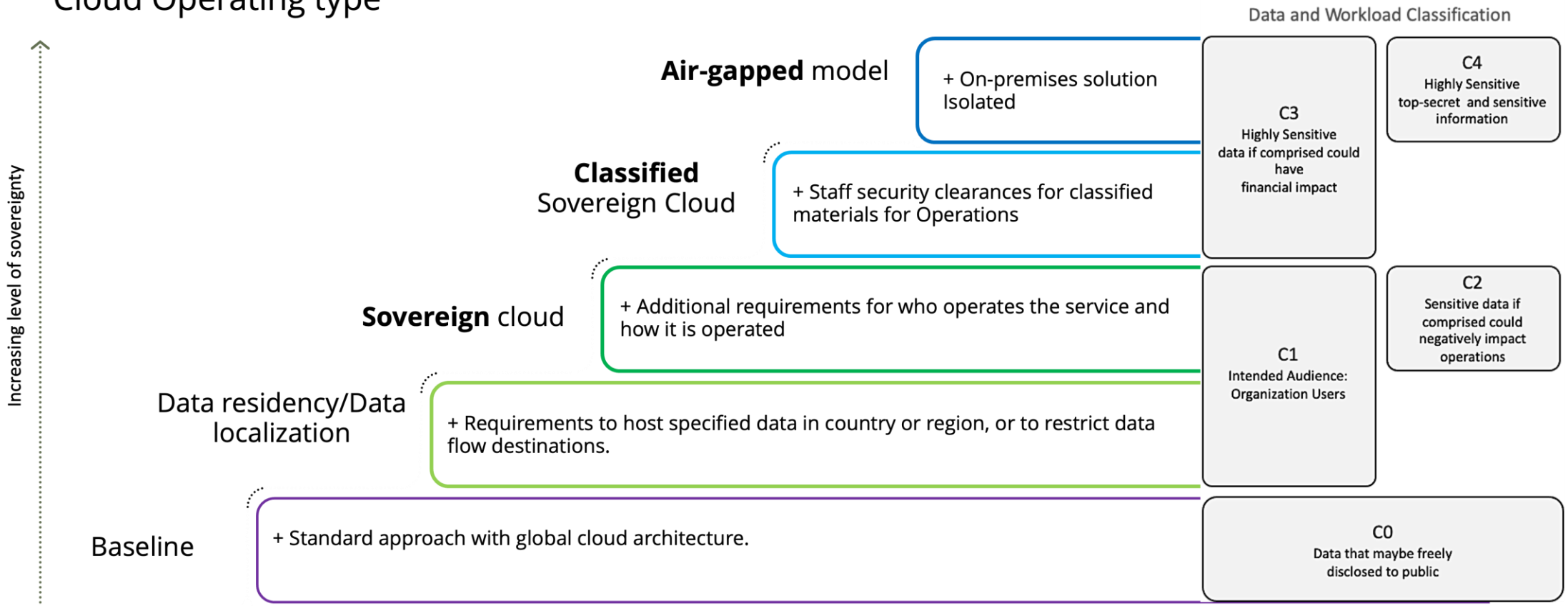


Augmenting Data Classification



Cloud Operating Models

Country's Data Classification example mapped to data residency Cloud Operating type




Gracias!
Merci!
Merci!
Spasiba!
Shukran!
Mahalo!
Grazie!
Thank you!
Spasiba!
Khob Khun Krap!
Aamsahamnida!
Tack!
Terima Kasih!
Tenà Koutou!
Asante Sana!
Terima Kasih!
धन्यवाद!

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Intensive 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!