OMG
OBJECT MANAGEMENT GROUP

Cloud Standards Customer Council

Data Residency:
Challenges and the Need for Standards

Webinar

May 11, 2017

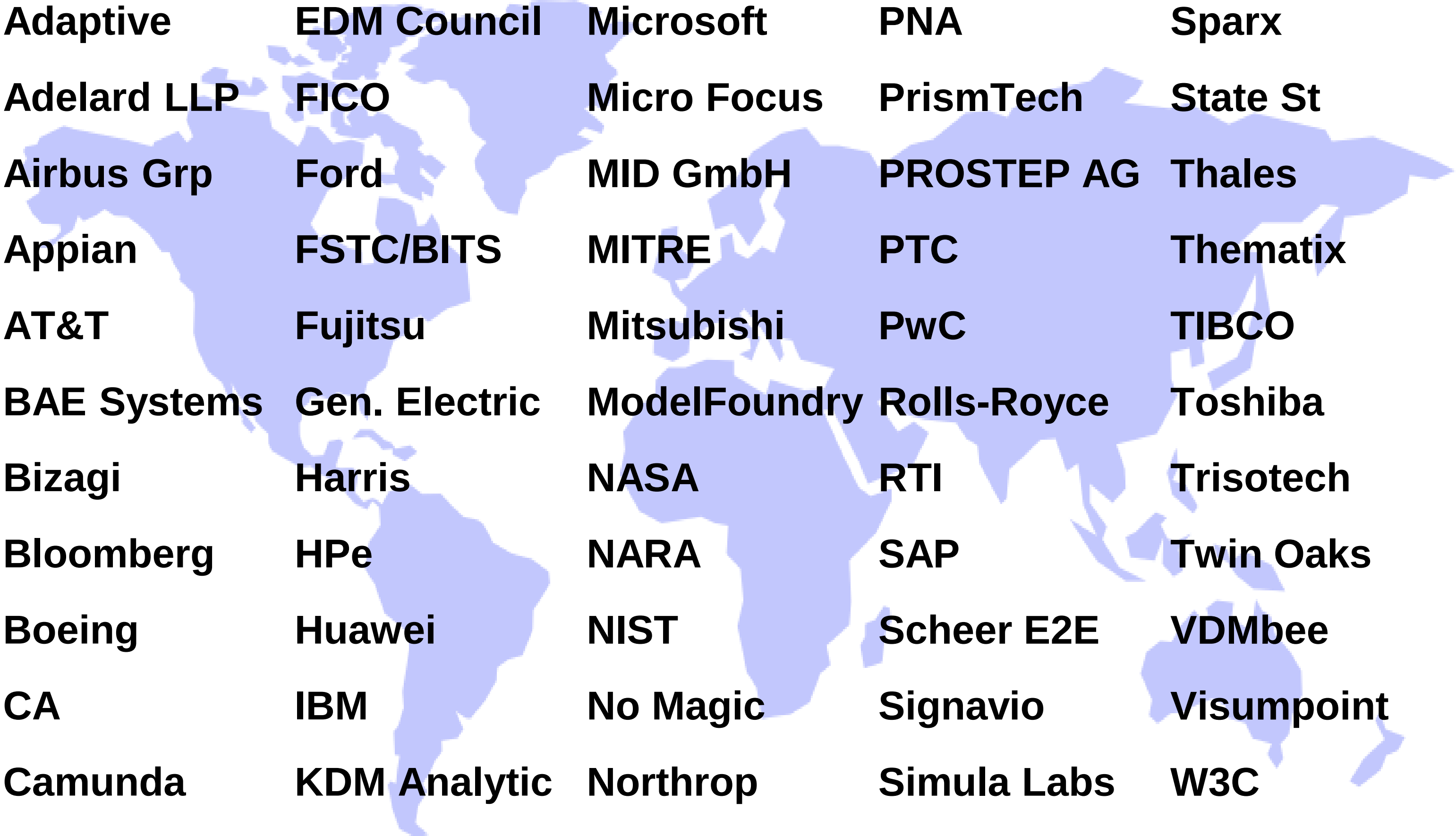
Speakers

	Tracie Berardi	Sr. Marketing Manager, OMG Moderator
	Andrew Watson	Technical Director, OMG
	Claude Baudoin	Principal, cébé IT & Knowledge Management Energy Domain Consultant, OMG Member of the CSCC Steering Committee

Introducing OMG

- **One of the most successful forums for creating open integration standards in the computer industry**
  - Middleware platforms (DDS, CORBA and related specs)
  - Modeling platforms (UML, BPMN, SysML and related work)
  - System Assurance (SACM, DAF for SSCD ...)
  - Vertical domain specifications (Finance, Healthcare, C4I, ...)
- **Member-controlled industrial consortium**
  - Both vendors and users
  - Not-for-profit
- **Adopted specifications are freely available to all**
  - Visit http://www.omg.org
- **Path to adoption by ISO and other standards bodies**

Worldwide Membership



- ACORD
- Adaptive
- Adelard LLP
- Airbus Grp
- Appian
- AT&T
- BAE Systems
- Bizagi
- Bloomberg
- Boeing
- CA
- Camunda
- Dell EMC
- Eclipse Fndn.
- EDM Council
- FICO
- Ford
- FSTC/BITS
- Fujitsu
- Gen. Electric
- Harris
- HPe
- Huawei
- IBM
- KDM Analytic
- Lockheed
- MEGA
- Microsoft
- Micro Focus
- MID GmbH
- MITRE
- Mitsubishi
- ModelFoundry
- NASA
- NARA
- NIST
- No Magic
- Northrop
- Oracle
- OSD
- PNA
- PrismTech
- PROSTEP AG
- PTC
- PwC
- Rolls-Royce
- RTI
- SAP
- Scheer E2E
- Signavio
- Simula Labs
- Softeam
- Software AG
- Sparx
- State St
- Thales
- Thematix
- TIBCO
- Toshiba
- Trisotech
- Twin Oaks
- VDMbee
- Visumpoint
- W3C
- (200+ more)

Introducing the CSCC

THE Customer's Voice for Cloud Standards!

- Provide customer-led guidance to multiple cloud standards-defining bodies
- Establishing criteria for open standards based cloud computing

2017 Projects

- **Data Residency discussion paper**
- Security for Cloud Services Ref. Architecture
- Impact of Cloud Computing on Healthcare v2
- Hybrid Integration Reference Architecture
- API Management Reference Architecture
- Blockchain Reference Architecture
- Multi-cloud Management whitepaper
- And more!

2016 Deliverables

- Prac Guide to Hybrid Cloud Computing
- Public Cloud Service Agreements, V2
- Cloud Security Standards, V2
- IoT Ref. Architecture
- e-Commerce Ref. Architecture
- Impact of Cloud Computing on Healthcare, V2
- Enterprise Social Collaboration Ref. Architecture

2015 Deliverables

- Web App Hosting Ref. Architecture
- Mobile Ref. Architecture
- Big Data & Analytics Ref. Architecture
- Security for Cloud Computing, V2
- Practical Guide to Cloud SLAs, V2
- Practical Guide to PaaS

2013/2014 Deliverables

- Convergence of Social, Mobile, Cloud
- Analysis of Public Cloud SLAs
- Cloud Security Standards
- Migrating Apps to Public Cloud Services
- Social Business in the Cloud
- Deploying Big Data in the Cloud
- Practical Guide to Cloud Computing, V2
- Migrating Apps: Performance Rqmnts
- Cloud Interoperability/Portability

650+ Organizations participating

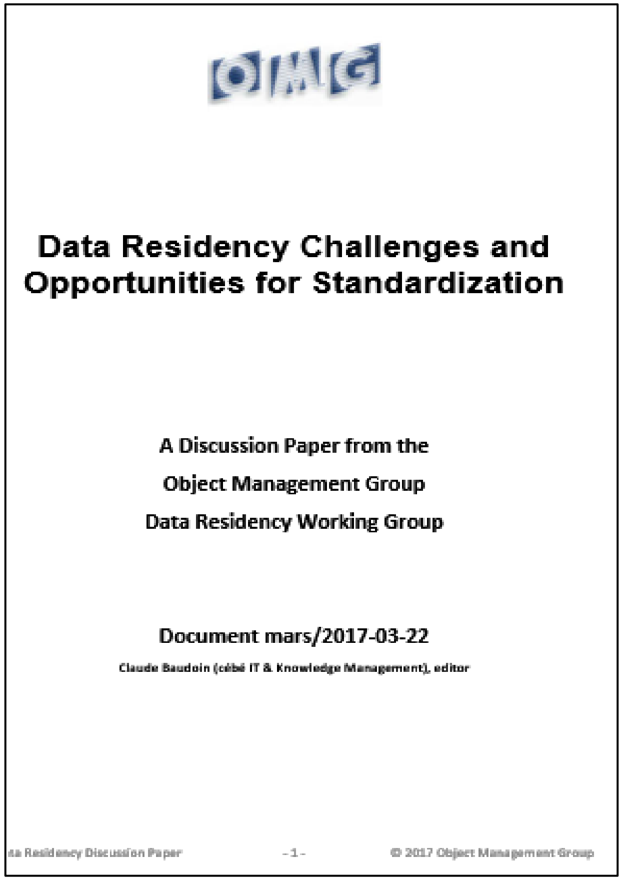
http://cloud-council.org

History of This Effort

- March 2015: initial request from an OMG member
- June 2015: first OMG Data Residency WG meeting (Berlin)
- Sep.-Dec. 2015: 2nd and 3rd meetings, prepared an RFI
- March-June 2016: 4th - 5th meetings, processed RFI results, decide to create a discussion paper as first deliverable
- Sep.-Dec. 2016: 6th - 7th meetings, preliminary draft of discussion paper, agreement to collaborate with CSCC and issue two separate but almost identical papers
- Q1 ‘17: collect contributions, edit paper, go the OMG approval process (8th meeting, Washington DC)
- April ‘17: create CSCC companion white paper, review process, release
- May ‘17: press releases and this webinar
- June ‘17: working group meeting and tutorial in Brussels

The Two Papers

- Both about 35 pages
- CSCC paper omits the history of the OMG effort and the discussion of OMG’s potential roadmap for standards



Data Residency Challenges and Opportunities for Standardization

A Discussion Paper from the

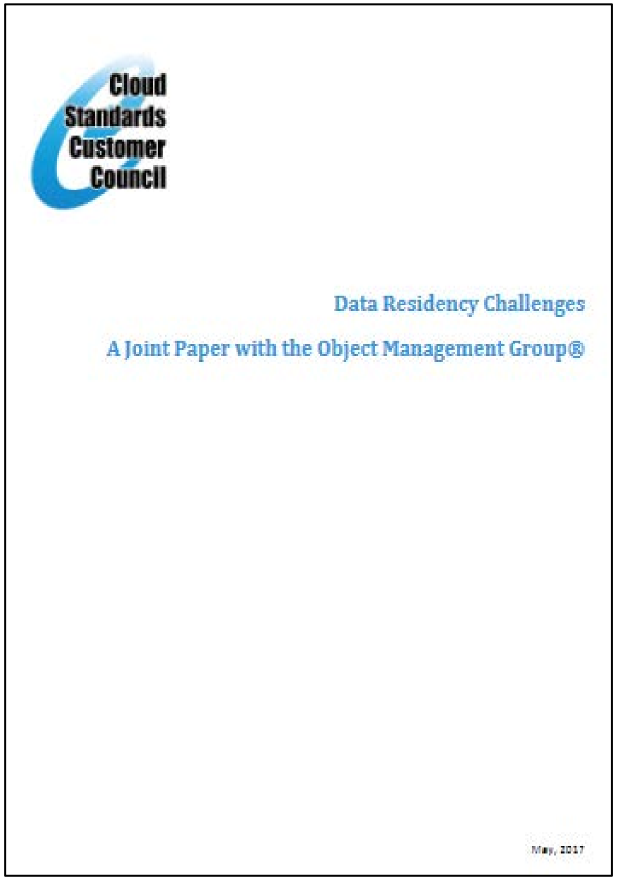
Object Management Group

Data Residency Working Group

Document mars/2017-03-22

Claude Baudoin (cébé IT & Knowledge Management), editor

ta Residency Discussion Paper - 1 - © 2017 Object Management Group



Cloud Standards Customer Council

Data Residency Challenges

A Joint Paper with the Object Management Group®

May, 2017

Data Residency Definition, Scope

- There are a number of definitions of data residency – as is usually the case in a new domain
- We propose this definition:

  Data residency is the set of issues and practices related to the location of data and metadata, the movement of (meta)data across geographies and jurisdictions, and the protection of that (meta)data against unintended access and other location-related risks

- Scope
  - Not just about the protection of personally identifiable information (PII)
  - Also concerns the right to move “sovereign” data, such as oil reserves data; international licensing of genomics data; distribution of biometrics data for security purposes; etc.

Risks Related to Data Residency

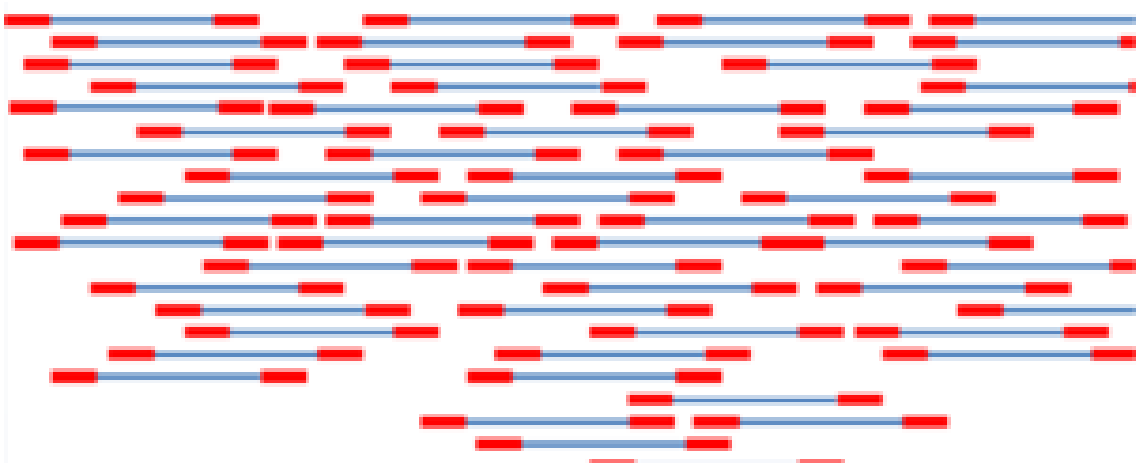
- Violating of a government law or regulation
- Unintended/unauthorized access by a foreign organization
- Demand by a foreign government's authorities to access data
- Having to provide a foreign government with secret keys to inspect encrypted data
- Violation of “domestic content” policies
- Increased cost of doing business in a given country
- Inability of a multinational organization to provide shared employee services, such as payroll and benefits
- Losing business to a local competitor
- Inability to qualify for government or private contracts
- Multiplication of locally managed data centers with smaller and less experienced security teams
- Diminished disaster recovery capabilities
- Delays in business transformation and technology modernization
- Consumer and citizen mistrust of technology, organizations, governments

Challenges: Example 1

- **Migration to the cloud**
  - Am I allowed to put my data in the cloud if it is going to be stored in another country, or if there is a *possibility* that the cloud provider might move it to another country later without my knowledge or consent?
  - Regulations may be unclear
  - Regulations may be used as a rationale to reject the cloud… even when they do not really exist (Mexico government example)
  - Authorization may require high-level approval (Danish bank example)

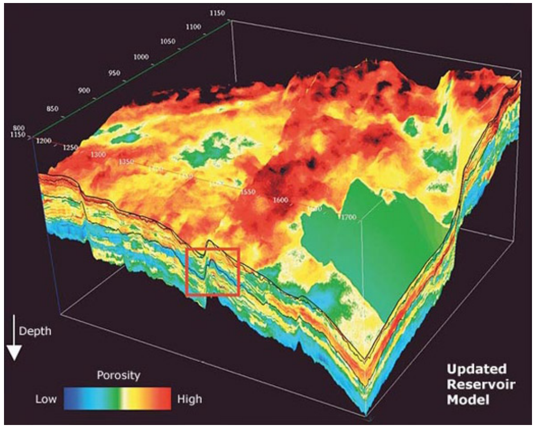
Challenges: Example 2

- **Genomic data sets**
  - Can I license a data set from another country to perform research on a larger sample?
  - How do I prove to regulators that the data no longer contains personally identifiable information (PII)?



Challenges: Example 3

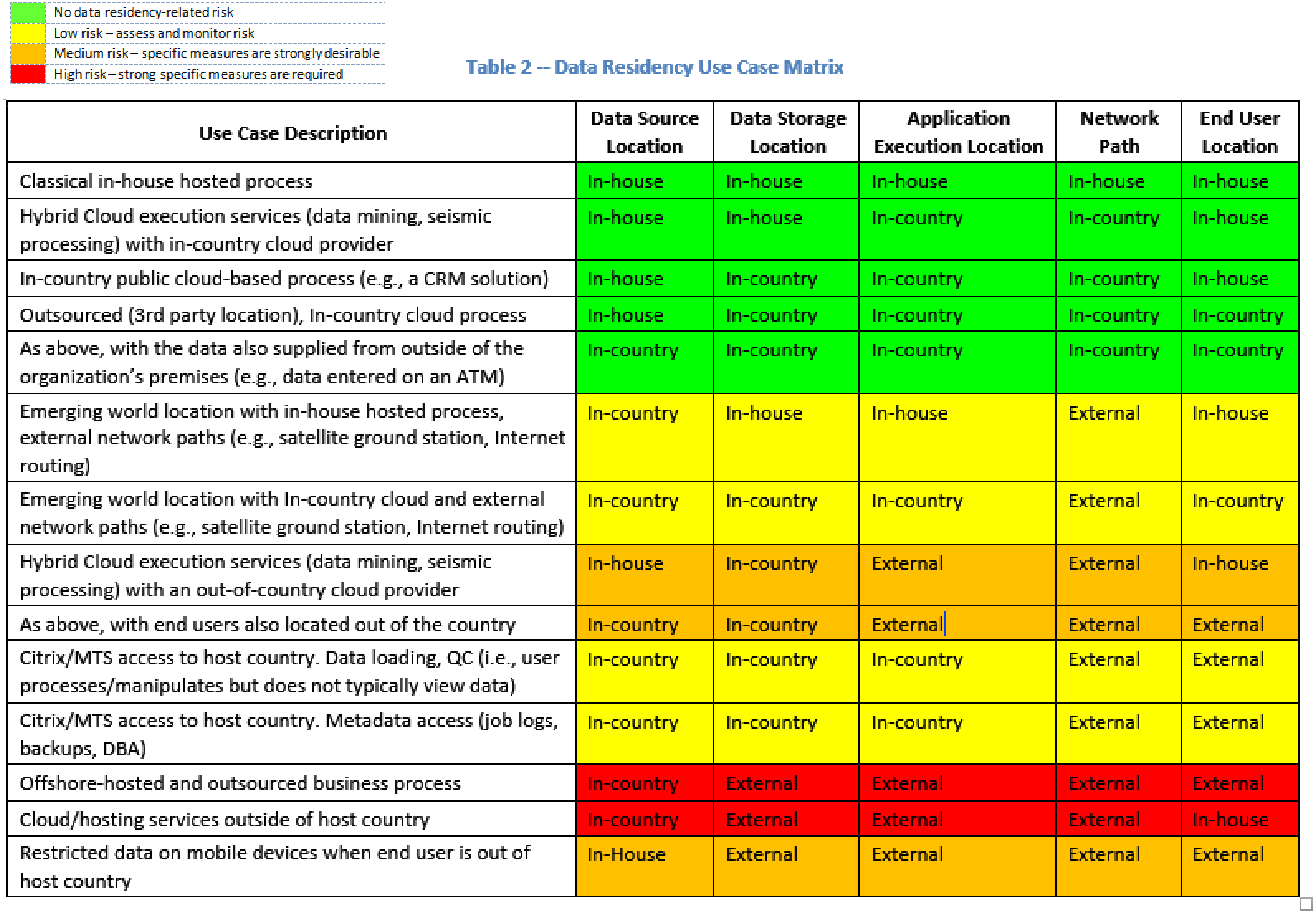
- **Processing data on petroleum reserves**
  - In countries with national companies, subsurface data is often considered a national asset
  - Exploration is subcontracted to foreign companies
    - ➢Can it remotely control an automated drilling operation from a monitoring center in another country?
    - ➢Can it move data to a foreign location in order to do better analytics?
    - ➢If it returns data interpreted in a center in another country, does it have to pay duties on the added value of those results?



Challenges: Example 4

- **Law enforcement vs. personal communication**
  - A US citizen is suspected of criminal activity
  - Some evidence may reside in their e-mail stored in the cloud by a US provider
  - However, the data is stored outside of the US, in a country with strong data protection laws
  - Which law prevails? Is the provider "damned if they do, damned if they don't" give the US government access to the data?

Use Case Matrix



🟩	No data residency-related risk
🟨	Low risk – assess and monitor risk
🟧	Medium risk – specific measures are strongly desirable
🟥	High risk – strong specific measures are required

Table 2 -- Data Residency Use Case Matrix

Use Case Description	Data Source Location	Data Storage Location	Application Execution Location	Network Path	End User Location
Classical in-house hosted process	In-house	In-house	In-house	In-house	In-house
Hybrid Cloud execution services (data mining, seismic processing) with in-country cloud provider	In-house	In-house	In-country	In-country	In-house
In-country public cloud-based process (e.g., a CRM solution)	In-house	In-country	In-country	In-country	In-house
Outsourced (3rd party location), In-country cloud process	In-house	In-country	In-country	In-country	In-country
As above, with the data also supplied from outside of the organization's premises (e.g., data entered on an ATM)	In-country	In-country	In-country	In-country	In-country
Emerging world location with in-house hosted process, external network paths (e.g., satellite ground station, Internet routing)	In-country	In-house	In-house	External	In-house
Emerging world location with In-country cloud and external network paths (e.g., satellite ground station, Internet routing)	In-country	In-country	In-country	External	In-country
Hybrid Cloud execution services (data mining, seismic processing) with an out-of-country cloud provider	In-house	In-country	External	External	In-house
As above, with end users also located out of the country	In-country	In-country	External	External	External
Citrix/MTS access to host country. Data loading, QC (i.e., user processes/manipulates but does not typically view data)	In-country	In-country	In-country	External	External
Citrix/MTS access to host country. Metadata access (job logs, backups, DBA)	In-country	In-country	In-country	External	External
Offshore-hosted and outsourced business process	In-country	External	External	External	External
Cloud/hosting services outside of host country	In-country	External	External	External	In-house
Restricted data on mobile devices when end user is out of host country	In-House	External	External	External	External

Laws and Regulations

- Multiple, inconsistent, overlapping, and still evolving laws and regulations around the world
- Range from non-existent to severe
- Sometimes (but not always) apply to government data / public records, not to private companies' data
- The European Union's General Data Protection Regulation (GDPR) of 2016 is among the most comprehensive
- Multiple motivations behind the laws:
  - Protecting the privacy of citizens
  - Enabling police and tax authorities to inspect data
  - Protectionism – force companies to create domestic facilities
  - Monetize the flow of data

Some Country-Specific Cases

- See Appendix in the papers – but remember that the situation keeps evolving
  - Australia
  - Canada
  - China
  - Denmark
  - European Union
  - France
  - Germany
  - India
  - Indonesia
  - Korea
  - Malaysia
  - Netherlands
  - Nigeria
  - Norway
  - Russia
  - Turkey
  - Ukraine
  - United States
  - Venezuela
  - Vietnam

Existing Relevant Standards

- There is currently no standard that deals specifically with data residency
- Data residency is related to the security and privacy aspects of
  - Several NIST publications (800-144, 500-299, 1500)
  - Several ISO/IEC standards (27001, 27017, 27018)
  - The work of the CSA's International Standardization Council (ISC)
  - Work being considered in ISO/IEC JTC 1/SC 38
  - The "Voluntary Data Protection Code" of CISPE (Cloud Infrastructure Service Providers in Europe)
- Some technical standards may prove useful
  - Information Exchange Framework (IEF) – OMG
  - Data Tagging and Labeling – OMG work in progress
  - XACML – eXtensible Access Control Markup Language
  - ORDL – Open Digital Rights Language

What is Needed

- Documentation and education
  - These papers are a good start
- Cataloguing of laws and regulations
  - See the Digital Trade Database from the European Centre for International Political Economy (ECIPE)
- Formal description of laws and regulations
  - Because natural language is ambiguous and does not lend itself to automated policy enforcement
- Formal description of the content of data
  - Extension of data tagging and labeling or IEF policy
- With both of the above, we might be able to better manage residency
- Several difficult challenges
  - Willingness to participate – requires recognizing there are issues
  - Implementation may be difficult due to legacy systems

Summary and How to Participate

- **Data residency is a serious challenge for suppliers as well as users**
  - Can (and already does) hurt the ability to do business
- **It may well get worse before it gets better**
- **Organizations need to learn about it and develop business and technical approaches**
- **OMG is looking into what standards may help**
  - Metadata describing data location constraints?
  - Formal description of data residency laws and regulations?
- **Call to action**
  - Participate in OMG Data Residency Working Group
  - and/or in the various Working Groups of the CSCC

Thanks – Q&A Time

More information at

www.omg.org/data-residency

and

www.cloud-council.org/resource-hub