Leveraging the Cloud: Strategies for Compliance
Presented by:
Helen Fotos, Metronome Consulting
Chris North, Esri Canada
April 13, 2016
Data Protection Regulations

• Canada has over 28 federal, provincial, and territorial statutes that govern the protection of personal information in the private, public, and health sectors.

• Generally private sector companies are covered by PIPEDA, health care organizations are covered by PHIPA, and government organizations are regulated by municipal MFIPPA or provincial FIPPA.

• Nova Scotia’s PIIDPA and British Columbia’s FoIPPA are unique in that they focus more on data residency and sovereignty that data security and protection – the result of a political backlash against the U.S. Patriot Act in the early 00’s.
FoIPPA Concerns for Cloud Adoption

- BC's data residency and sovereignty regulations are considered amongst the strictest in the world
- FoIPPA specifies that certain types of personally identifiable information (PII) cannot leave Canada
- Warnings about the "Mosaic Effect" – where seemingly innocuous pieces of data can be pieced together to identify an individual – have added to confusion over what PII is
- FoIPPA has been both a real and imagined obstacle to cloud adoption in the BC public sector - but it doesn’t have to be!
Why Use the Cloud?

• Cloud solutions, including Esri’s ArcGIS Online, provide a number of proven benefits for organizations, including:
  - Increasing Operational Efficiencies with On-Demand GIS
  - Streamlining Application Development and Deployment
  - Flexibility, Elasticity, and Scalability

• Organizations are increasingly advocating a “Cloud First” approach for efficient project delivery – but concerns over compliance have caused confusion and delays in BC’s Cloud adoption
A Structured Approach to Compliance

- Often organizations make assumptions about compliance without adequately assessing the regulatory requirements, data, and compliance strategies (including technical architecture options).
- By using a structured approach and proven strategies for compliance, public sector organizations in British Columbia can start to realize the benefits of the cloud.
- High level Compliance process throughout project lifecycle:
  1. Conduct initial assessment during *project initiation & planning*
  2. Leverage compliance strategies throughout *implementation*
  3. Re-assess & document compliance strategy prior to “Go-Live”
Cloud Compliance Best Practice: Initial Compliance Assessment

Initial assessment, typically done during Project Initiation & Planning

- What regulations, if any, does your project need to comply with?
- Investigate the exact compliance requirements – don’t make assumptions and get guidance if needed
- Assess the project’s data collection and storage requirements
- Determine the overall approach for compliance*

*Plan the high level compliance strategy during this phase, but don’t commit to a solution yet! Both the technology and the regulations are evolving – the best practice is to make decisions around compliance and the technical solution at the “Last Responsible Moment”
Cloud Compliance Strategy: Scrutinize Data Requirements

Assess data requirements throughout the project lifecycle

- “Lean” the data! Pare down the collection of personally identifiable information (PII) - many applications collect and store too much non-value-added sensitive data

- Is the data really even PII? The definition of PII excludes personal information related to a person’s name in a professional capacity, or their business contact information, including phone number and address
Cloud Compliance Strategy: Deflect Sensitive Personal Info & Get Consent

Keep unnecessary PII out of system, and inform users of Cloud storage

- Use disclaimers and warnings on to inform and educate users
- Train internal staff on proper collection and storage of PII
- Incorporate consent and "Opt-In" language:
  - "This application uses ArcGIS Online, a Cloud-based mapping service. By using the application and/or submitting any personal information, you are consenting to the storage of this data on servers which may be located in the United States and/or locations outside of Canada in secure, state-of-the-art data centres."
Cloud Compliance Strategy: Consider Technical Architecture Options

If sensitive PII needs to be stored, consider technical workarounds

• ArcGIS Online can be used as a stand alone solution, or as part of a hybrid approach
• There are soon to be 4 different architectural approaches for projects that need to handle sensitive PII
  1. ArcGIS Server On Premise
  2. Hybrid ArcGIS Server / ArcGIS Online
  3. Cloud Builder
  4. Hybrid Cloud Builder / ArcGIS Online
Technical Architecture Option 1: Completely On-Premises Deployment

- Portal
  - Custom Roles
  - Service Directory
- Webmaps
- Device
- Web Apps
- Desktop
- ArcGIS Server
- Enterprise Geodatabase
- ArcGIS Server
Technical Architecture Option 2: Hybrid ArcGIS Server / ArcGIS Online

- **Web Apps**
- **Desktop**
- **Service Directory**
  - ArcGIS Enterprise
  - ArcGIS Geodatabase
- **Organization**
  - Custom Roles
  - Webmaps
  - Service Directory
- **Device**
- **Online Content Services**
  - e.g. Basemaps, Geocoder
Technical Architecture Option 3: Cloud Builder

- Cloud Builder
- Portal
- Service Directory
- Web Apps
- Webmaps
- Device
- Custom Roles
- ArcGIS Server
- Enterprise Geodatabase
- ArcGIS Server
Cloud Builder Tools

Both Microsoft & Amazon will have Canadian Regions in 2016
Technical Architecture Option 4: Hybrid Cloud Builder / ArcGIS Online

- Web Apps
- Desktop
- Service Directory
- ArcGIS Enterprise
- ArcGIS Server
- ArcGIS Geodatabase

- Web Apps
- Device
- Webmaps
- Custom Roles
- Service Directory
- Online Content Services e.g. Basemaps, Geocoder
Cloud Compliance Best Practice: Define & Document Compliance Strategy

Review and document compliance strategy prior to Go Live

- Review the materials from the initial Compliance Assessment
- Define compliance requirements, assumptions, risks, and options
- Document the technical architecture selected for the project, and any additional risk mitigation strategies used
- Ensure compliance strategy is well understood by project sponsors and key stakeholders
- This information can be used when submitting the Privacy Impact Assessment (PIA)
Additional Resources

- https://www.oipc.bc.ca/guidance-documents/1427