RIMS CANADA™

Proudly Presents...

Navigating the Cloud Across the US & Canada Border

Presenters

Rob Groves, B.A., M.B.A.,
Director, Finance and Business Services,
Calgary Catholic School District
Rob Groves is the Director, Finance and Business Services for Calgary Catholic School District which is the largest Catholic School District in Alberta with over 45,000 students, 4500 staff, 110 district facilities and a budget of just under $0.5 billion. With a primary role in budget preparation, Mr. Groves is also responsible for risk management which is his passion. He is also chair of the Technical Team for the Urban Schools Insurance Consortium (USIC) – a partnership of fourteen of the largest school districts in Alberta – which operates under an insurance reciprocal arrangement. USIC is implementing the iVos web-based event reporting to assist in risk management.
Calgary Catholic already has significant risk management and occupational health & safety programs which are all linked through the iVos event reporting program. This allows for relevant risk management information to be collected enabling members to be proactive in loss prevention and risk management.

David Black, Chief Information Security Officer
Aon eSolutions
David Black is the CISO for Aon eSolutions, the leading global provider of web-enabled integrated risk management tools and resources. Mr. Black is responsible for Aon eSolutions strategy and approach to IT risks as well execution of initiatives for protection of all our products and services as well as our corporate environment.
Previously Mr. Black was the Director of Information Security for EarthLink, Inc, Manager within KPMG's Information Risk Management Practice, and held various information security and technology positions during his time at The Coca-Cola Company. During his 14-year information security career, Mr. Black has performed security roles from technical design and implementation to development and execution of comprehensive strategic security and IT risk management programs. His experience spans across industries with consulting and corporate tenures directing global security initiatives and teams.
david.black@aon.com | t: +1.678.784.4664

Session Overview

- *Cloud computing enables companies to free up resources, lower operating costs, and focus on core business functions. While safe, secure and cost-effective to implement, utilizing them across the U.S. and Canada border can be tricky, with concerns around the Patriot Act. Learn the benefits of working in the cloud and the differences between private and public clouds. Acquire information that will assist U.S. and Canadian companies understand the laws and risks of cloud computing and help maximize value, while minimizing risk. Hear the experiences of a Canadian organization working with a U.S. based firm, while complying with data laws.*

Session Agenda

- *Cloud Evolution & Terms*
- *Cloud Implications/Risks*
- *U.S. PATRIOT Act*
- *Cloud Governance*
  - *Canada Federal*
  - *Provincial Laws*
- *Real-world Solution Example*

What is “Cloud Computing”

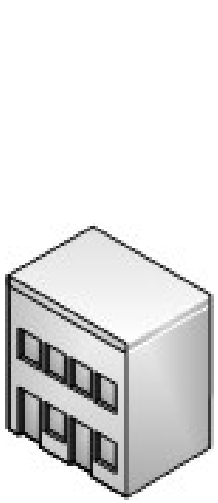
- Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand, like electricity
- Computing in which services and storage are provided over the Internet (or "cloud")
- Refers to accessing computing resources that are typically owned and operated by a third-party provider on a consolidated basis in one, or more, data center locations

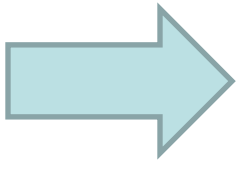
Cloud Evolution

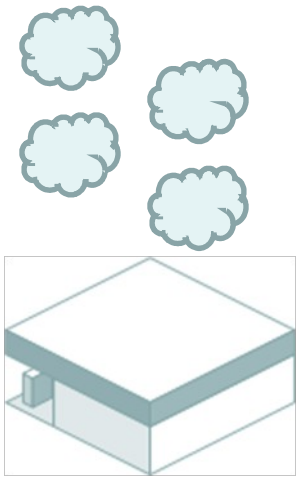
Self Hosted & Managed

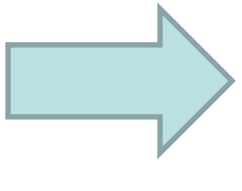
"Private*" Cloud Computing

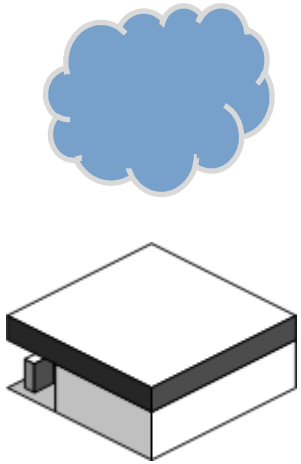
"Public*" Cloud Computing











Traditional Data Center

Company employees or 3rd party manages applications & infrastructure components & data

Hosted/SaaS Provider

Partner manages applications & infrastructure components & data

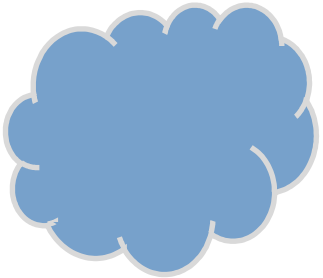
Hosted/SaaS Provider

Partner manages partners that manage applications & infrastructure components & data

Cloud Evolution (cont'd)

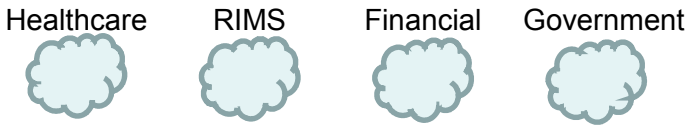
Corporate "Private" Clouds

Internal uses of cloud technologies to provide services to corporate "clients" with self-managed & owned infrastructure



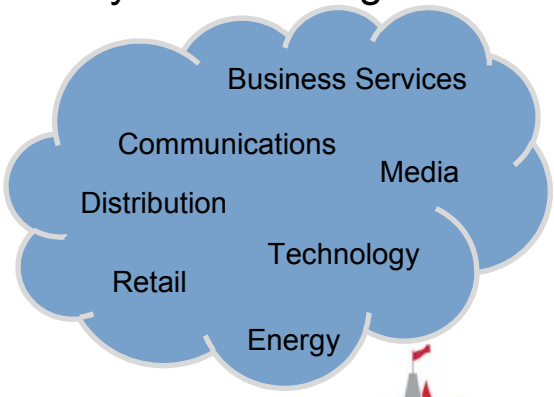
Community Clouds

External cloud infrastructures dedicated to specific industries, sectors or purposes. Also known as "vertical clouds"

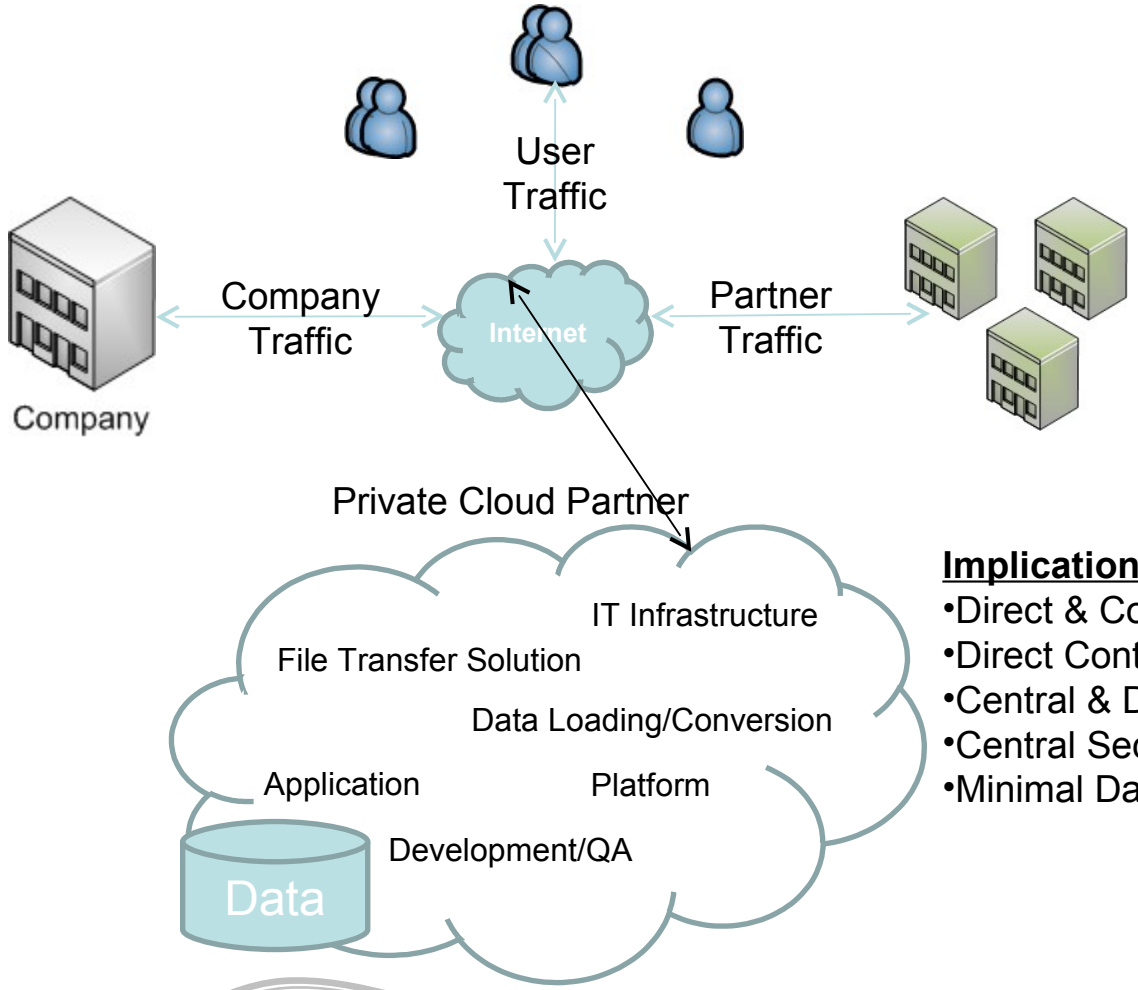


Commodity Clouds

External cloud infrastructures open to host any application types for virtually any purpose and can be brokered by a cloud integrator



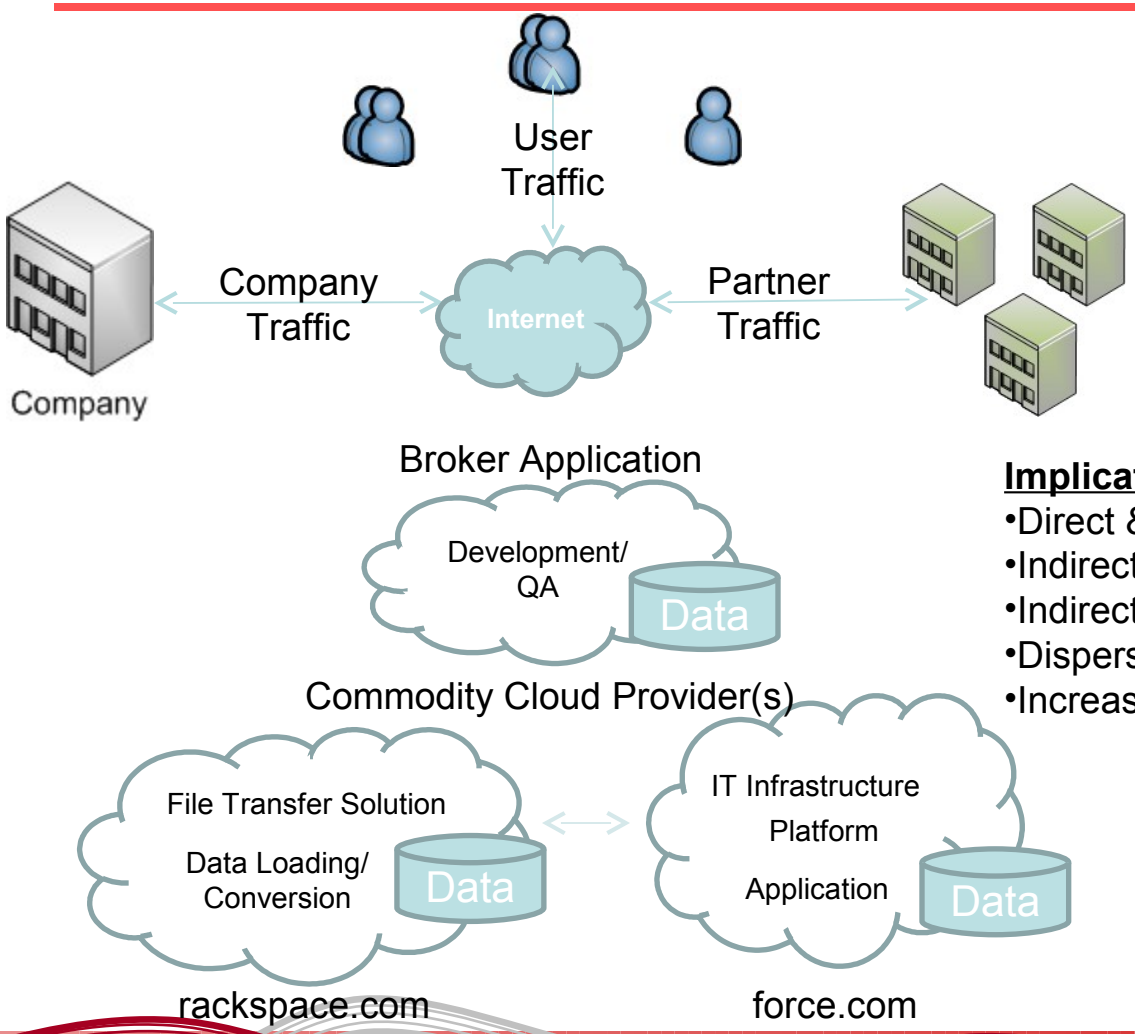
Cloud Solution Provider



Implications

- Direct & Complete Partner Relationship
- Direct Contractual Protections/SLAs
- Central & Direct IT/Application Management
- Central Security, Controls and Certifications
- Minimal Data Duplication/Exposure

Cloud Solution Broker



Implications

- Direct & Indirect Partner Relationships
- Indirect Contractual Protections/SLAs
- Indirect IT/Application Management
- Disperse Security, Controls and Certifications
- Increased Data Duplication/Exposure

Cloud Solution Risks

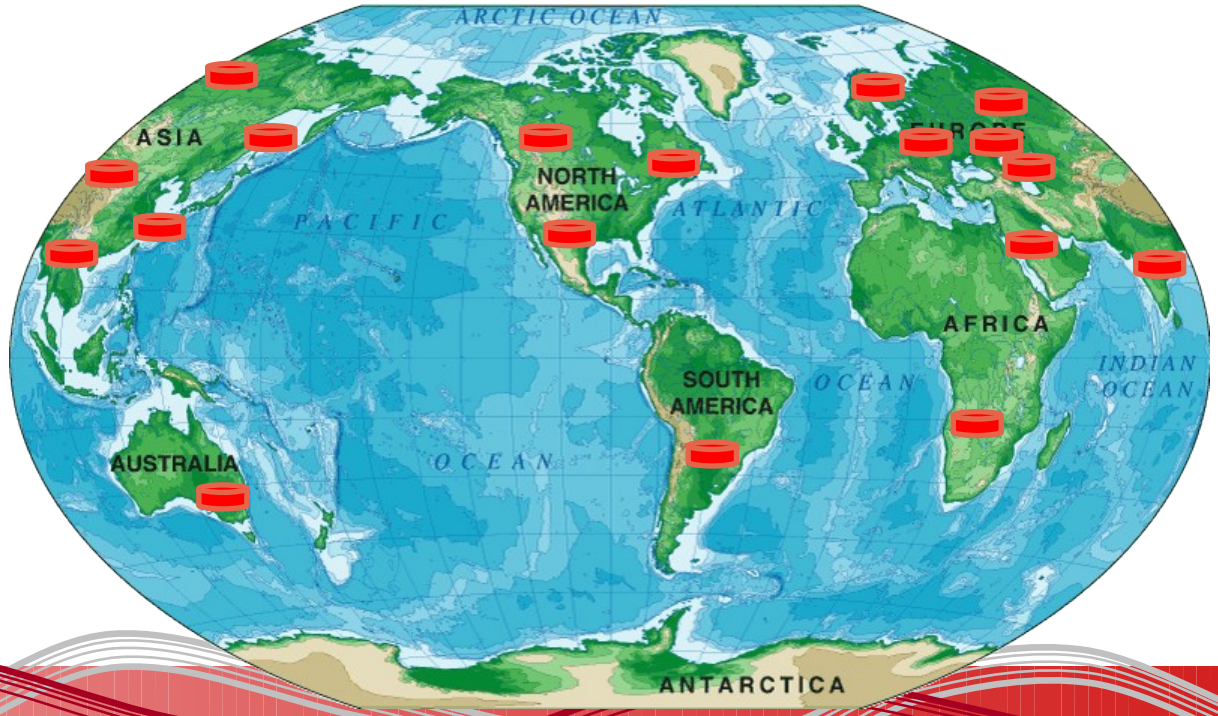
- Normal “outsourcing” risks
  - Cost Reduction Expectations
  - Process Discipline
  - Loss of Business Knowledge
  - Vendor Failure to Deliver
  - Scope Creep
  - Culture
  - Turnover of Key Personnel
  - Knowledge Transfer
- Data Breach
- Government Oversight/Regulation

Data Breach Risk

- Duplication/Replication of Data (multi-vendor solutions)
- Complexities in scope of security and control needs
- Different types of cloud solutions require differing levels of security and audit requirements.
- Potential for use of outsourced and/or offshore resources

Government Oversight/Regulation

- Local and Federal governance requirements for:
  - The organization
  - The cloud provider/broker
  - Any additional providers serving the broker



The USA PATRIOT Act

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
- Intended to facilitate the fight against terrorism
- Introduced 4 key changes from previous information and evidence gathering laws
  - Search and surveillance authority more widely available
  - Threshold lowered
  - Subject-matter scope broadened
  - National Security Letter regime expanded

PATRIOT Act

- U.S. government could compel the disclosure of Canadian citizen information that is stored within U.S. controlled areas
- Such disclosure could be viewed as a violation of privacy
- There are examples of the U.S. taking advantage of the PATRIOT Act to collect information

Side note: Canada has very similar act/permissions:

- Canada's Anti-terrorism Act of 2001
- PIPEDA subsection 7(3)(c.1)

Canadian Federal Privacy

- Private sector transfer of personal information from Canada to the U.S. is not a violation of Canadian Federal law.
- Government sector transfer of personal information from Canada to the U.S. is not a violation of Canadian Federal law.
- The transfer of personal information from Canada to the U.S. by financial sector companies is not a violation of Canadian Federal law.
- With a few exceptions, provincial laws permit the transfer of personal information from Canada to the U.S.

Use vs. Disclosure

- A transfer for processing is a “use” of the information; it is not a “disclosure”. Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer for processing is not required.

Provincial Law

- Federal law for **public** organizations (PIPEDA) does not apply to provincially-regulated organizations within provinces where privacy laws have received substantially similar status from the Governor in Council.

Provincial Specifics

- British Columbia: Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004. The law requires public bodies to ensure that "personal information in its custody or under its control is stored only in Canada and accessed only in Canada."
- Quebec: Aligns with British Columbia
- Nova Scotia: Personal Information International Disclosure Protection Act, 2006. Follows British Columbia's Bill 73.
- Alberta: Freedom of Information and Protection of Privacy Act permits the disclosure of personal information controlled by a public body in response to a "subpoena, warrant or order" only if issued by a court with "jurisdiction in Alberta.

Cloud Challenges

- Canadian organizations spread across multiple provinces
- Dynamic and Complex laws/regulations
- U.S. PATRIOT Act
- Misconceptions and confusion created by differing laws/regulations
- Organization Policies
- Brand/reputation impact

Key Cloud Considerations

- Where is your data actually located?
- Who has the ability to access your data?
- How are service levels measured/maintained?
- How do you escalate issues?
- How do contractual protections apply?
- Does cloud computing support your compliance requirements?
- Does the provider offer ASP-Hosted or self-hosted solutions?
- Which recommendations/checklists should we leverage based on industry/sector/data types?

“Due-diligence” Steps

1. Determine which Canadian (Federal & Provincial) data privacy regulations apply to your organization
2. Demonstrate focus on privacy during all phases of solution selection
3. Identify Personal information is defined in section 3 of the Privacy Act
4. Perform an invasion-of-privacy test - http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp07-eng.asp
5. Perform a Privacy Impact Assessment (PIA) or a Preliminary PIA (PPIA) - http://www.priv.gc.ca/fs-fi/02_05_d_33_e.cfm
6. Complete Privacy Protection Checklist for each prospective solution - http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp08-eng.
7. Build security and privacy into contract

Case Study: USIC

- USIC is the Urban Schools Insurance Consortium in Alberta (14 Boards with different requirements and issues).
- Purchased iVos event reporting and customized for needs.
- “Where” information was to be stored created added complexity to purchase and implementation – required Canadian host location.
- With a separate hosting arrangement (TELUS initially), other arrangements needed for dba and system admin. Additional costs and delays in implementation.
- Too many fingers in the pot – ended up with a dba in Ontario, TELUS contacts in both Ontario and Alberta, iVos implementation team in Florida and California, users in Alberta.
- Perseverance, a clear vision of the goal, and ample

RIMS CANADA™

Thank you for attending the Ottawa Capital Connexions Conference

Ottawa 2011 Capital ConneXions