Finding Privacy and Security in the Cloud

Presented by:	**Matt Reed**	**Privacy, Compliance and Training Branch, Ministry of Finance**
	Ken Prosser	**Information Security Branch, MTICS/OCIO**

Agenda:

- BC Government Cloud use goals
- Privacy & Security Evaluations so far
- Privacy in the Cloud
- Security in the Cloud

Province of BC's direction/goals

- Explore opportunities
- Learn environment and issues
- Determine where use is acceptable
- Develop standards and guidelines

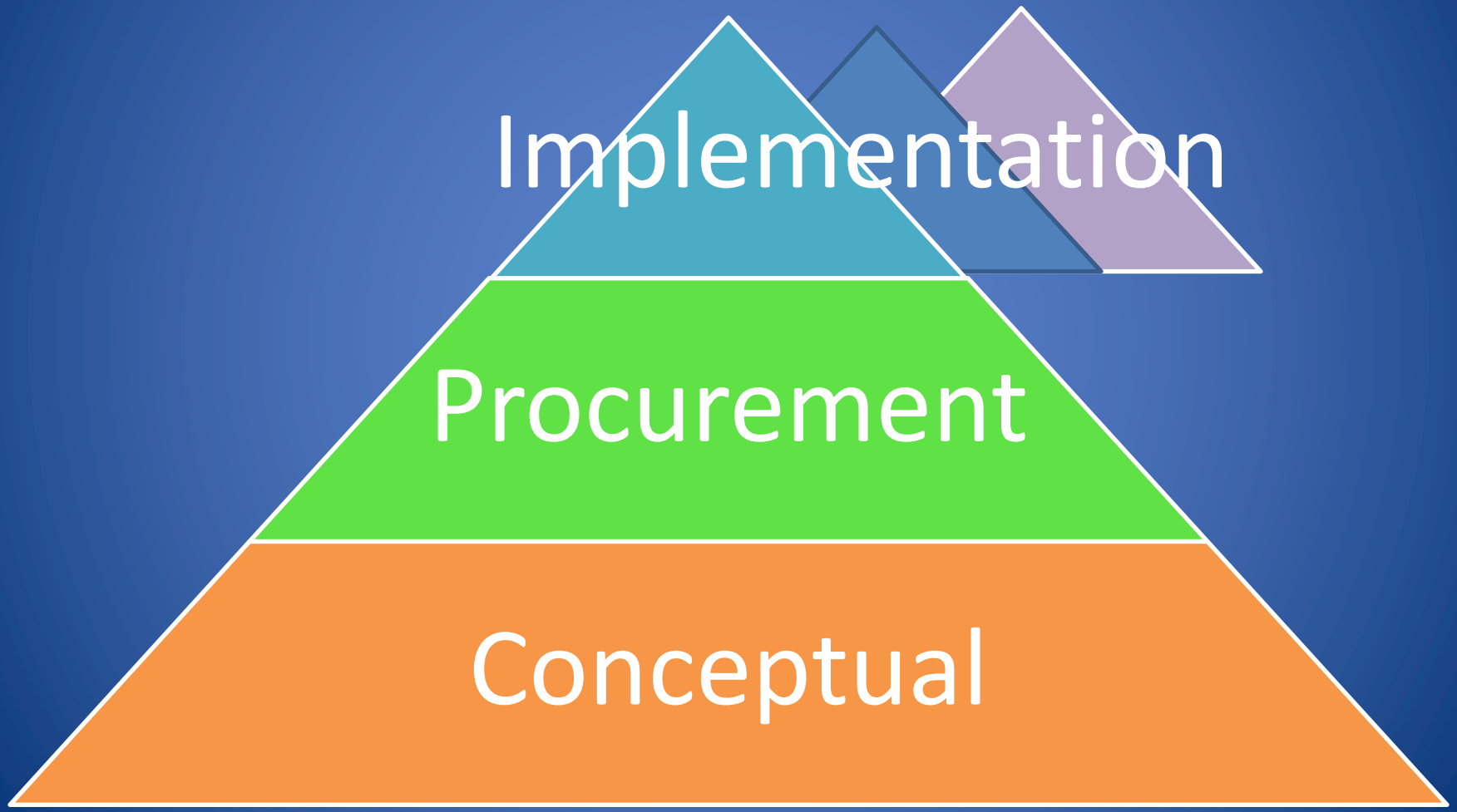
Preliminary work done

- Evaluations on Public cloud (Yammer, etc.)
- Evaluations on SAAS (Salesforce, O365)
- Development of Cloud BC (Private Cloud)
- Development of Cloud Security Standard
- In-depth assessment of Office365 use case

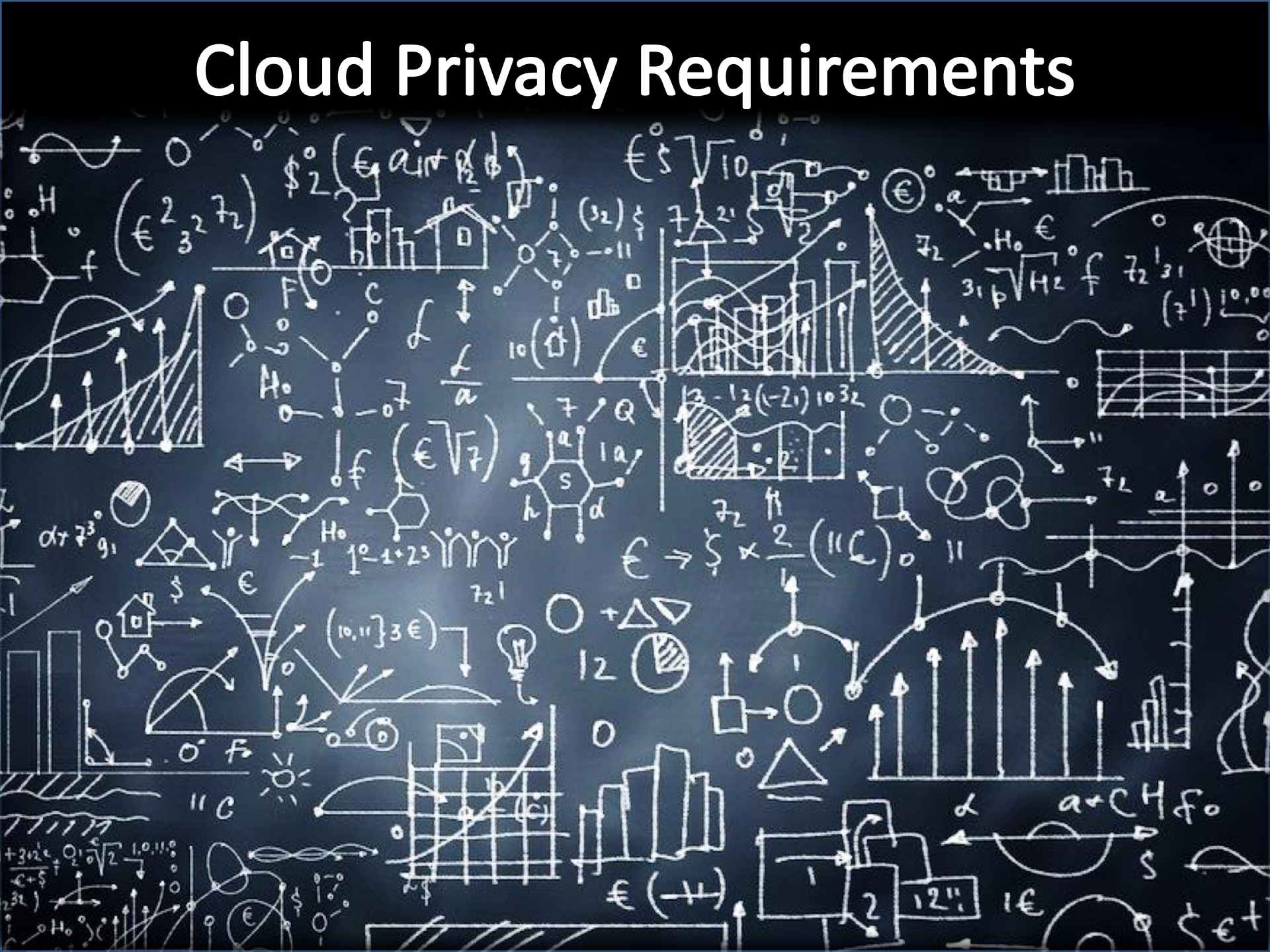
Privacy in the Cloud

How do you even start assessing the Cloud?

Methodology and approach



Cloud Privacy Requirements



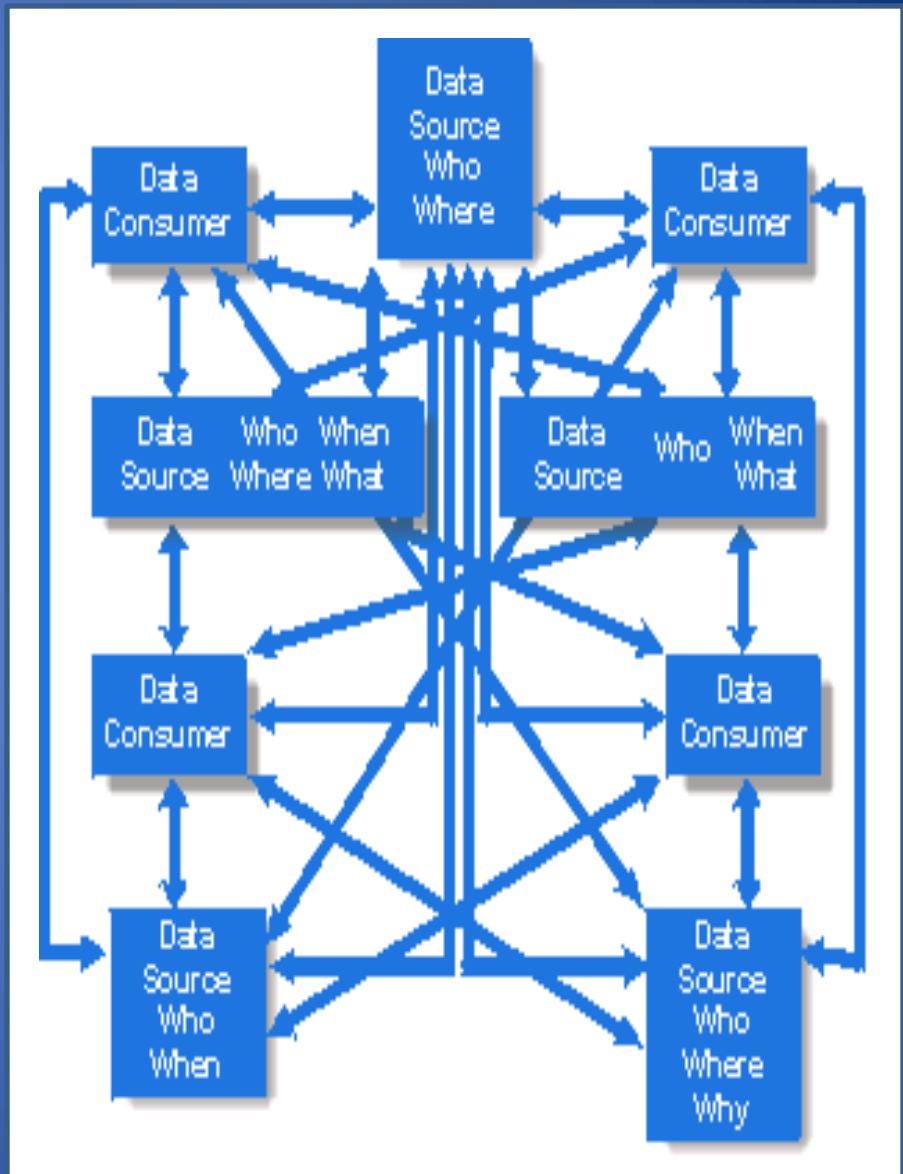
Cloud Privacy Requirements

1. All customer data containing personal information resides in Canada* (i.e. Canadian datacentres)
2. Service Provider access to customer data is controlled by Province (e.g. through technical and/or procedural measures)
3. Contractual provisions support FOIPPA compliance (e.g. jurisdiction, corporate governance, etc.)
4. Appropriate security provisions are in place

*unless an exception applies

Shifting Dichotomous Thinking

VS.



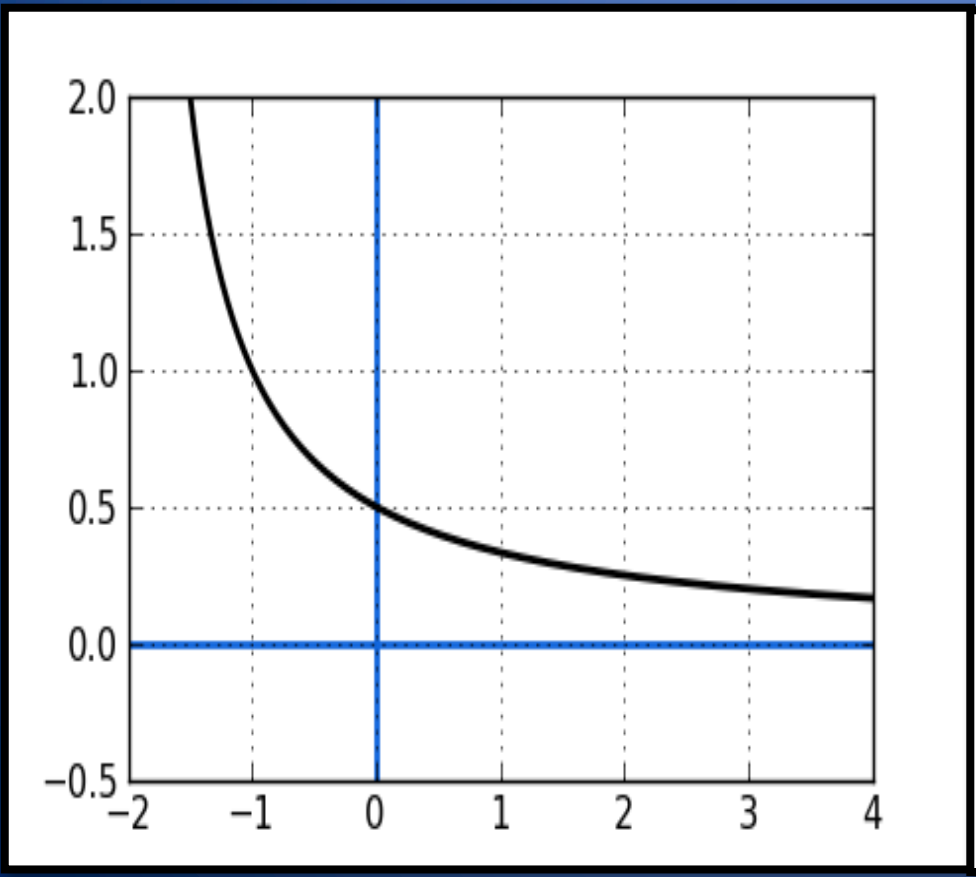
Use Cases

- Technical Maintenance
- Foreign Demand
- Breach Protocol

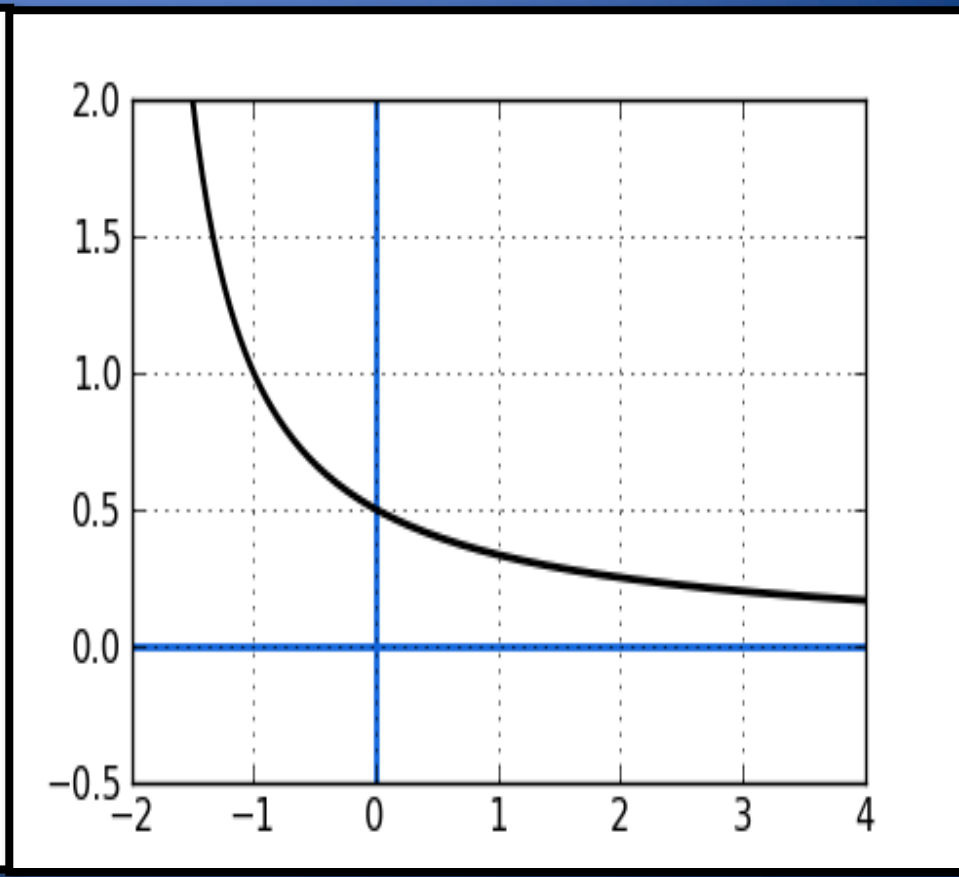
Let's talk about risk, maybe.

(Let's talk about you and me)

The limit is zero.



There is no limit.



Assessment process - OIPC

Looking to the Future

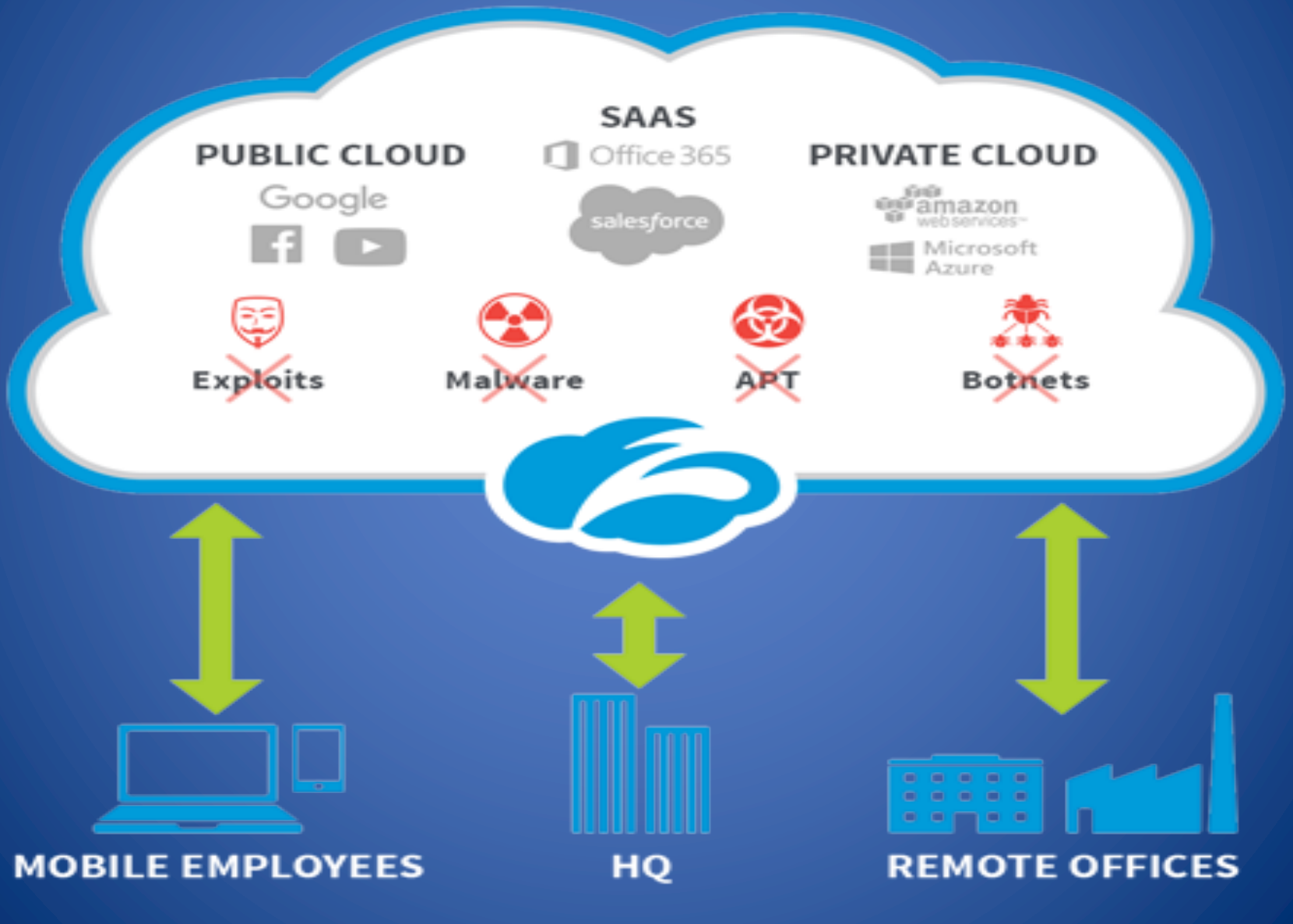
- Assessing different contexts
  - Different information
  - Different sensitivities
  - Different volumes
- Indirect cloud providers
  - E.g. new cloud service provided on other providers cloud infrastructure

Ken Prosser, Director Cybersecurity Intelligence and Investigations
Office of the Chief Information Officer, Province of BC

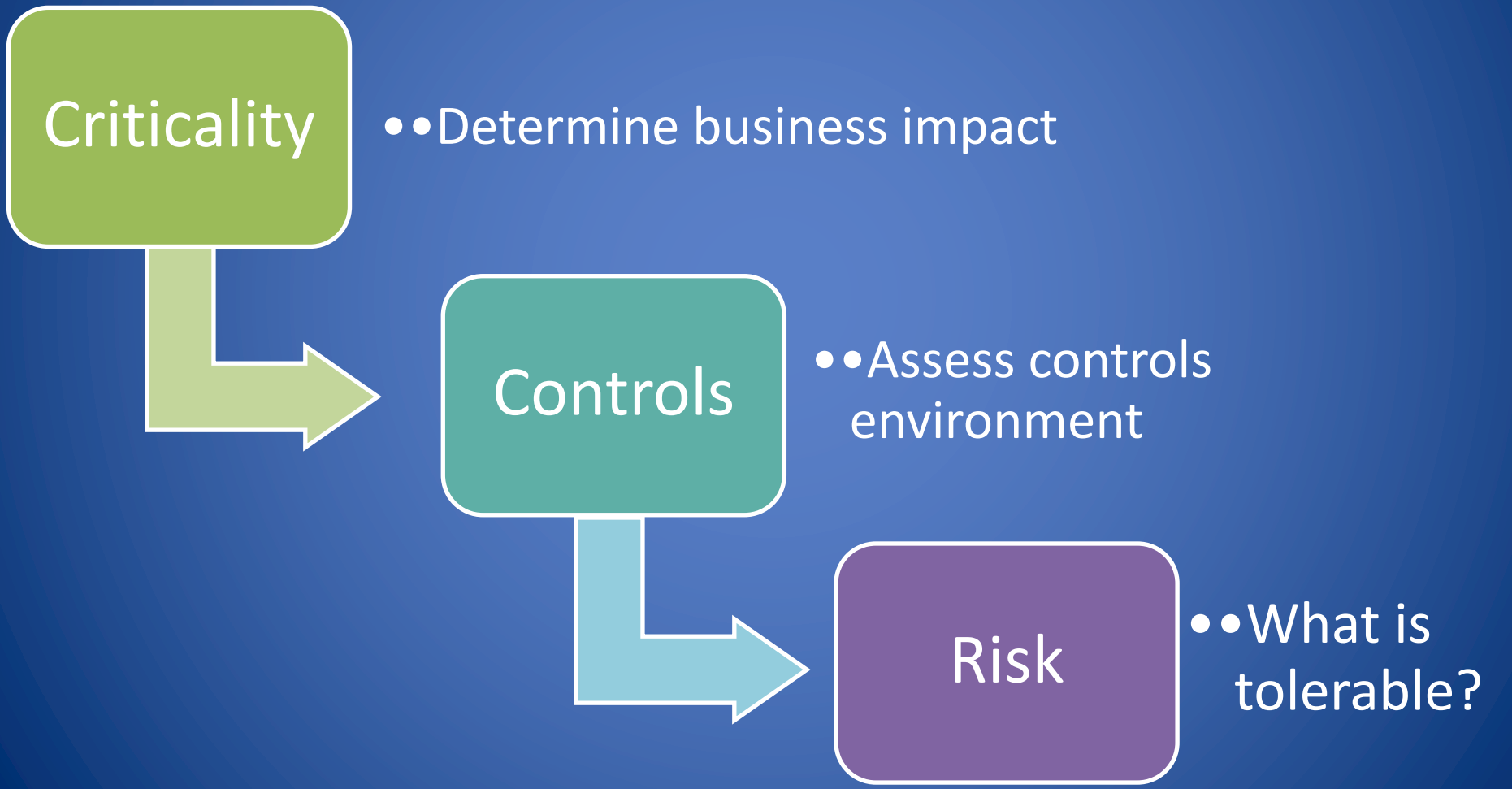
Why go to the Cloud?

- SCALABILITY
- AFFORDABILITY
- ACCESSIBILITY
- VARIETY
- SECURITY…?

The Cloud environment



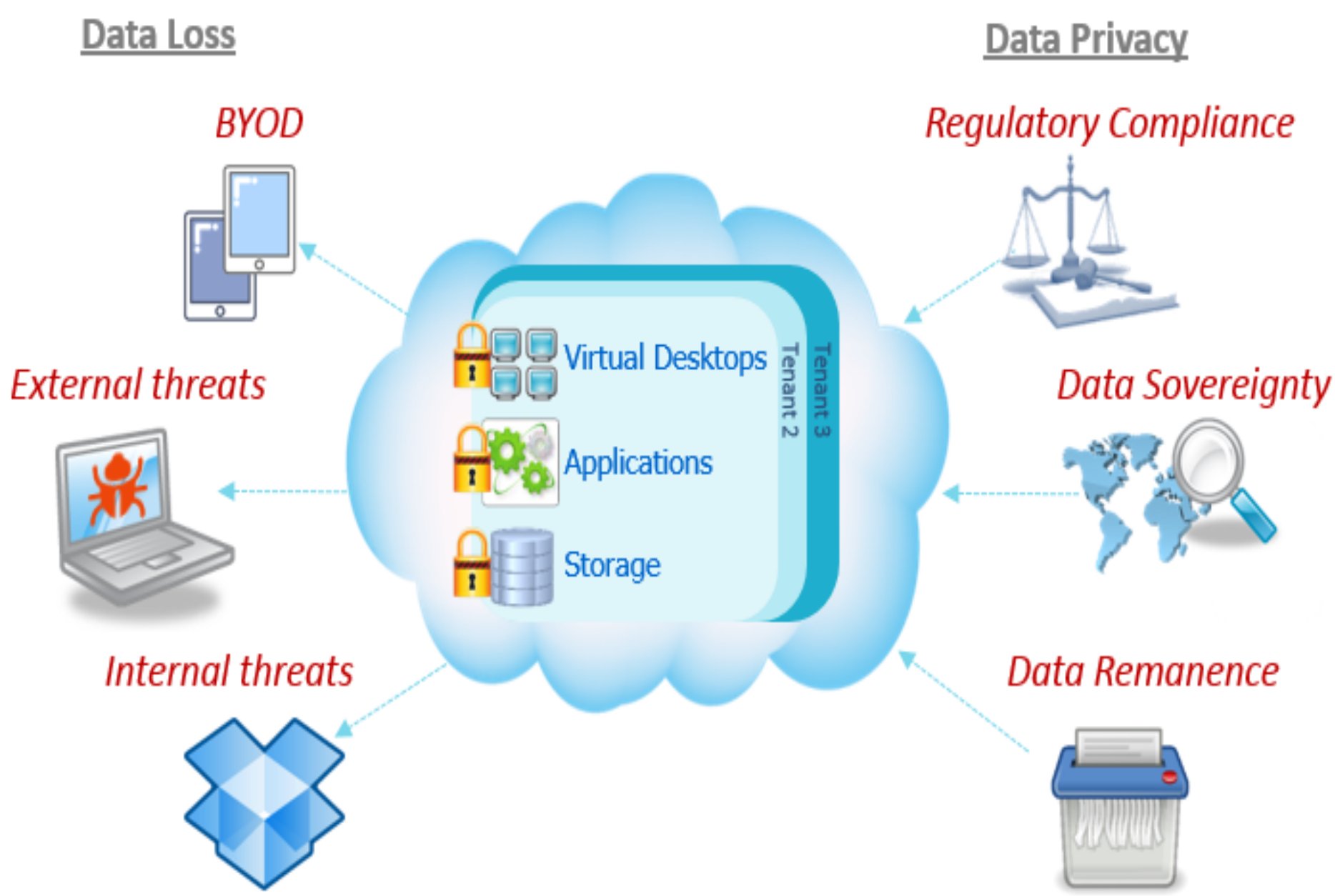
SECURITY RISK ASSESSMENT PROCESS



Risk Assessment Context

- Reliant on service for infrastructure controls
- Does the service meet security standards?
- How are we going to use the service?
- Privacy and Security Terms and Conditions

Securing Cloud Data



COMPLIANCE ASSURANCE

ISO 27001/2

ISO 27017

ISO 27018

NIST 800

SAS 70

PCI - DSS

SECURITY ISSUES

- Globalization of services
- Rapid change environment
- Complexity in Hybrid model
- Reliance on Public Network
- Lack of Contractual controls

THIS GUY!

Lessons Learned

- Team integration

  (#PrivacySecurity #StrongerTogether)
- Demand proof from Vendors
- Just cause they said it, doesn’t make it so!
- Get legal involved early and often

BRITISH COLUMBIA

THANKS FOR LISTENING

ANY Questions?