



CloudPathfinder

Pre-Reading Material

Information Pack for BC Gov Ministry Teams considering
Cloud

Updated
Sep 13, 2021

Topics

- 1. About BC Gov Cloud
- 2. SEA at BC Gov
- 3. Procurement Value Proposition
- 4. Shared Responsibility
- 5. Providing an SEA service
- 6. Contracting
- 7. Billing
- 8. Service Focus
- 9. Questions & Answers

What is BC Gov Cloud Pathfinder?

Acronyms

- GoC = Government of Canada
- CSP = Cloud Service Provider
- SEA = Secure Environment Accelerator, an AWS & GoC cloud multi-tenancy guardrail product

- We're a central team in BC Gov tasked with delivering Cloud
- We've onboarded to the GoC Cloud Brokerage
- We have a service order with 1 Cloud Service Provider that includes an SEA



Canada 



What is BC Gov Cloud Pathfinder?

Acronyms

- AWS = Amazon Web Services
- GoC = Government of Canada
- CSP = Cloud Service Provider

- We are on a mission to collaborate with the GoC to use several CSPs
- We want to offer a consistent service experience across several clouds; our on-prem OpenShift container platform, AWS, and others.
- Our clients are all Ministries in BC Government

 Canada

Customer Focus

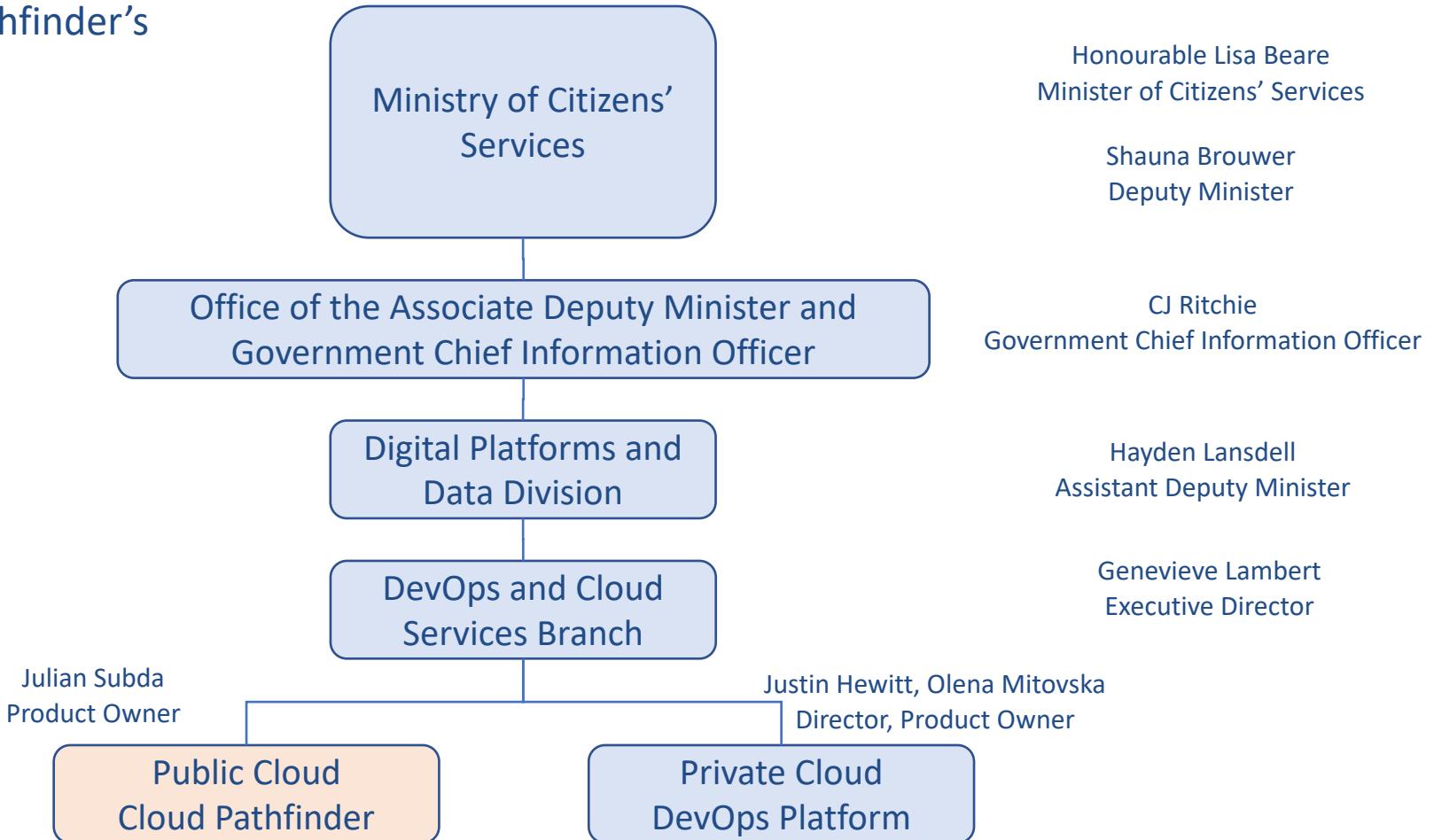
Acronyms

- OCIO = Office of the Associate Deputy Minister and Government Chief Information Officer
- SecOps = OCIO Security Operations Team

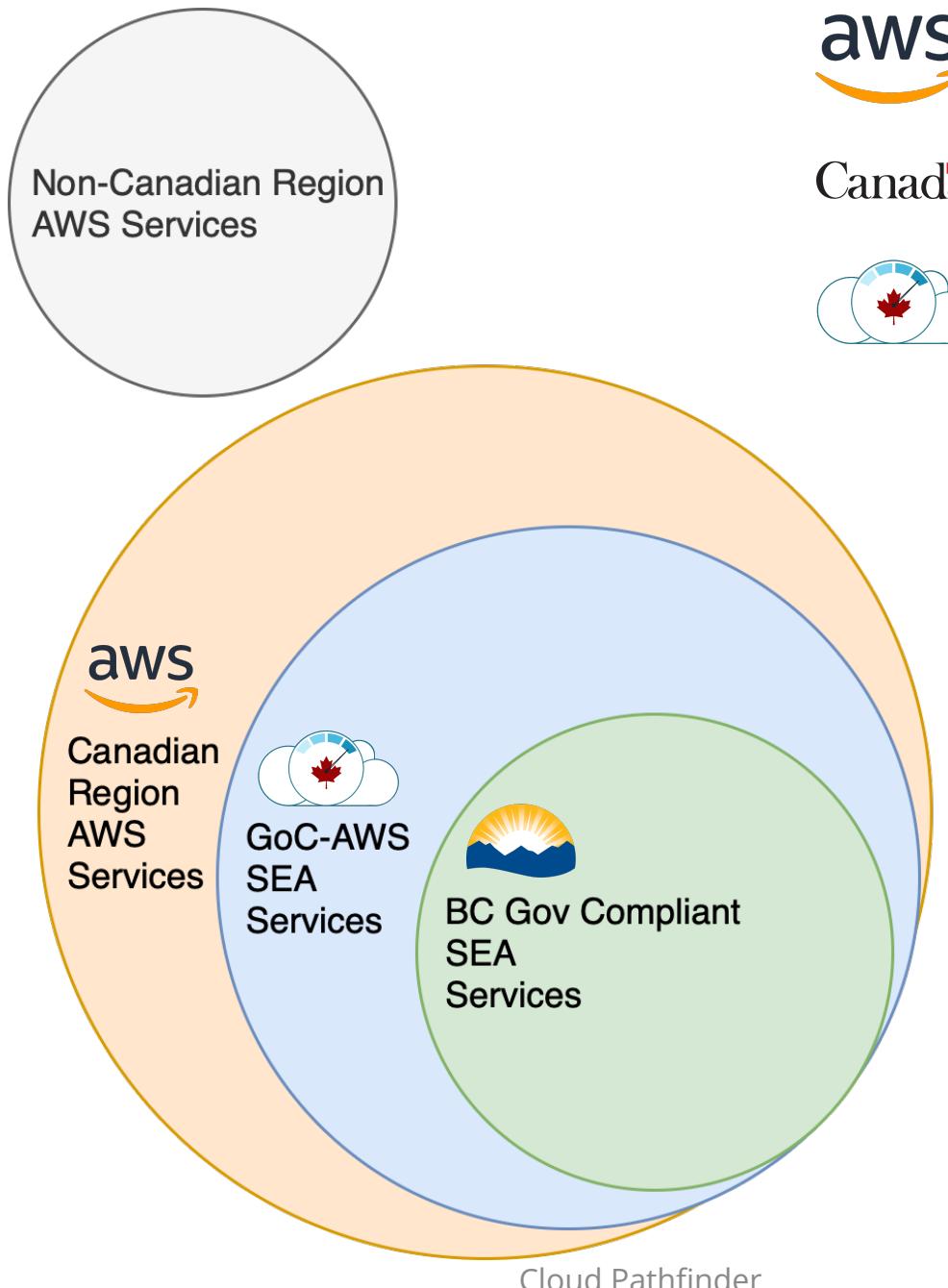
- Our Customers: Project Managers / Product Owners / Expense Authorities
- Our Users: Developer Teams
- Special Users: Security Operations OCIO

Good Service

Who do I go to if I have quality issues with Cloud Pathfinder's service?



BC Gov's SEA Cloud



AWS = Amazon Web Services Cloud

Out of the box "Vanilla" AWS account that anyone can buy

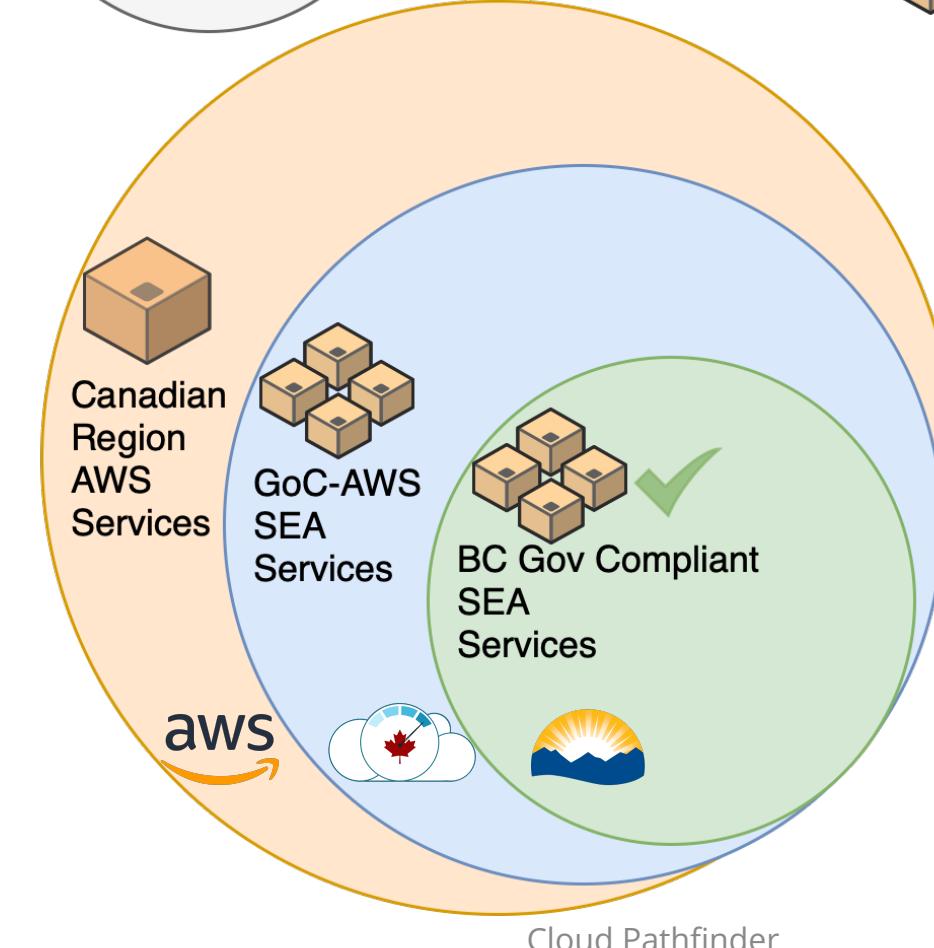
GoC = Government of Canada

Partnered with AWS to create the SEA

SEA = Secure Environment Accelerator

A software deployed virtual data centre in the cloud sitting in AWS space

SEA Concepts



AWS = Amazon Web Services Cloud

Out of the box "Vanilla" AWS account that anyone can buy

GoC = Government of Canada

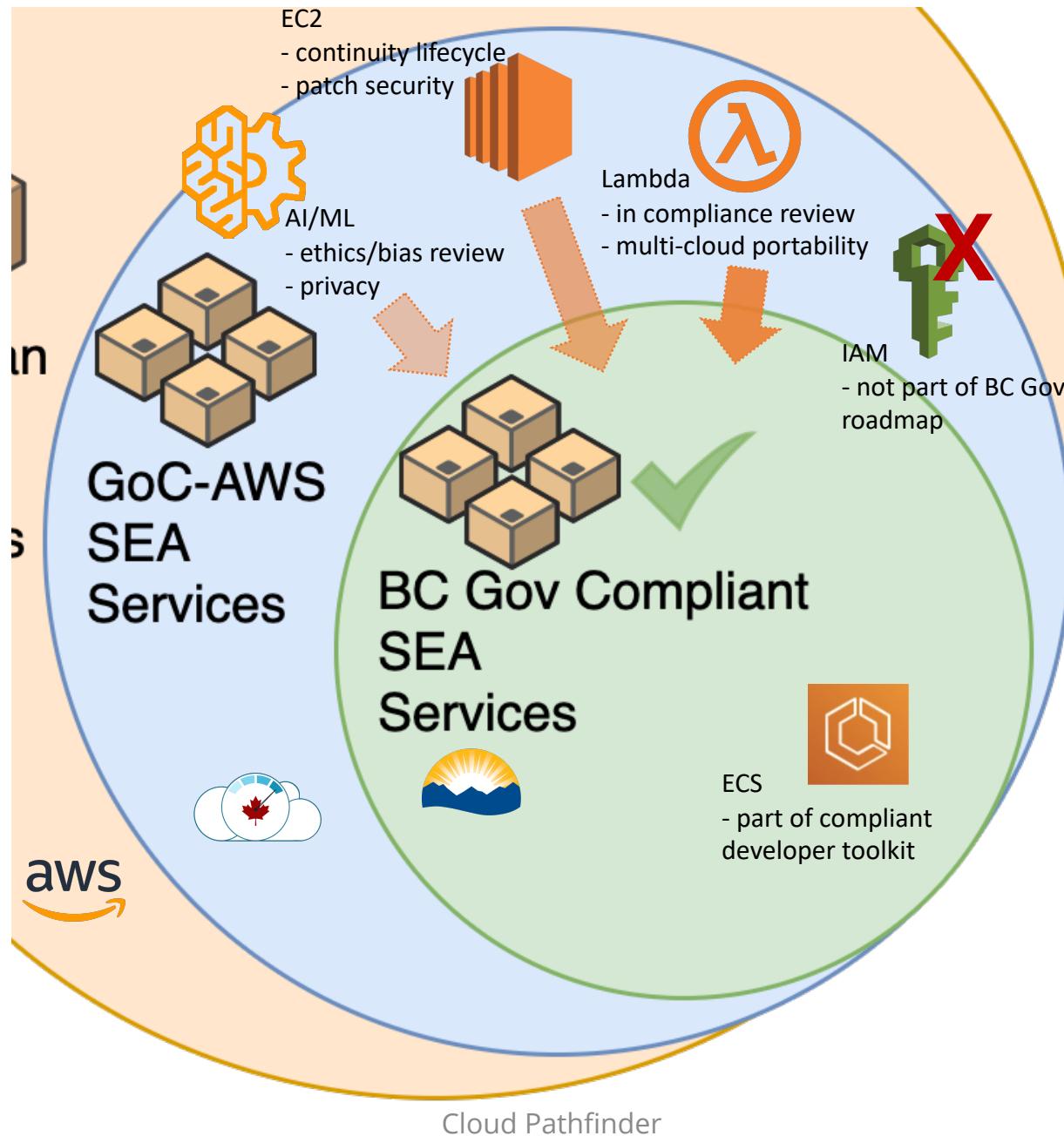
Partnered with AWS to create the SEA

SEA = Secure Environment Accelerator

A software deployed virtual data centre in the cloud sitting in AWS space



Compliant Services



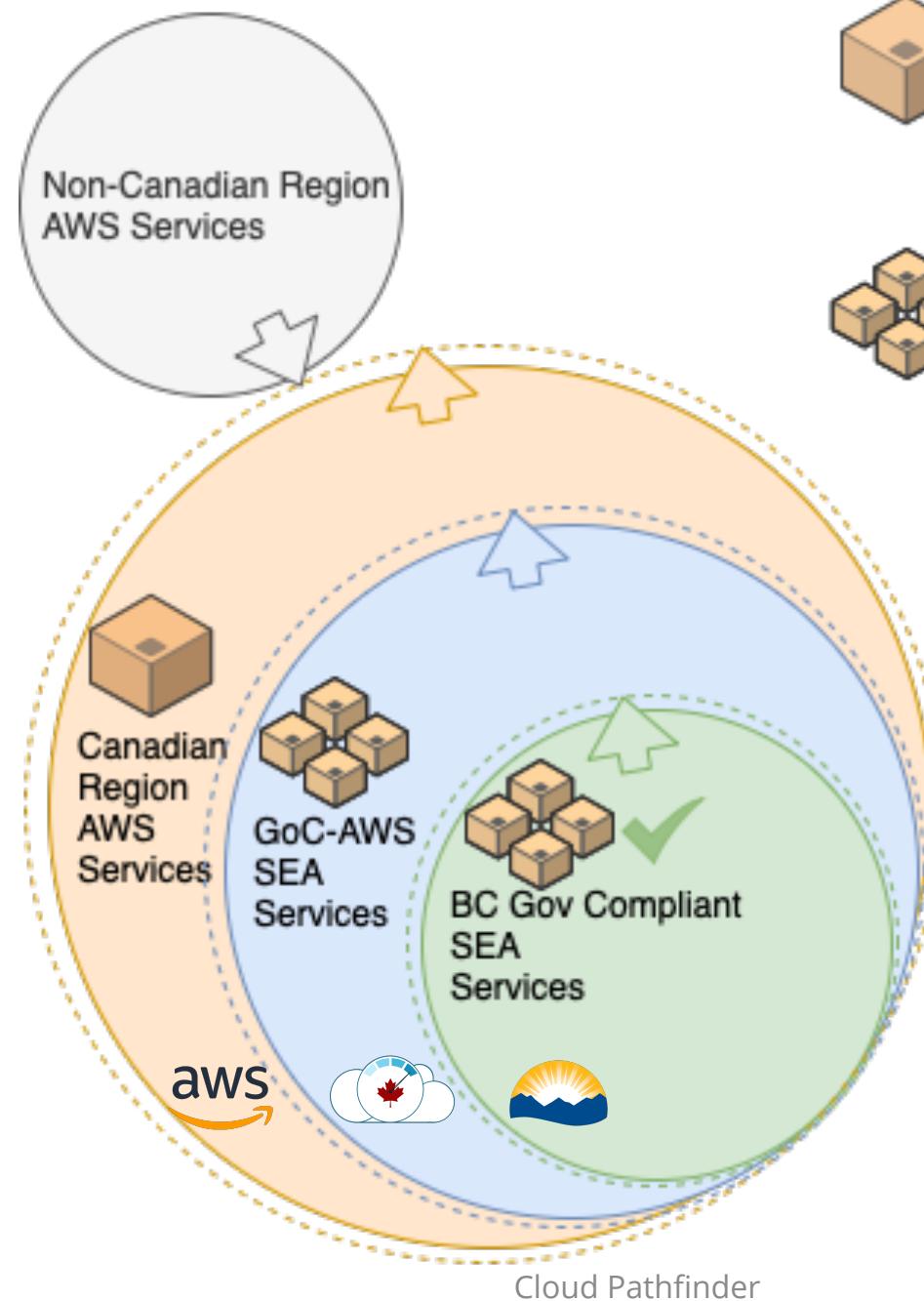
When? Estimates:

- 3 weeks - Lambda Serverless
- 3 months - EC2 VMs
- 6 months or more - AI/ML

Acronyms

- ECS = Elastic Container Service
- EC2 VMs = Elastic Compute Cloud Virtual Machines
- CSP = Cloud Service Provider
- Lamdas = a serverless technology where code is run on CSP maintained servers, turned off when not in use
- IAM = Identity Access Management of users in the CSP
- AI/ML = Artificial Intelligence and Machine Learning cloud services

SEA Future Growth



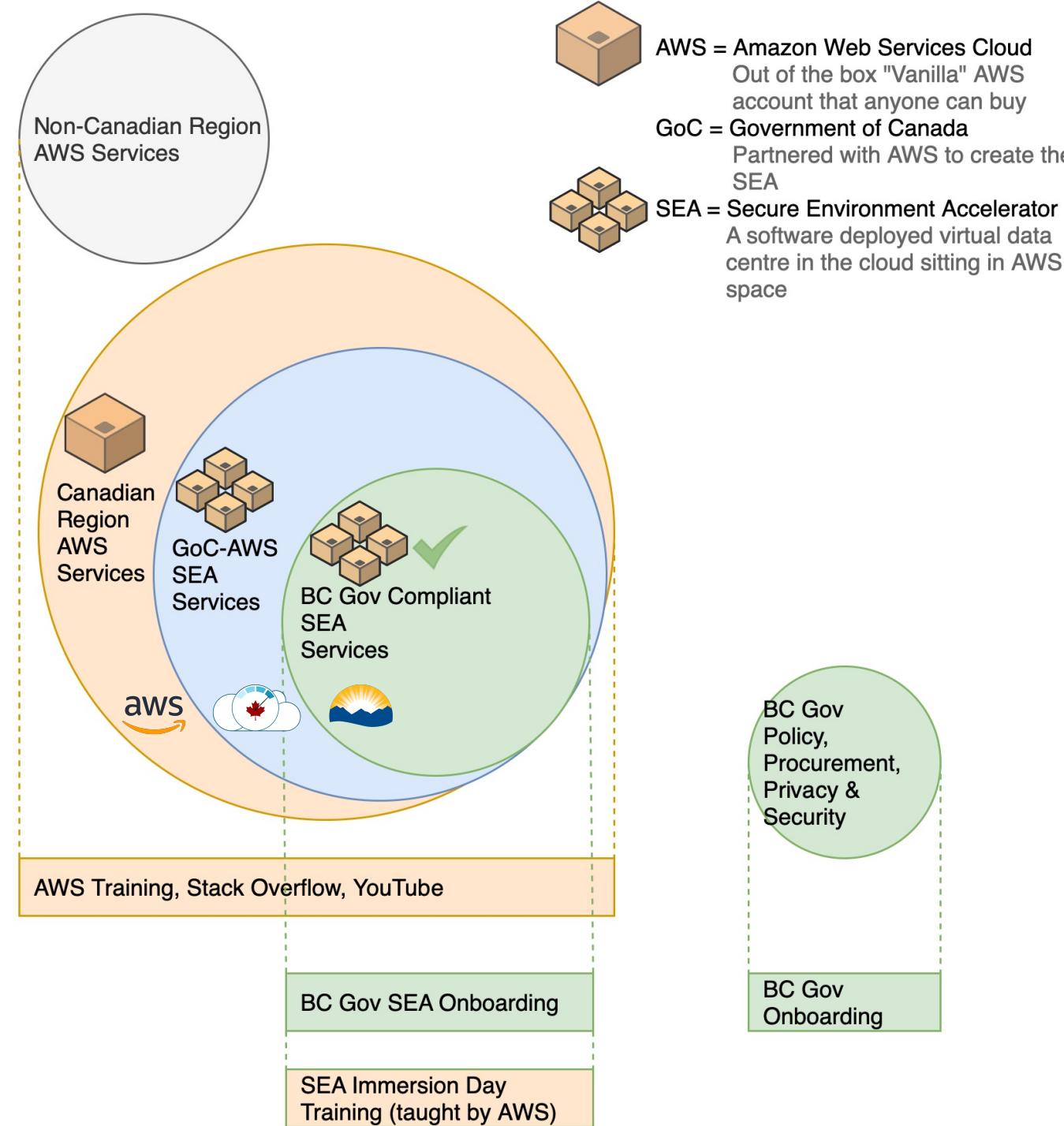
AWS = Amazon Web Services Cloud
Out of the box "Vanilla" AWS account that anyone can buy



GoC = Government of Canada
Partnered with AWS to create the SEA

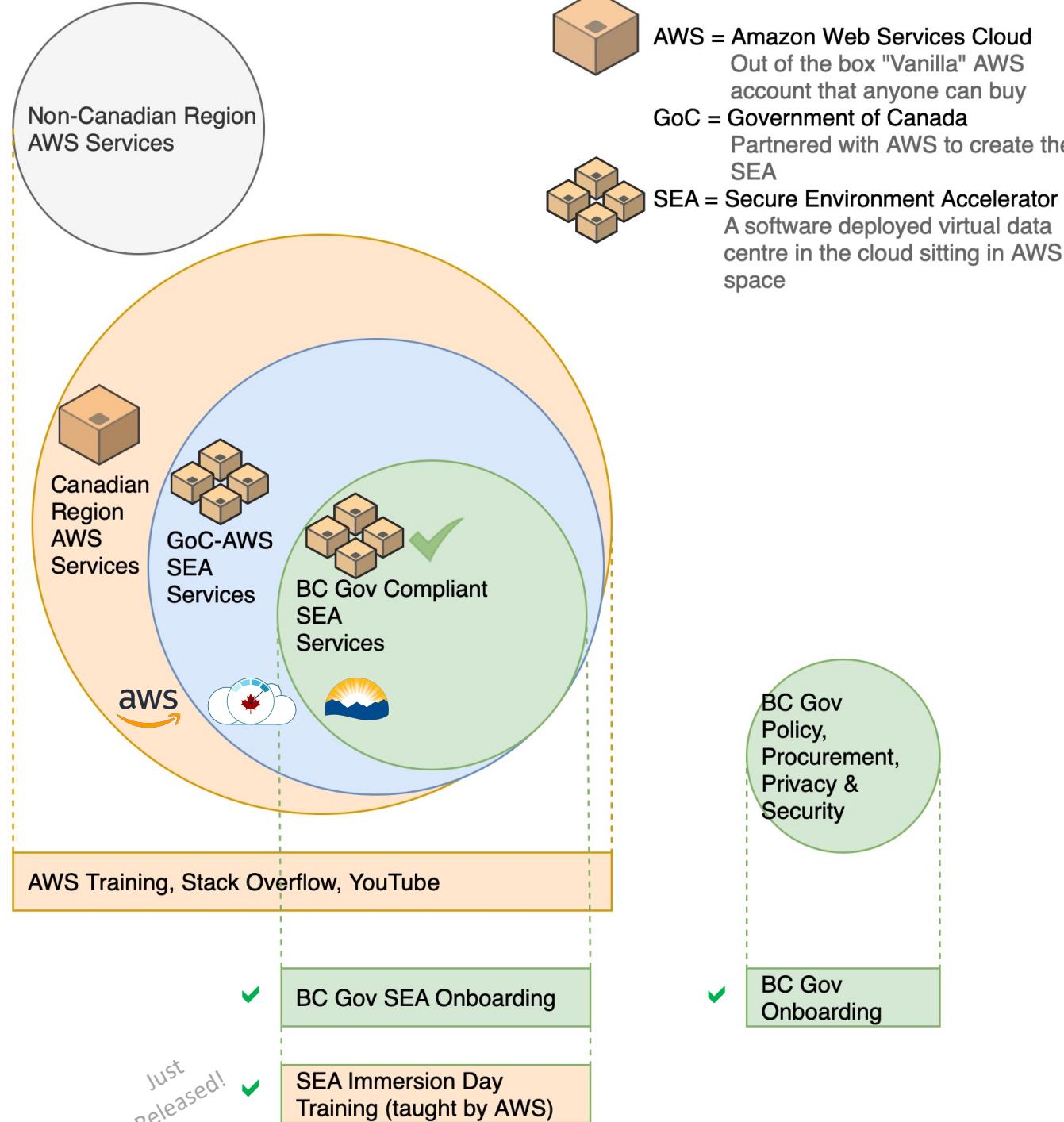
SEA = Secure Environment Accelerator
A software deployed virtual data centre in the cloud sitting in AWS space

Training Landscape



Training Components

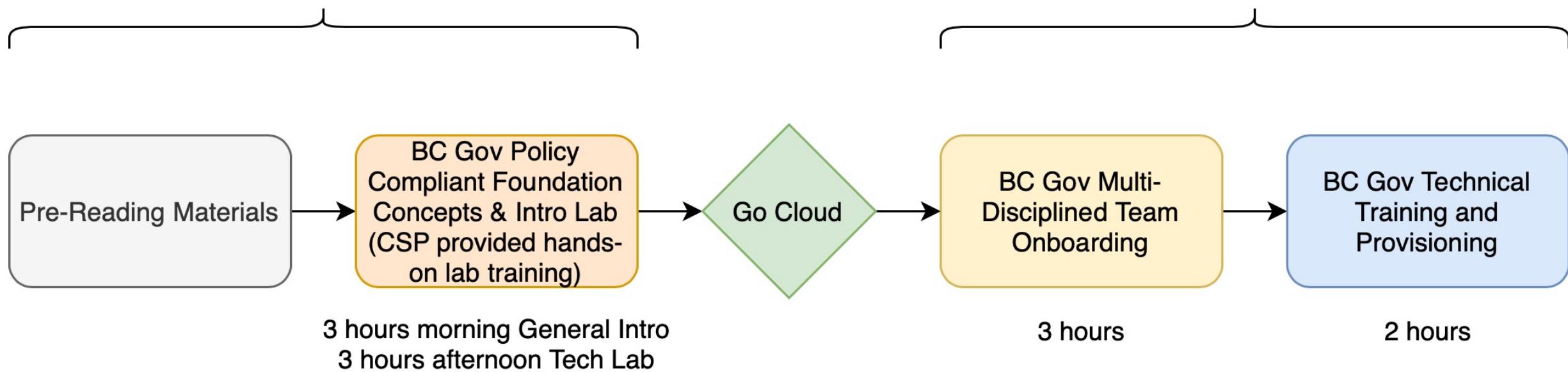
Avoid,
Lacks
SEA



Training Track

Before a team decides on Cloud

After a team decides on Cloud



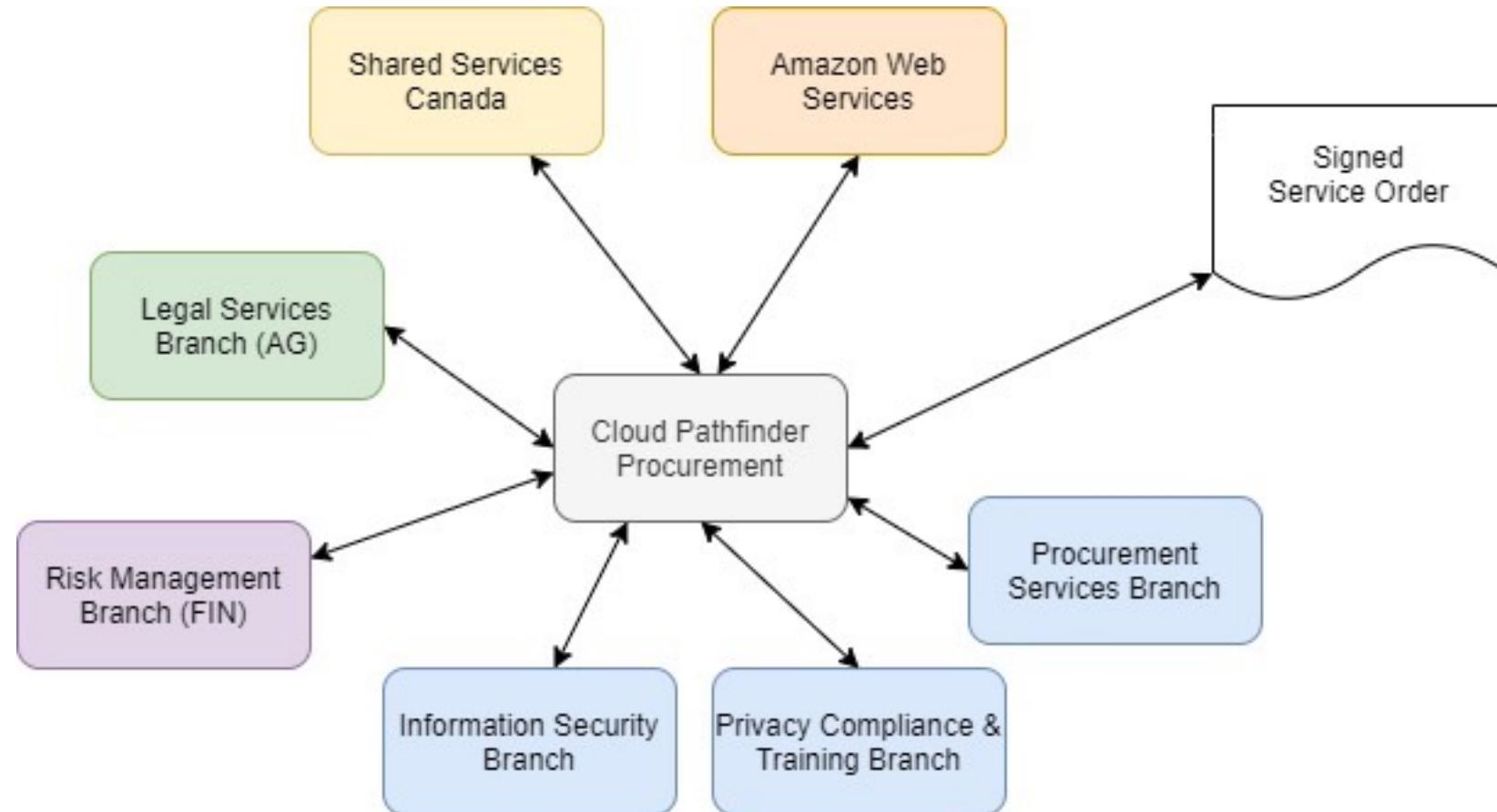
Audience

- POs, Devs and Compliance; group start
- Shared understanding from the beginning
- Journey together

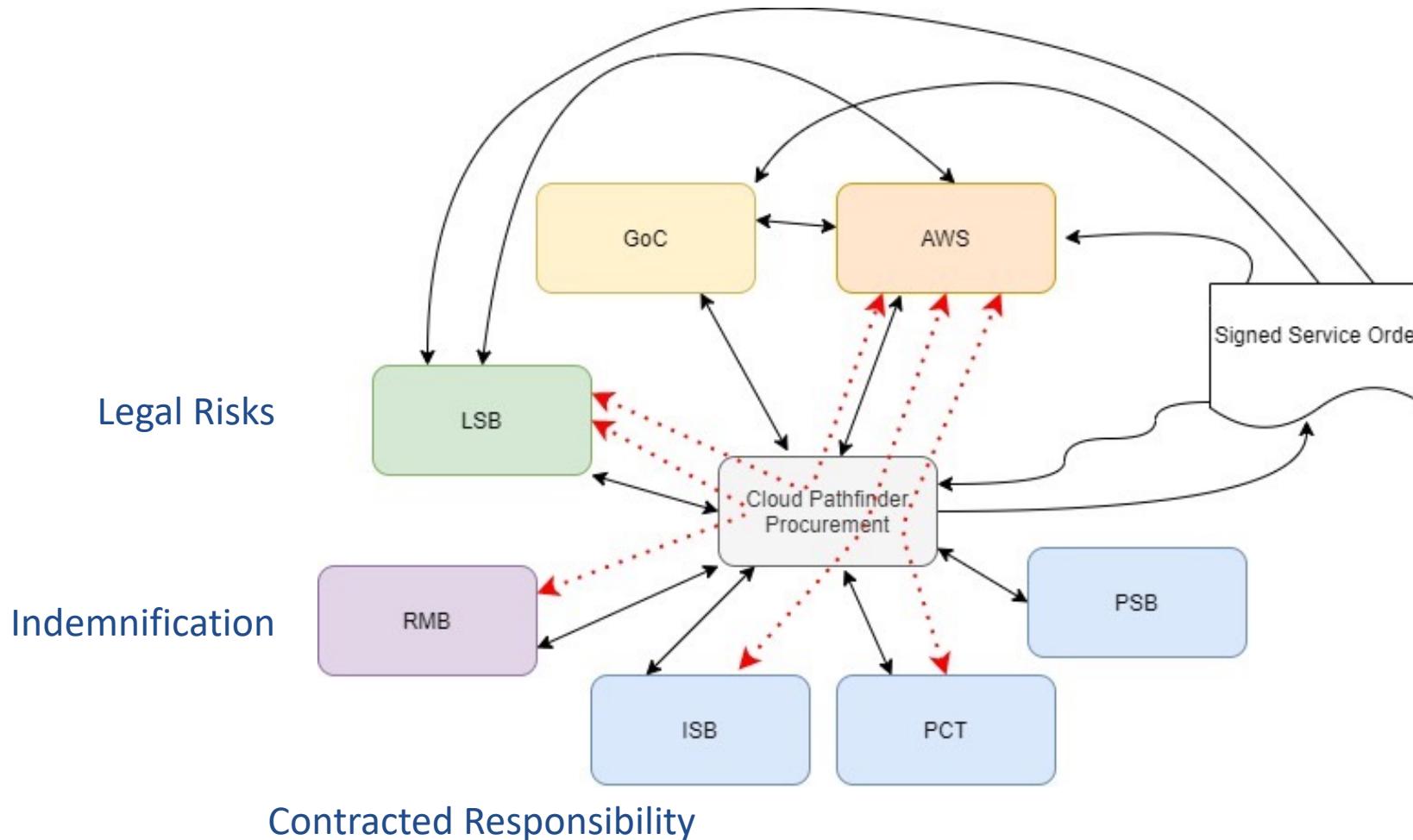


Image credit to [Creative Commons](#)

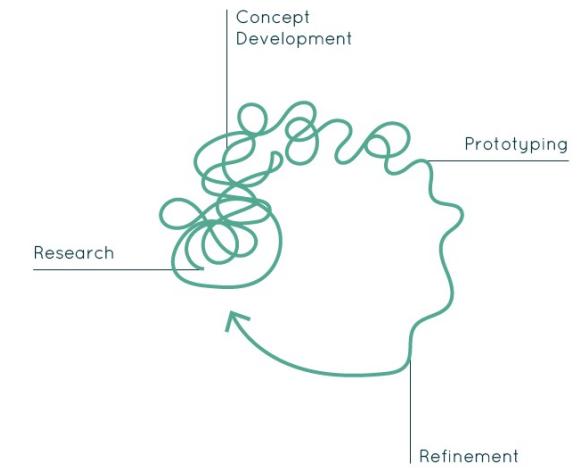
Negotiation of our First Service Order



Actually, it went more like this



- Government of Canada
- Amazon Web Services
- Procurement services Branch
- Legal Services Branch
- Risk Management Branch
- Information Security Branch
- Privacy Compliance & Training



Procurement Value Add for Ministries

Don't have to
negotiate privacy,
security, legal
terms with
vendors

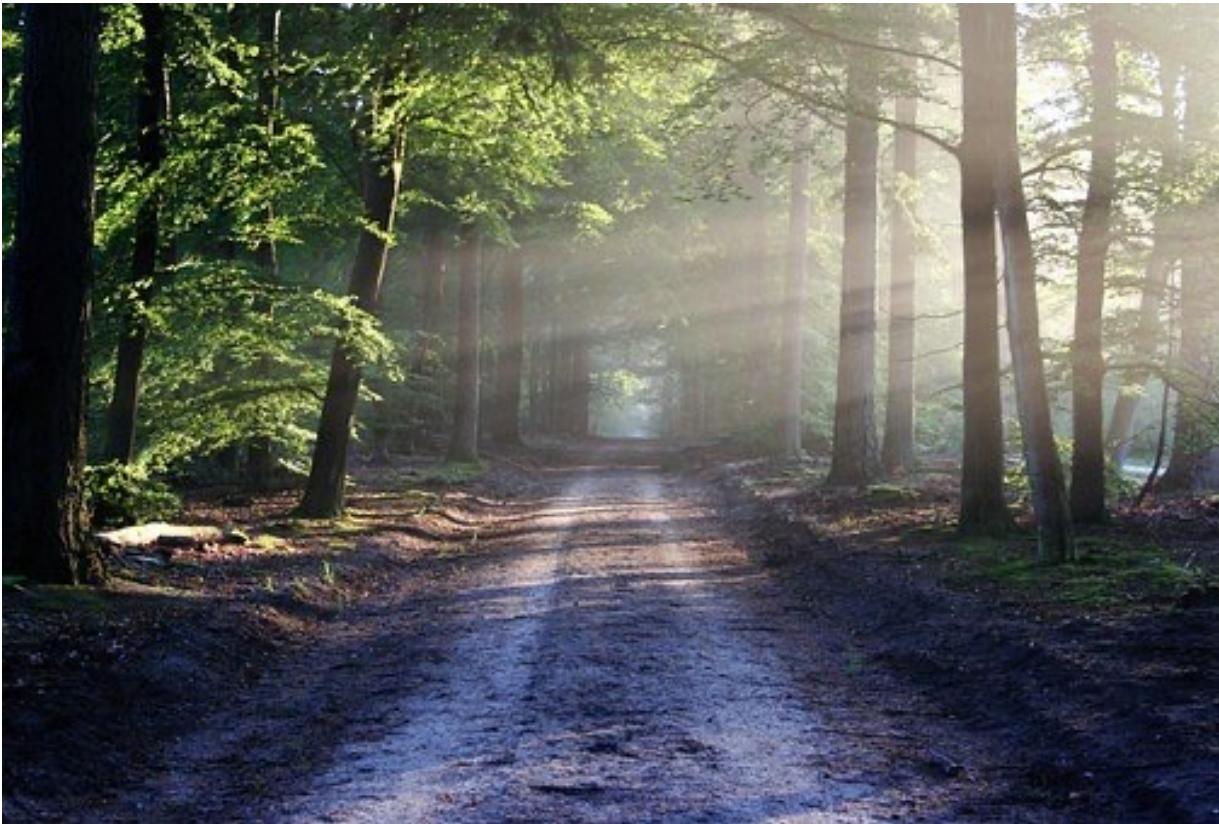
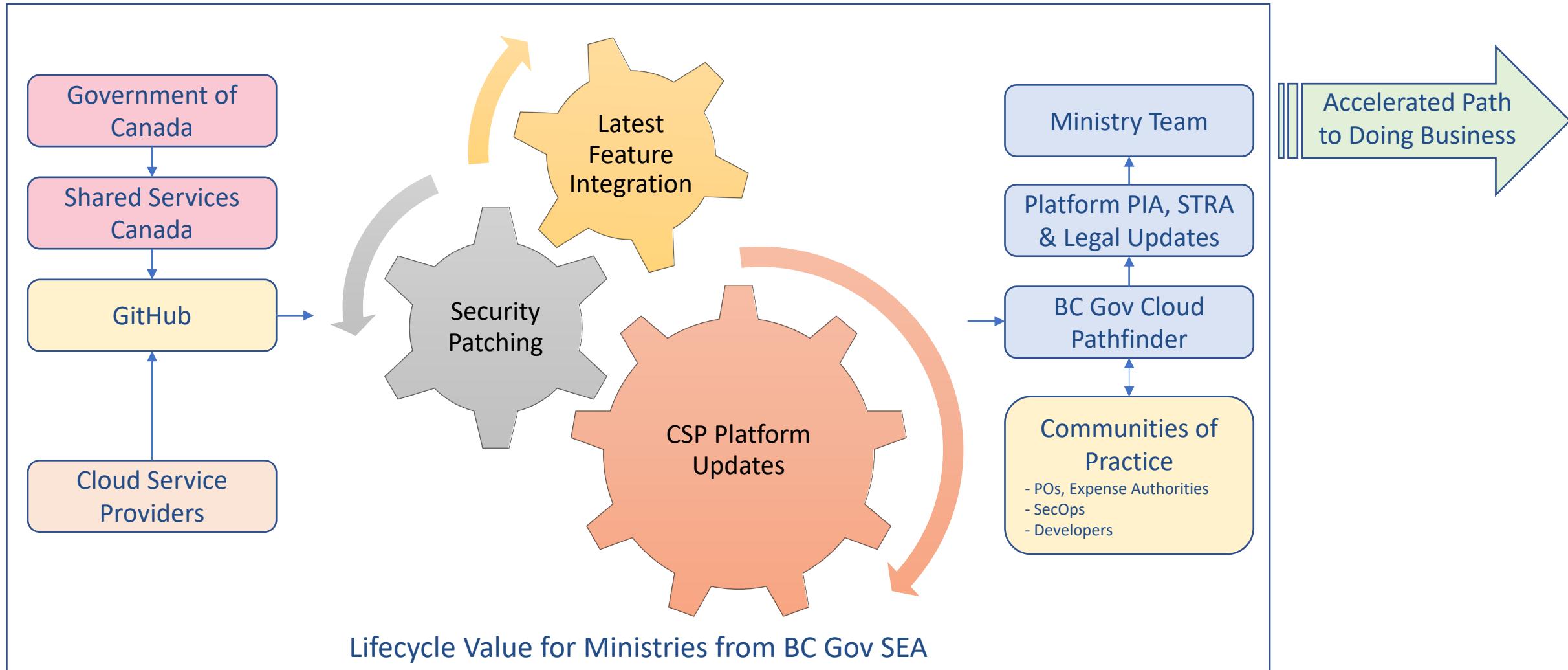


Image credit to [pixabay](#)

Don't have to dig
into the cloud
services

Only need to
focus on
describing their
project in the PIA
and STRA

Cloud Lifecycle Value Add for Ministries



Shared Responsibility Model

Teams	Contracts & Billing	Security & Privacy	Technology Stack
Ministry Teams - Applications & Data	<ul style="list-style-type: none"> Apply Financial Controls, monitor costs, pay for resources used Contract for development, with cloud security schedule + privacy schedule 2nd stage procurement or process to justify selection of cloud service provider 	<ul style="list-style-type: none"> App-specific Security & Access Management, logging, incident response, protection of data in transit and at rest STRA & SOAR for application and any 3rd party tools Ministry Program PIA Information Management as per CPPM Ch 12 	<ul style="list-style-type: none"> Manage Application Lifecycle Code Management (GitHub) Build & Deploy Pipelines Support app and any 3rd party tools Backup and restore DR plan and test
Communities of Practice - DevOps Commons, others	Regular cadence of meetings, support from members of teams that are on the same journey, curated vendor and product introductions and updates, highlighting of well aligned teams and their best practices		
Public Cloud Accelerator Service Team (and service delivery partners) - Corporate Services & Governance	<ul style="list-style-type: none"> Parse CSP bills to provide bills to ministries. Establish governance framework for admin access to accounts, billing, monitoring (including visibility into costs), audit-ability. <p>Automate policy and standards compliance as much as possible - includes platform security (and patching) above the virtualization layer</p> <ul style="list-style-type: none"> 1st stage procurement, negotiation of contracts, to establish CSA or similar Cloud Security and Privacy Schedules for inclusion in contracts 	<ul style="list-style-type: none"> Corporate PIA for cloud service types, for each CSP Corporate STRA for each CSP Centralized logging Platform level incident response & investigation 	<ul style="list-style-type: none"> Ordering & Provisioning Infrastructure Manage catalogue(s) of compliant cloud services (initially compute and storage) Develop library of scripts for automated provisioning of cloud infrastructure
Cloud Service Provider - Data Centre Security and Reliability	<ul style="list-style-type: none"> Provide tools for monitoring and reporting on resources used Offer a selection of pricing models (reserved instances, saving plans ...) -> bill for consumption 	<ul style="list-style-type: none"> Security (including patching) of everything up to and including the virtualization layer Compliance with industry standards: FedRAMP; EU/US Privacy Shield; ISO 9001, 27001, 27017, 27018 ... 	<ul style="list-style-type: none"> Compute Storage Network
			<ul style="list-style-type: none"> Data Centre Operations Hardware Infrastructure - Regions, Availability Zones, Edge Locations

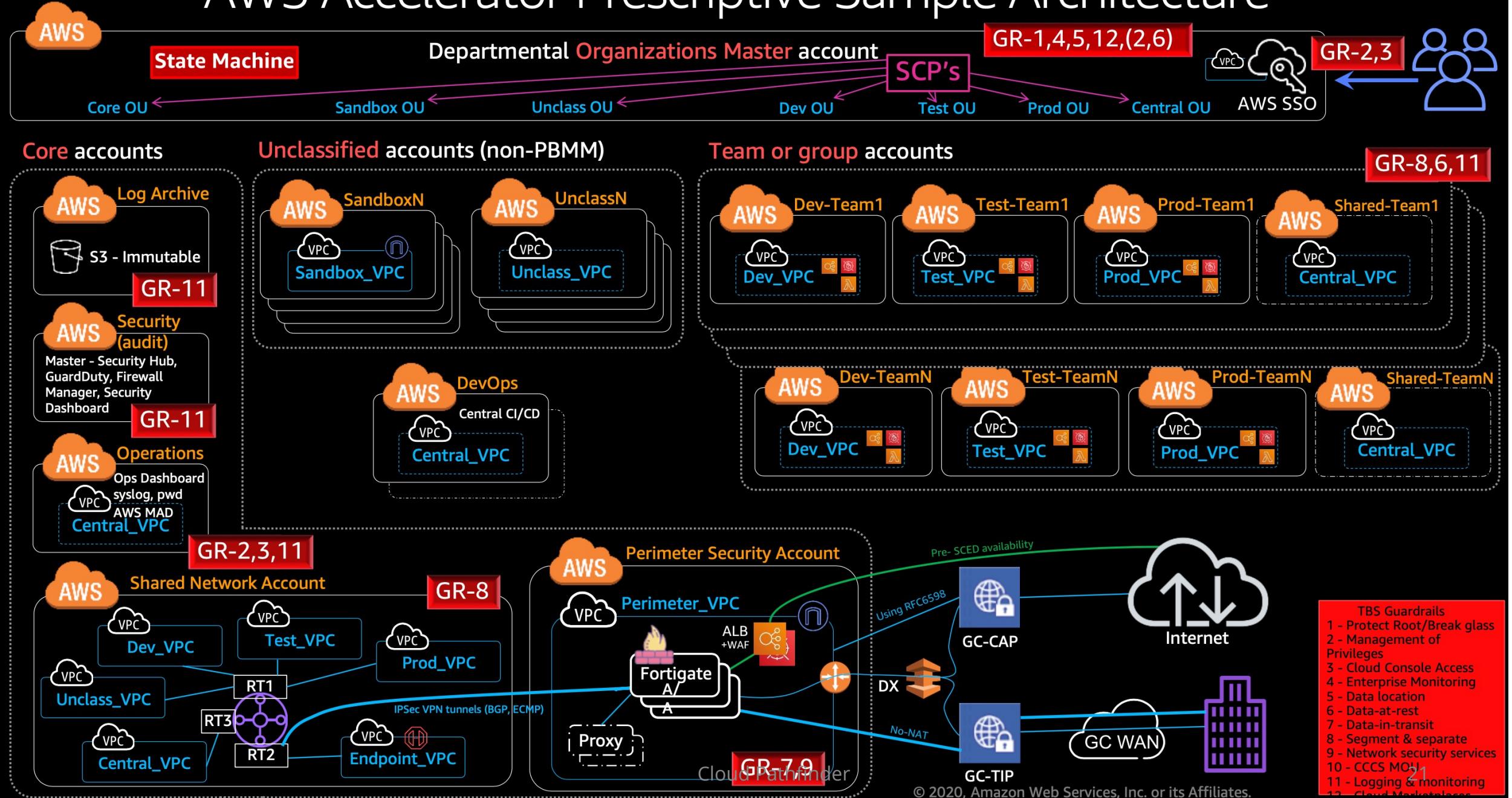
The SEA is non-trivial

- There is a lot of complexity that is simplified by Cloud Pathfinder providing SEA as a service to Ministries
- Several thousand dollars per month to run empty
- Requires a full-time highly-skilled team to stay on top of it

The next two slides show this...

AWS Accelerator Prescriptive Sample Architecture

v1.2a



Glossary

- ProServe = AWS Professional Services, a paid formal engagement
- LZ = Landing Zone
- GoC = Government of Canada
- CP – Cloud Pathfinder

Cloud Pathfinder - Easiest Path Report (Cloud 1 AWS)

Ministries Alone

Custom ProServe

Control Tower

SEA

High

Effort

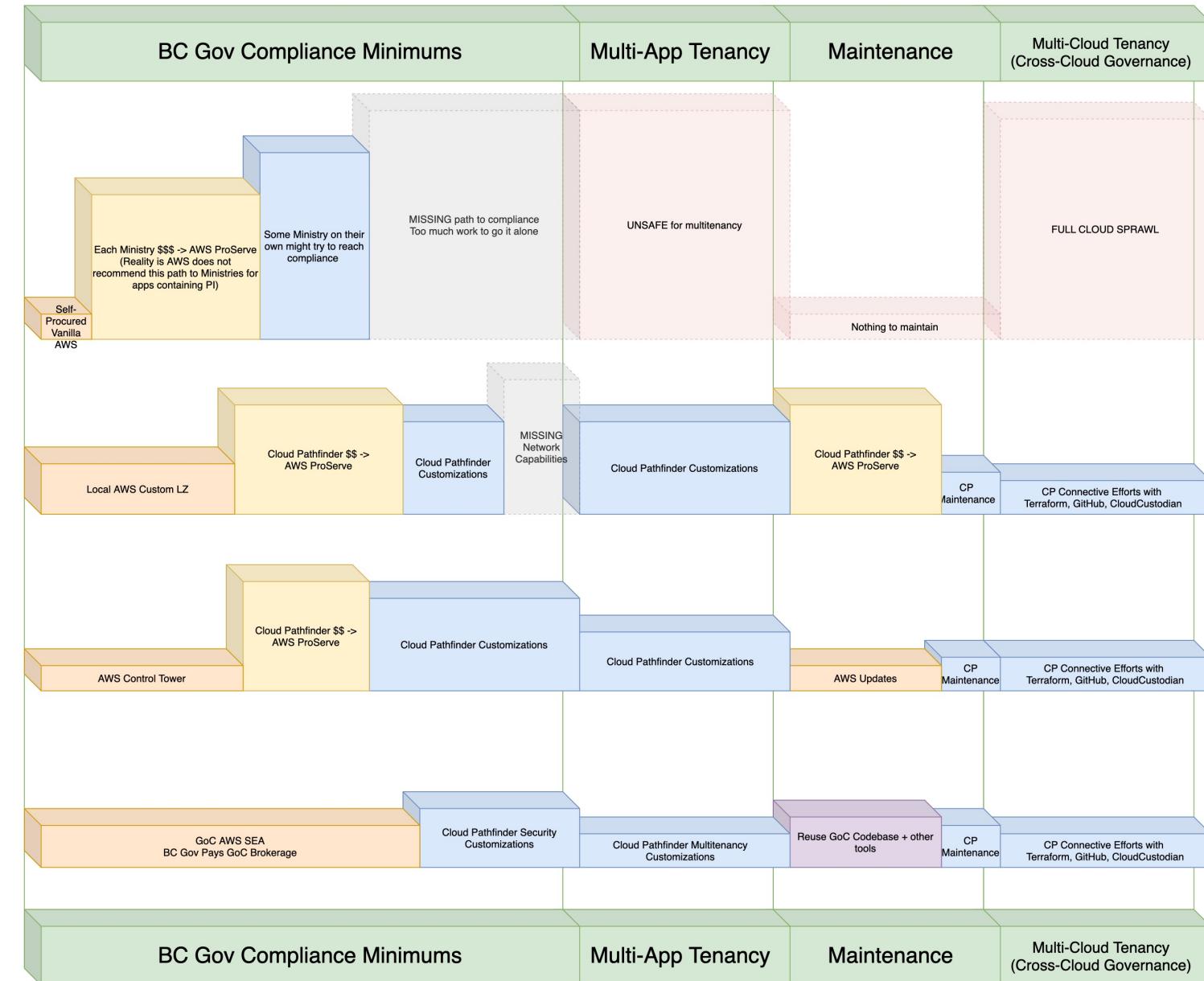
Low

Worst

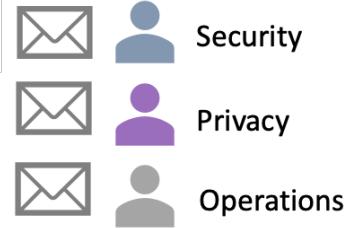
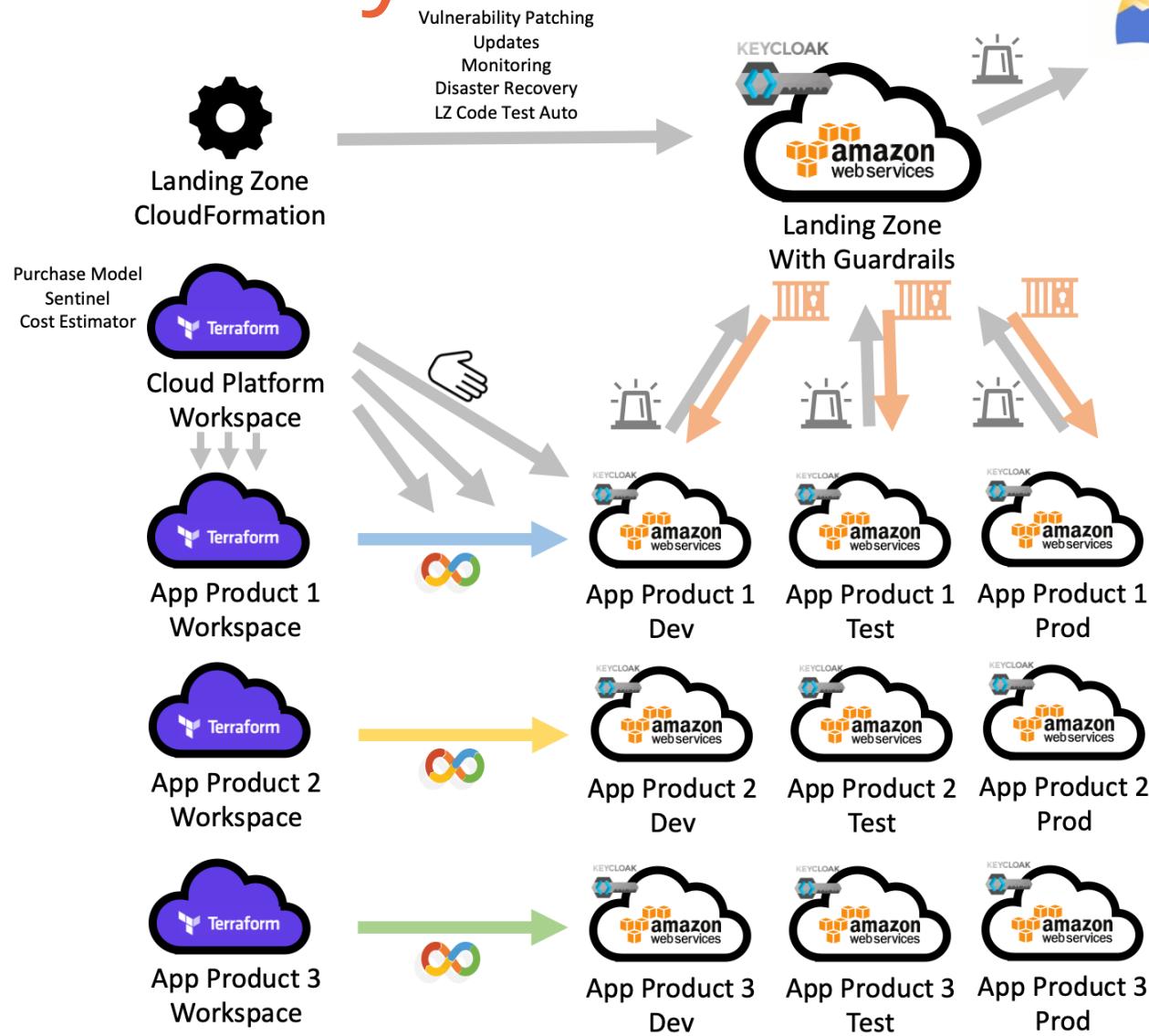
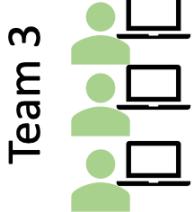
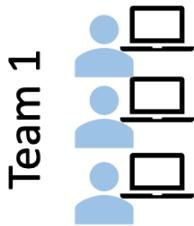
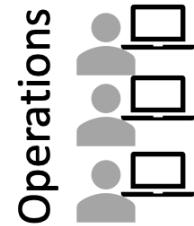
Third

Second

Best

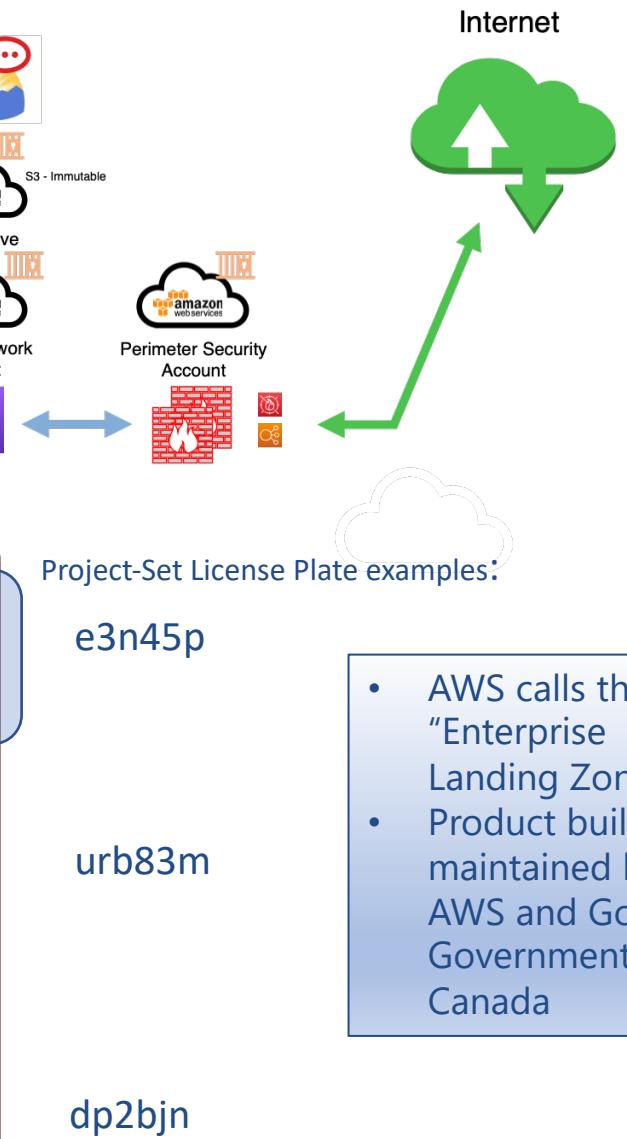
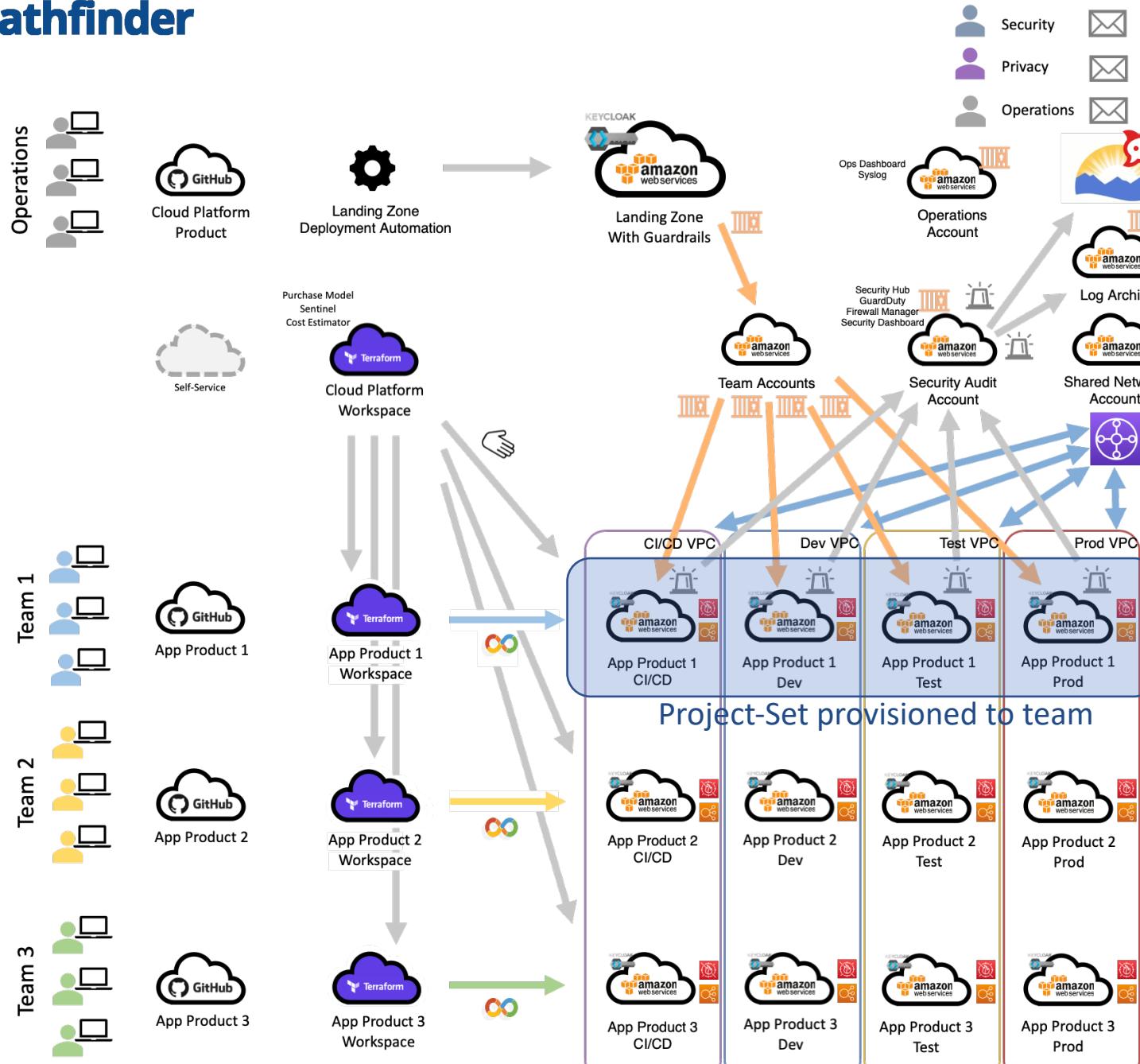


BC Gov AWS Early Version



- AWS calls this a “Lightweight Landing Zone”
- Product Custom built by AWS Professional Services “ProServe”

BC Gov AWS SEA



Glossary

- ProServe = AWS Professional Services, a paid formal engagement
- LZ = Landing Zone
- GoC = Government of Canada
- CP – Cloud Pathfinder

Ministries Alone

High

Effort

Low

Custom ProServe

Worst

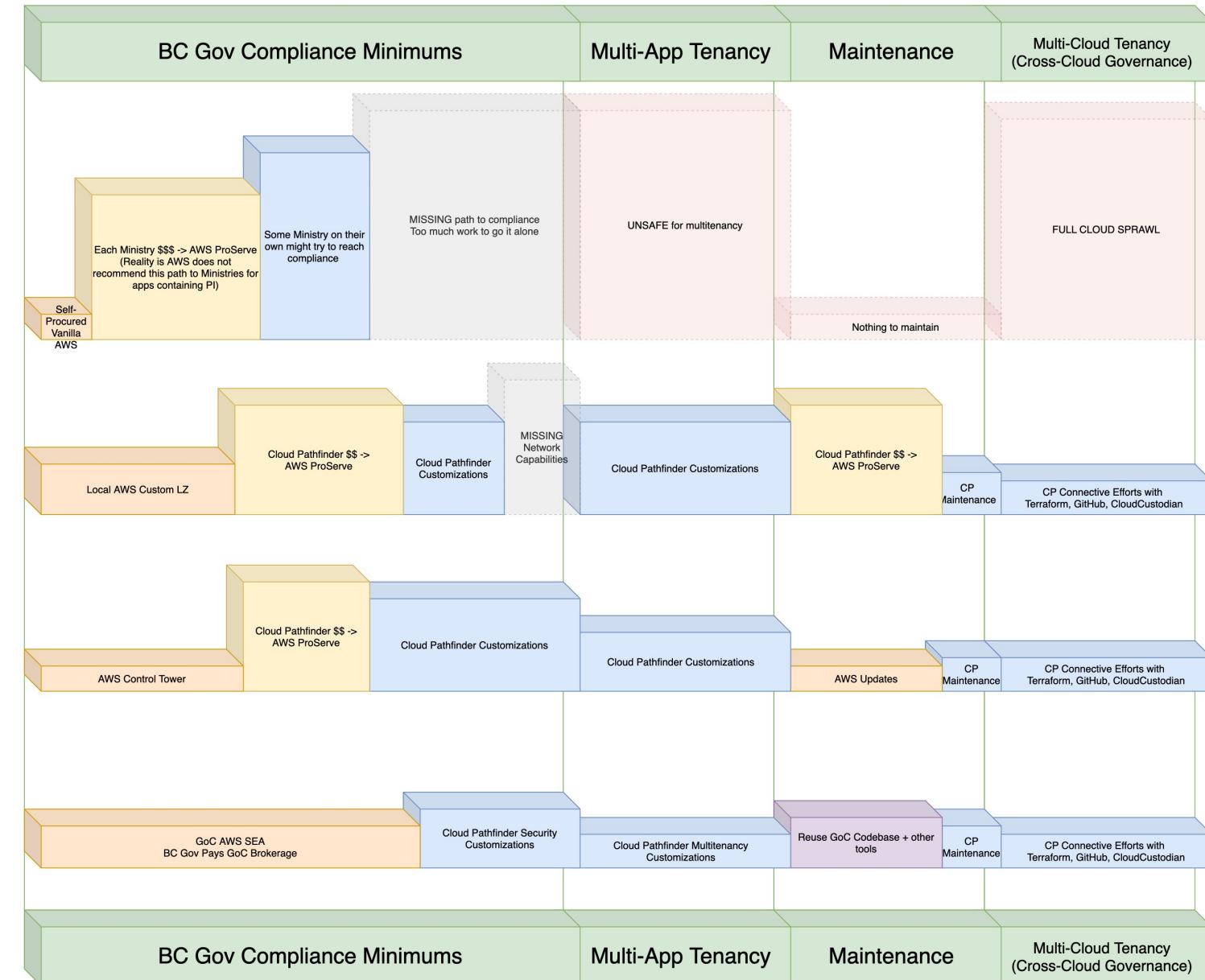
Third

Second

Best

Control Tower

Cloud Pathfinder - Easiest Path Report (Cloud 1 AWS)





Billing Examples T-Shirt Estimates

AWS Services*	T-Shirt Estimate Scenario 1 - Small	
	Metrics	Estimated Expense / Month
Traffic	25 visitors a day	
Amazon Simple Storage Service	80 GB	\$2.00
Elastic Load Balancer	300KB/second/client connection	\$25.00
Amazon DynamoDB	1GB, 1 million requests	\$4.00
Elastic Container Service - Fargate	1 container deployed twice, each 2 vCPU, 4GB	\$48.39
Data Transfer Out	50GB	\$4.50
Amazon CloudWatch Logs	50 GB	\$28.00
AWS SEA Services (*)	Amazon GuardDuty, AWS Config, KMS	\$40.00
Estimated Monthly Total		\$129.14

ALB: 1.08GB/hr,
 25connections/sec, 2min
 duration,1 request per second

Factor in backups, cold storage, dev & test environments which will increase costs depending on how far a team chooses to implement.



Billing Examples T-Shirt Estimates

AWS Services*	T-Shirt Estimate Scenario 2 - Medium	
	Metrics	Estimated Expense / Month
Traffic	250 visitors a day	
Amazon Simple Storage Service	800 GB	\$20.00
Elastic Load Balancer	300KB/second/client connection	\$88.00
Amazon DynamoDB	10GB, 10 million requests	\$18.00
Elastic Container Service - Fargate	3 containers deployed twice, each 2 vCPU, 4GB	\$145.16
Data Transfer Out	500GB	\$45.00
Amazon CloudWatch Logs	500GB	\$278.00
AWS SEA Services (*)	Amazon GuardDuty, AWS Config, KMS	\$40.00
Estimated Monthly Total		\$634.16
ALB: 10.8gb/hr, 250connections/sec, 2min duration,10 request per second		

Factor in backups, cold storage, dev & test environments which will increase costs depending on how far a team chooses to implement.



Billing Examples T-Shirt Estimates

AWS Services*	T-Shirt Estimate Scenario 3 - Large	
	Metrics	Estimated Expense / Month
Traffic	2500 visitors a day	
Amazon Simple Storage Service	8,000 GB	\$200.00
Elastic Load Balancer	300KB/second/client connection	\$712.00
Amazon DynamoDB	100GB, 100 million requests	\$178.00
Elastic Container Service - Fargate	3 containers deployed twice, each 2 vCPU, 4GB	\$145.16
Data Transfer Out	5000GB	\$450.00
Amazon CloudWatch Logs	5000GB	\$2,775.00
AWS SEA Services (*)	Amazon GuardDuty, AWS Config, KMS	\$40.00
Estimated Monthly Total		\$4,500.16
ALB: 10.8gb/hr, 250connections/sec, 2min duration,10 request per second		

Factor in backups, cold storage, dev & test environments which will increase costs depending on how far a team chooses to implement.

Custom cost examples?

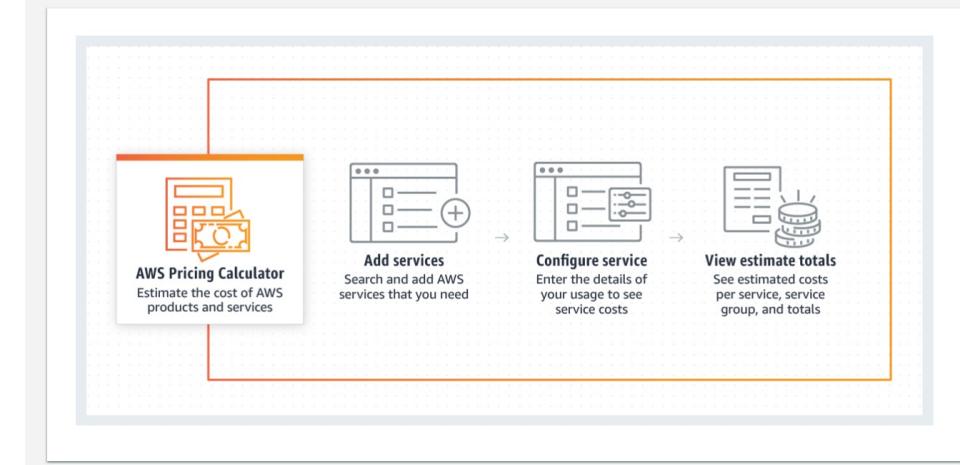
- Yes!
- <https://calculator.aws> for now

AWS Pricing Calculator

Estimate the cost for your architecture solution.

Configure a cost estimate that fits your unique business or personal needs with AWS products and services.

How it works



Billing Process Example

- These are samples of periodic billing report files we generate for Ministry Teams

	A	B	C	D	E	F	G	H	I	J	K	L
1	year	month	line_item_usage_account_id	Account_Name	Project	License_Plate	Environment	Billing_Group	Owner Name	Owner Email	line_item_product_code	line_item_blended_cost
2	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AWSCloudTrail	0.0409165
3	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AWSecretsManager	0.00002
4	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AWSecurityHub	3.782
5	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AmazonCloudWatch	0.00800433
6	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AmazonEC2	6.160000477
7	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AmazonGuardDuty	0.49761076
8	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AmazonMacie	0.01644
9	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				AmazonS3	0.016365968
10	2021	5	klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS				awskms	0.506306879
11	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AWSCloudTrail	0.03174
12	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AWSConfig	0.204
13	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AWSecretsManager	0.00002
14	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AWSecurityHub	3.858
15	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AmazonCloudWatch	3.4735E-06
16	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AmazonGuardDuty	0.49386712
17	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AmazonMacie	0.01644
18	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				AmazonS3	0.001437369
19	2021	5	shared-services	Landing Zone Core	shared-services	Core	SEA Core				awskms	0.167749424
20	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AWSCloudTrail	0.043608
21	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AWSConfig	0.024
22	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AWSecretsManager	0.00002
23	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AWSecurityHub	4.313
24	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AmazonCloudWatch	0.008591734
25	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AmazonEC2	6.160000699
26	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AmazonGuardDuty	0.538942
27	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AmazonMacie	0.05932
28	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				AmazonS3	0.016811731
29	2021	5	trnfhm-sandbox	Cloud Pathfinder	trnfhm	sandbox	CPF				awskms	0.839460072
30	2021	5	klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS				AWSCloudTrail	0.032292
31	2021	5	klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS				AWSELB	2.603673464
32	2021	5	klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS				AWSecretsManager	0.069199784
33	2021	5	klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS				AWSecurityHub	3.953
34	2021	5	klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS				AmazonCloudWatch	0.003554328

Cloud Pathfinder AWS Billing Report

Tenant: Cloud Pathfinder

Year	Month	AWS Account ID	AWS Service	Charge amount
2021	2	000123456789	AWSBudgets	\$0.00
			AWSCloudTrail	\$0.22
			AWSConfig	\$0.87
			AWSLambda	\$0.00
			AWSQueueService	\$0.00
			AWSSecretsManager	\$0.00
			AWSecurityHub	\$22.33
			AmazonCloudWatch	\$0.00
			AmazonGuardDuty	\$3.22
			AmazonMacie	\$1.58
			AmazonS3	\$0.03
			AmazonSNS	\$0.00
			awskms	\$3.16
		000234567891	AWSBudgets	\$0.00
			AWSCloudTrail	\$0.22
			AWSConfig	\$1.07
			AWSELB	\$19.65
			AWSLambda	\$0.02
			AWSQueueService	\$0.00
			AWSecretsManager	\$0.42
			AWSecurityHub	\$22.50
			AmazonCloudWatch	\$0.03
			AmazonGuardDuty	\$3.18
			AmazonS3	\$0.03
			AmazonSNS	\$0.00
			awskms	\$3.16
		000345678912	AWSBudgets	\$0.00
			AWSCloudTrail	\$0.23
			AWSConfig	\$1.89
			AWSELB	\$36.74
			AWSLambda	\$0.02
			AWSQueueService	\$0.00
			AWSecretsManager	\$0.42
			AWSecurityHub	\$22.56
			AmazonCloudWatch	\$0.18
			AmazonDynamoDB	\$0.00
			AmazonECR	\$0.05
			AmazonECS	\$5.78
			AmazonGuardDuty	\$3.86
			AmazonMacie	\$1.58
			AmazonS3	\$0.03
			AmazonSNS	\$0.00
			awskms	\$3.16
		Total		\$159.74

Value of Communities

- A strong community will
 - Provide an answer before the platform team can
 - Operational cost savings
 - Faster service turnarounds
 - Self-organize to co-create reusable artifacts
 - Reduce duplication and one-offs
 - Lighten application maintenance lifecycle requirements
 - Create Stewards
 - Early adopters become Influencers
 - Influencers become Stewards

Customer Focus – 3 CoPs

Acronyms

- OCIO = Office of the Associate Deputy Minister and Government Chief Information Officer
- CoP = Community of Practice
- SecOps = OCIO Security Operations Team

- Our Customers: Project Managers / Product Owners / Expense Authorities
- Our Users: Developer Teams
- Special Users: Security Operations OCIO

Service Design Customer Focus

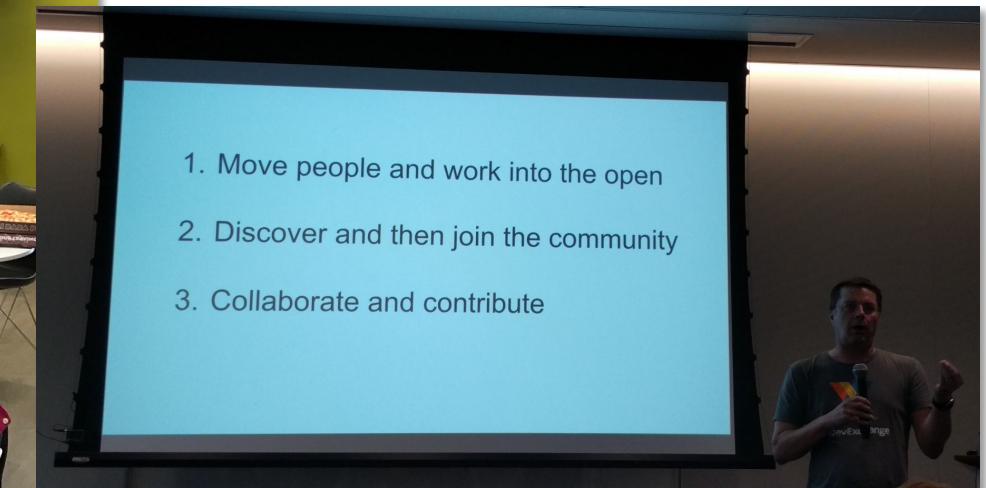
Acronyms

- UX = User Experience experts
- SD = Service Designer

- UX / SD engage with 3 Customer/Users groups
 - Gain deep understanding of needs, workflows, pain points
 - Create tickets from this work prioritizing needs
 - Focus on delivery time
 - Self-serve or fast turnaround
 - Reliability
 - Tools teams need

Strong Communities in BC Gov

DevOps Commons



Features

- Every 2 months
- History from 2016 onwards
- Community focused
- Daily Open Participation

Promotes

- Collaboration on shared efforts
- Networking across silos
- Best practices via stewards

Focus of Teams

- Teams
 - “The Workshop”, it
 - Internally connects team
 - Eases conferencing out
 - Is focused primarily on
 - Leadership
 - Scrum Masters
 - Employees



Image credit to www.mikewashburn.net/blog/2020/2/19/but-what-are-you-making

Focus of RocketChat

- RocketChat
 - “The Bazaar”, and just like OCIO Connect, it
 - Connects People
 - Highlights Best Practices
 - Is Inclusive
 - Contractors
 - Vendors
 - Leadership
 - Scrum Masters
 - Employees



Image credit to placestovisit.city/places-in-jodhpur

Recommend Both!

- Bazaars and Workshops
 - Together both provide
 - team's collaboration space and
 - access to community
 - Allow
 - others to find your team
 - modern video call meetings



A Teams Platform



A Community Platform



Image credit to [Creative Commons](#)

Bazaar Frontage with Workshops

Cloud Pathfinder is available on both

Cloud Pathfinder Service Levels

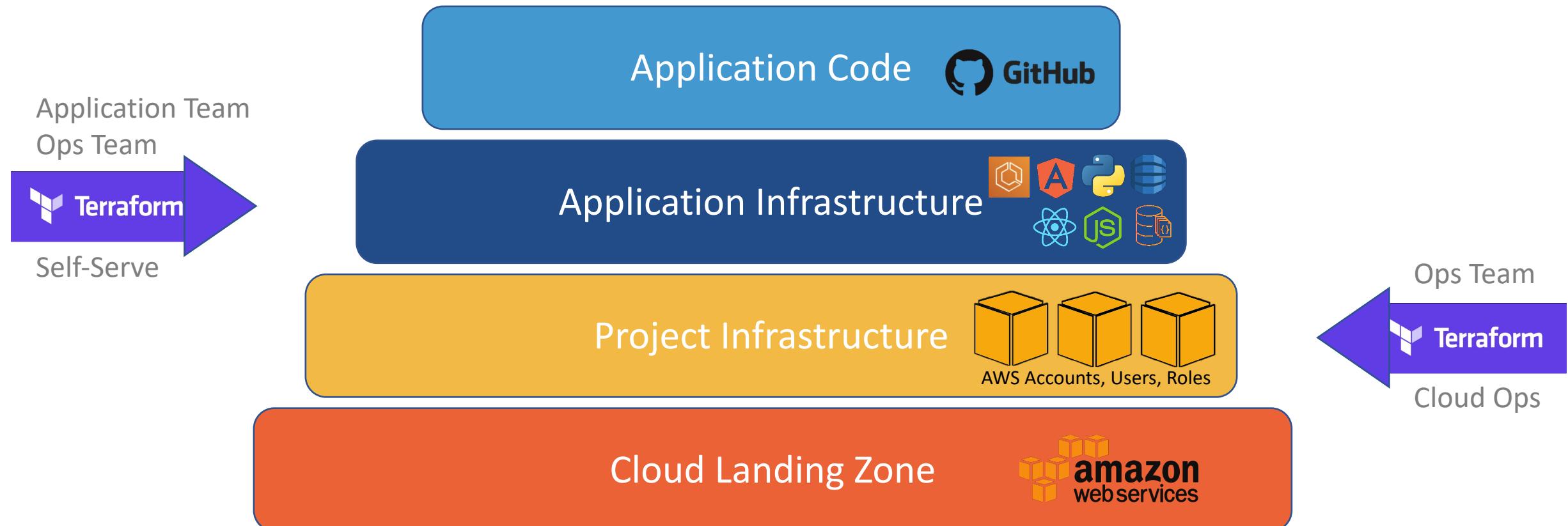
- Provide training for teams
- Provision new team members (0.5 business day turnaround)
- Facilitate and respond to open and private support channels
- Connect vendor support (cut through vendor complexity)
- Review and include new requests for cloud components (usually 3 week turnaround)
- Provide clear billing in multi-tenancy
- Remove overhead of offboarding contractors or departing employees (IDIR gone? AWS gone!)

Demo of Authentication to AWS

- Showing lack of users to manage
- Make your life easy to not have to delete users

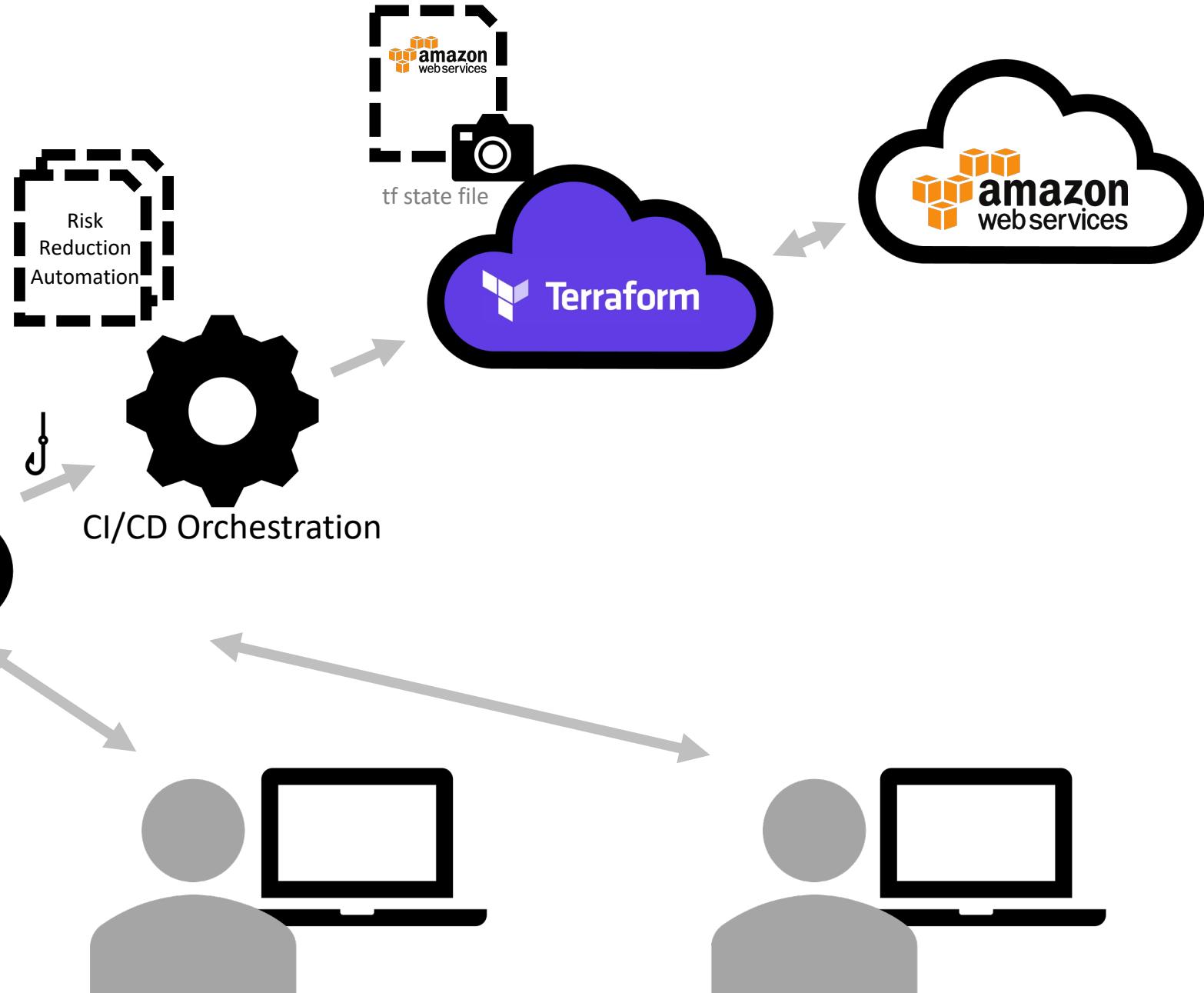
Questions & Answers

BC Gov AWS Cloud Layers



TF Cloud

Teams use a shared
TF Cloud state file



Demo App: CI/CD Workflow

- **All-In-One**

- Terraform workspace for each team account environment (Dev, Test, Prod)



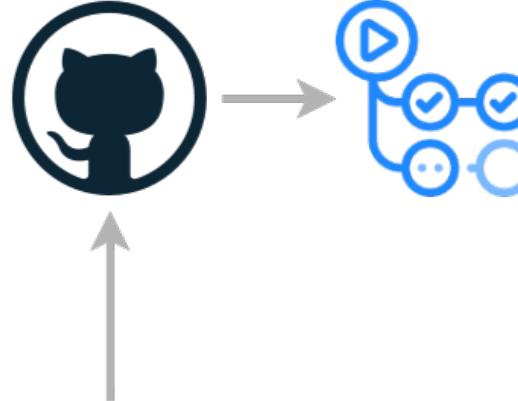
- **Microservice**

- Terraform workspace for each service in a team account environment (Dev-App1, Dev-App2, Test-App1, Test-App2, etc)

- **Combination**

- Workspaces for common infrastructure
- Workspaces for each service

GitHub Repo GitHub Action



```

name: CI/CD

on:
  push:
    branches: [dev, test, prod]
  pull_request:
    branches: [dev, test, prod]

jobs:
  ci:
    name: CI
    runs-on: ubuntu-20.04
    steps:
      - name: Check out the repo
        uses: actions/checkout@v2
      - name: Build
        run: make build
      - name: Test
        run: make test
      - name: Push Docker Image
        run: make push

  cd:
    name: CD
    runs-on: ubuntu-20.04
    steps:
      - name: Check out the repo
        uses: actions/checkout@v2
      - name: Terraform Format Check
        run: terraform fmt -check
      - name: Terraform Init
        run: terraform init
      - name: Static analysis security scanner for Terraform code
        run: tfsec
      - if: github.event_name != 'pull_request'
        name: Deploy
        run: terraform apply

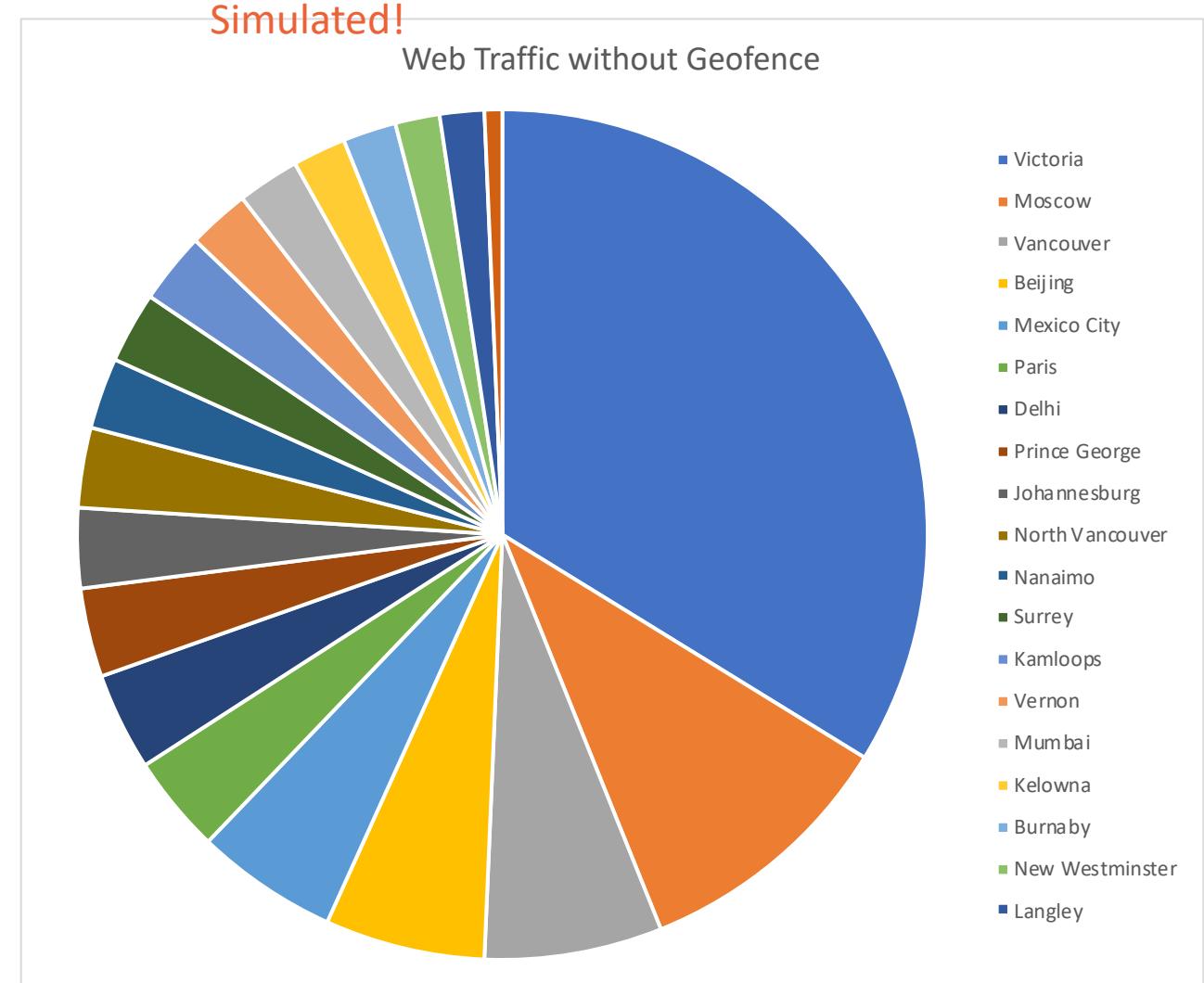
```

Terraform Cloud
Workspace



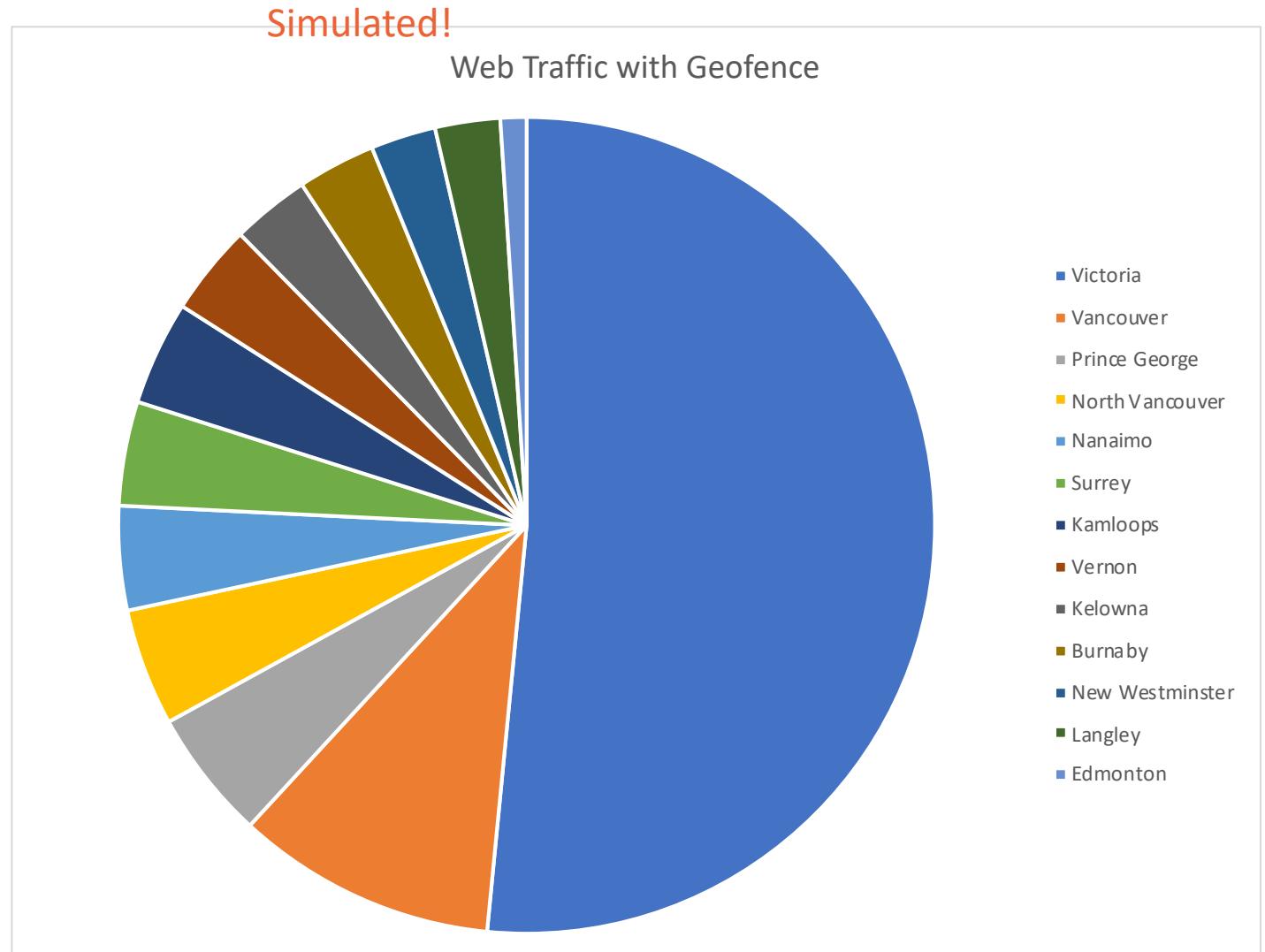
Geofencing

- Thought experiment
 - Imagine our traffic looks like this:



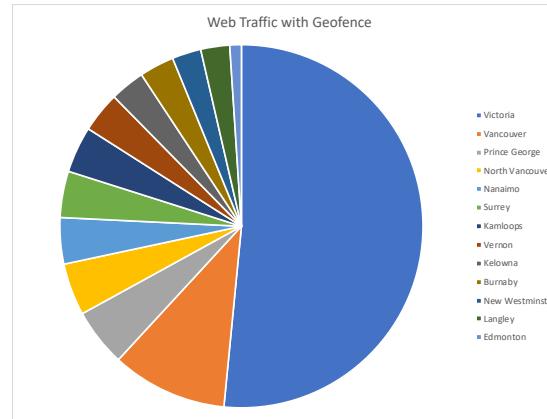
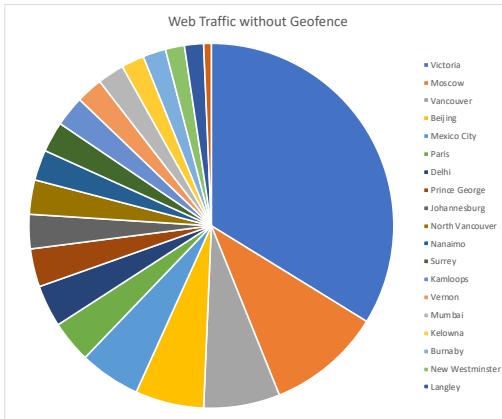
Geofencing

- After implementing
 - Imagine our traffic could look like this:



Geofencing Part 2

- Recall last demo...
 - Geofencing can reduce automated door-knocking traffic
 - Portable to Demo app



- We have this ready to share with teams
 - We use it on our login page to block traffic external to Canada
 - We provide this for teams to add to their apps via our demo app