CloudPathfinder

Pre-Reading Material

Information Pack for BC Gov Ministry Teams considering Cloud

Updated

Jan 13, 2022

CloudPathfinder

Topics

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

CloudPathfinder

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

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

CloudPathfinder

Customer Focus

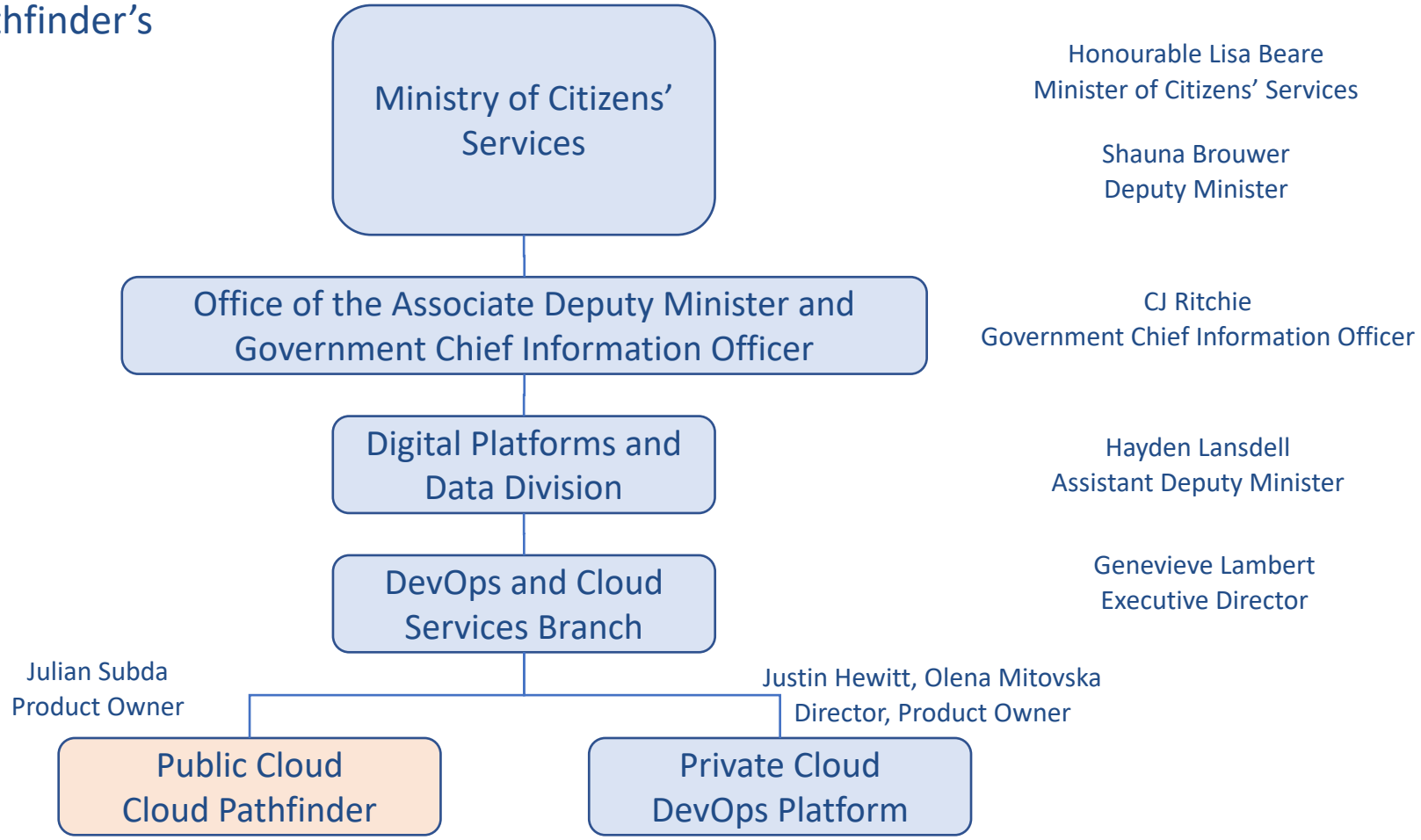
Acronyms
- OCIO = Office of the Associate Deputy Minister and Government Chief Information Officer
- SecOps = OCIO Security Operations Team

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

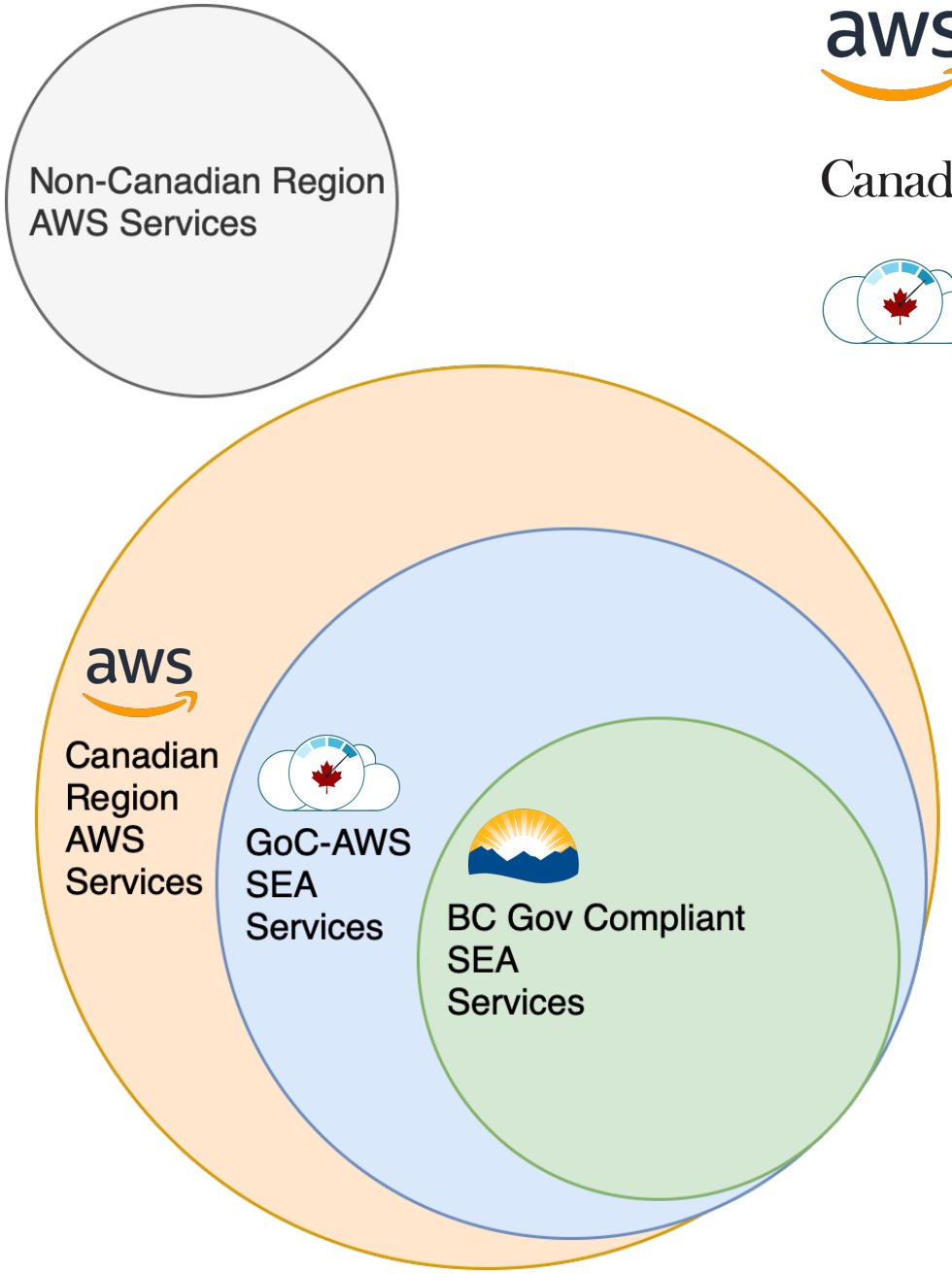
CloudPathfinder

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

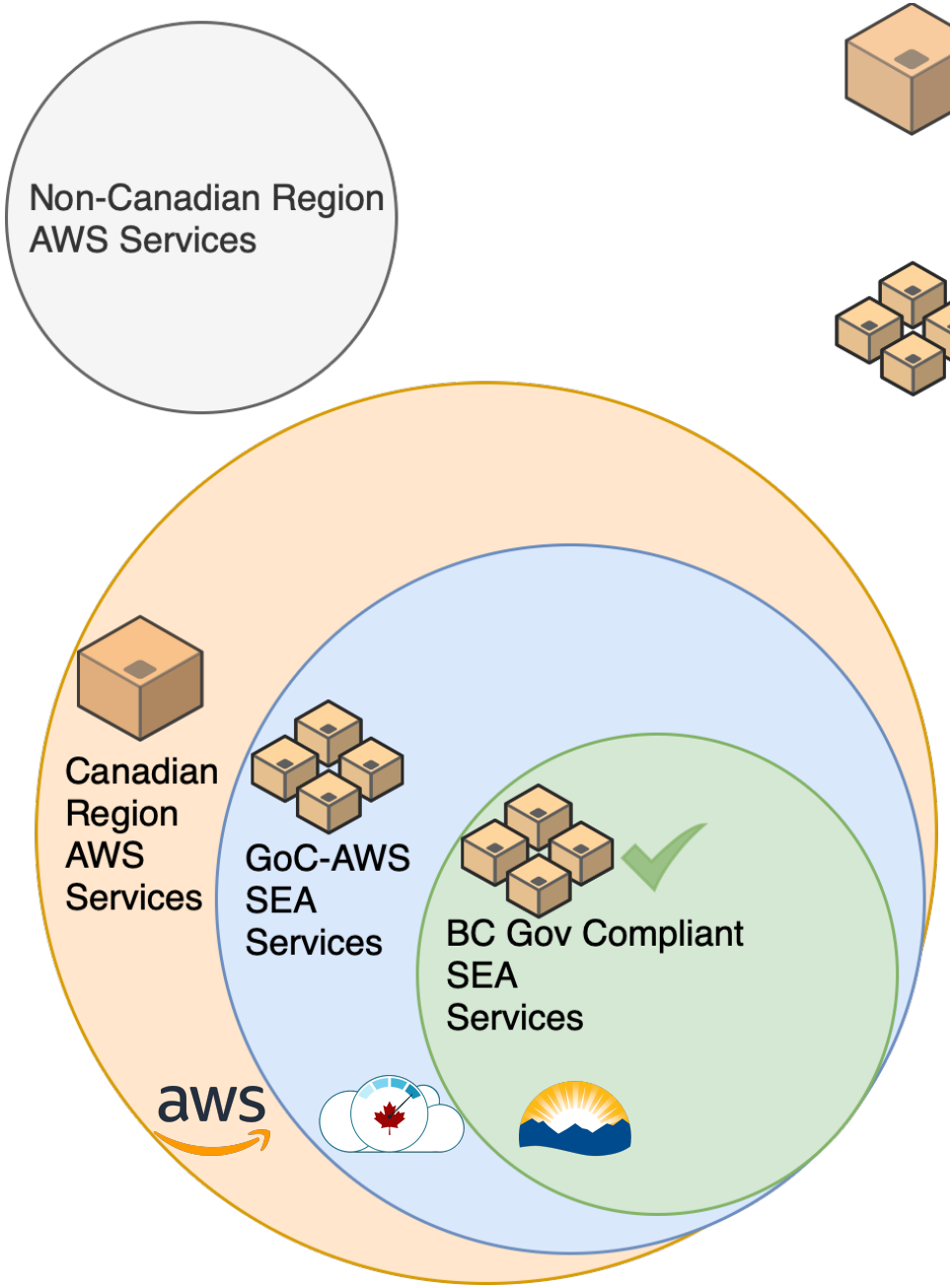
SEA = Secure Environment Accelerator
A software deployed virtual data centre in the cloud sitting in AWS space

This shows the relationship between services offered in different scopes of the various contexts of the AWS SEA. BC Gov teams will be working primarily in the green area with some services from the blue.

The green services have been tested by the Cloud Pathfinder team for good fit within the guardrails of the environment.

Some services are not compatible but in general there is a pattern for teams to use the blue ones if needed.

SEA Concepts

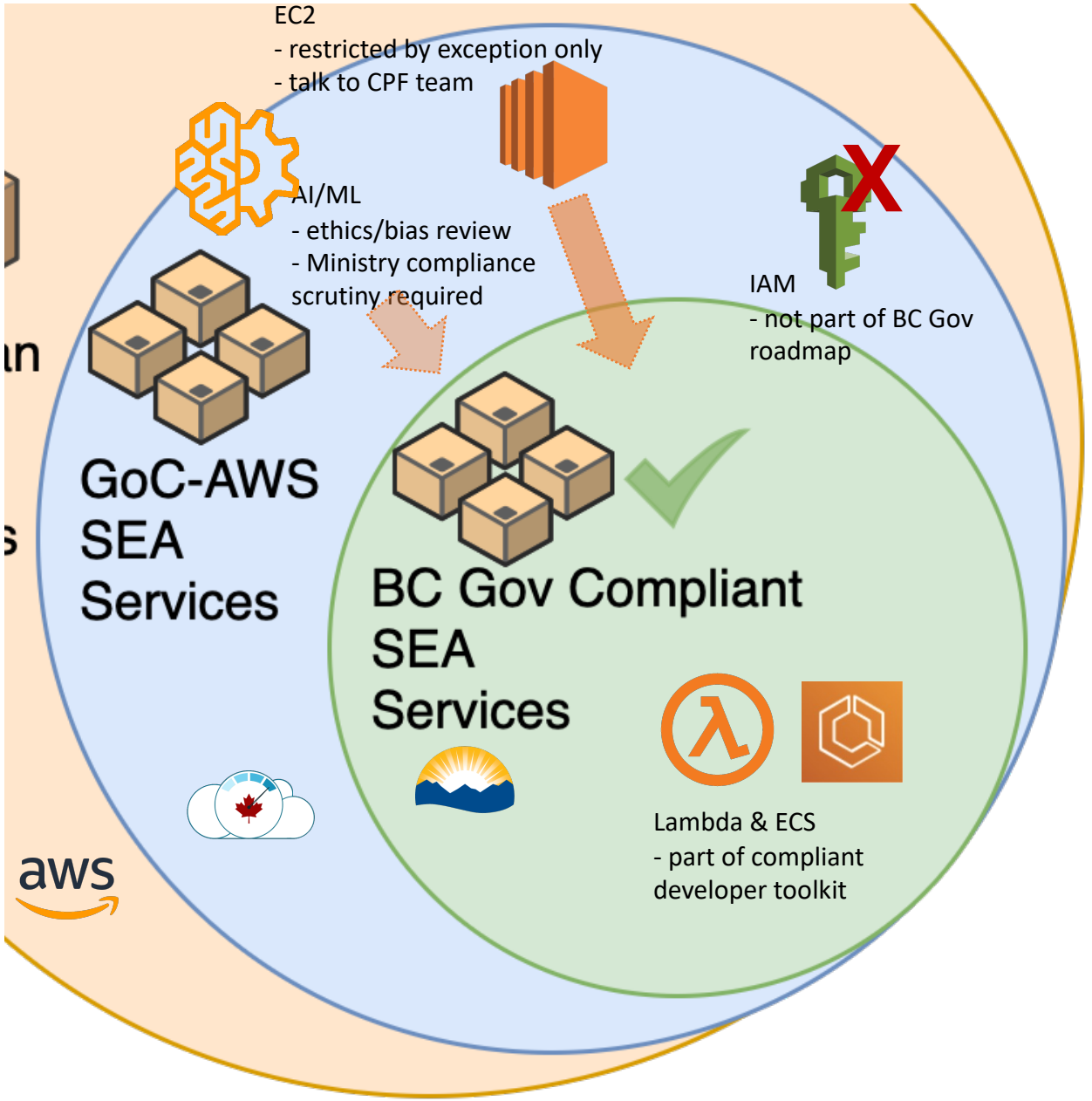


AWS = Amazon Web Services Cloud
Out of the box "Vanilla" AWS account that anyone can buy

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

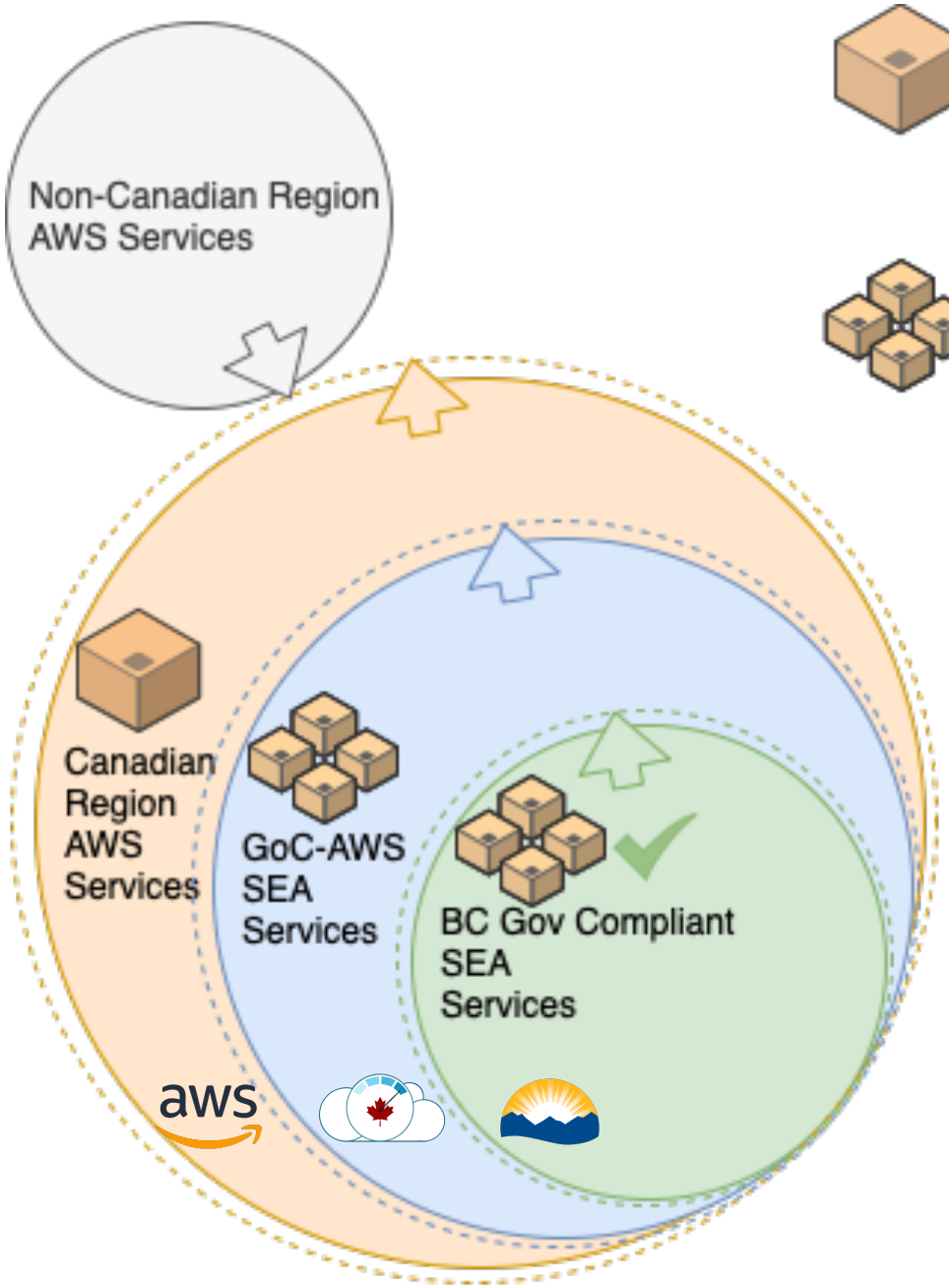
Compliant Services



Acronyms

- CPF = Cloud Pathfinder Team
- 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

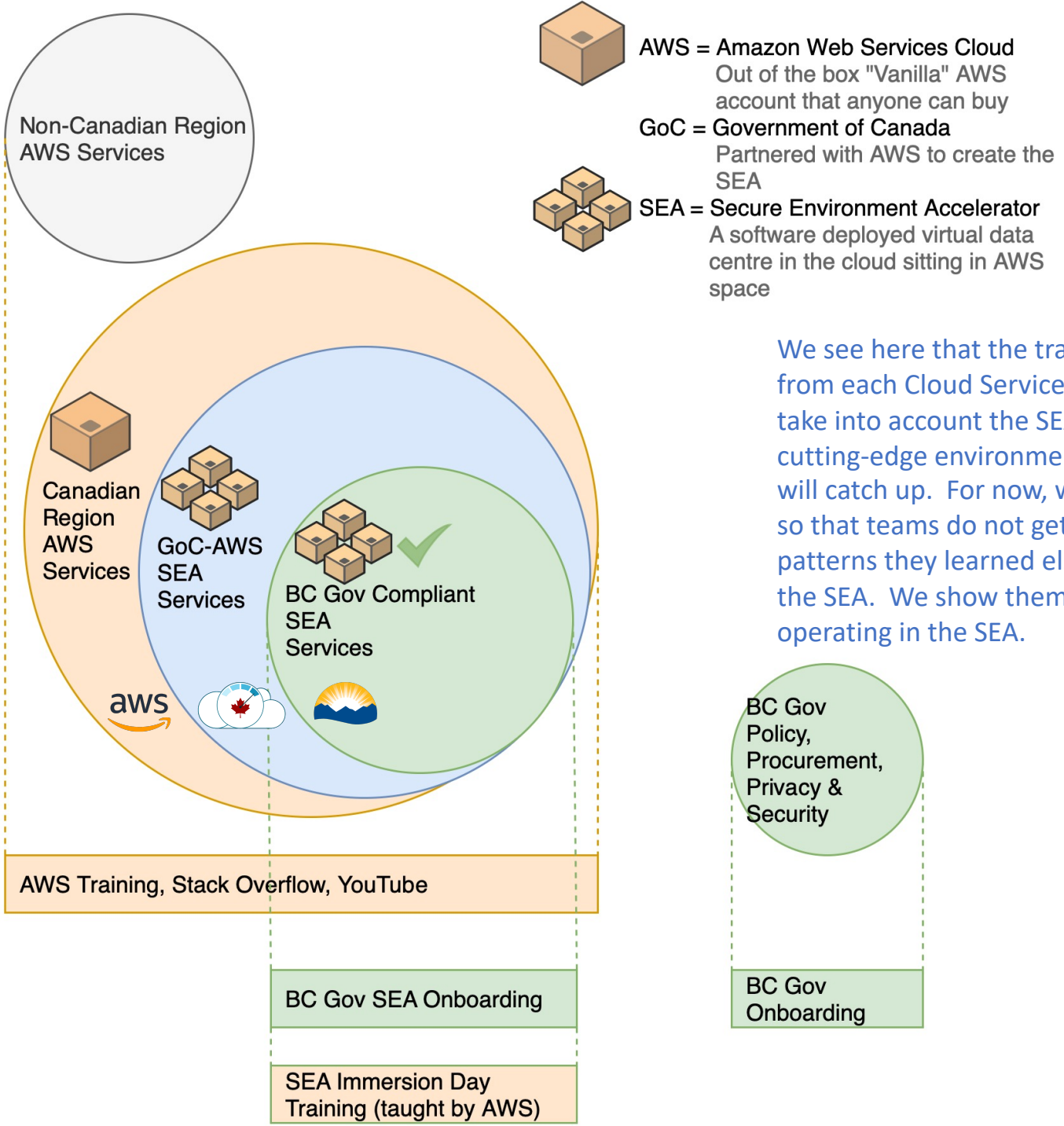
GoC = Government of Canada
Partnered with AWS to create the SEA

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

Over time, the number of services in the SEA available to BC Gov teams will go up and we expect the green set of services to mostly overlap the blue.

CloudPathfinder

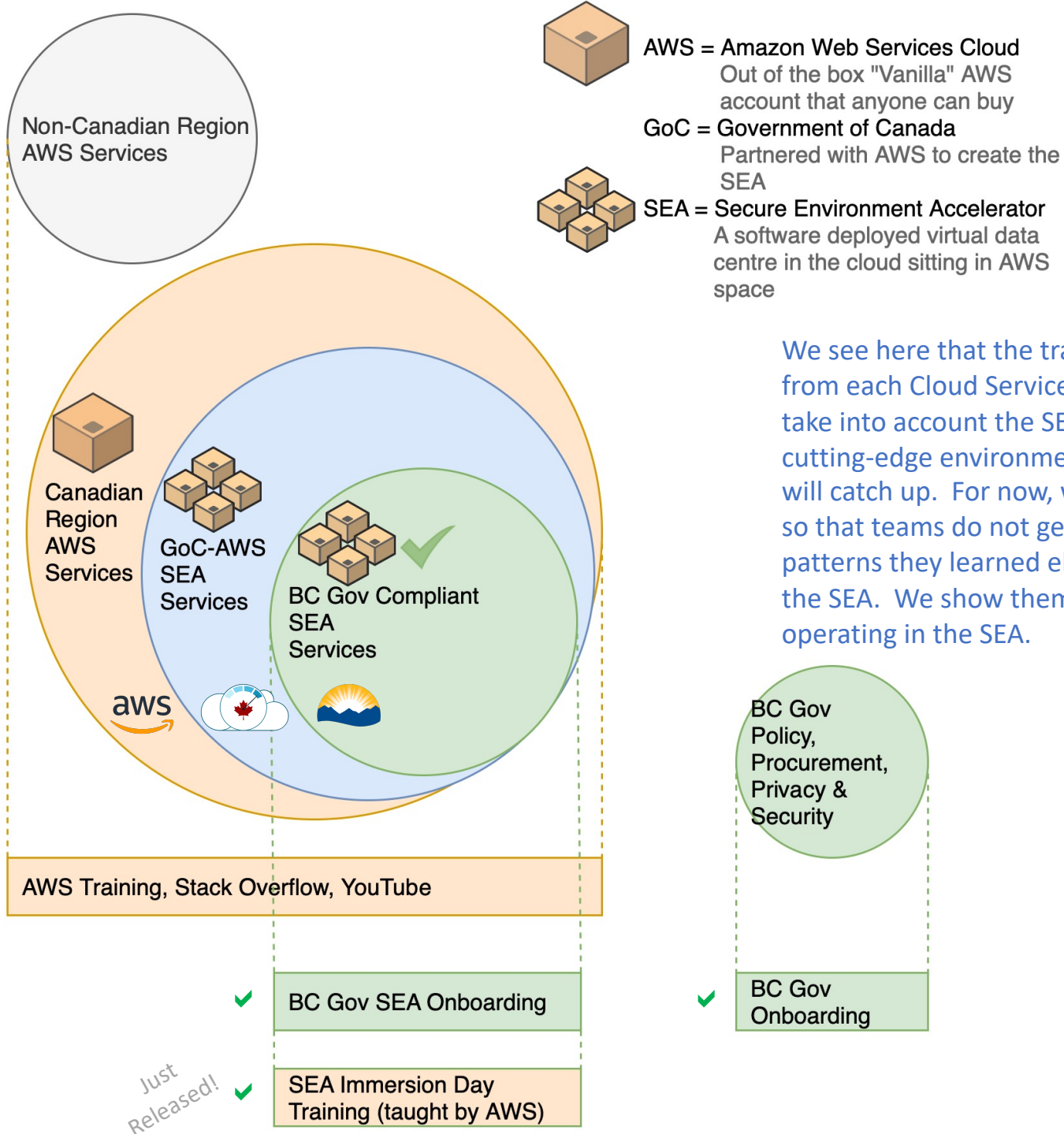
Training Landscape



We see here that the training available online and from each Cloud Service Provider like AWS does not take into account the SEAs as these are very cutting-edge environments. Over time the training will catch up. For now, we have customized training so that teams do not get confused when the patterns they learned elsewhere do not function in the SEA. We show them equivalent, safe ways of operating in the SEA.

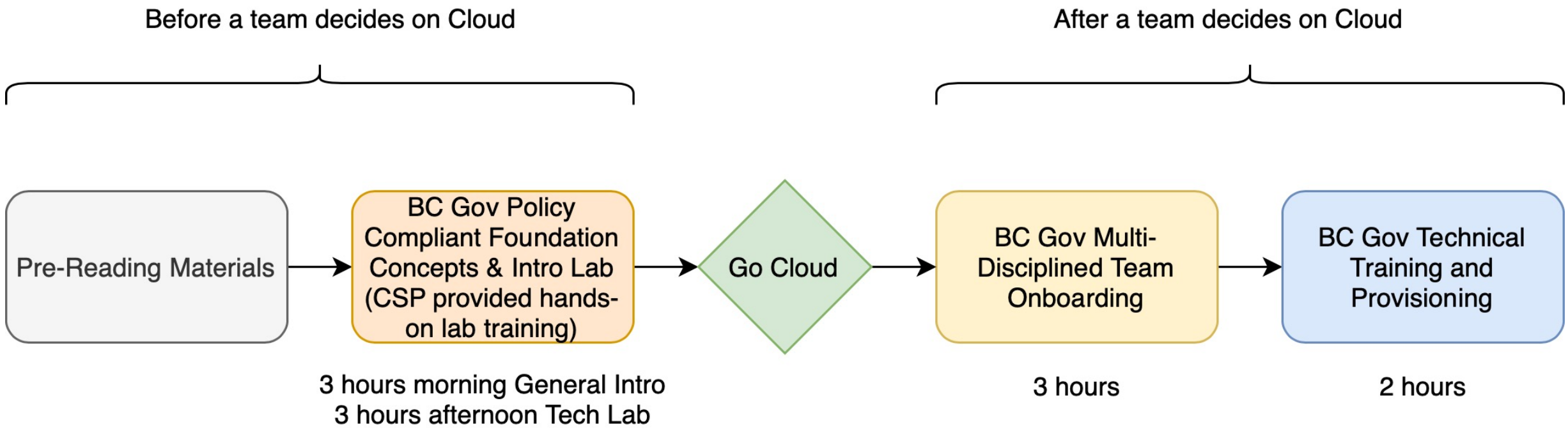
CloudPathfinder

Training Components



We see here that the training available online and from each Cloud Service Provider like AWS does not take into account the SEAs as these are very cutting-edge environments. Over time the training will catch up. For now, we have customized training so that teams do not get confused when the patterns they learned elsewhere do not function in the SEA. We show them equivalent, safe ways of operating in the SEA.

Training Track



CloudPathfinder

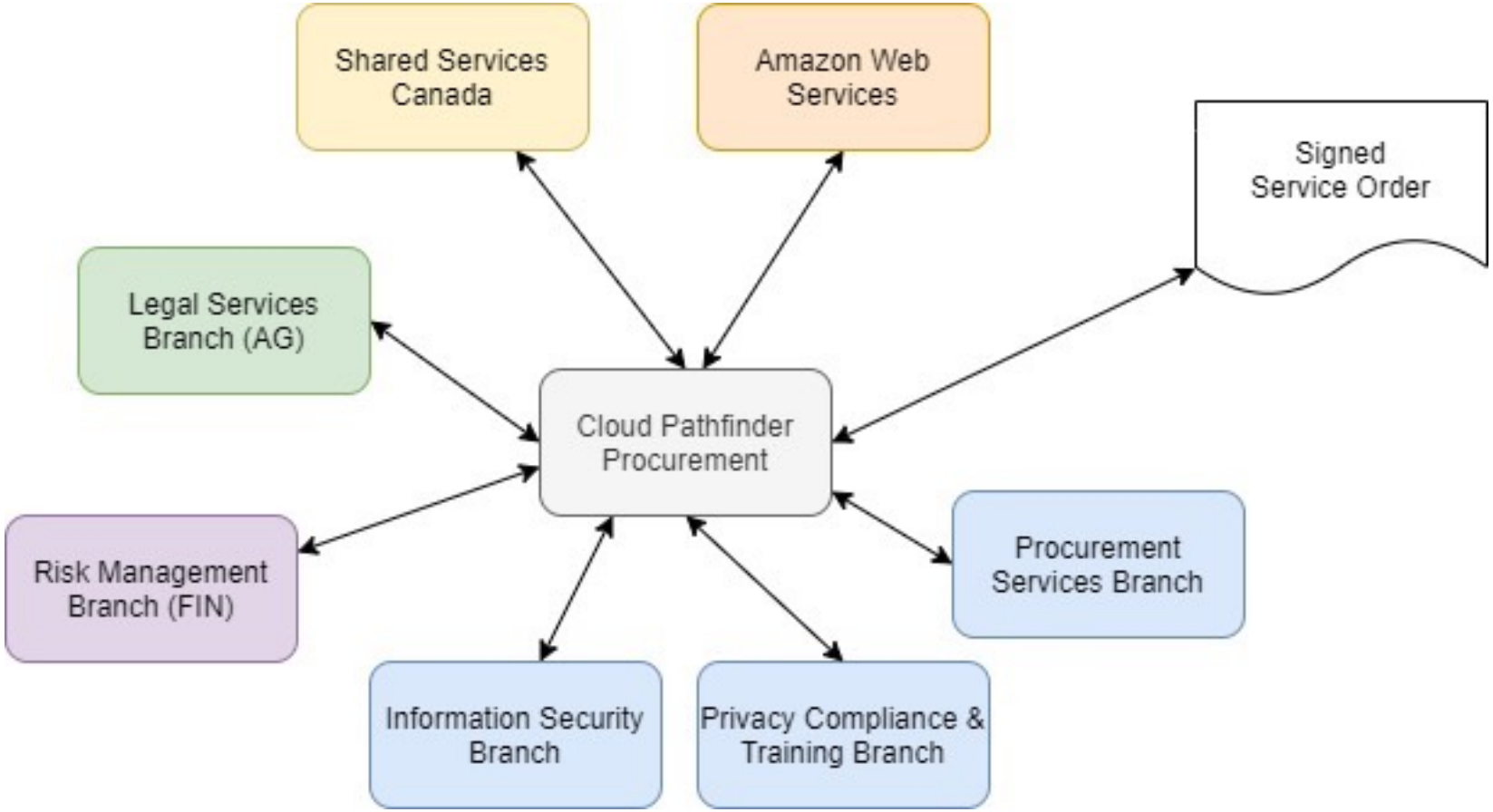
Audience

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

Image credit to Creative Commons

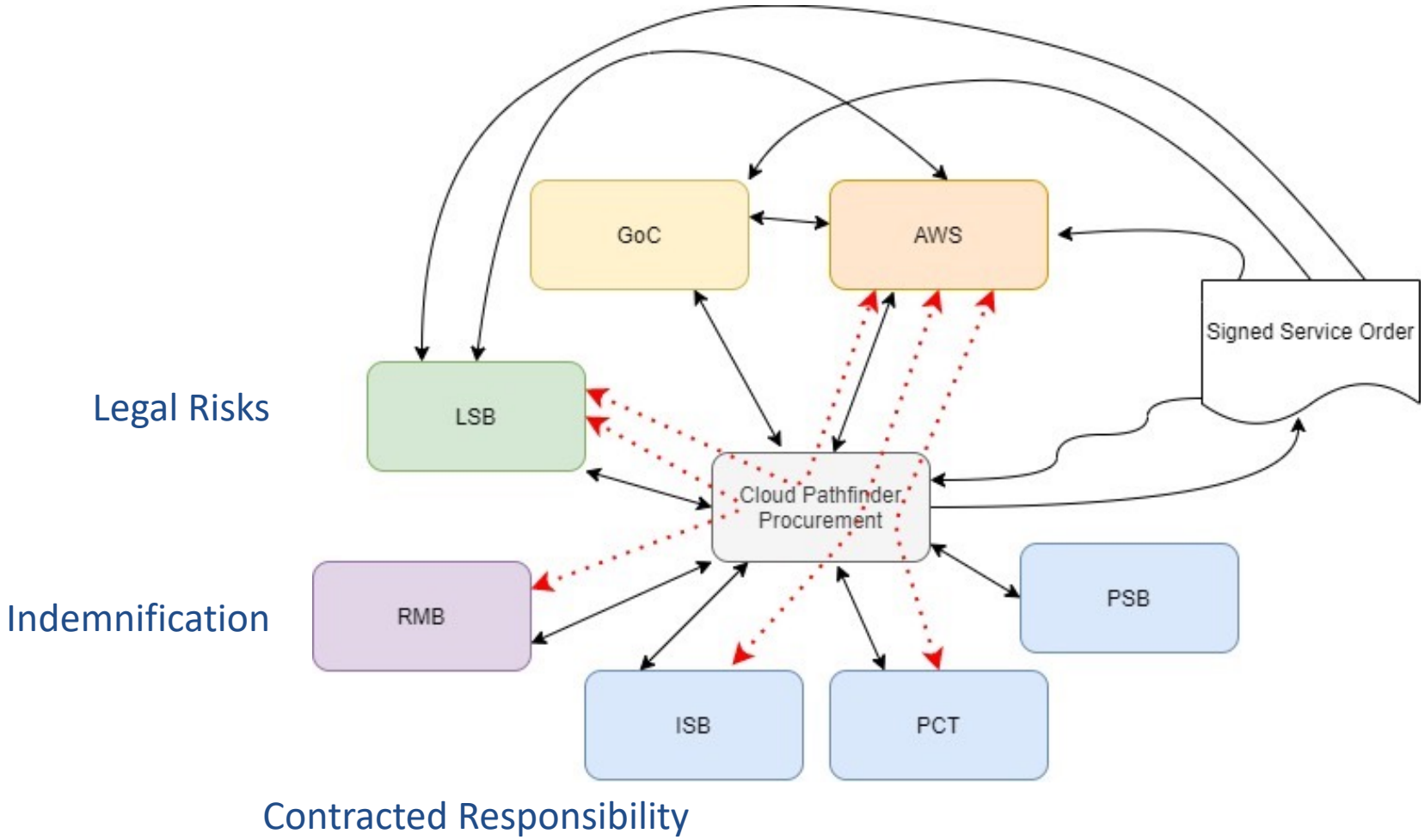
CloudPathfinder

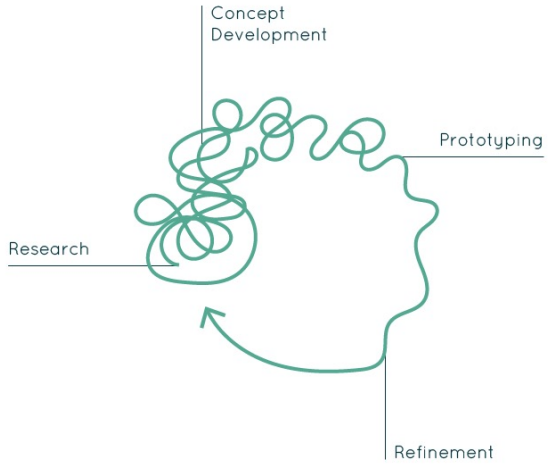
Negotiation of our First Service Order



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 dig into the cloud services

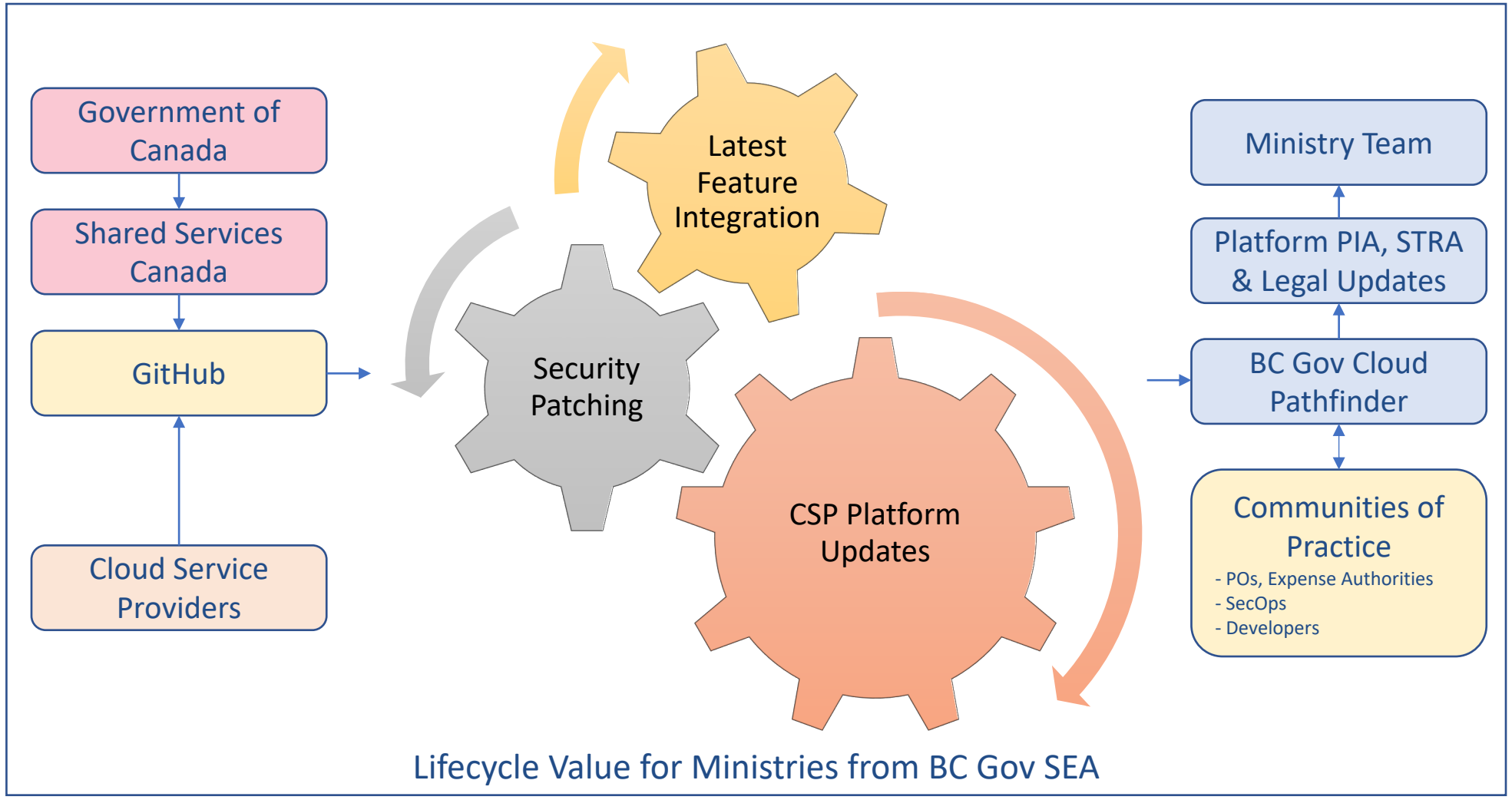
Don’t have to negotiate privacy, security, legal terms with **vendors**

Image credit to pixabay

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

CloudPathfinder

Cloud Lifecycle Value Add for Ministries

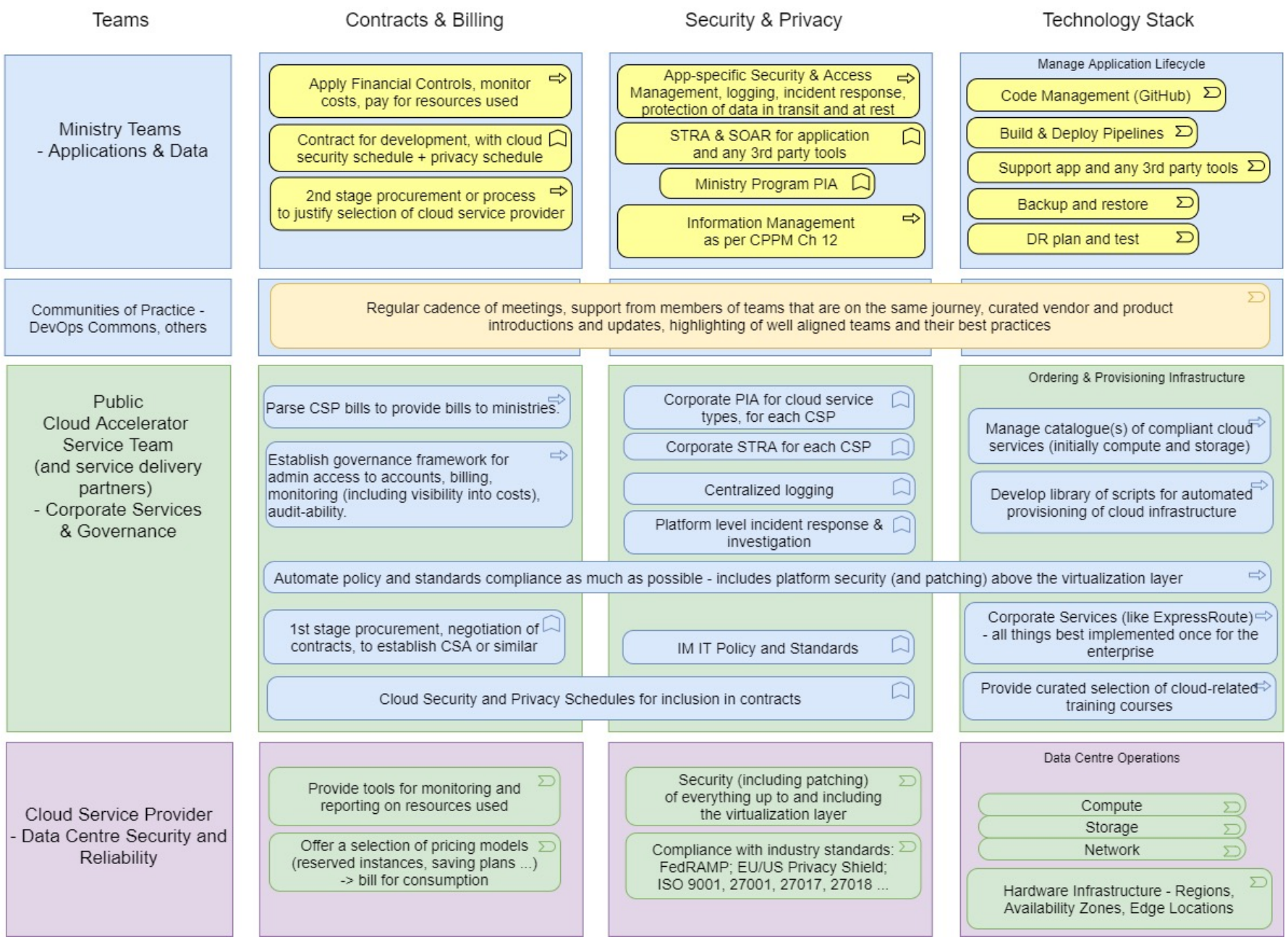


CloudPathfinder

Public Cloud Accelerator Service Shared Responsibilities Model

for compute and storage

Shared Responsibility Model



CloudPathfinder

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

AWS

State Machine

Departmental Organizations Master account

GR-1,4,5,12,(2,6)

SCP's

Core OU | Sandbox OU | Unclass OU | Dev OU | Test OU | Prod OU | Central OU

VPC AWS SSO

GR-2,3

Core accounts

AWS Log Archive

S3 - Immutable

GR-11

AWS Security (audit)

Master - Security Hub, GuardDuty, Firewall Manager, Security Dashboard

GR-11

AWS Operations

Ops Dashboard
syslog, pwd
AWS MAD

VPC Central_VPC

GR-2,3,11

Unclassified accounts (non-PBMM)

AWS SandboxN

VPC Sandbox_VPC

AWS UnclassN

VPC Unclass_VPC

AWS DevOps

Central CI/CD

VPC Central_VPC

Team or group accounts

GR-8,6,11

AWS Dev-Team1 — VPC Dev_VPC

AWS Test-Team1 — VPC Test_VPC

AWS Prod-Team1 — VPC Prod_VPC

AWS Shared-Team1 — VPC Central_VPC

AWS Dev-TeamN — VPC Dev_VPC

AWS Test-TeamN — VPC Test_VPC

AWS Prod-TeamN — VPC Prod_VPC

AWS Shared-TeamN — VPC Central_VPC

AWS Shared Network Account

GR-8

VPC Dev_VPC

VPC Test_VPC

VPC Prod_VPC

VPC Unclass_VPC

RT1

RT3

RT2

VPC Central_VPC

IPSec VPN tunnels (BGP, ECMP)

VPC Endpoint_VPC

AWS Perimeter Security Account

VPC Perimeter_VPC

ALB +WAF

Fortigate A/A

Proxy

GR-7,9

Pre- SCED availability

Using RFC6598

No-NAT

DX

GC-CAP

GC-TIP

Internet

GC WAN

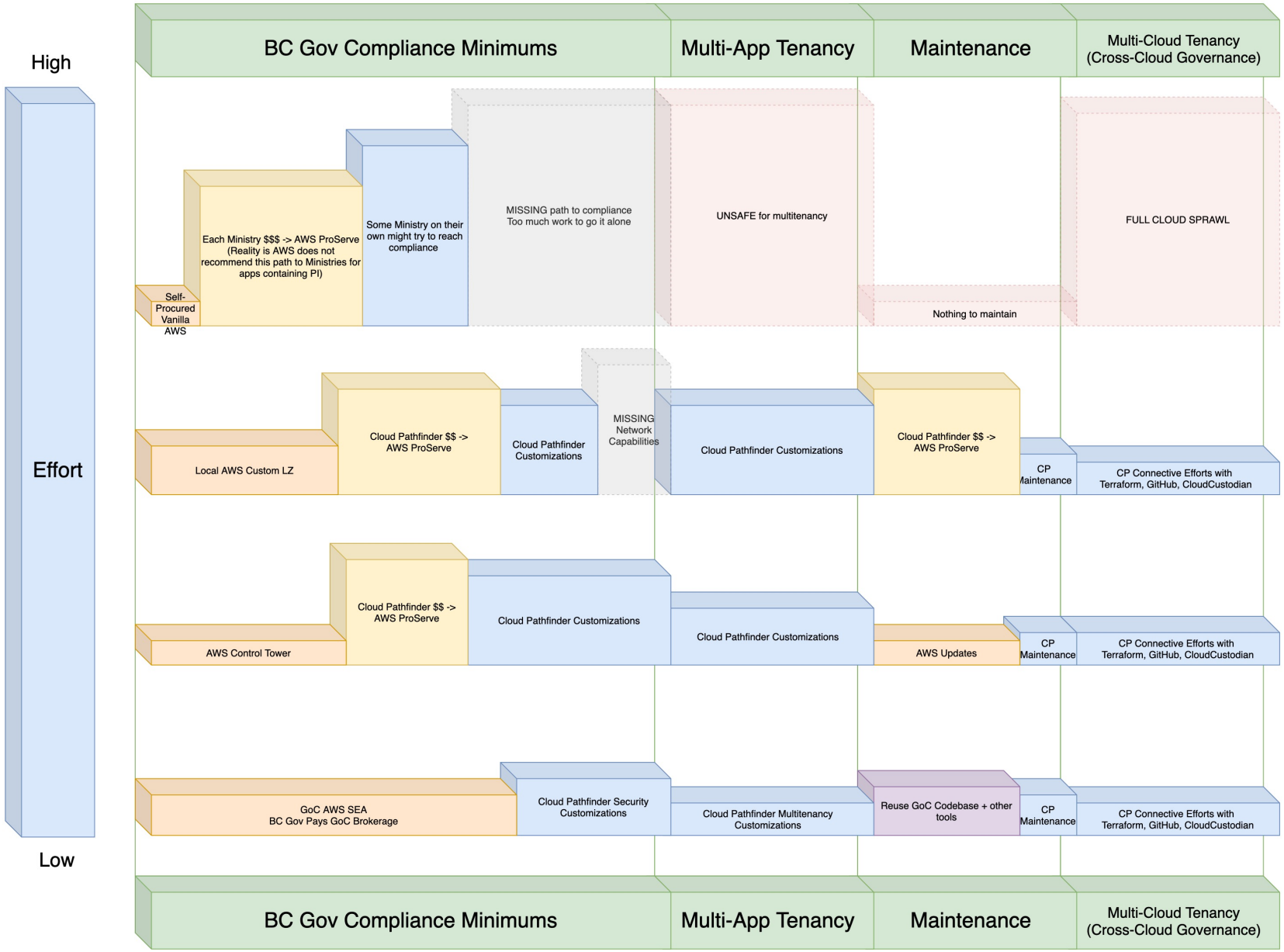
TBS Guardrails
1 - Protect Root/Break glass
2 - Management of Privileges
3 - Cloud Console Access
4 - Enterprise Monitoring
5 - Data location
6 - Data-at-rest
7 - Data-in-transit
8 - Segment & separate
9 - Network security services
10 - CCCS MOU
11 - Logging & monitoring

Cloud Pathfinder

Glossary

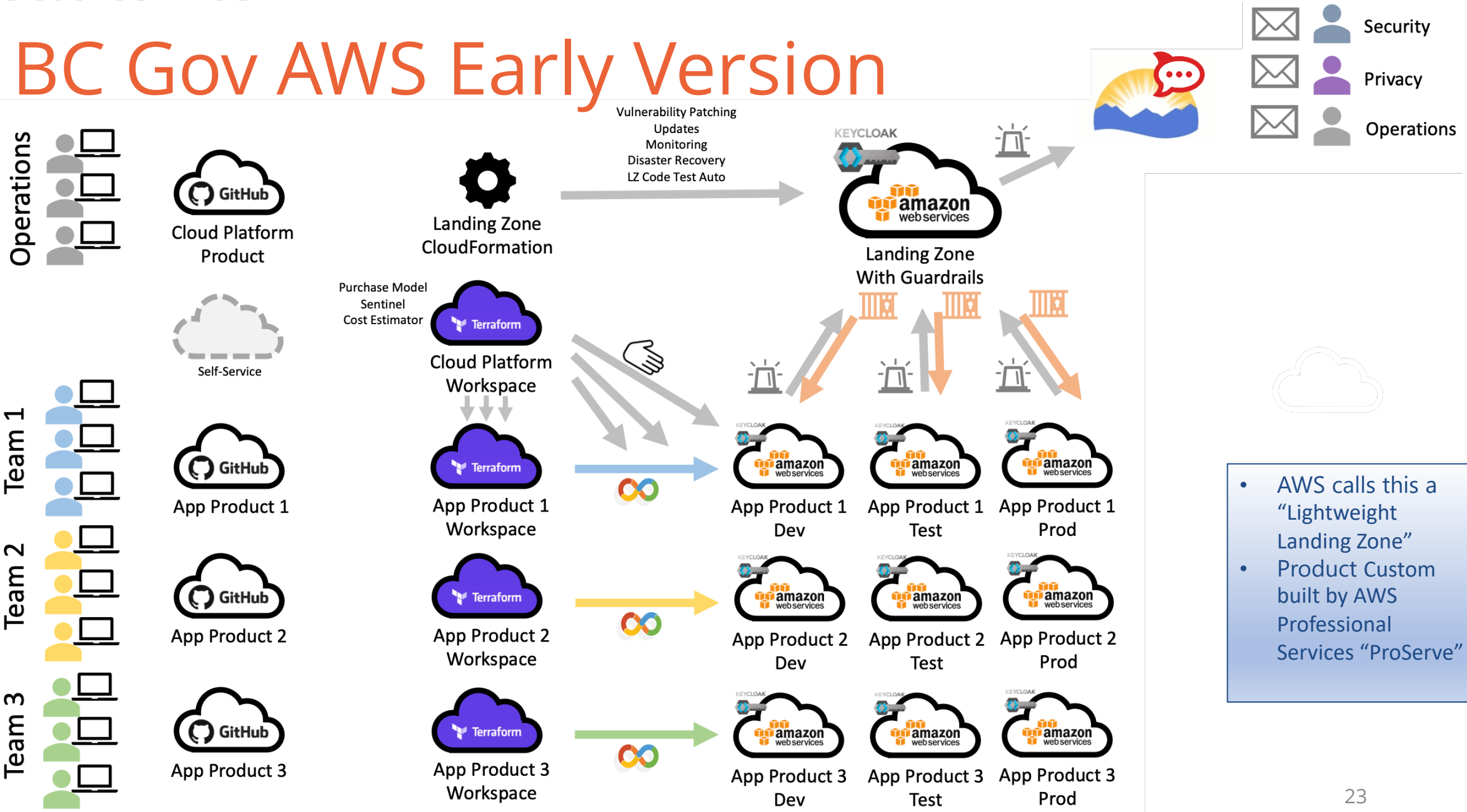
- ProServe = AWS Professional Services, a paid formal engagement
- LZ = Landing Zone
- GoC = Government of Canada
- CP – Cloud Pathfinder

Cloud Pathfinder - Easiest Path Report (Cloud 1 AWS)



CloudPathfinder

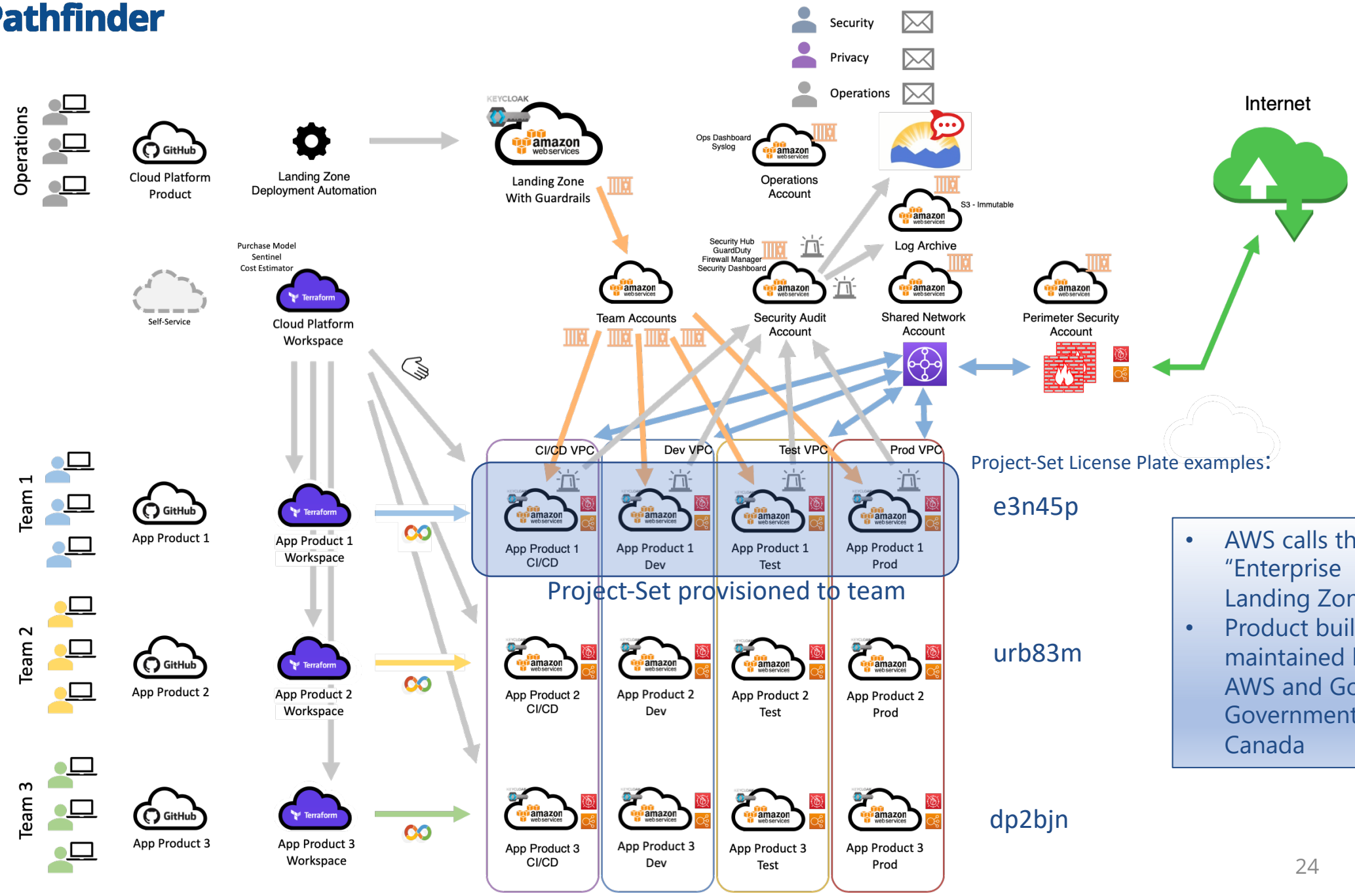
BC Gov AWS Early Version



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

CloudPathfinder

BC Gov AWS SEA



Project-Set License Plate examples:

e3n45p

urb83m

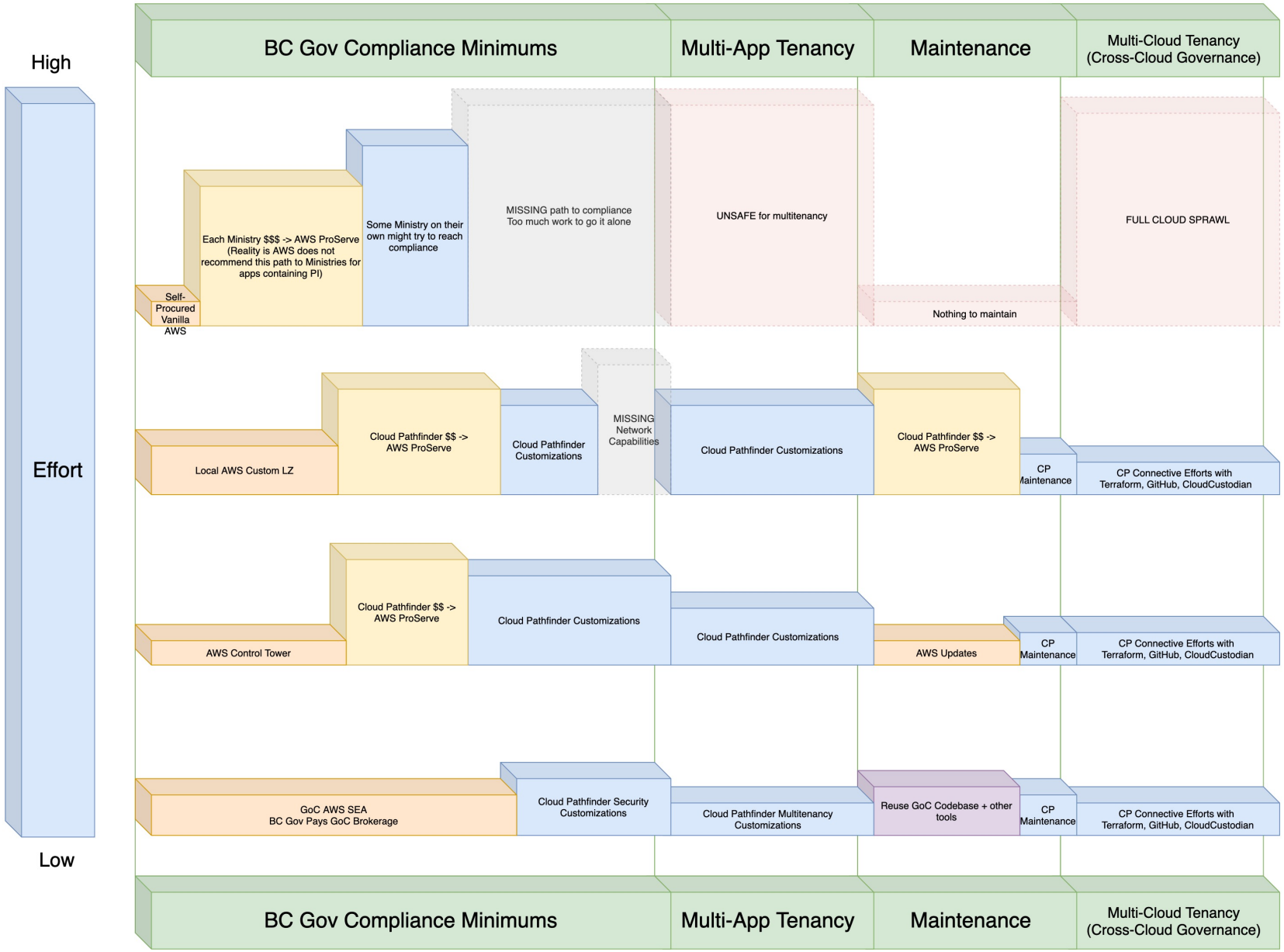
dp2bjn

- AWS calls this an "Enterprise Landing Zone"
- Product built & maintained by AWS and GoC Government of Canada

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)



Billing Examples T-Shirt Estimates

AWS Services*	T-Shirt Estimate Scenario 1 - Small	
* usage based and expense may increase or decrease	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	
* usage based and expense may increase or decrease	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.

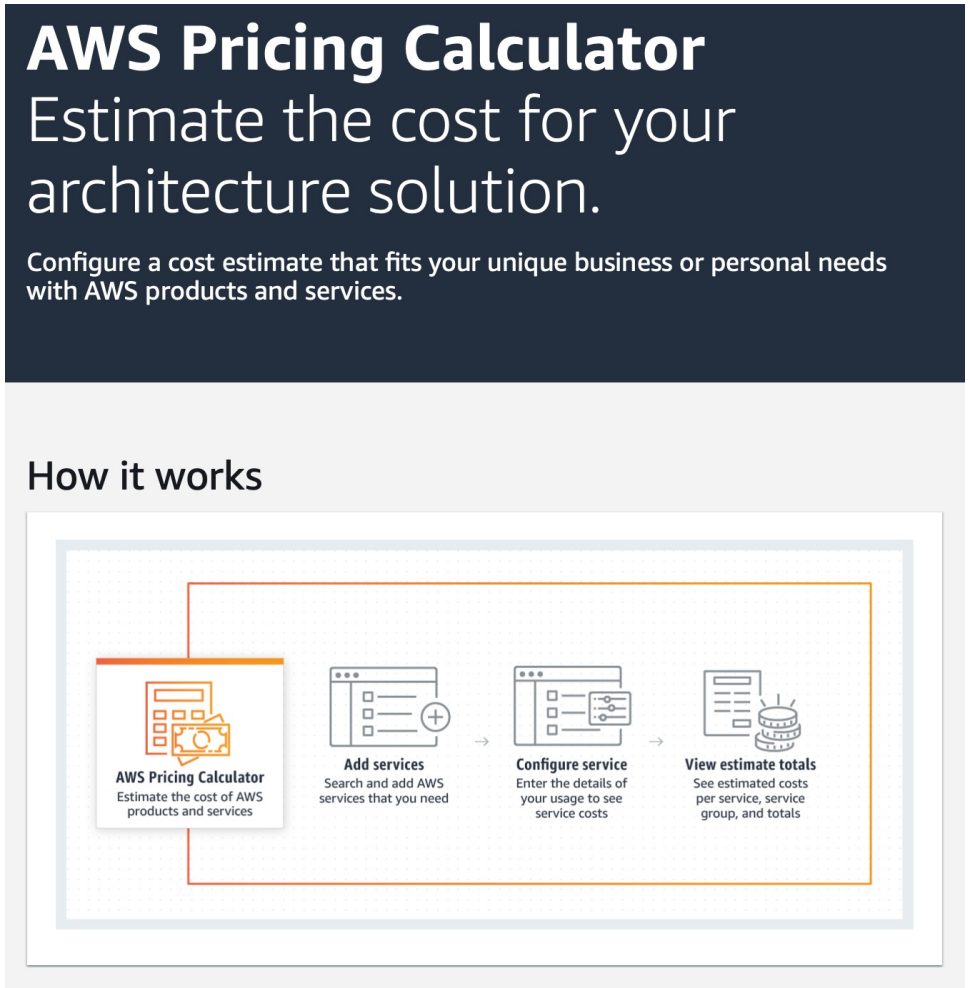
Billing Examples T-Shirt Estimates

AWS Services*	T-Shirt Estimate Scenario 3 - Large	
* usage based and expense may increase or decrease	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



CloudPathfinder

Stakeholder
Ministry POs,
Expense Authorities

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	Environmen	Billing_Gr	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			AWSSecretsManager	0.00002
4	2021	5		klwrig-sandbox	Enhanced Travellers Screening	klwrig	sandbox	HLTHETS			AWSSecurityHub	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			AWSSecretsManager	0.00002
14	2021	5		shared-services	Landing Zone Core	shared-services	Core	SEA Core			AWSSecurityHub	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		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AWSCloudTrail	0.043608
21	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AWSConfig	0.024
22	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AWSSecretsManager	0.00002
23	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AWSSecurityHub	4.313
24	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AmazonCloudWatch	0.008591734
25	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AmazonEC2	6.160000699
26	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AmazonGuardDuty	0.538942
27	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AmazonMacie	0.05932
28	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	sandbox	CPF			AmazonS3	0.016811731
29	2021	5		tnfhhm-sandbox	Cloud Pathfinder	tnfhhm	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			AWSSecretsManager	0.069199784
33	2021	5		klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS			AWSSecurityHub	3.953
34	2021	5		klwrig-prod	Enhanced Travellers Screening	klwrig	prod	HLTHETS			AmazonCloudWatch	0.003554328

Cloud Pathfinder AWS Billing Report

Tenant: Cloud Pathfinder

				Charge amount
Year	Month	AWS Account ID	AWS Service	
2021	2	000123456789	AWSBudgets	$0.00
			AWSCloudTrail	$0.22
			AWSConfig	$0.87
			AWSLambda	$0.00
			AWSQueueService	$0.00
			AWSSecretsManager	$0.00
			AWSSecurityHub	$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
			AWSSecretsManager	$0.42
			AWSSecurityHub	$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
			AWSSecretsManager	$0.42
			AWSSecurityHub	$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

CloudPathfinder

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

CloudPathfinder

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

CloudPathfinder

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

CloudPathfinder

Strong Communities in BC Gov

DevOps Commons

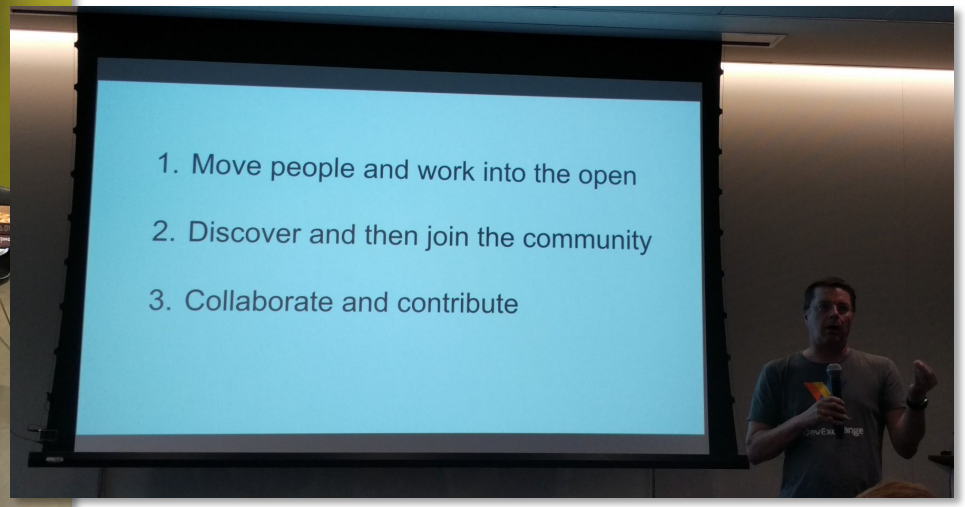
Features

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

Promotes

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

BRITISH COLUMBIA



CloudPathfinder

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

CloudPathfinder

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

CloudPathfinder

Recommend Both!

Channel: aws-lz2
https://chat.pathfinder.gov.bc.ca/group/aws-lz2

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

Image credit to Creative Commons

Bazaar Frontage with Workshops

A Teams Platform

A Community Platform

Cloud Pathfinder is available on both

CloudPathfinder

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

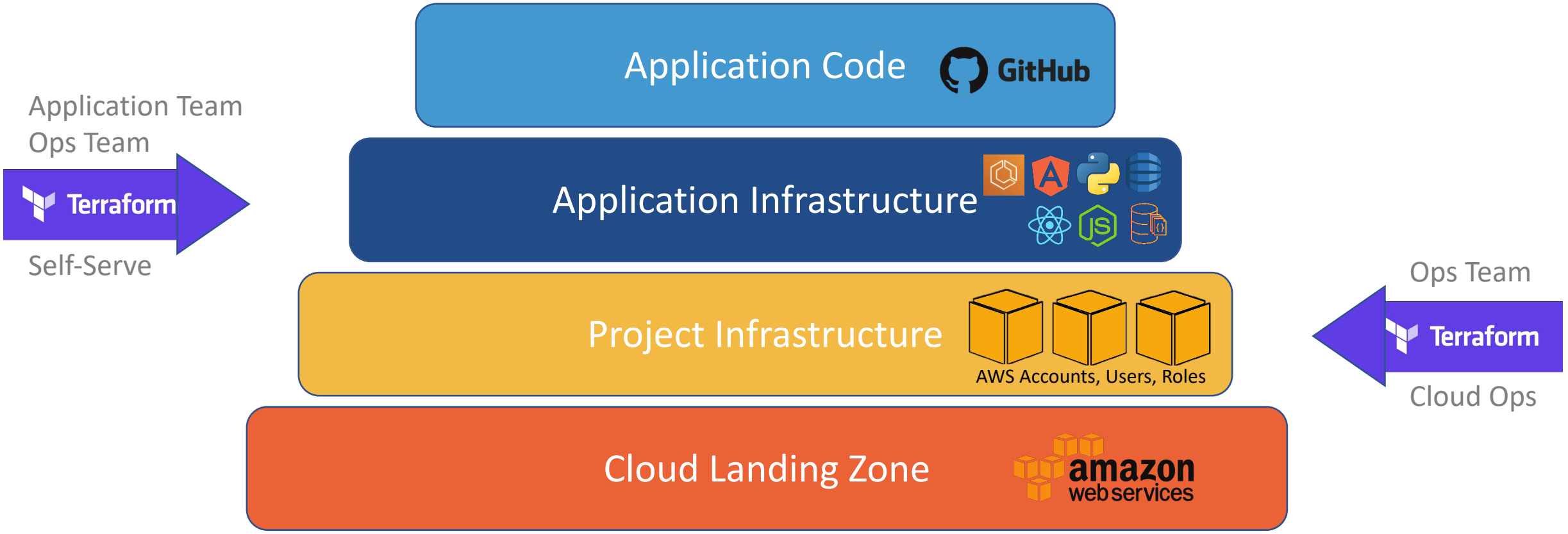
- Showing lack of users to manage
- Make your life easy to not have to delete users

CloudPathfinder

Questions & Answers

CloudPathfinder

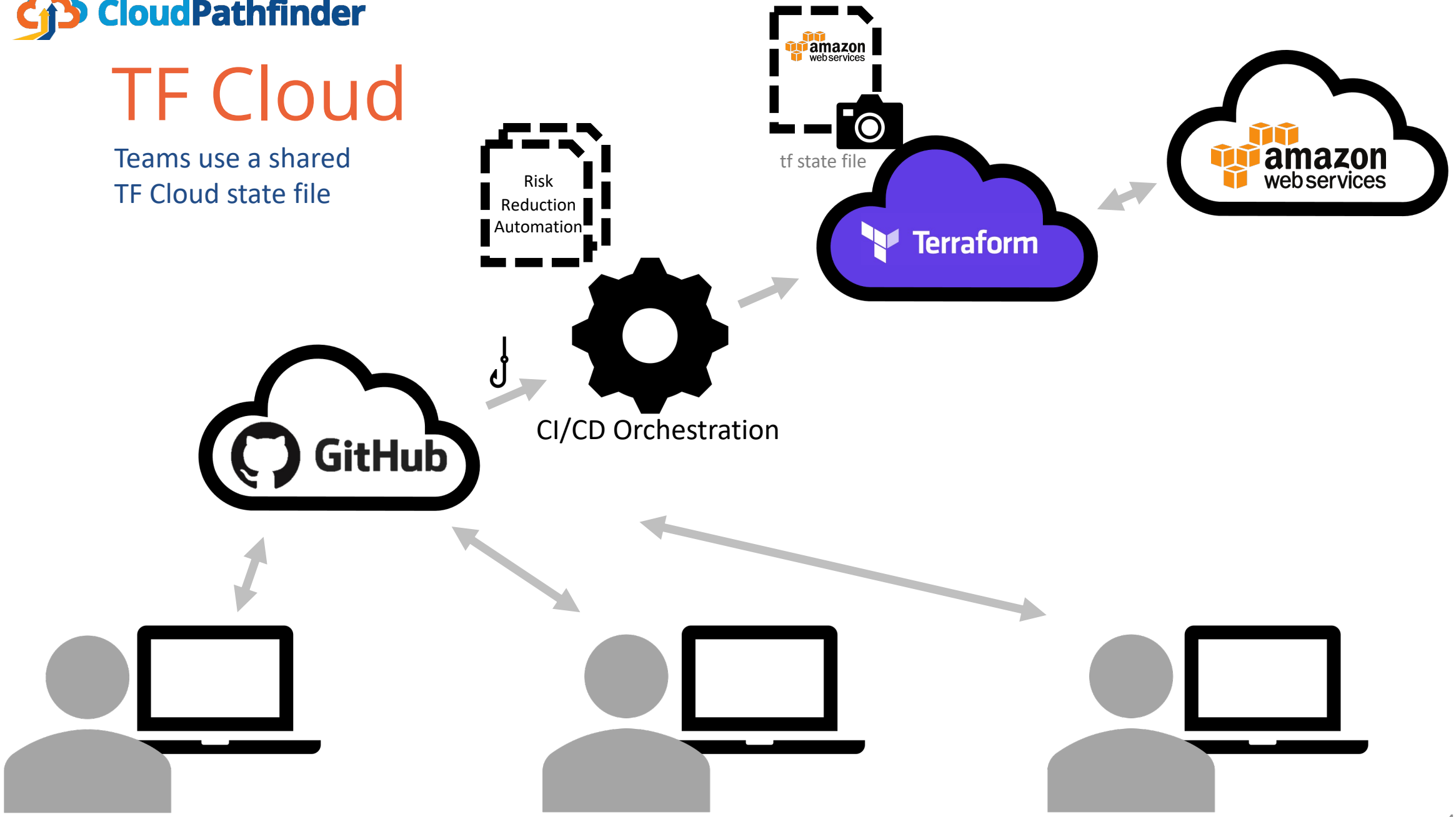
BC Gov AWS Cloud Layers



CloudPathfinder

TF Cloud

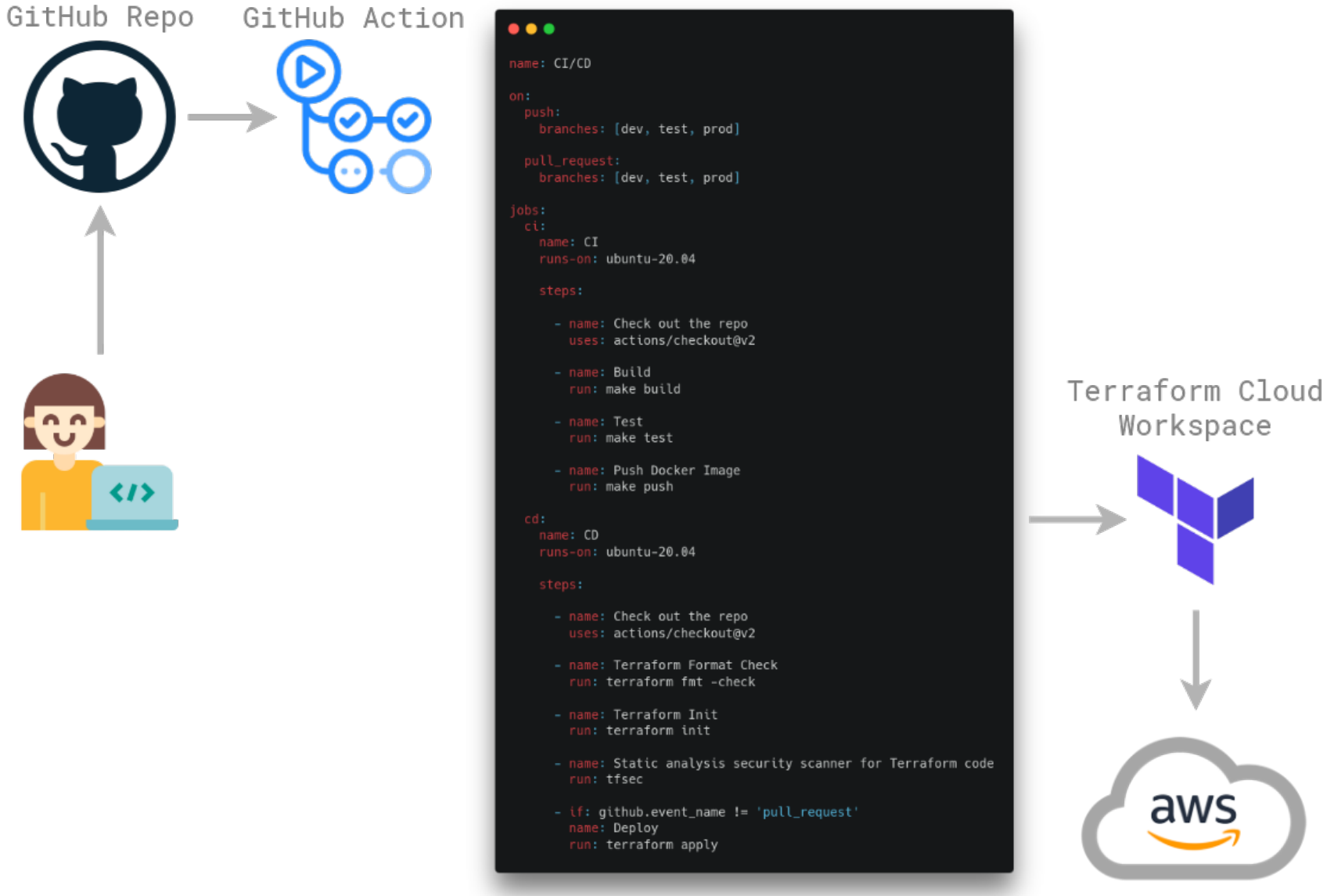
Teams use a shared
TF Cloud state file



CloudPathfinder

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**
  - Workspace for common infrastructure
  - Workspaces for each service

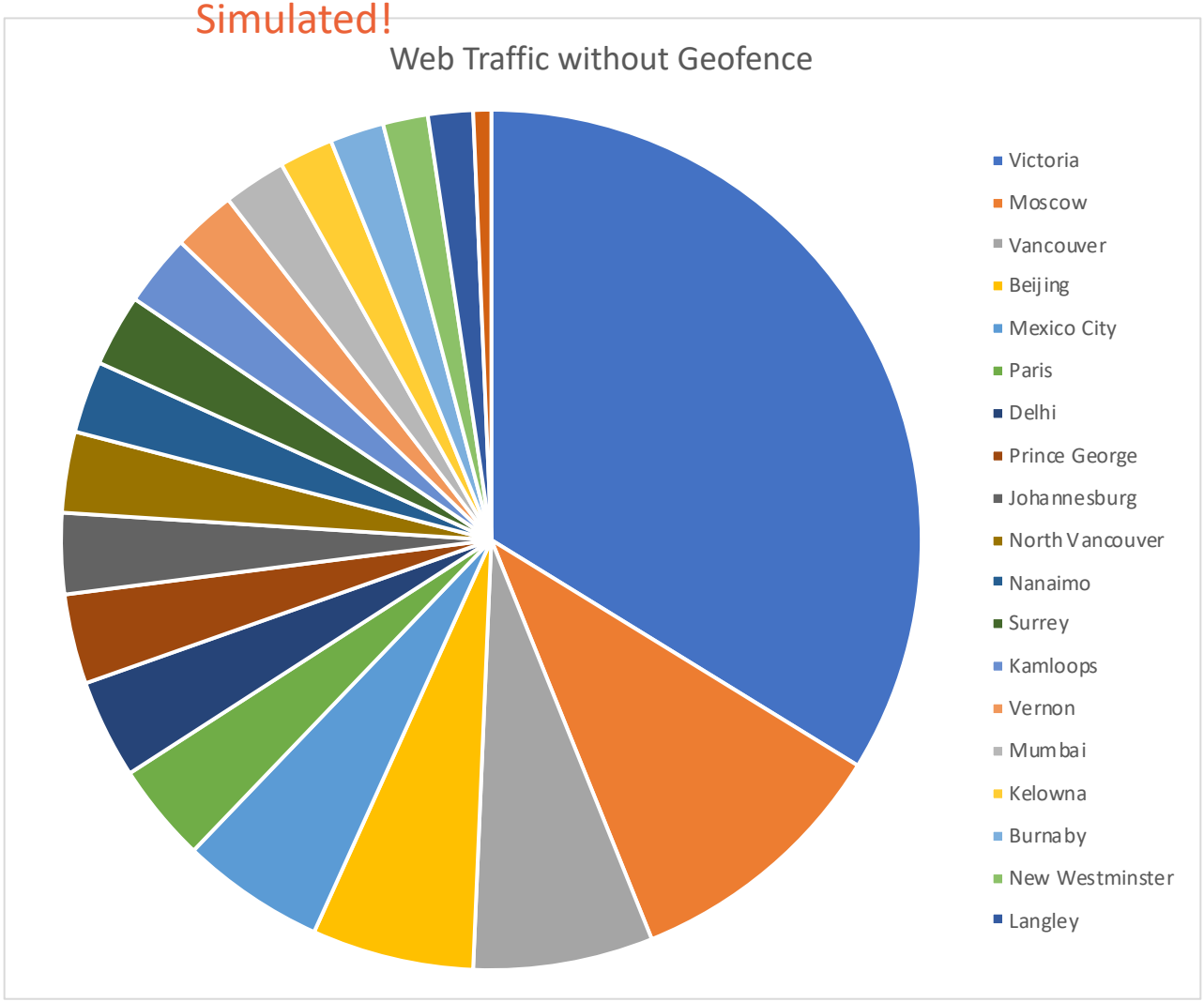


CloudPathfinder

Geofencing

- Thought experiment
  - Imagine our traffic looks like this:

Simulated!

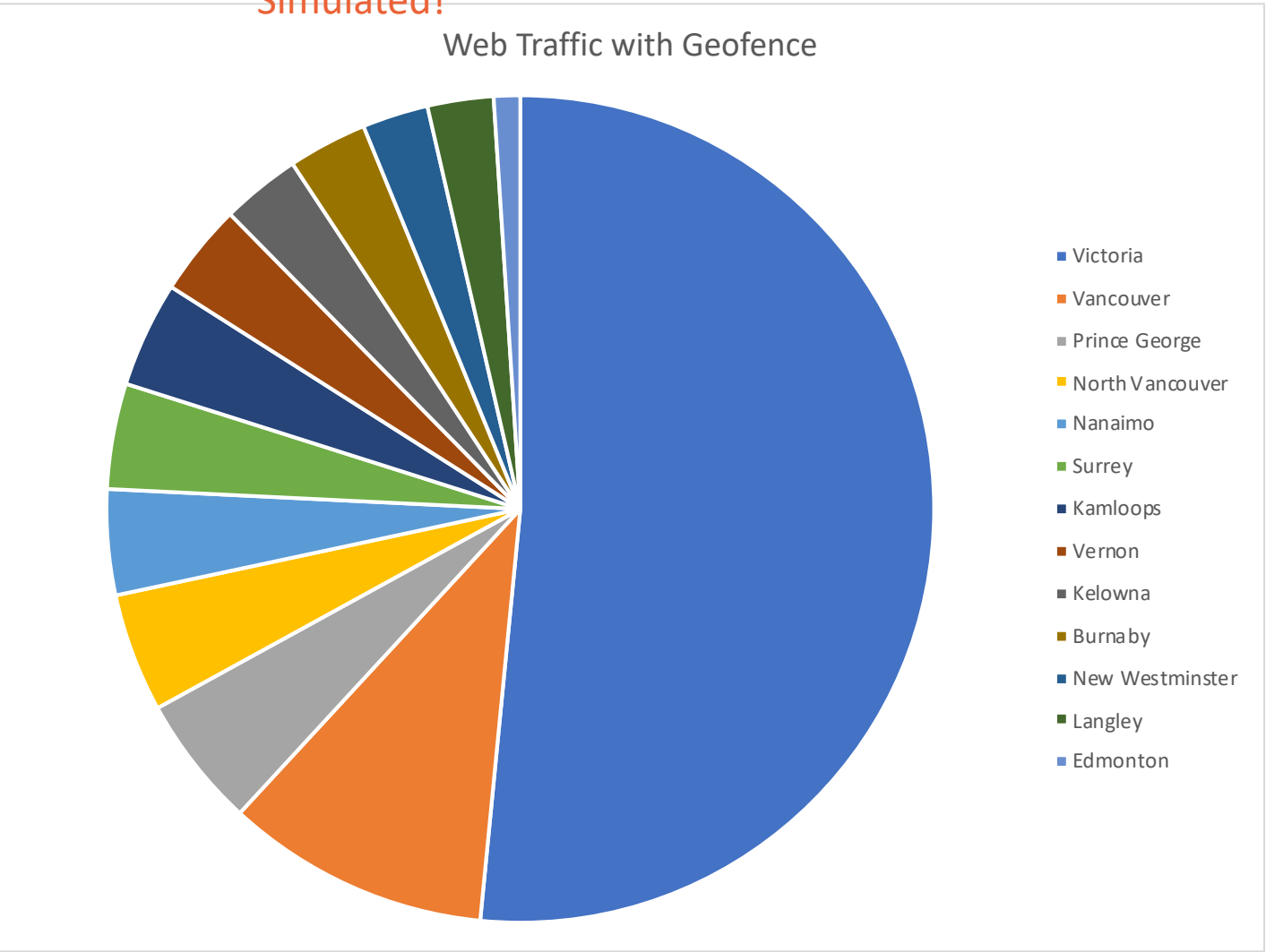


CloudPathfinder

Geofencing

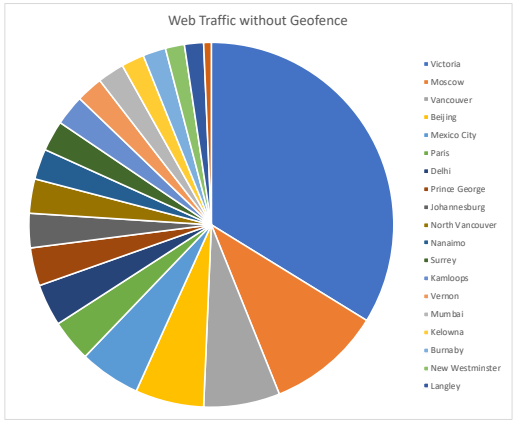
- After implementing
  - Imagine our traffic could look like this:

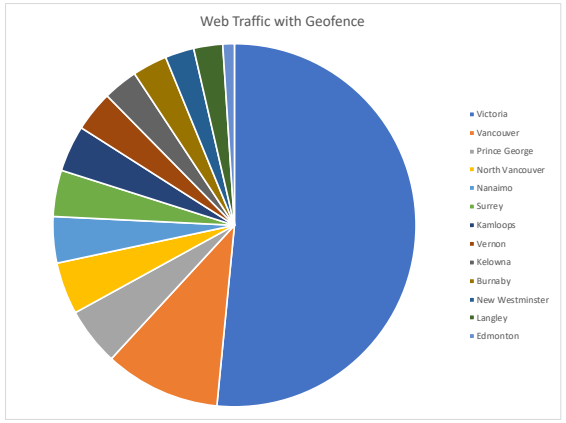
Simulated!

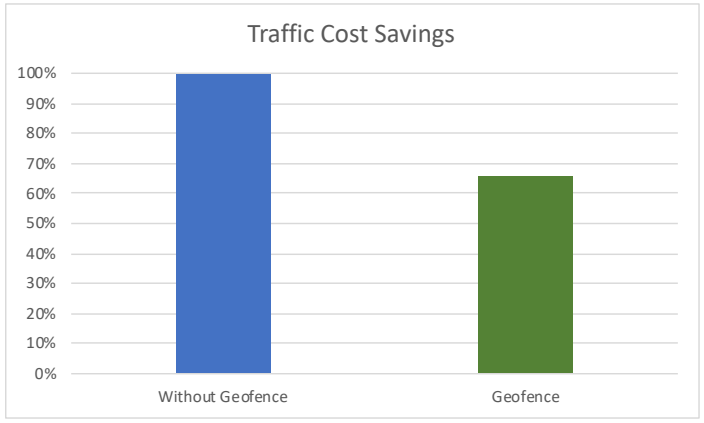


Geofencing Part 2

- 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