



# CloudPathfinder

## Contents

<b>1 Who are you ?</b>	<b>2</b>
1.1 Take a look at your team . . . . .	2
1.2 Product Owner . . . . .	2
1.3 Security . . . . .	3
1.4 Developer . . . . .	4
1.5 Audience . . . . .	5
<b>2 ECF at BC Government</b>	<b>6</b>
2.1 BC Government Enterprise Cloud Factory (ECF) . . . . .	7
2.2 ECF Concepts . . . . .	8
2.3 Public Cloud ECF Services . . . . .	9
2.4 ECF Future Growth . . . . .	11
2.5 Training Landscape . . . . .	12
2.6 Training Components . . . . .	12
2.7 Training Track . . . . .	13
<b>3 Procurement Value Proposition</b>	<b>14</b>
3.1 Negotiation of our First Service Order . . . . .	14
3.2 Procurement Value Add for Ministries . . . . .	16
3.3 Cloud LifeCycle Value Add for Ministries . . . . .	17
<b>4 Shared Responsibility Model</b>	<b>17</b>
4.1 The ECF is non-trivial . . . . .	17
4.2 BC Government AWS ECF . . . . .	20
<b>5 Billing</b>	<b>20</b>
5.1 Billing Examples T-Shirt Estimate Scenario 1 - Small . . . . .	20
5.2 Billing Examples T-Shirt Estimate Scenario 2 - Medium . . . . .	21
5.3 Billing Examples T-Shirt Estimate Scenario 3 - Large . . . . .	21
5.4 Custom Cost Examples ? . . . . .	22
5.5 Billing Process Example . . . . .	23
5.6 JV Process . . . . .	25
<b>6 Communities of practice</b>	<b>25</b>
6.1 Value of Communities . . . . .	25
6.2 Customer Focus – 3 CoPs . . . . .	26
6.3 Service Design Customer Focus . . . . .	26
6.4 Strong Communities in BC Government . . . . .	26
6.5 Focus of Teams and Rocket Chat . . . . .	28

<b>7 Service Levels</b>	<b>31</b>
<b>8 Demo</b>	<b>31</b>
<b>9 Questions ?</b>	<b>32</b>
<b>10 Training &amp; Resources</b>	<b>32</b>
<b>11 Overview</b>	<b>33</b>

## 1 Who are you ?

### 1.1 Take a look at your team

- Teams are comprised of
  - Government employees
  - Contractors
- Roles and titles like
  - Project Manager, Product Owner, Manager, Expense Authority... Ministry Information Security Officer, Ministry Privacy Officer, Architect... Full Stack Developer, DevOps, Technologist, Site Reliability Specialist...

### 1.2 Product Owner



Figure 1: Product owner

### 1.3 Security



#### Security

An incident is where security control has failed or been breached, and the confidentiality, integrity or availability of an asset or a service has been compromised. Anything of harm or potential harm to our environment is seen as an incident.

Each incident has a procedure and a playbook, and some incidents may trigger multiple playbooks if there are multiple components.

Example playbooks: the PICERL (Preparation, Identification, Containment, Eradication, Recovery and Lessons learned), Phishing compromised, Server compromised, Workstations and Credential abuse.



Figure 2: Security

## 1.4 Developer

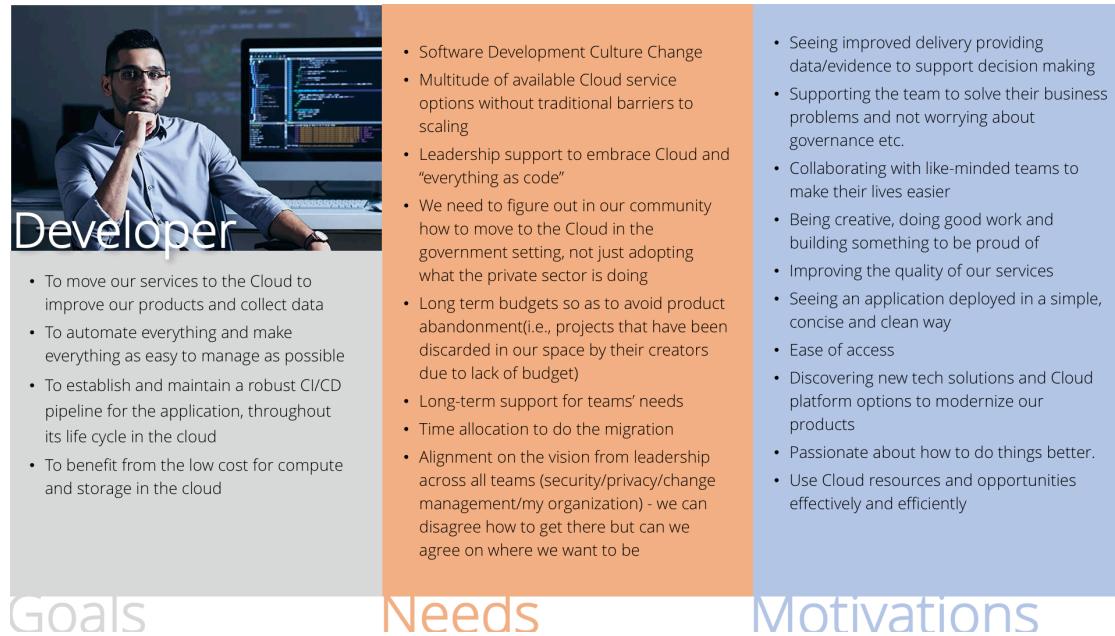


Figure 3: Developer

## 1.5 Audience



Figure 4: people jumping into a swimming pool together

- POs, Devs and Compliance; group start
- Shared understanding from the beginning
- Journey together # About BC Government Cloud
- What is BC Government Cloud Pathfinder ?

::: tip Acronyms

- **GoC** = Government of Canada
- **SEA** = Secure Environment Accelerator
- **CSP** = Cloud Service Provider

:::

- We are a central team in BC Government tasked with delivering Cloud
- We have onboarded to the GoC Cloud Brokerage
- We have a service order with 1 Cloud Service Provider that includes a SEA
- 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

- Customer Focus
  - Our Customers: Project Managers / Product Owners / Expense Authorities
  - Our Users: Developer Teams
  - Compliance Users: Security Operations OCIO
- Good Service
  - Who do I go to if I have quality issues with Cloud Pathfinder's service?

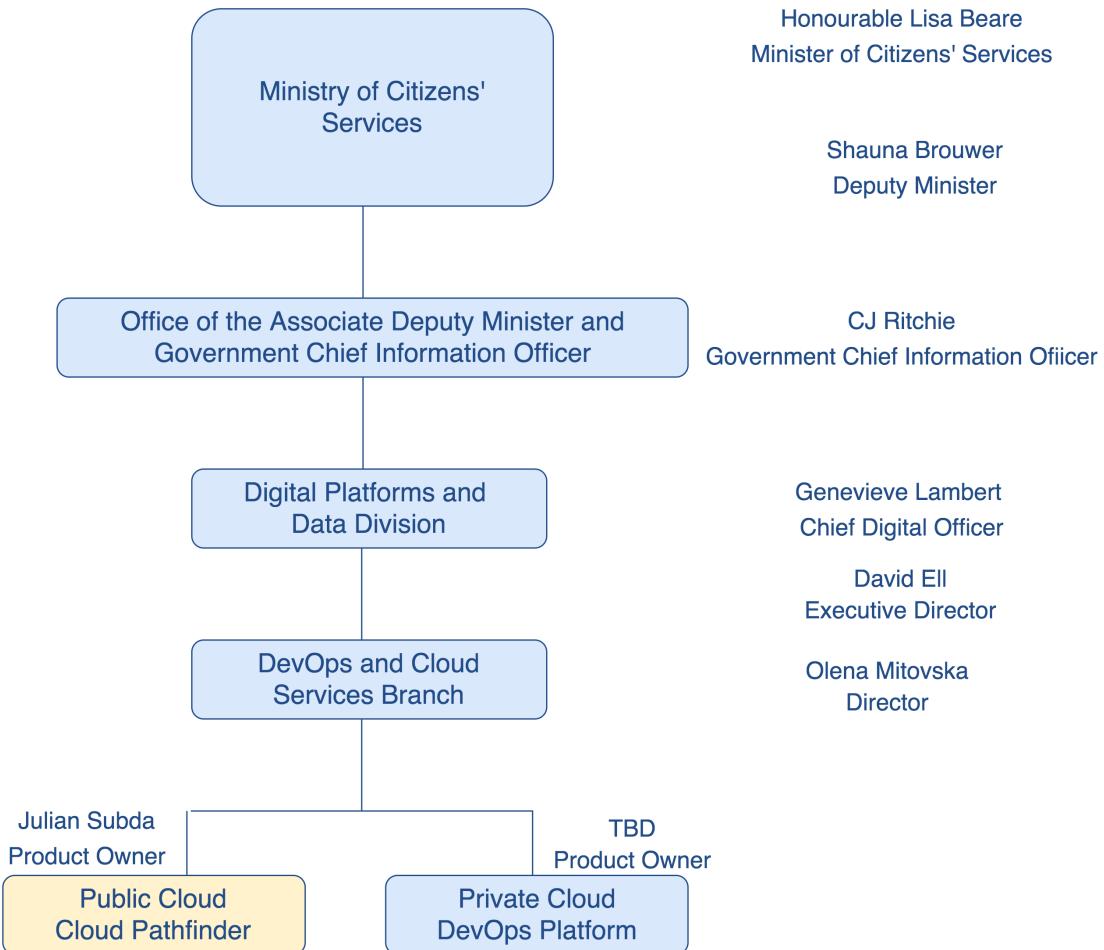


Figure 5: organization ladder

## 2 ECF at BC Government

- The Cloud Pathfinder team have added Automation and Customization layers on top of the Secure Environment Accelerator(SEA) product solution provided by Government of Canada and Cloud Service Provider and calls it Enterprise Cloud Factory.

## 2.1 BC Government Enterprise Cloud Factory (ECF)

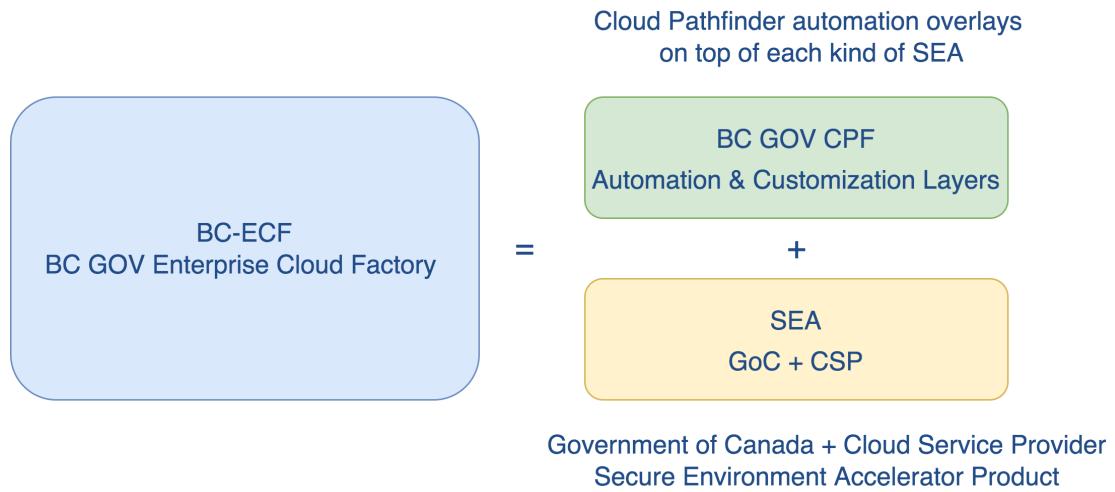


Figure 6: AWS ECF

- AWS ECF at BC Government

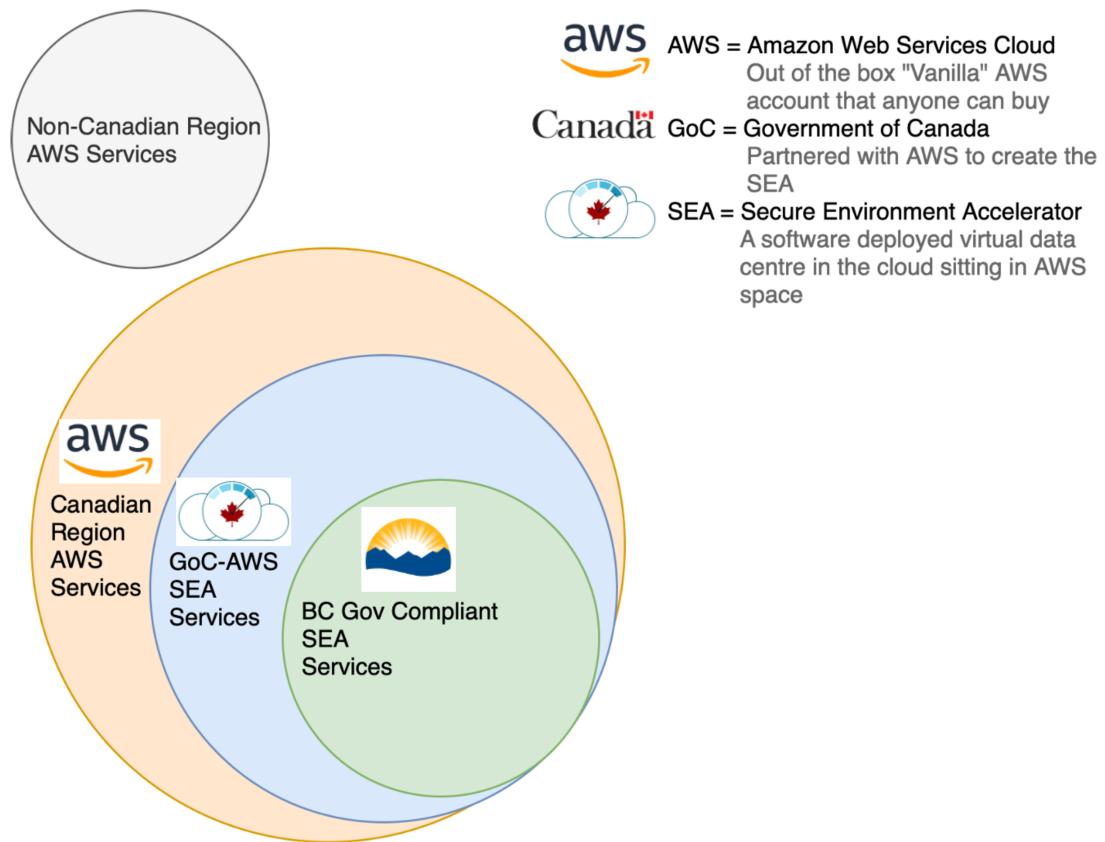


Figure 7: AWS ECF

- The above images shows the relationship between services offered in different scopes of the various contexts of the AWS ECF. BC Government 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.

## 2.2 ECF Concepts

- AWS ECF Concept

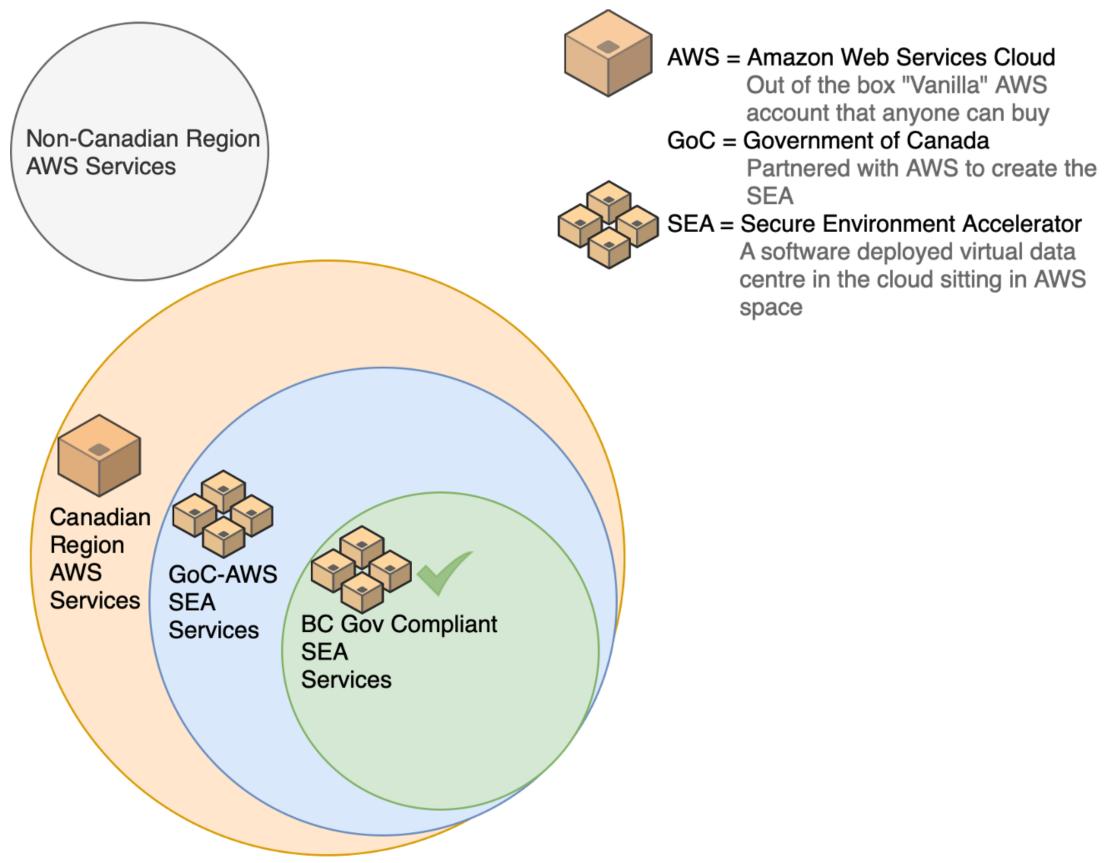


Figure 8: AWS ECF concepts

## 2.3 Public Cloud ECF Services

- AWS

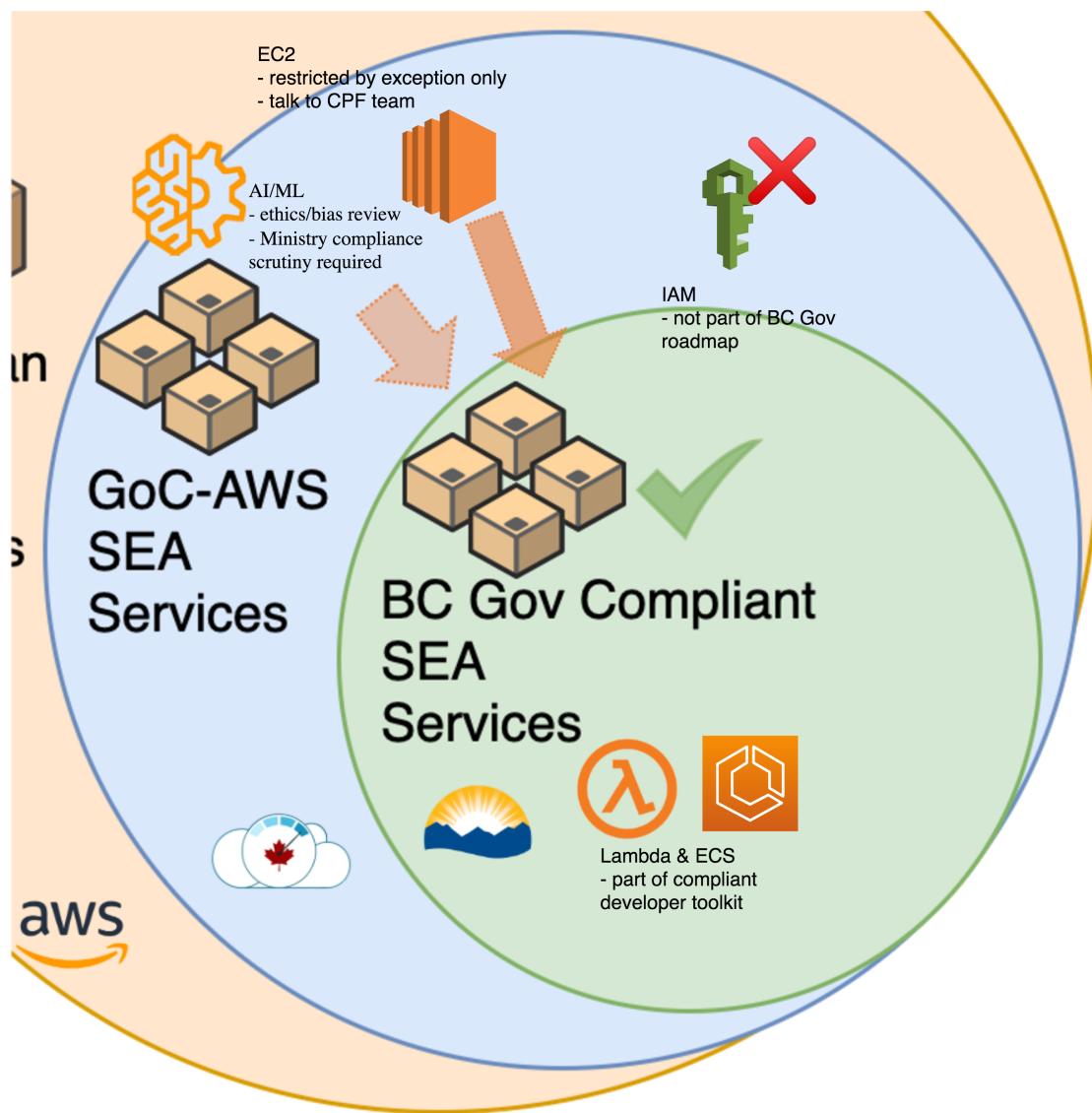


Figure 9: compliant services in aws

::: tip Acronyms

- **CPF:** Cloud pathfinder Team
- **ECS** = Elastic Container Service
- **EC2** = Elastic Compute Cloud/Virtual Machines
- **CSP** = Cloud Service Provider
- **Lambdas** = 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

...:

- We are aiming for a common service experience regardless of which cloud you are consuming in BC Government.

## 2.4 ECF Future Growth

Depicted as follows is the growth of services in AWS over time

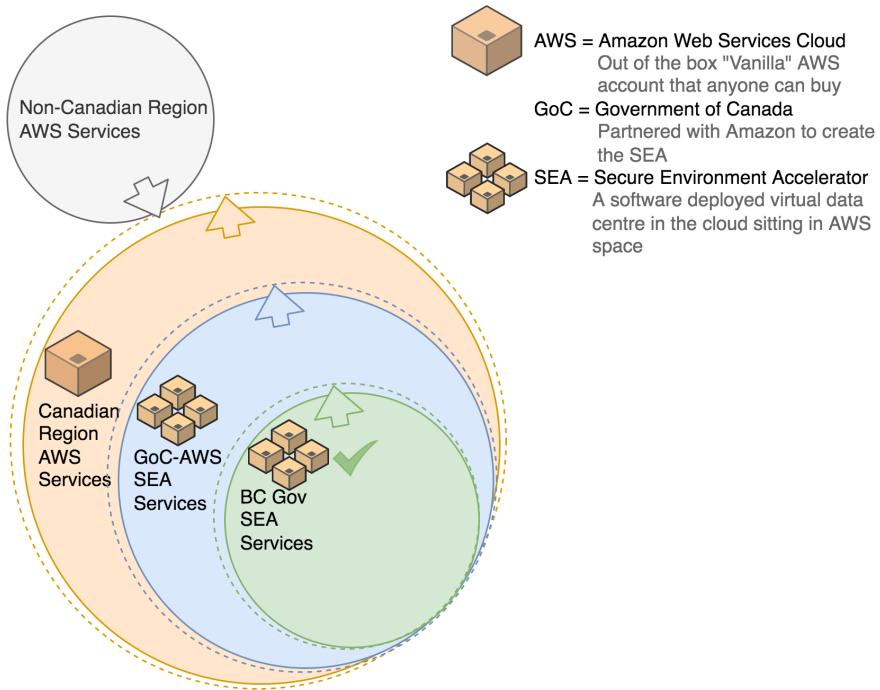


Figure 10: Future growth of AWS ECF

- Over time, regardless of the particular brand of the cloud, the number of services in the ECF available to BC Government teams will go up and we expect the green set of services

to mostly overlap the blue.

## 2.5 Training Landscape

Below is the Training landscape for the AWS

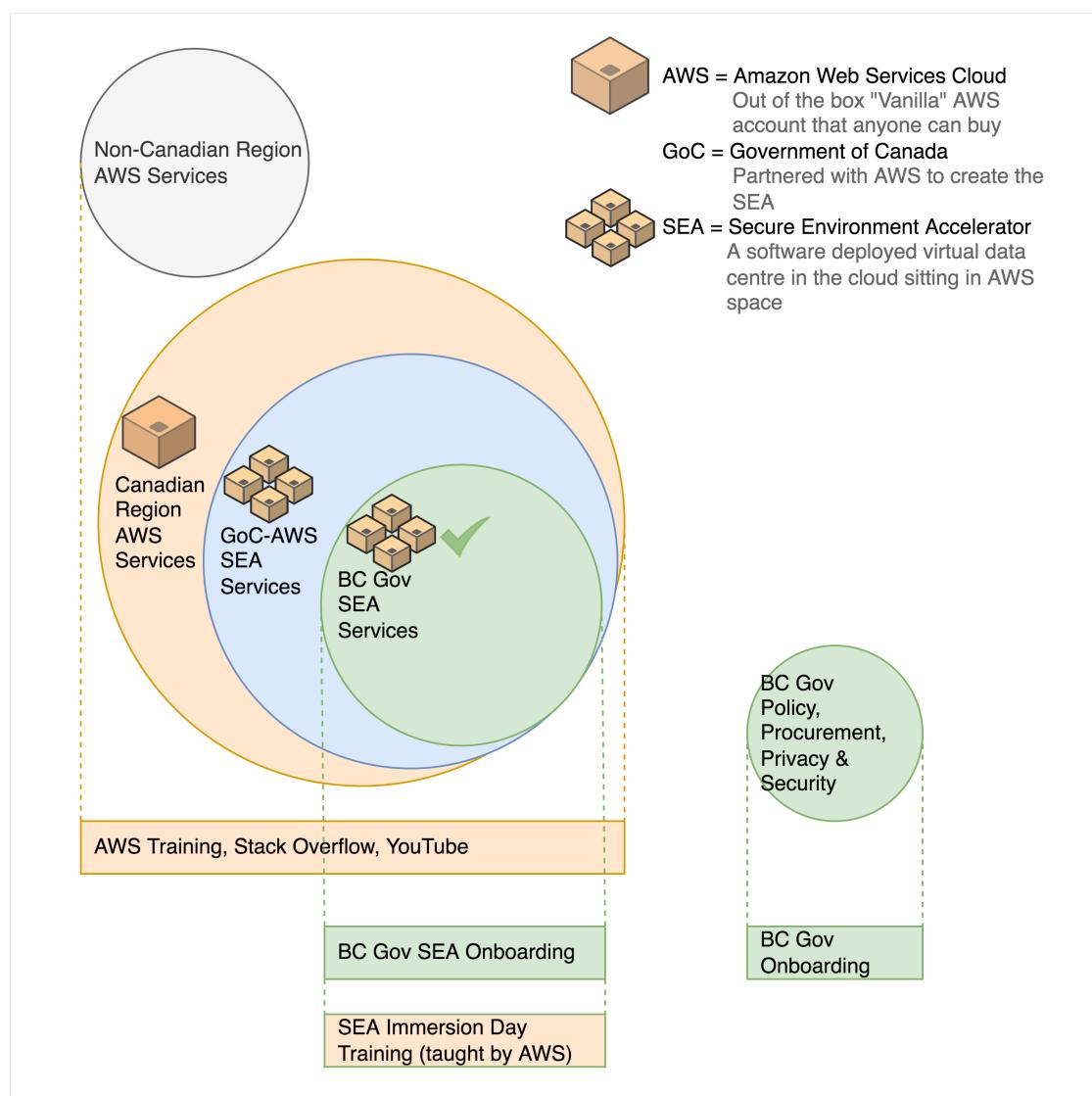


Figure 11: Trainig Landscape

## 2.6 Training Components

- AWS ECF Training Components

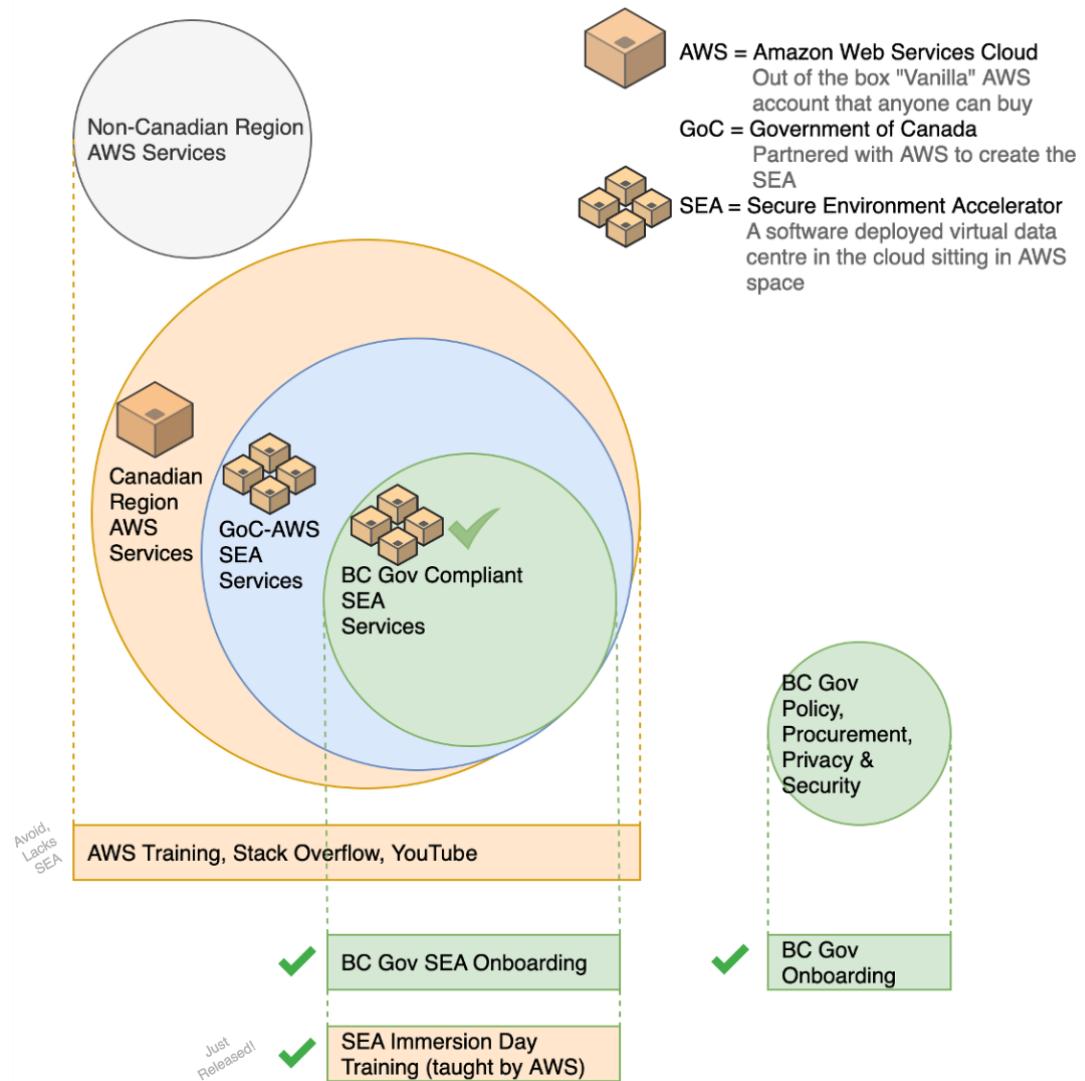


Figure 12: Training Components

- 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 ECF. We show them equivalent, safe ways of operating in the ECF.

## 2.7 Training Track

- Training Track (all CSP pattern)

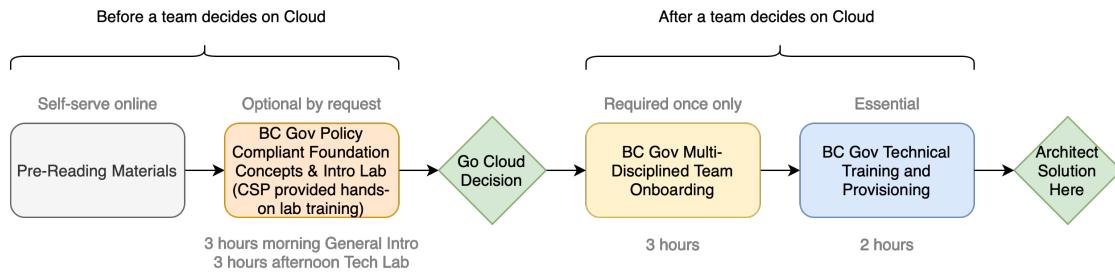


Figure 13: Trainig Track

### 3 Procurement Value Proposition

#### 3.1 Negotiation of our First Service Order

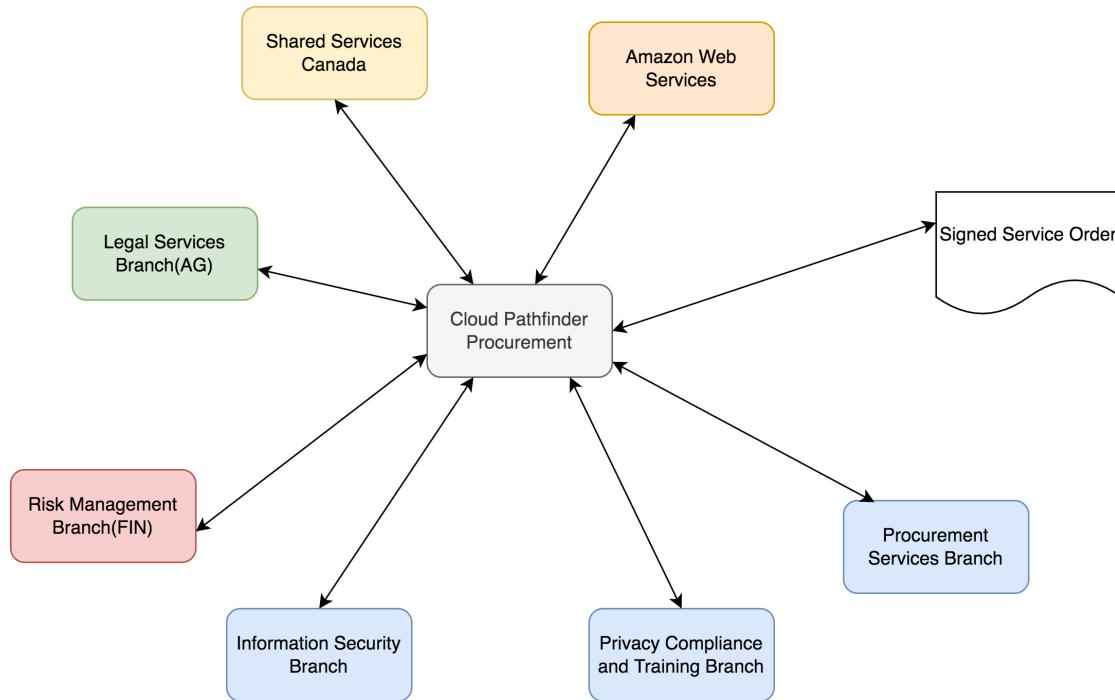


Figure 14: negotiation of our first service order

Actually it went more like this

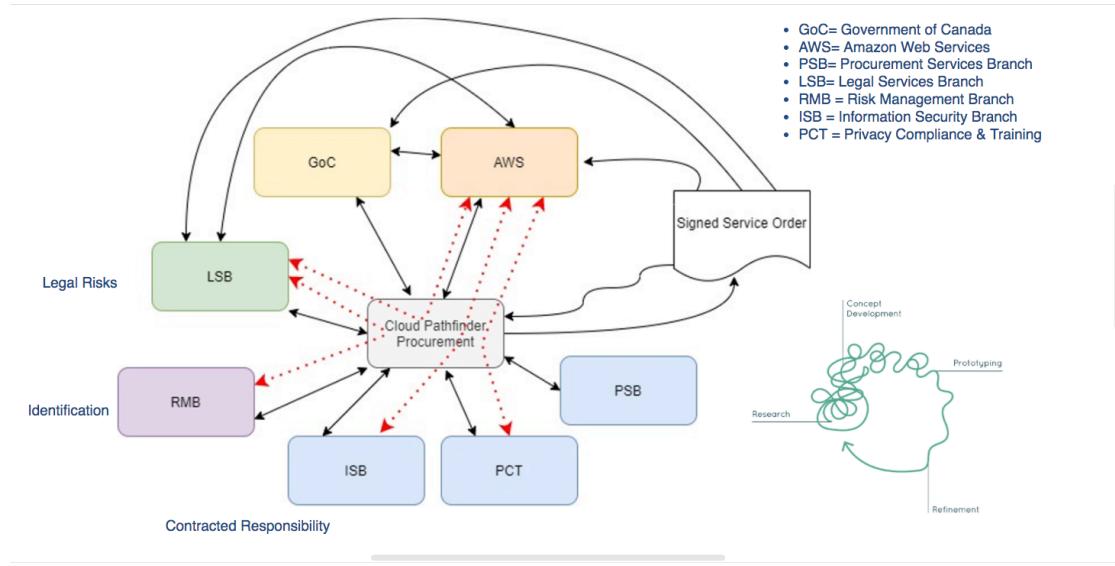


Figure 15: How it actually went

### 3.2 Procurement Value Add for Ministries

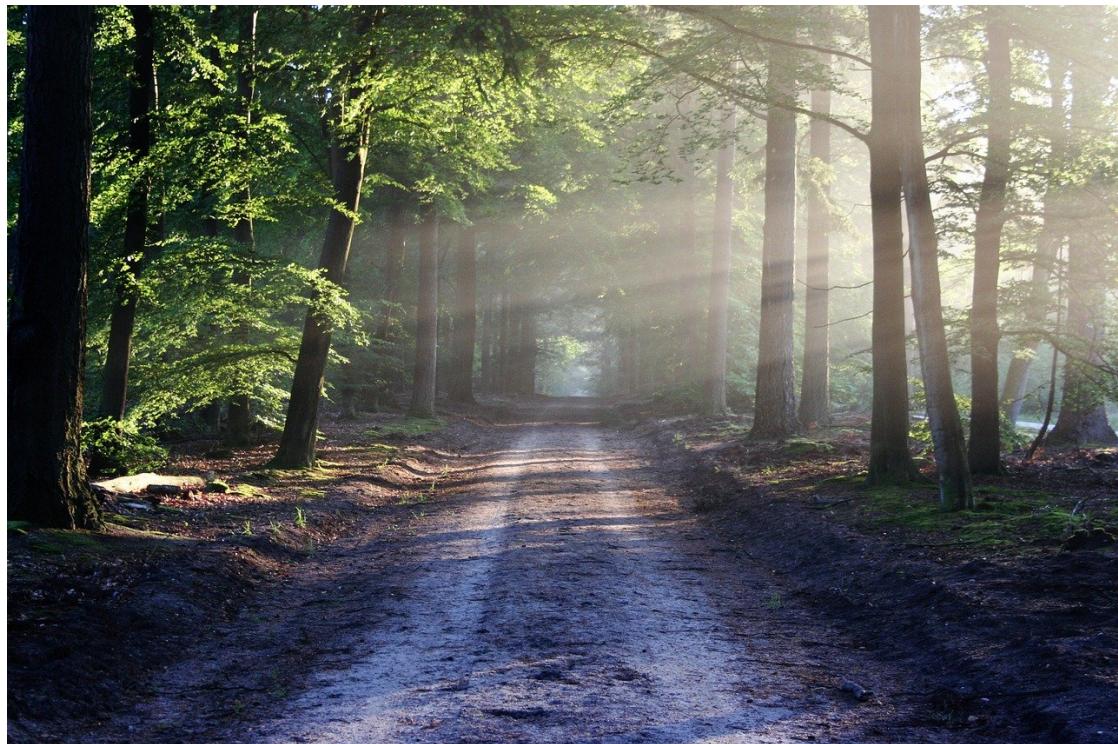


Figure 16: pathway in a forest with trees on either side

- Don't have to negotiate privacy, security, legal terms with vendors
- Don't have to dig into the cloud services
- Only need to focus on describing their project in the PIA and STRA

### 3.3 Cloud LifeCycle Value Add for Ministries

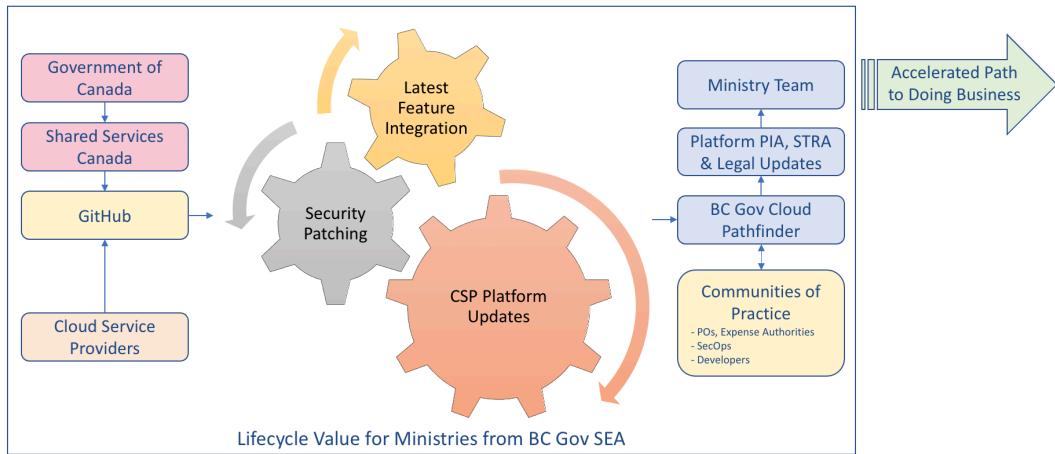


Figure 17: cloud value for ministries

## 4 Shared Responsibility Model

Please refer to DevHub for the Shared Responsibility Model. # Providing an ECF Service

### 4.1 The ECF is non-trivial

- There is a lot of complexity that is simplified by Cloud Pathfinder providing ECF 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 Below Images shows the Complexity of the ECF

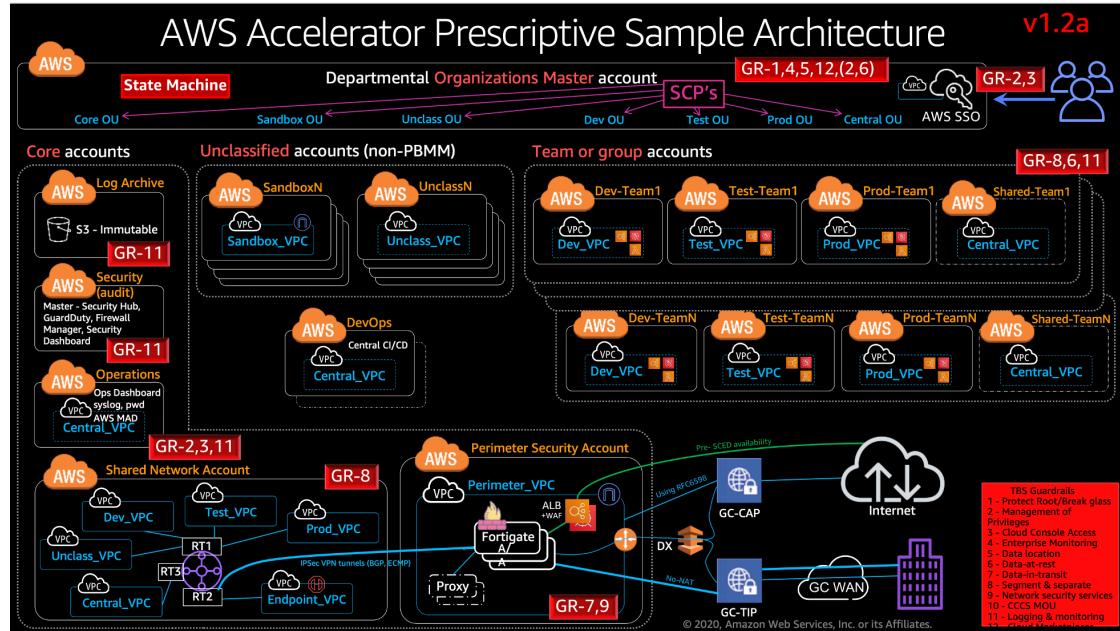


Figure 18: The ECF Architecture

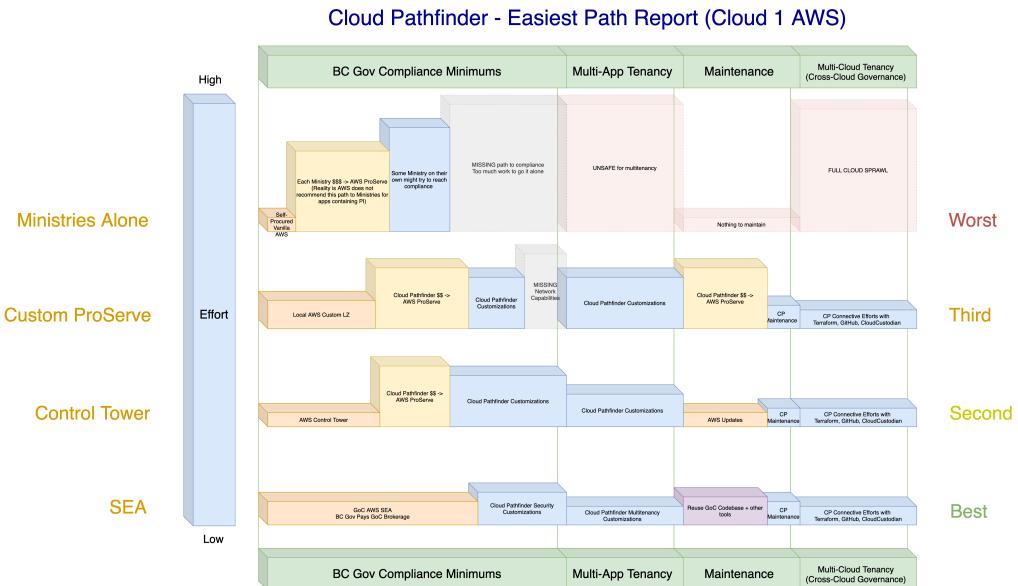


Figure 19: Cloud pathfinder easiest path report

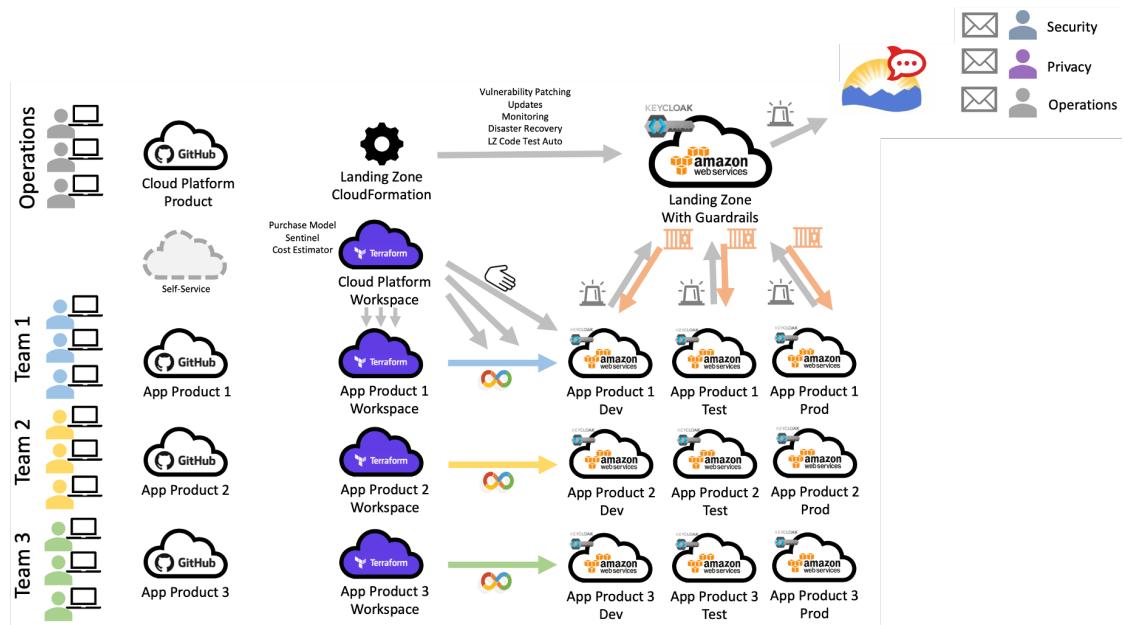


Figure 20: BC Government AWS Early version

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

## 4.2 BC Government AWS ECF

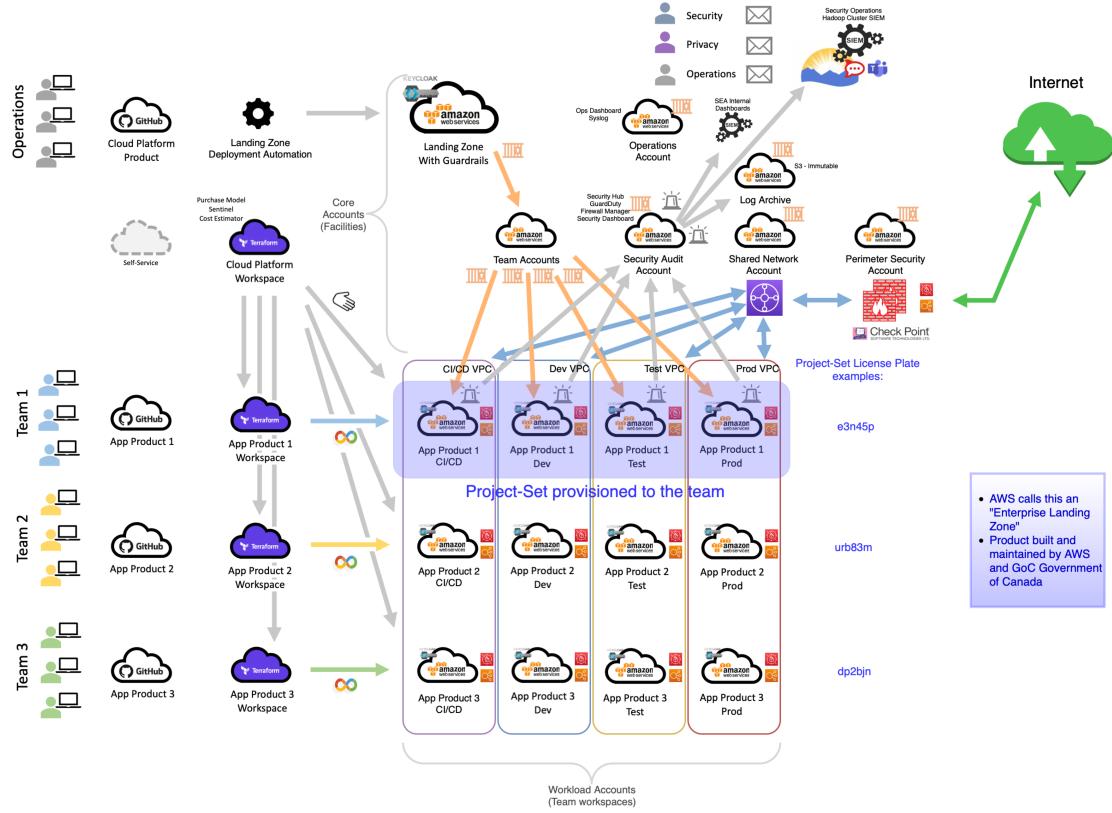


Figure 21: BC Government AWS ECF

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

## 5 Billing

### 5.1 Billing Examples T-Shirt Estimate Scenario 1 - Small

! Usage based Expense may increase or decrease

AWS Services	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	1 GB, 1 million requests	\$ 4.00

AWS Services	Metrics	Estimated Expense / Month
Elastic Container Service - Fargate	1 container deployed twice, each 2 vCPU, 4GB	\$ 48.39
Data Transfer Out	50 GB	\$ 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.

## 5.2 Billing Examples T-Shirt Estimate Scenario 2 - Medium

! Usage based Expense may increase or decrease

AWS Services	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	10 GB, 10 million requests	\$ 18.00
Elastic Container Service - Fargate	3 container deployed twice, each 2 vCPU, 4GB	\$ 145.16
Data Transfer Out	500 GB	\$ 45.00
Amazon CloudWatch Logs	500 GB	\$ 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.

## 5.3 Billing Examples T-Shirt Estimate Scenario 3 - Large

! Usage based Expense may increase or decrease

AWS Services	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	100 GB, 100 million requests	\$ 178.00
Elastic Container Service - Fargate	3 container deployed twice, each 2 vCPU, 4GB	\$ 145.16
Data Transfer Out	5000 GB	\$ 450.00
Amazon CloudWatch Logs	5000 GB	\$ 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.

## 5.4 Custom Cost Examples ?

Yes!

- AWS Pricing Calculator

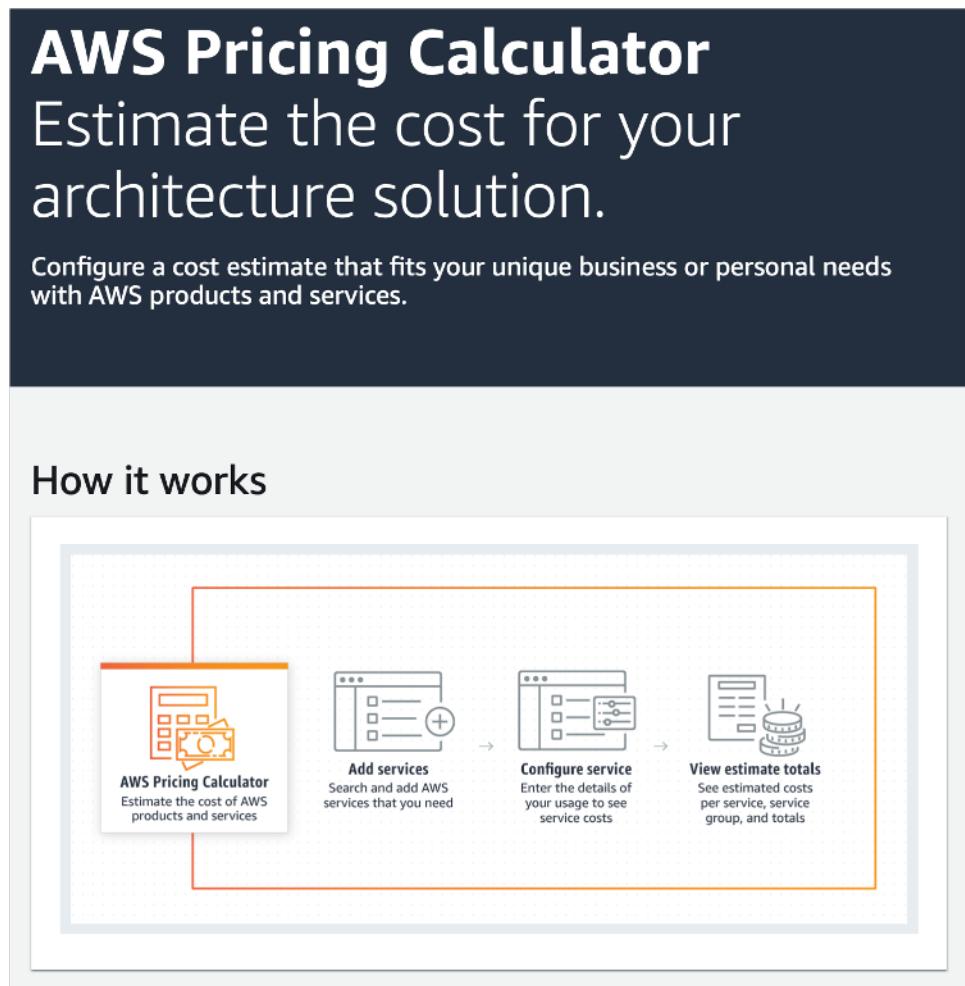


Figure 22: Screen Shot of the AWS Price Calculator page

- Use AWS Pricing Calculator for now

## 5.5 Billing Process Example

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

FW: Cloud Consumption Report \$78.14 for 27-04-2022 to 03-05-2022.



On 2022-05-04, 9:44 AM, "[info@cloud.gov.bc.ca](mailto:info@cloud.gov.bc.ca)" <[info@cloud.gov.bc.ca](mailto:info@cloud.gov.bc.ca)> wrote:

Hello [REDACTED]

Please find attached your billing reports for the period from 27-04-2022 to 03-05-2022.

Total Charges: \$78.14 CAD

Projects:



Regards,

The Cloud Pathfinder Team

---

Figure 23: sample weekly billing report email

- Email sent out to owners of the project every week with attached consumption report.
- The Email contains information about the total cloud consumption cost across the environments and the details of the environments for the period mentioned in the email.
- The Excell spredsheet attached to the email contains the cost spent on each resource inside the environment
- Note that the cost also include the baseline costs for running the Secure Environment Accelerator guardrail and logging services within each account. You will see service charges from CloudTrail, CloudWatch, Systems Manager, Secrets Manager, S3, Simple Queue Service, Simple Notification Service, AWS Config, Elastic Load Balancing, GuardDuty, Key Management Service, Lambda, Macie, Security Hub, NAT gateway. If your team has a SandBox account workload environment, you will see EC2 charges due to the independent direct networking. We will will be migrating teams away from SandBoxes to more protected workload environments better aligned to the guardrails.

1	year	month	line_item_usage_account_id	Account_Name	Project	License_Plate	Environment	Billing_Group	Owner_Name	Owner_Email	line_item_product_code	product_product_name	line_item_billed_cost	CAD	
2	2022	4				dev	AWSCloudTrail	AWS CloudTrail	\$0.59			\$0.24			
3	2022	4				dev	AWSConfig	AWS Config	\$0.59			\$0.24			
4	2022	4				dev	AWSLambda	AWS Lambda	\$0.00			\$0.00			
5	2022	4				dev	AWSLambda	AWS Lambda	\$0.00			\$0.00			
6	2022	4				dev	AWSQueueService	AWS Simple Queue Service	\$0.00			\$0.00			
7	2022	4				dev	AWSSecretsManager	AWS Secrets Manager	\$0.05			\$0.07			
8	2022	4				dev	AWSSecurityHub	AWS Security Hub	\$3.10			\$9.97			
9	2022	4				dev	AWSStepFunctions	AWS Step Functions	\$0.00			\$0.00			
10	2022	4				dev	AwsGuardDuty	Aws GuardDuty	\$0.39			\$0.50			
11	2022	4				dev	AwsMacie	Aws Macie	\$0.01			\$0.02			
12	2022	4				dev	AwsMacie	Aws Macie	\$0.00			\$0.00			
13	2022	4				dev	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
14	2022	4				dev	AwsMacieNS	Aws Macie	\$0.00			\$0.01			
15	2022	4				test	AWSCloudTrail	AWS CloudTrail	\$0.03			\$0.04			
16	2022	4				test	AWSConfig	AWS Config	\$1.77			\$2.26			
17	2022	4				test	AWSCloudWatchLogs	AWS CloudWatch Logs	\$0.53			\$0.61			
18	2022	4				test	AWSLambda	AWS Lambda	\$0.00			\$0.00			
19	2022	4				test	AWSSimpleQueueService	AWS Simple Queue Service	\$0.00			\$0.00			
20	2022	4				test	AWSStepFunctions	AWS Step Functions	\$0.00			\$0.00			
21	2022	4				test	AWSSecurityHub	AWS Security Hub	\$3.35			\$4.30			
22	2022	4				test	AwsCloudWatchLogs	Aws CloudWatch Logs	\$0.42			\$0.44			
23	2022	4				test	AwsGuardDuty	Aws GuardDuty	\$0.01			\$0.02			
24	2022	4				test	AwsMacie	Aws Macie	\$0.00			\$0.00			
25	2022	4				test	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
26	2022	4				test	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
27	2022	4				test	Awskms	AWS Key Management Service	\$0.40			\$0.51			
28	2022	4				sandbox	AWSCloudTrail	AWS CloudTrail	\$0.03			\$0.04			
29	2022	4				sandbox	AWSConfig	AWS Config	\$0.51			\$0.65			
30	2022	4				sandbox	AWSGlue	AWS Glue	\$0.00			\$0.00			
31	2022	4				sandbox	AWSGlueService	AWS Glue Service	\$0.00			\$0.00			
32	2022	4				sandbox	AWSGuardManager	AWS Guard Manager	\$0.00			\$0.00			
33	2022	4				sandbox	AWSIdentityHub	AWS Identity Hub	\$3.00			\$3.85			
34	2022	4				sandbox	AWSLambda	AWS Lambda	\$0.00			\$0.00			
35	2022	4				sandbox	AWSLambda	AWS Lambda	\$0.00			\$0.01			
36	2022	4				sandbox	AwsDynamoDB	Aws DynamoDB	\$0.00			\$0.00			
37	2022	4				sandbox	AwsDynamoDB	Aws DynamoDB	\$4.73			\$6.09			
38	2022	4				sandbox	AwsDynamoDB	Aws DynamoDB	\$0.28			\$0.34			
39	2022	4				sandbox	AmazonMacie	Amazon Macie	\$0.03			\$0.03			
40	2022	4				sandbox	AwsMacie	Aws Macie	\$0.00			\$0.00			
41	2022	4				sandbox	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
42	2022	4				sandbox	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
43	2022	4				sandbox	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
44	2022	4				prod	AWSCloudTrail	AWS CloudTrail	\$0.03			\$0.04			
45	2022	4				prod	AWSConfig	AWS Config	\$1.77			\$2.27			
46	2022	4				prod	AWSCloudWatchLogs	AWS CloudWatch Logs	\$0.53			\$0.61			
47	2022	4				prod	AWSGuardManager	AWS Guard Manager	\$0.00			\$0.00			
48	2022	4				prod	AWSIdentityHub	AWS Identity Hub	\$0.00			\$0.00			
49	2022	4				prod	AWSLambda	AWS Lambda	\$0.00			\$0.00			
50	2022	4				prod	AWSLambda	AWS Lambda	\$0.00			\$0.00			
51	2022	4				prod	AwsCloudWatchLogs	Aws CloudWatch Logs	\$0.00			\$0.00			
52	2022	4				prod	AwsGuardDuty	Aws GuardDuty	\$0.26			\$0.31			
53	2022	4				prod	AwsMacie	Aws Macie	\$0.01			\$0.02			
54	2022	4				prod	AwsMacieNS	Aws Macie	\$0.01			\$0.02			
55	2022	4				prod	AwsMacieNS	Aws Macie	\$0.00			\$0.00			
56	2022	4				prod	AwsMacieNS	Aws Macie	\$0.00			\$0.00			

Figure 24: Example SpreadSheet Report

## 5.6 JV Process

- Accounting process that enables
  - Cloud Services Providers and Shared Services Canada to invoice BC Government, and
  - You the ministry teams to pay-per-use to cover this cost while
  - We endeavour to provide a transparent experience
- Occurs every 3 months

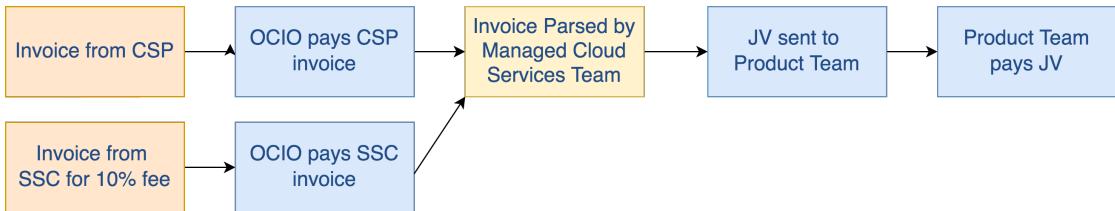


Figure 25: JV Process

## 6 Communities of practice

### 6.1 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

## 6.2 Customer Focus – 3 CoPs

::: tip Acronyms

- **OCIO** = Office of the Associate Deputy Minister and Government Chief Information Officer
  - **CoP** = Community of Practise
  - **SecOps** = OCIO Security Operations Team
  - **MISO** = Ministry Information Security Officer, embedded as part of the developer team
- :::
- Our Customers: Project Managers / Product Owners / Expense Authorities
  - Our Users: Developer Teams
  - Compliance Users: Security Operations OCIO, MISOs

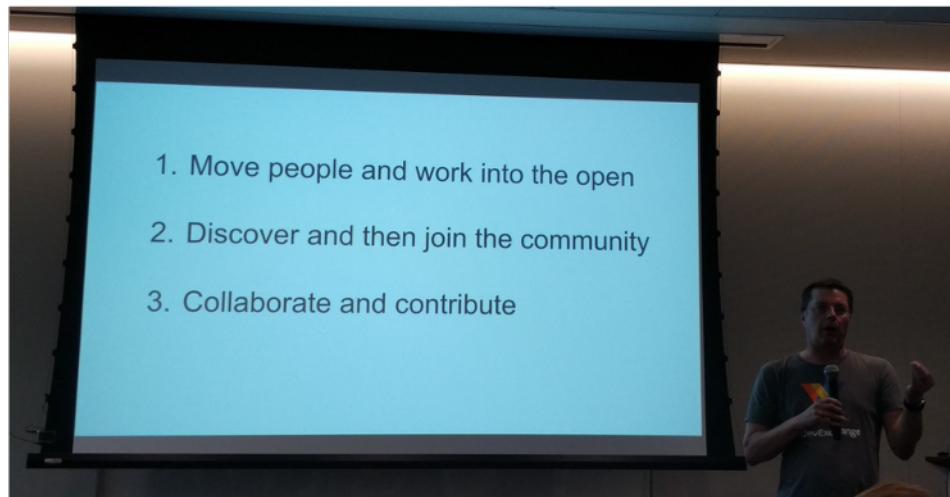
## 6.3 Service Design Customer Focus

::: tip 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

## 6.4 Strong Communities in BC Government

- 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

## 6.5 Focus of Teams and Rocket Chat

Focus on Teams



Image credit to [www.mikewashburn.net/blog/2020/2/19/but-what-are-you-making](http://www.mikewashburn.net/blog/2020/2/19/but-what-are-you-making)

Figure 26: image of microsoft teams

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

Focus of RocketChat

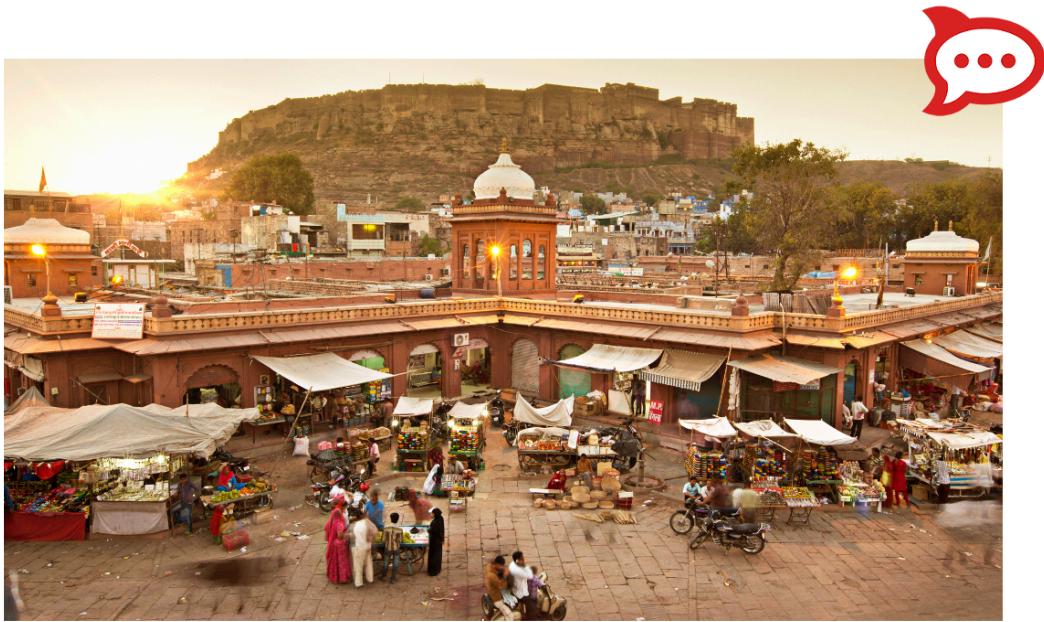


Image credit to [placetovisit.city/places-in-jodhpur](http://placetovisit.city/places-in-jodhpur)

Figure 27: image of rocketchat

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

Recommend Both!



Image credit to [Creative Commons](#)

Bazaar Frontage with Workshops

Figure 28: image of rocket chat

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

A Teams platform



Figure 29: logo of microsoft teams

A Community platform



Figure 30: Rocket chat logo

- Cloud Pathfinder is available on both
- Cloud Pathfinder Rocket chat channel : aws-lz2

## 7 Service Levels

- 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!)

## 8 Demo

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

## 9 Questions ?



Figure 31: image for questions and answers

- \*This is where we would normally have a discussion if we were doing a live session

## 10 Training & Resources

- Secure Environment Accelerator (Canada)
- Building a serverless web application architecture for the AWS Secure Environment Accelerator
- AWS Serverless Application Repository
- AWS Secure Environment Accelerator (ASEA) connectivity with VMware Cloud on AWS
- Canadian Centre for Cyber Security adds additional AWS services to its assessment of the AWS Canada (Central) Region



Figure 32: logo called Cloud Pathfinder

## 11 Overview

Welcome to the Cloud Pathfinder Pre-Reading Material which is the information Pack for BC Gov Ministry Teams Considering Cloud.

Today we will go over the below topics

- Who are You ?
- About BC Gov Cloud
- ECF at BC Gov
- Procurement Value Proposition
- Shared Responsibility
- Providing an ECF service
- Billing
- Communities of Practice
- Service Levels
- Demos
- Questions & Answers
- Training & Resources