An Introduction to GCC 2.0 and its Key Constructs

Tang Bing Wan
Principal Infrastructure Architect
CODEX / GDS Central
10 March 2022

Viewing Bing Wah GovTech's...

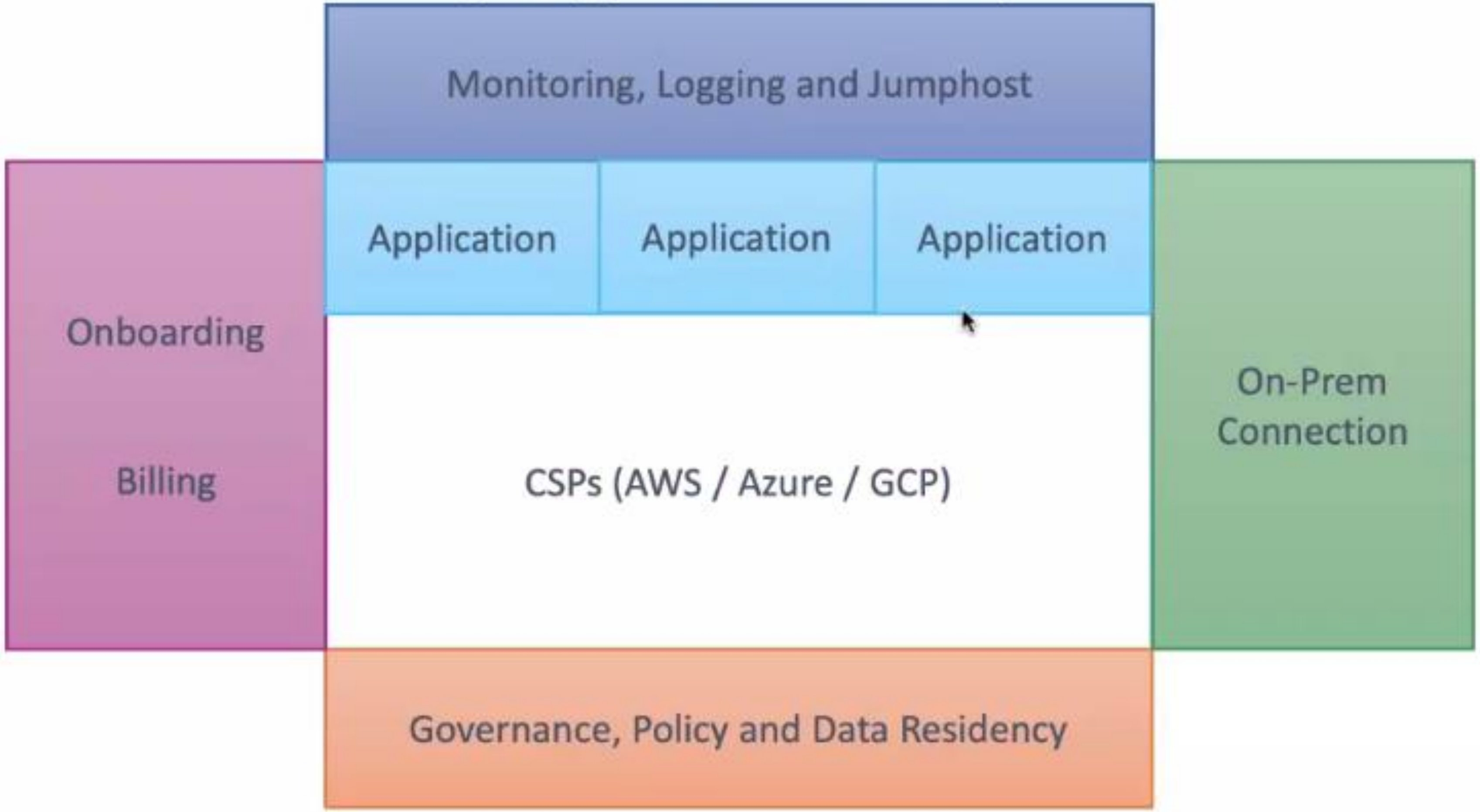
TABLE OF CONTENTS

1. Introduction
2. Endpoint Management
3. New Onboarding Experience
4. Networking Constructs

Viewing Bing Wan GovTech's...

What We Learnt in GCC 1.0

CSPs not quite ready for enterprise (more appliance-based than service)

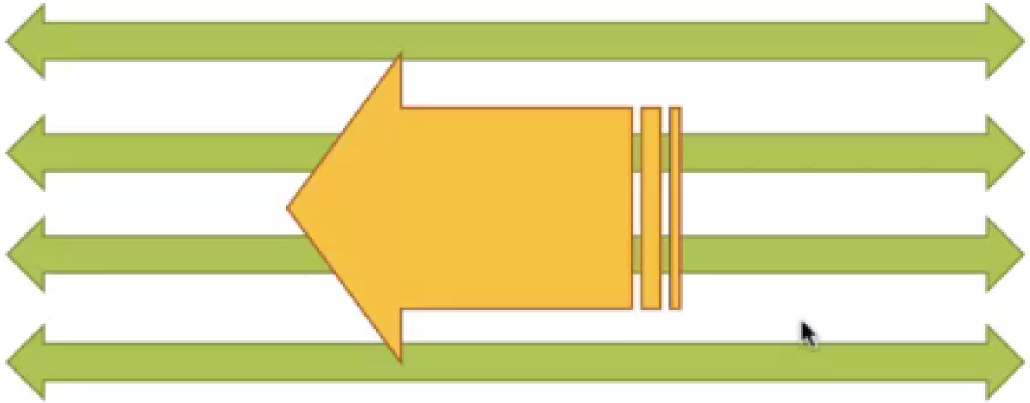


Multiple accounts is the greatest friction for effective use

Connectivity to on-premise remains important

Implementation of system policies need not be one-size-fits-all

A Rethink is Needed for GCC



Cloud	**On-premise**
Software	Hardware
Service	Appliance
IAM-focused	Firewall-focused
Generalists	Specialists

- Make cloud platform code first-class
- Encourage the use of cloud services over appliance
- Set up a basis of strong IAM controls
- Build in-house capability to engineer the cloud platform

Viewing Bing Wan GovTech's...

GCC 2.0 – Where are the Focus Areas

Government on Commercial Cloud

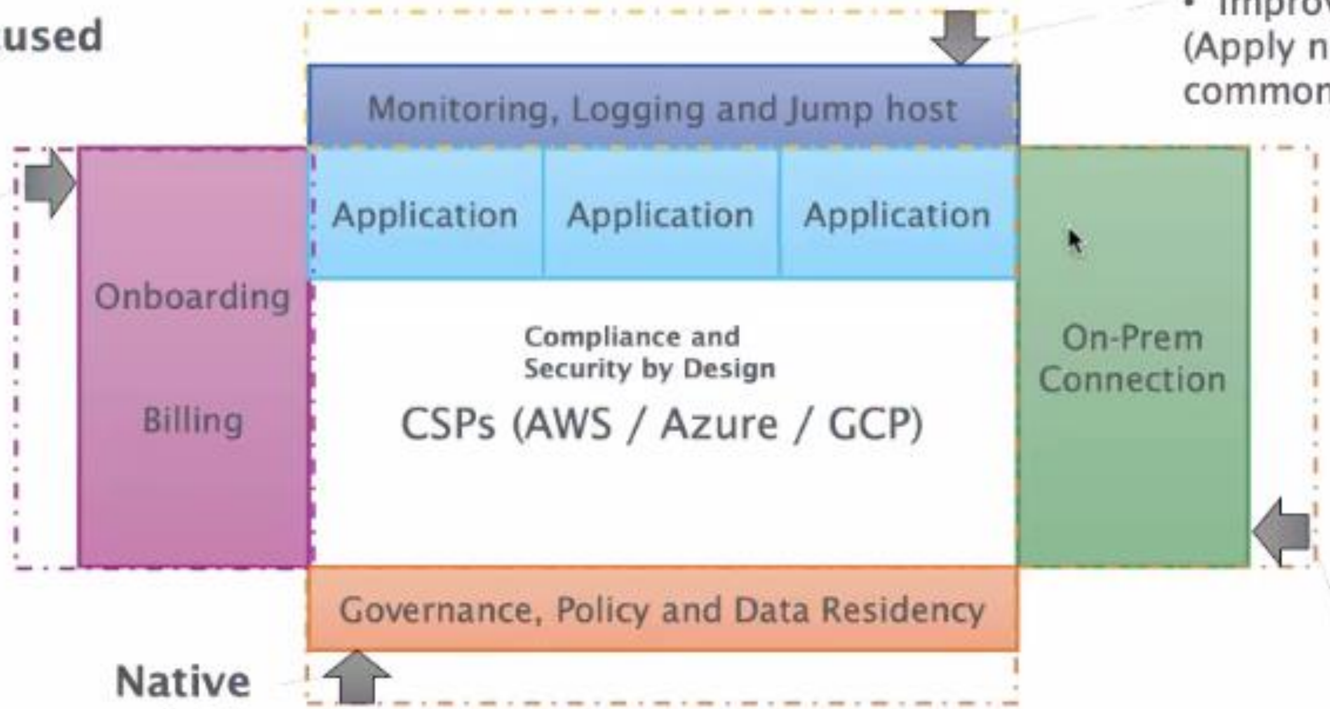
Improved Observability and Auditability

- GCC Jump Host Removal and Cost Reduction
- Improved monitoring

(Apply native jump host solution and common logging to mitigate security risk)

Customer-focused

Accelerate & Simplify Onboarding (Leverage TechPass)


Monitoring, Logging and Jump host
Application
Application
Application
Onboarding
Billing
Compliance and Security by Design
CSPs (AWS / Azure / GCP)
On-Prem Connection
Governance, Policy and Data Residency

Automate Everything

Accelerate Firewall Opening (Work with CSG / Nucleus to speed up firewall opening)

Native solutions over builds

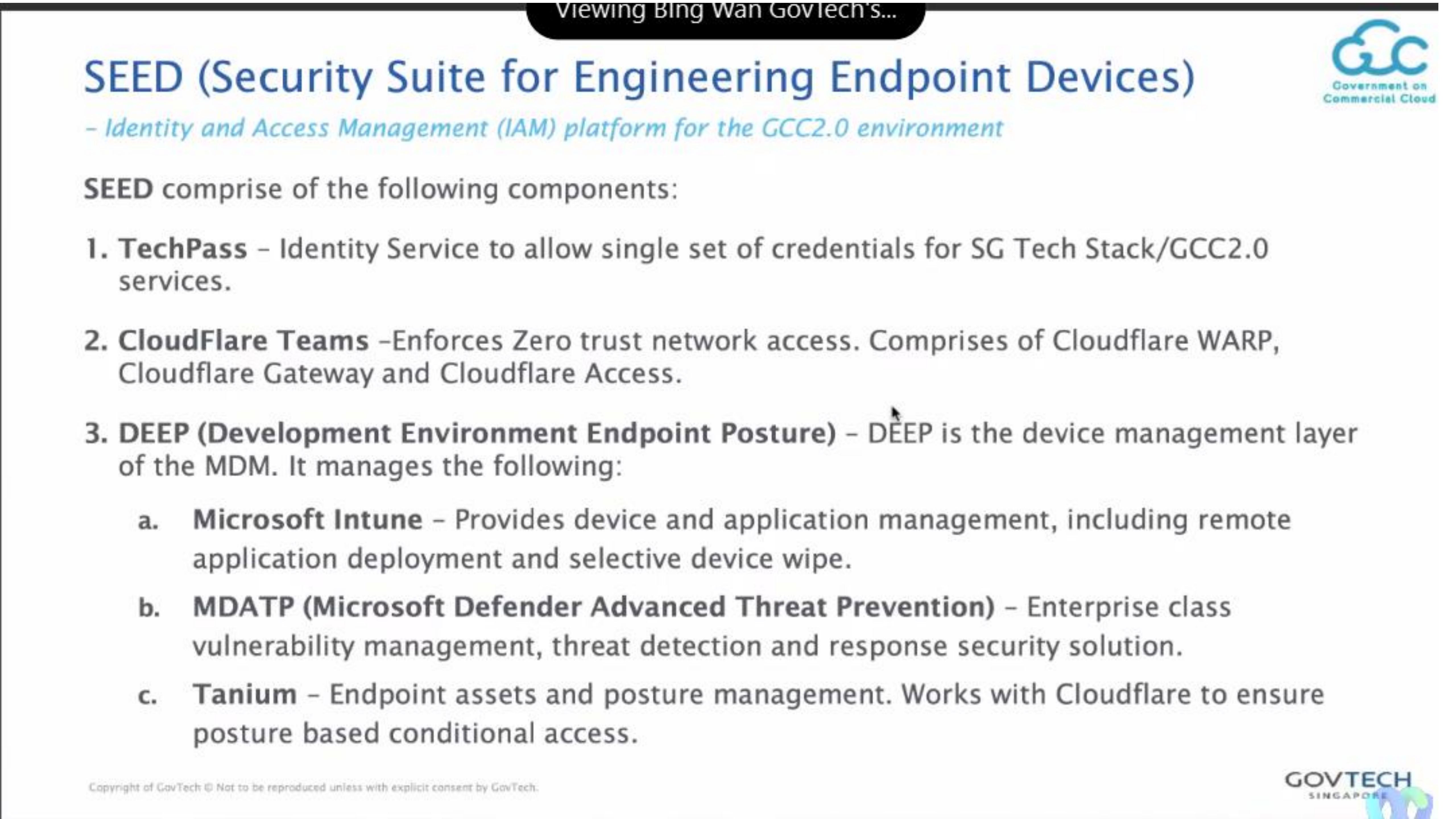
GOVTECH SINGAPORE

Viewing Bing Wan GovTech's...

Endpoint Management

New Endpoint Management Constructs (Common Terms)

- **GFE – Government Furnished Equipment**
  - A device that is issued by a Government Agency.
- **GSIB – Government Standard Image Build**
  - Standard Operating Environment (SOE) devices issued by Government.
- **SEED - Security Suite for Engineering Endpoint Device**
  - Mobile Device Management platform for GCC2.0 and more.
- **DEEP - Developers' Environment Endpoint Posture**
  - 'Brains' of the Posture Attestation.
- **GMD – Government Managed Device**
  - An internet device that has been onboarded to SEED (MDM). The original device can be a GFE or Vendor supplied equipment.



SEED (Security Suite for Engineering Endpoint Devices)

– Identity and Access Management (IAM) platform for the GCC2.0 environment

SEED comprise of the following components:

1. **TechPass** – Identity Service to allow single set of credentials for SG Tech Stack/GCC2.0 services.
2. **CloudFlare Teams** –Enforces Zero trust network access. Comprises of Cloudflare WARP, Cloudflare Gateway and Cloudflare Access.
3. **DEEP (Development Environment Endpoint Posture)** – DEEP is the device management layer of the MDM. It manages the following:
   a. **Microsoft Intune** – Provides device and application management, including remote application deployment and selective device wipe.
   b. **MDATP (Microsoft Defender Advanced Threat Prevention)** – Enterprise class vulnerability management, threat detection and response security solution.
   c. **Tanium** – Endpoint assets and posture management. Works with Cloudflare to ensure posture based conditional access.

TechPass

TechPass

TechPass is a Single Sign-On, Identity & Access Management solution for developer services in Singapore Government Technology Stack (SGTS), not only enabling users to access and transition seamlessly between services but also improving downstream user experiences

I am New to GCC 2.0 – What Should I do?

Government on Commercial Cloud

1. If you are requesting a new setup in GCC2.0, you should first arrange to signup to TechPass for your team (Public Officers and Vendors). You can reuse your existing Public Officer Techpass account if you already have one.

Public Officers

Visit https://portal.techpass.gov.sg/public/home to do a Self Signup for a TechPass account using your WoG email account. Please select **"Onboarding to SEED is required" at sign-up.** An invitation email with instructions will be sent to your email.

- If you are a SE-GSIB user, please reach out to us separately for specific TechPass onboarding instructions.

Vendors

Agencies will need to consolidate the list of Vendors to onboard to TechPass and submit via SR form **(approach Agency for the URL)**. The information needed are:

- Name / Company email address / Mobile Number / Company / Department.

2. We will then update the Intune backend with these information and the SEED client applications will be automatically pushed to your internet devices. You will receive the setup instructions (refer to https://docs.developer.tech.gov.sg/docs/security-suite-for-engineering-endpoint-devices/#/) to setup your internet devices as GMDs.

Viewing Bing Wan GovTech's...

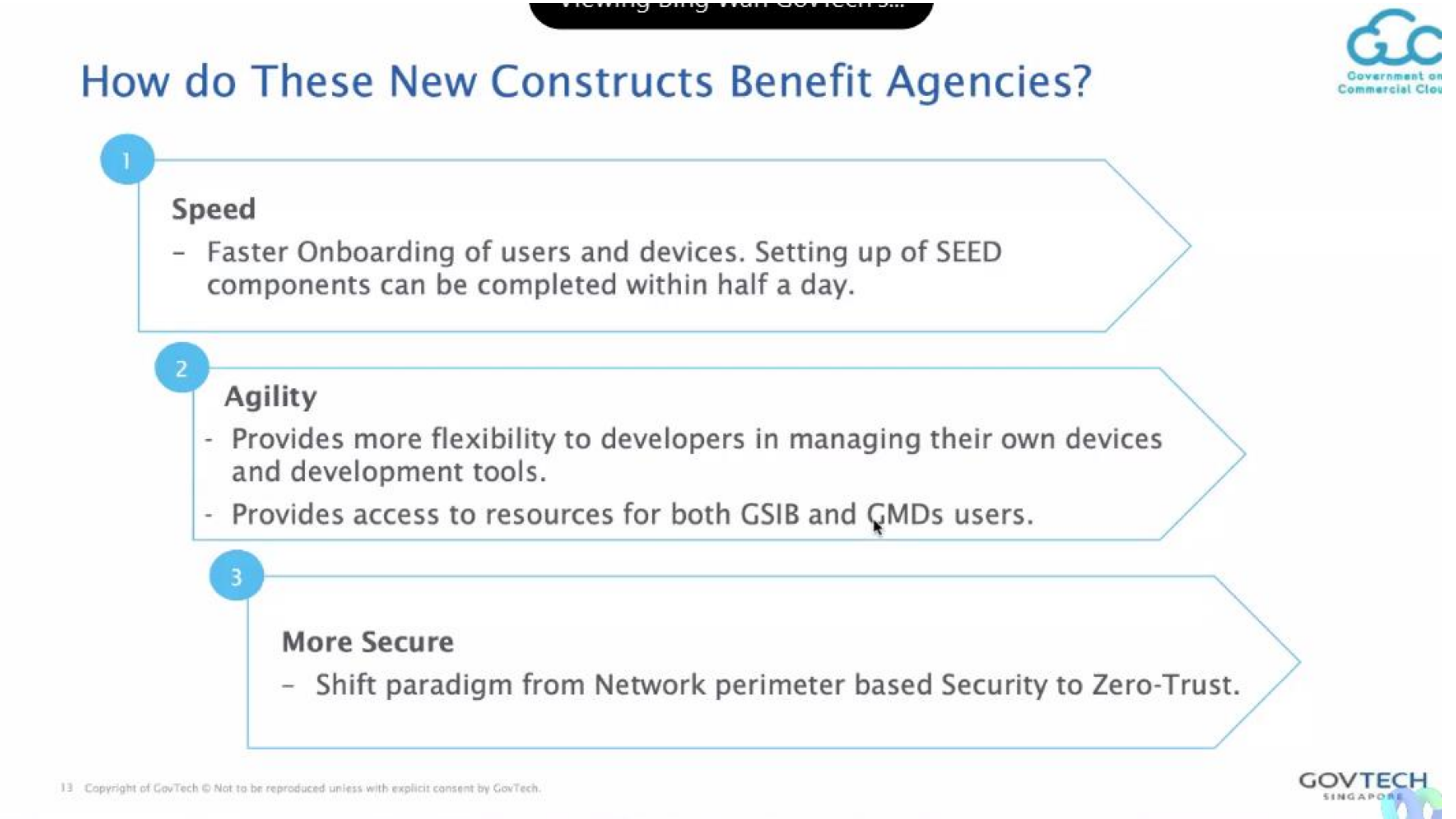
Government on Commercial Cloud

I am Already on GCC 1.0. How Will this Impact me?

- Current GCC 1.0 can signup for SEED to address the MDM requirement (deadline currently extended to Jul 2022).
- You can access GCC1.0 workloads via Global Protect VPN using your Cloud/VPN IDs* as usual, but will need to ensure that you turn off Cloudflare before doing so.
- Onboarding to SEED now allows you to have a smother transition when migrating to GCC2.0 in future, as you device will already have the access prerequisites for GCC2.0.

* Users will be defined by WoG ID. Currently set as Single ID to Single Device. Cloud IDs will also be associated to users on a 1 to 1 basis due to the MDM reinstatement.

GOVTECH SINGAPORE



How do These New Constructs Benefit Agencies?

1

Speed

- Faster Onboarding of users and devices. Setting up of SEED components can be completed within half a day.

2

Agility

- Provides more flexibility to developers in managing their own devices and development tools.
- Provides access to resources for both GSIB and GMDs users.

3

More Secure

- Shift paradigm from Network perimeter based Security to Zero-Trust.

Vendor Endpoint Management

Common Scenarios :

- **My contractor already has own machines provisioned for GCC 1.0 for my agency. What should I do?**
  - You can onboard the machines to SEED while keeping the Cloud/VPN IDs and Global Protect VPN. This way you can access GCC1.0 using Global Protect and GCC2.0 using Cloudflare. Do note that you can only access one at a time, i.e. Global Protect must be turned off when using Cloudflare and vice versa.
- **I know some of my contractors development and infrastructure management team already have machines onboarded to SEED/TechPass/Cloudflare for other projects. Can they reuse these for my project?**
  - If the project classification allows for the shared devices, technically they can be reused.
- **My contractor is using the machine used to support my Agencies, and they plan to use it for other projects for other Agencies. Can this be allowed and what should I do?**
  - If the project classification allows for the shared devices, technically they can be reused.

Vendor Endpoint Management

Common Scenarios :

- **My contract with the contractor does not include the provisioning of these required machines, hence I would need to lease/procurement my own equipment for my Agency. What is your guidance for me?**
  - Ensure the leased/procured devices meet minimal OS requirements of Windows 10 Pro/Enterprise versions or on macOS Catalina 10.15 and later versions.
  - The devices should not be on another MDM prior to onboarding to SEED.
- **My contractor, using machines "sponsored" by another Agency have completed their project for that Agency. What is your suggested process for me – re-onboard CloudFlare/SEED/TechPass or some other steps would be required?**
  - These contractors may retain their TechPass accounts but they should offboard their devices from SEED and return them to the sponsoring agency. They can request for SEED onboarding for new devices using the same TechPass IDs.

Viewing Bing Wan GovTech's...

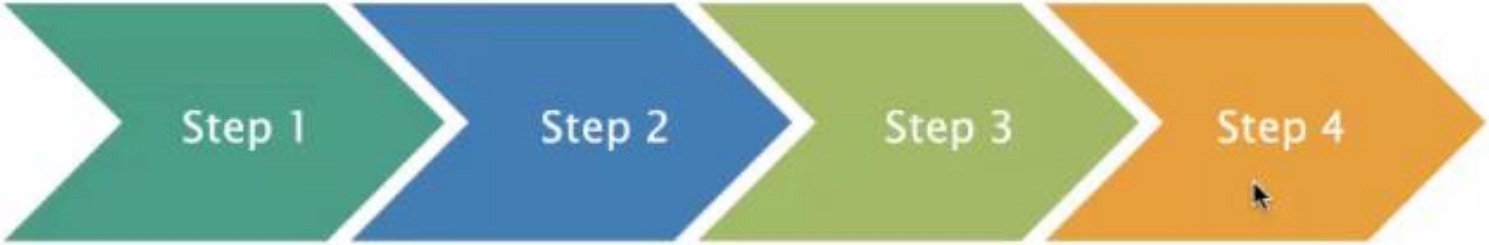
CMP Onboarding Experience

GOVTECH SINGAPORE

Viewing Bing Wan GovTech's...

Government on Commercial Cloud

New CMP - Onboarding Definition



Accessing CMP 2.0

Creating a Tenant Account

Creating an AWS Account

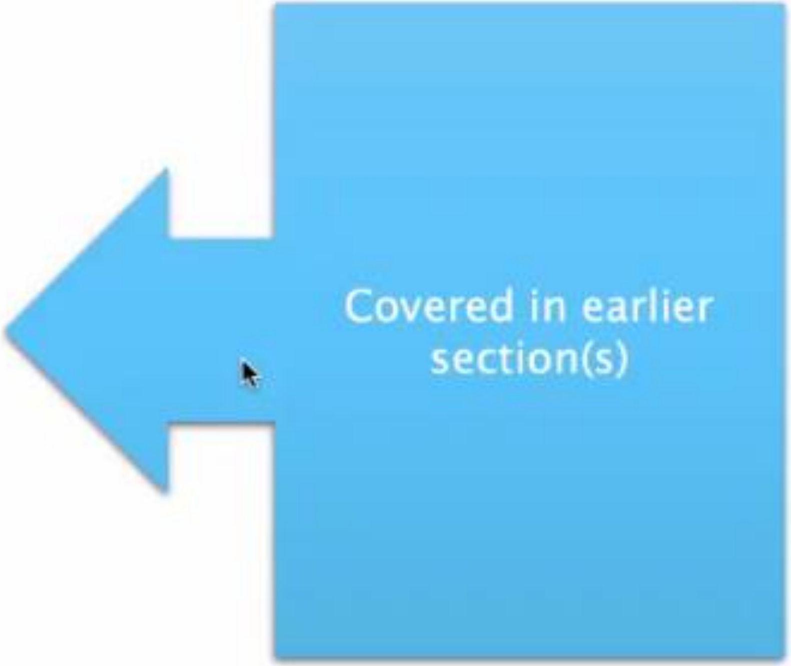
Accessing your AWS Account (via AWS Console)

GOVTECH SINGAPORE

Government on Commercial Cloud

1. Accessing CMP 2.0

- Register for a TechPass account
  - Once your TechPass account is successfully registered, you may already access GCC2.0 CMP via your non-SE GSIB at https://cmp.gcc.gov.sg
- Enroll in SEED (optional – *only if* access via GMDs is required)

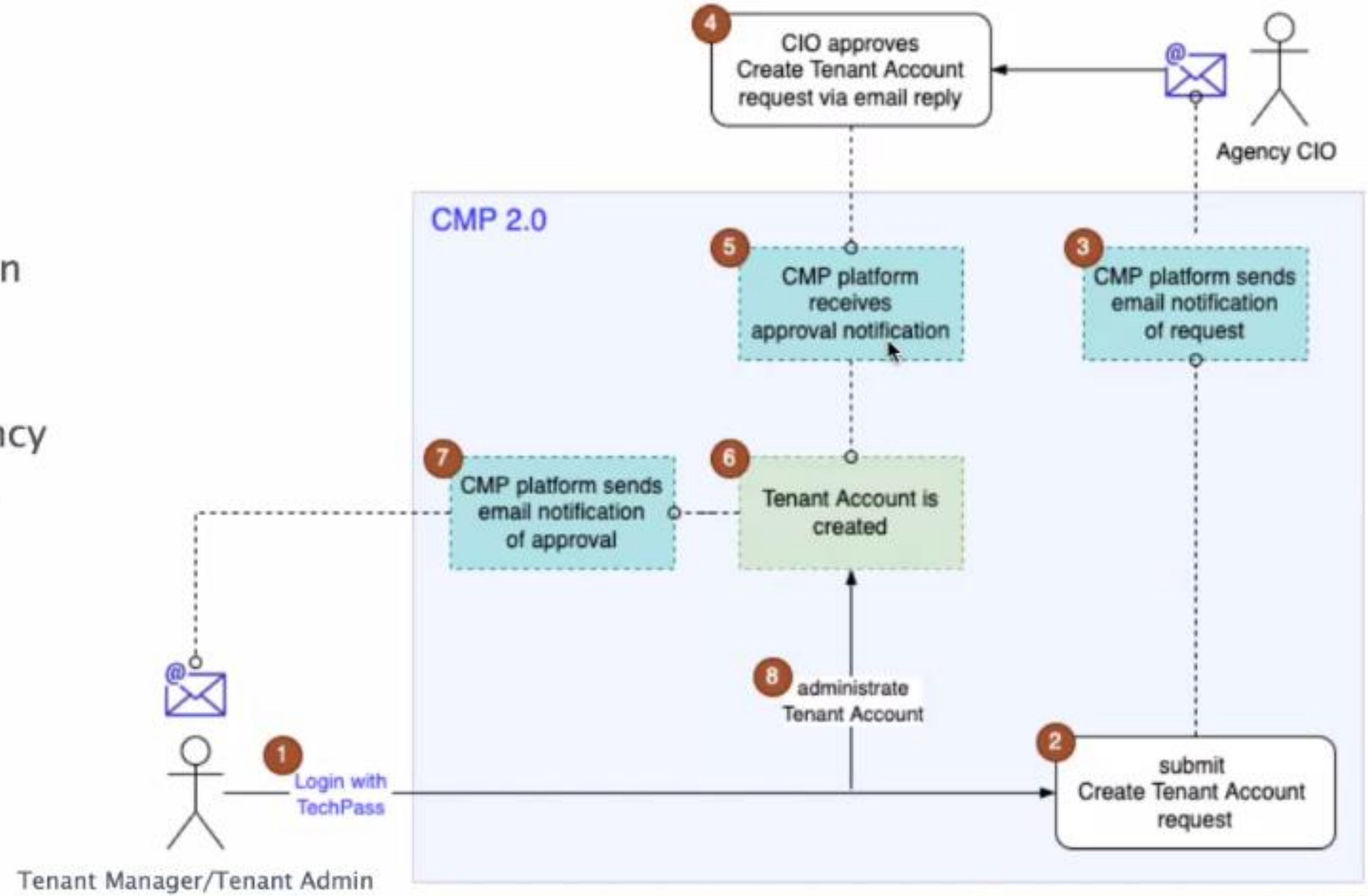


Covered in earlier section(s)

GOVTECH SINGAPORE

2. Creating a Tenant Account

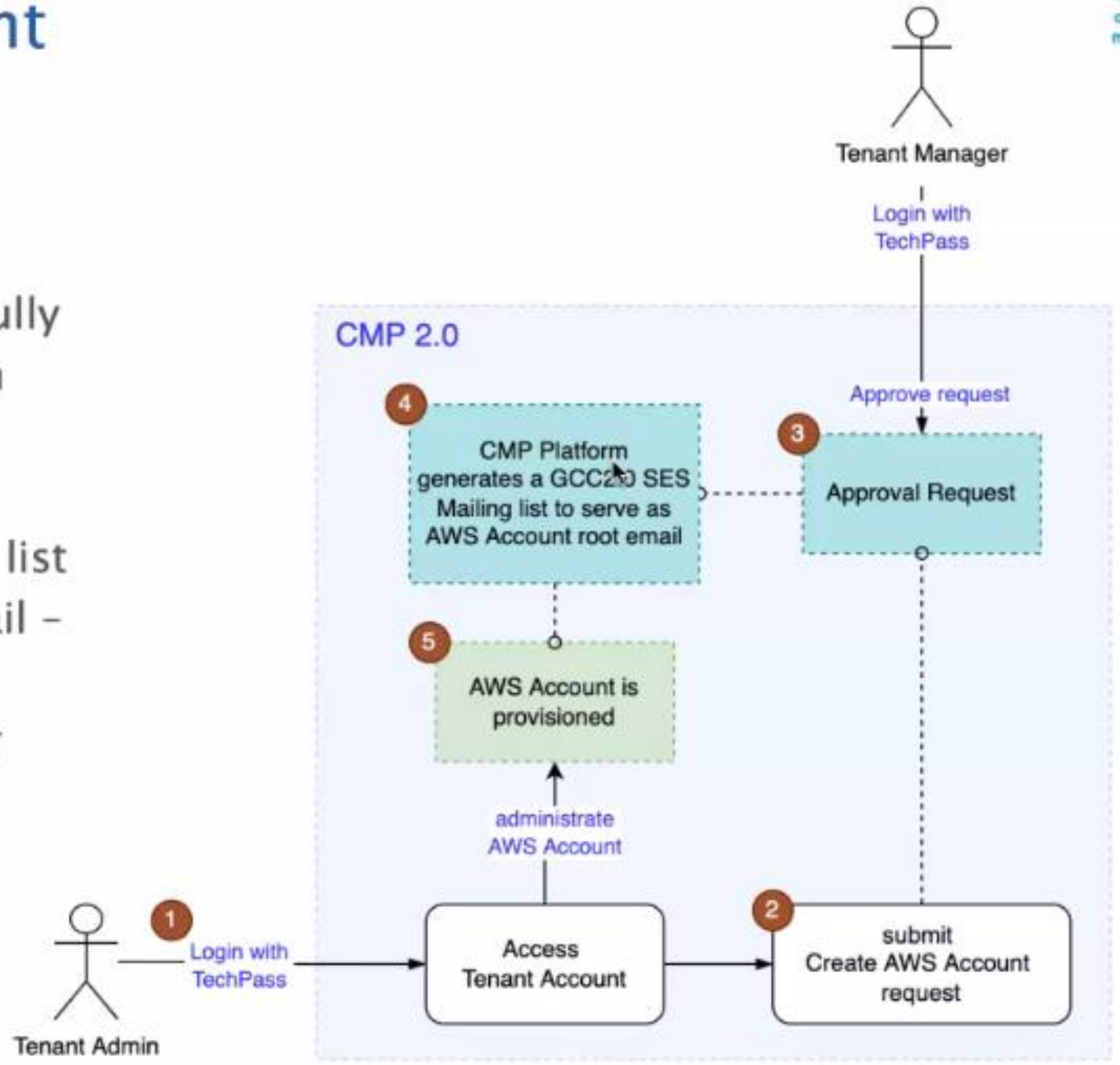
Tenant Account creation process will be a fully automated self-service workflow between agency officer and agency CIO.


4
CIO approves Create Tenant Account request via email reply
Agency CIO
CMP 2.0
5
CMP platform receives approval notification
3
CMP platform sends email notification of request
7
CMP platform sends email notification of approval
6
Tenant Account is created
8
administrate Tenant Account
1
Login with TechPass
2
submit Create Tenant Account request
Tenant Manager/Tenant Admin

3. Creating an AWS Account

AWS Account creation process will be a fully automated self-service workflow between Tenant Manager and Tenant Admin.

CMP 2.0 will auto-generate a SES-mailing list address to serve as the root account email – this eliminates the need for Agencies to apply for a dedicated SG-Mail account for each AWS Account.

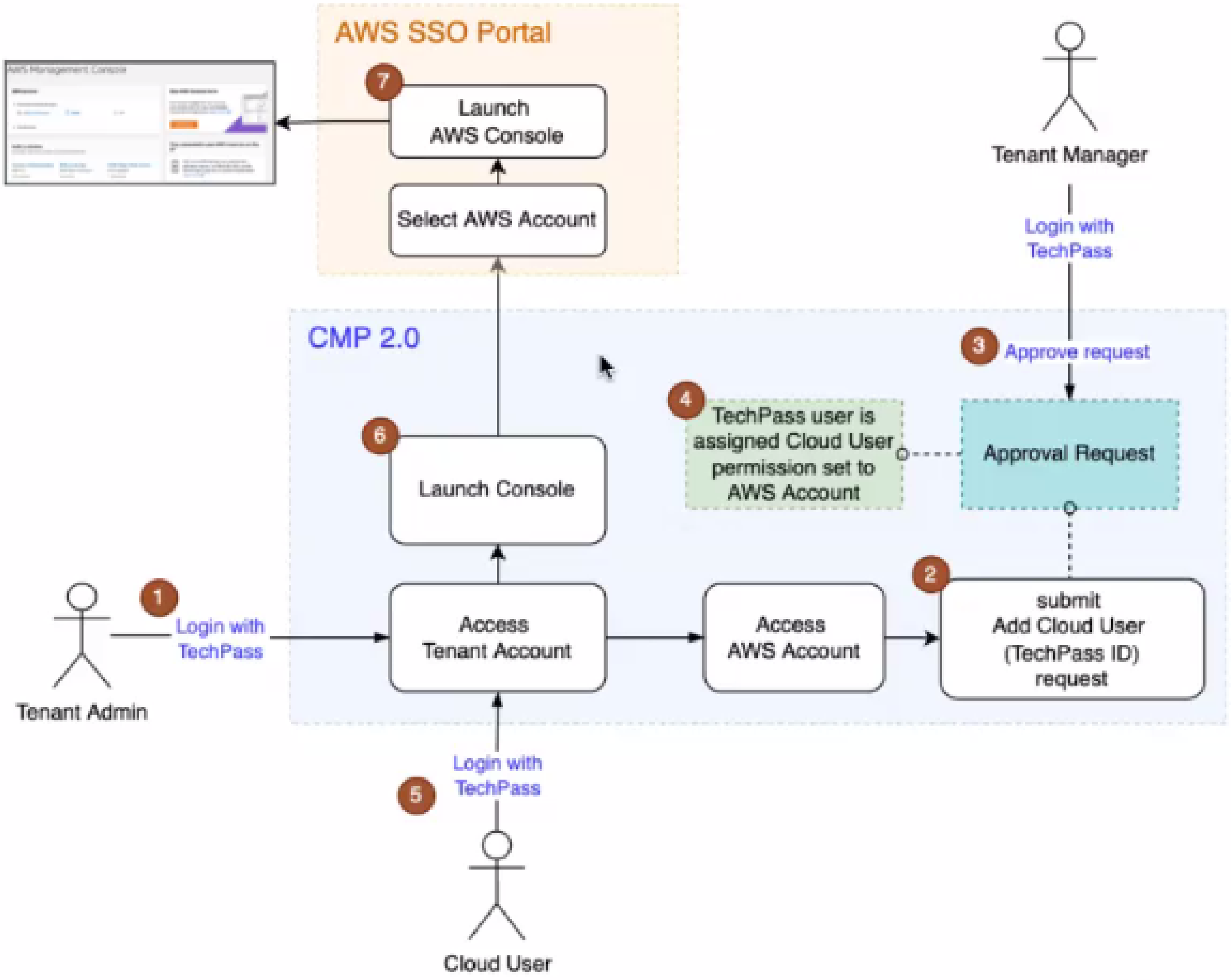


4. Accessing your AWS Account

Access to your AWS Account will require Agencies to explicitly manage their cloud user assignment.

Management of Cloud users for each AWS Account will be a fully automated self-service workflow between Tenant Manager and Tenant Admin.

Identity for Cloud Users will also be via TechPass.



Networking

GCC 2.0 Networking Introduction

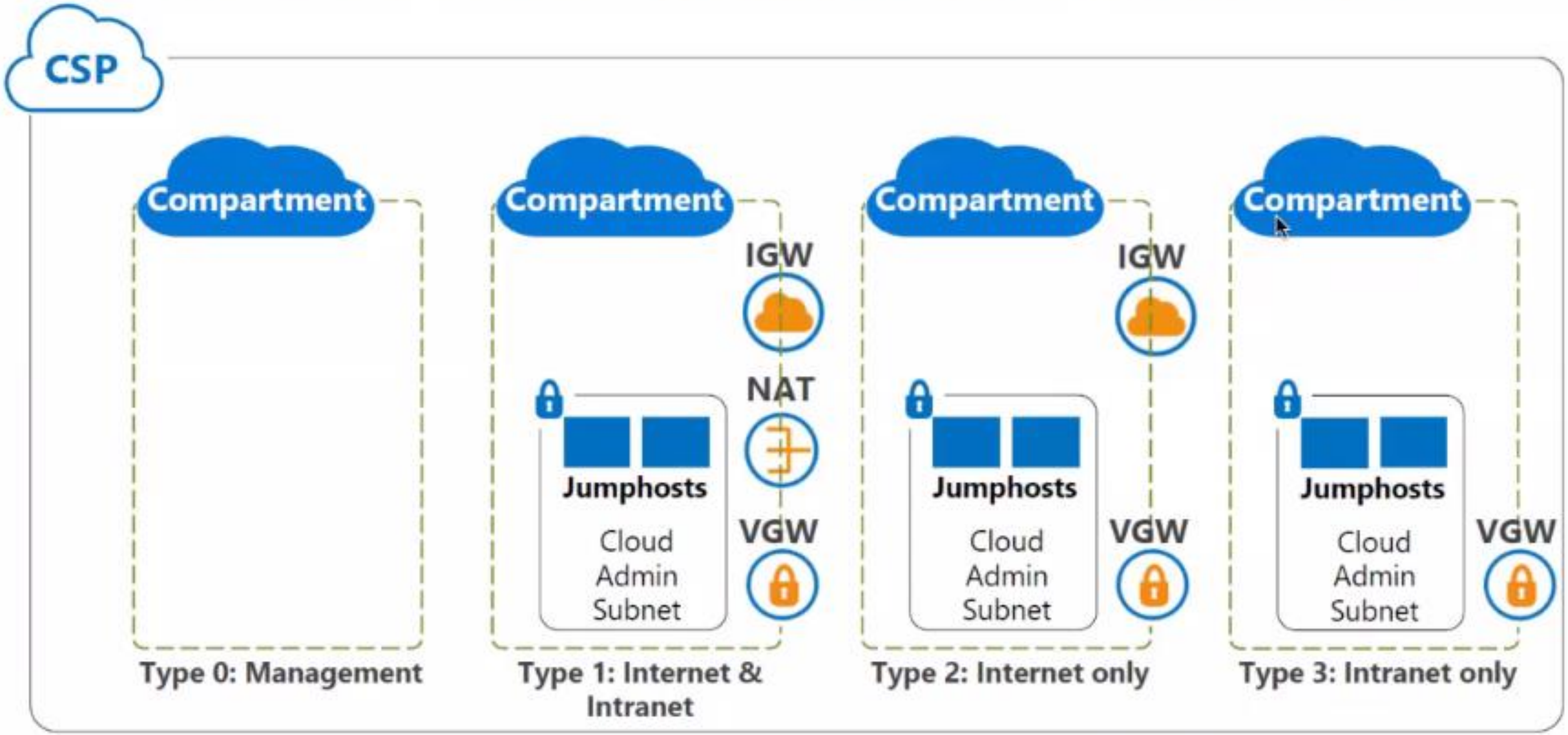
How does GCC 2.0 Network Design differ from GCC 1.0?

- There will be **no GCC provisioned Jump hosts**.
- Workload management activities will be using **CSP Native Workload Administration Tools** (AWS SSM Session Manager, Fleet Manager & Azure Bastion).
- There will be **Internet Compartments** (Agency Self-Managed), **GEN Routable & Non-GEN Routable Compartment** (GCC Centrally-managed) and options with (or without) integration to GCC Common Services.
- The availability of Agency-managed **AWS Transit Gateway (TGW)**.
- **Stronger use of Policy as Code (PaC)** to detect Non-Compliances as opposed to only using Service Control Policies (SCPs). Example include attaching of Internet Gateway (IGW) to an intranet (GEN-routable) compartment, which will be flagged by PaC.

GCC 1.0 Network Compartments (Recap)

Government on Commercial Cloud

The Four Types of Network Compartments



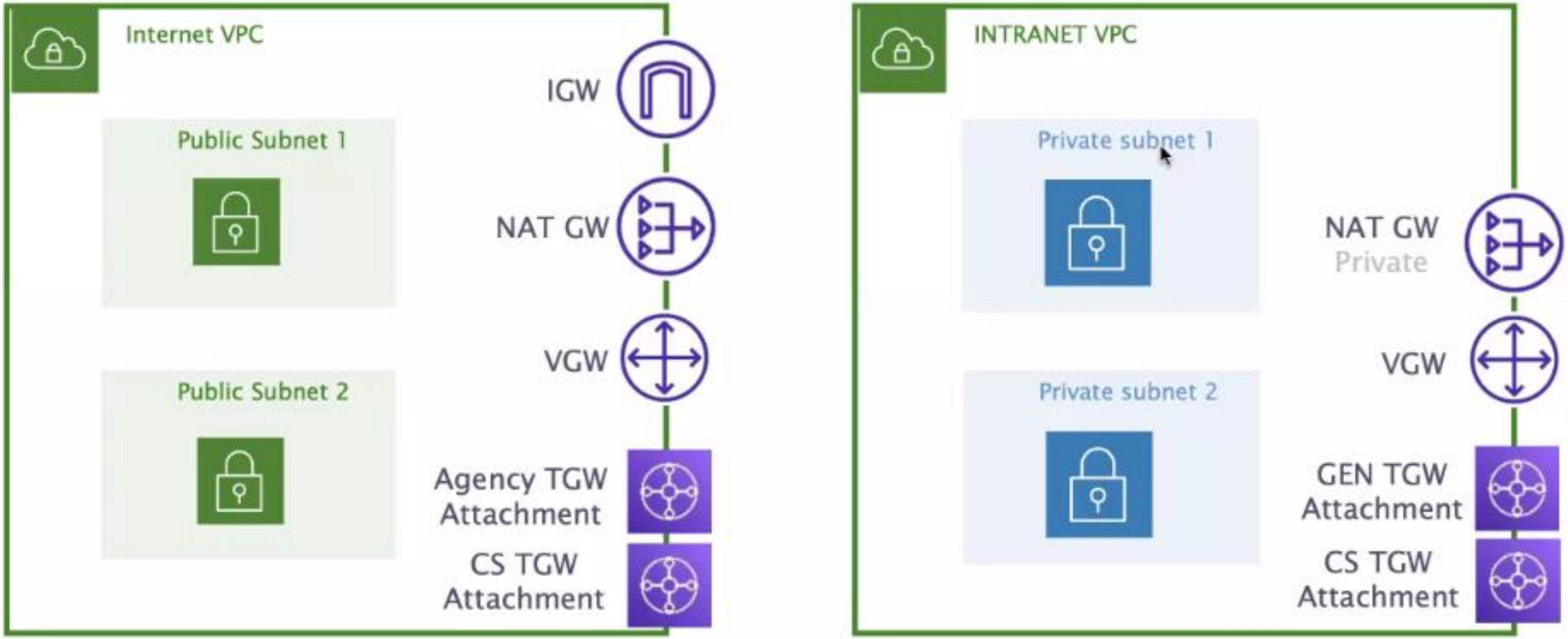
* Extracted from GCC Foundation Training slide 104

GOVTECH SINGAPORE

GCC 2.0 Network Compartments

Non-GEN Routable Compartment

GEN Routable Compartment



Internet VPC

IGW

Public Subnet 1

NAT GW

VGW

Public Subnet 2

Agency TGW Attachment

CS TGW Attachment

INTRANET VPC

Private subnet 1

NAT GW Private

VGW

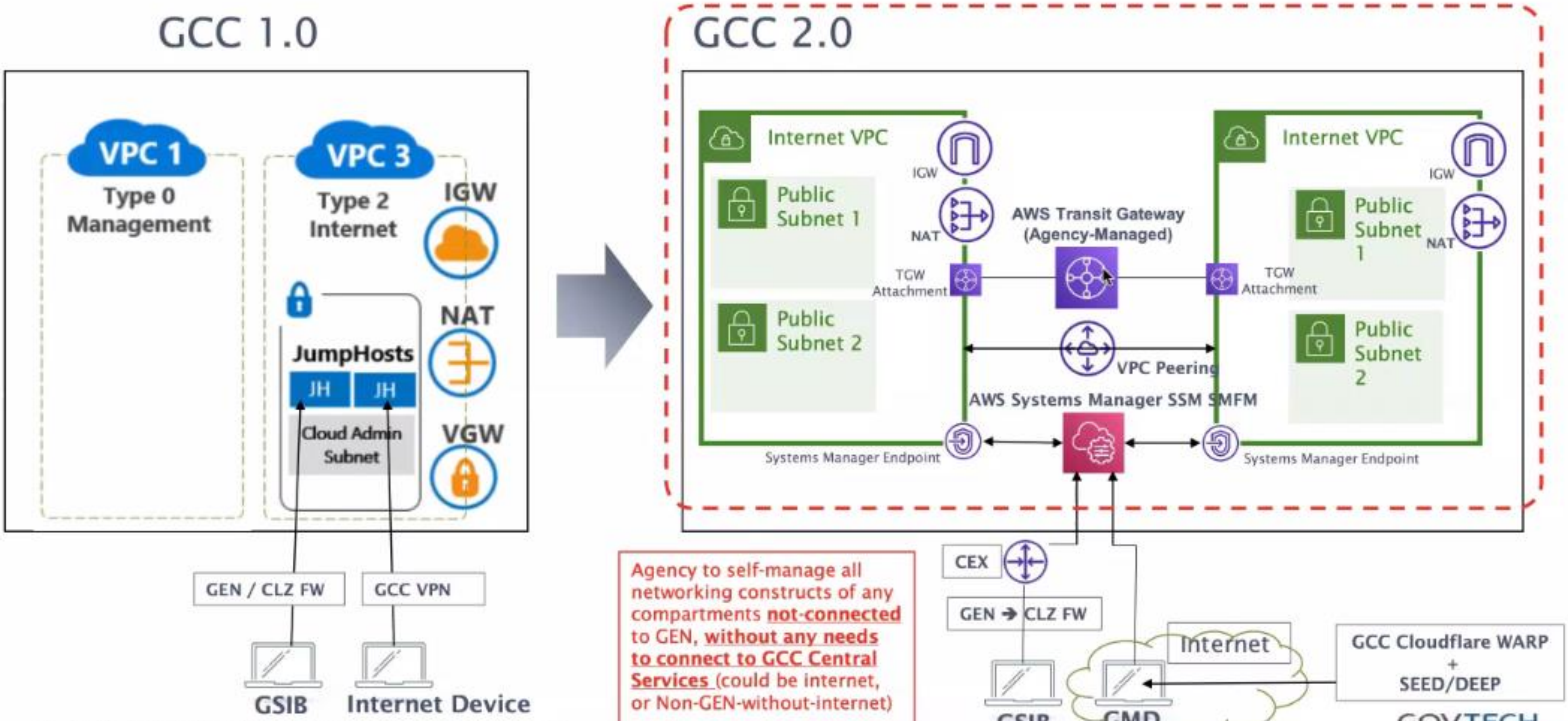
Private subnet 2

GEN TGW Attachment

CS TGW Attachment

Non-GEN Routable Compartments

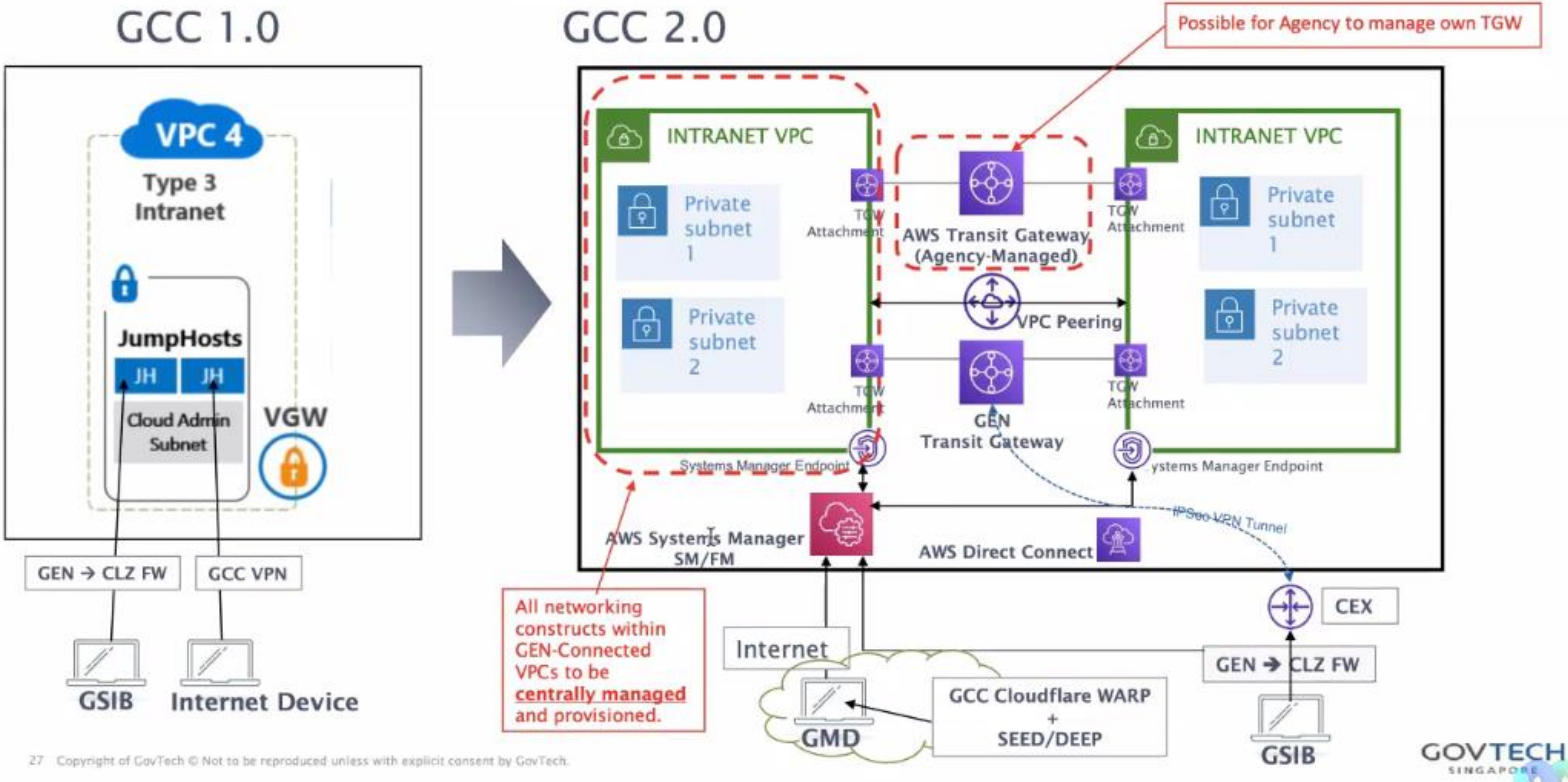
Government on Commercial Cloud



Agency to self-manage all networking constructs of any compartments **not-connected** to GEN, **without any needs to connect to GCC Central Services** (could be internet, or Non-GEN-without-internet)

GOVTECH SINGAPORE

GEN Routable Compartments



GCC 1.0

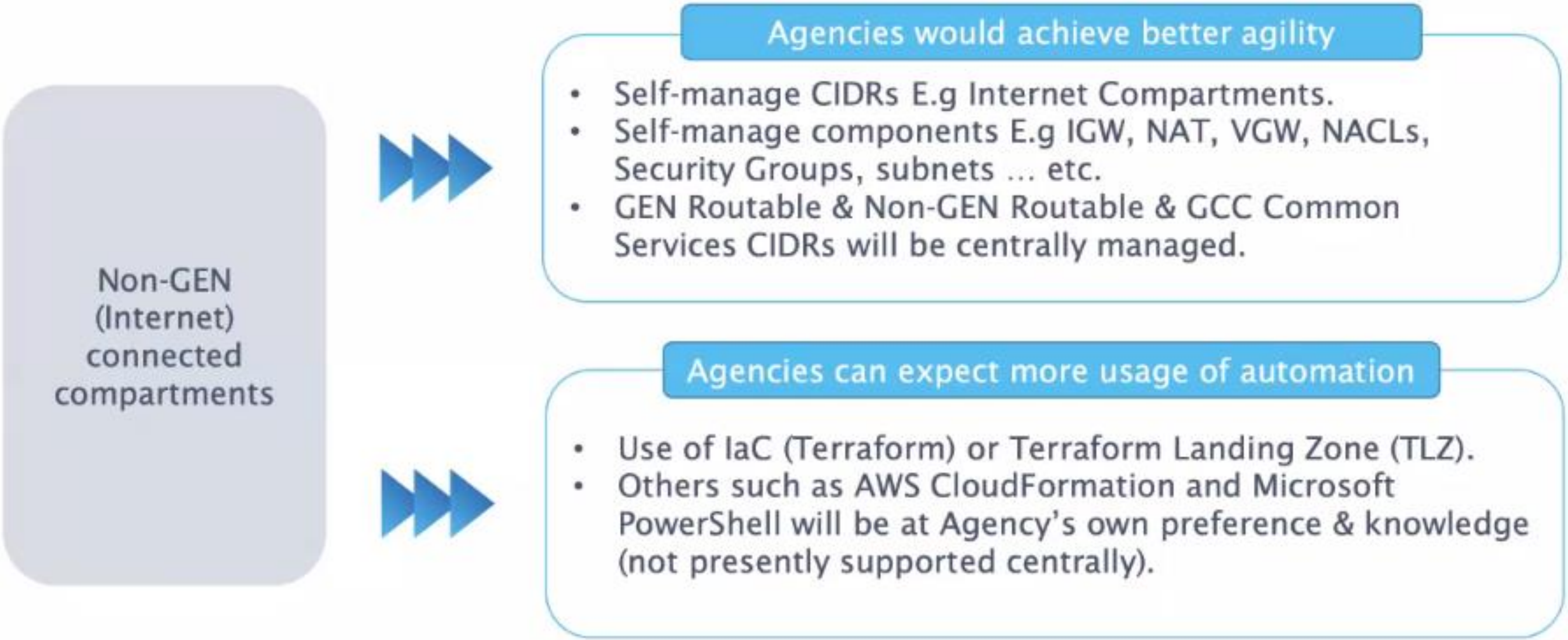
GCC 2.0

Possible for Agency to manage own TGW

All networking constructs within GEN-Connected VPCs to be **centrally managed** and provisioned.

Government on Commercial Cloud

Networking Design Consideration



Non-GEN (Internet) connected compartments

Agencies would achieve better agility

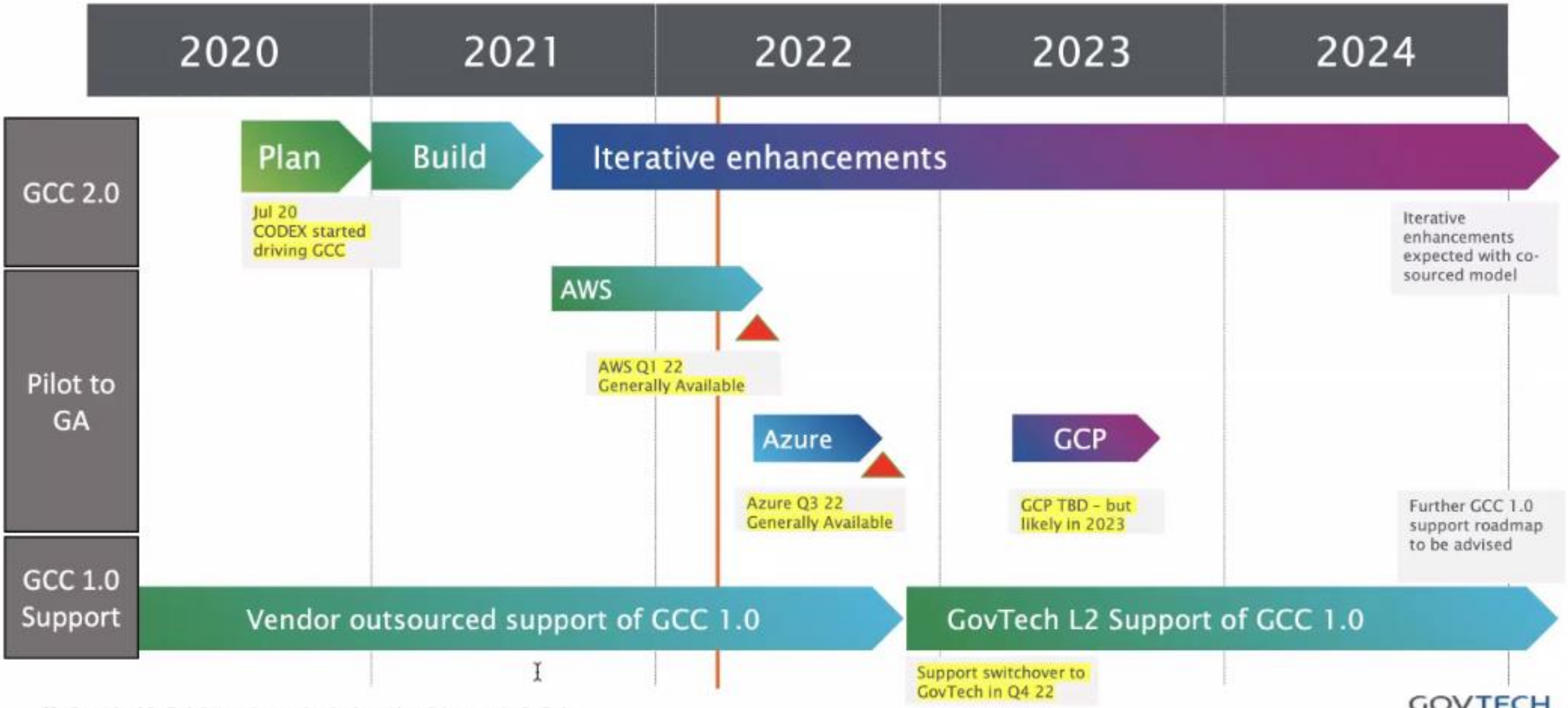
- Self-manage CIDRs E.g Internet Compartments.
- Self-manage components E.g IGW, NAT, VGW, NACLs, Security Groups, subnets … etc.
- GEN Routable & Non-GEN Routable & GCC Common Services CIDRs will be centrally managed.

Agencies can expect more usage of automation

- Use of IaC (Terraform) or Terraform Landing Zone (TLZ).
- Others such as AWS CloudFormation and Microsoft PowerShell will be at Agency's own preference & knowledge (not presently supported centrally).

GOVTECH SINGAPORE

GCC 2.0 Roadmap



Jul 20 CODEX started driving GCC

Iterative enhancements expected with co-sourced model

AWS Q1 22 Generally Available

Azure Q3 22 Generally Available

GCP TBD – but likely in 2023

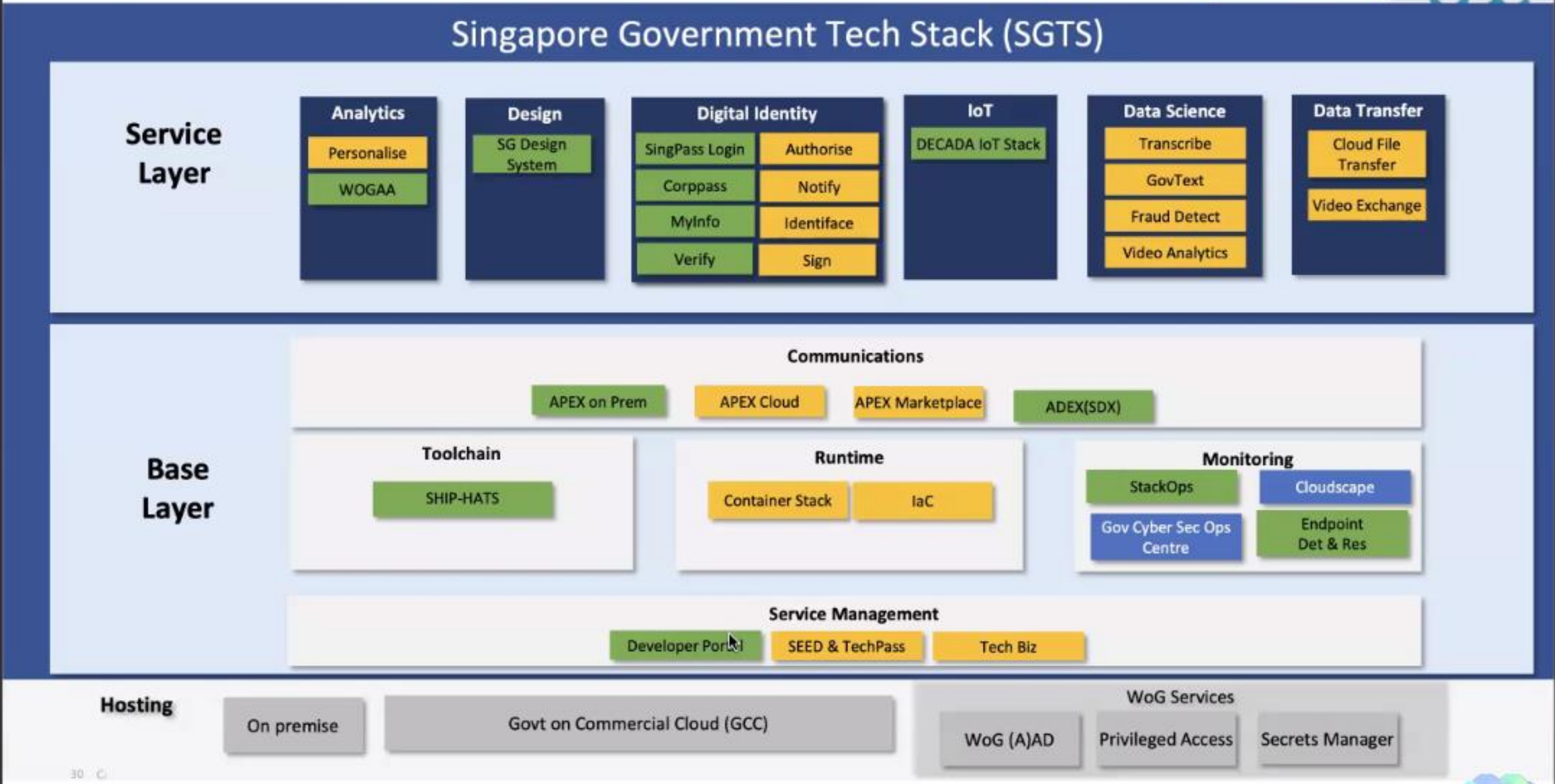
Further GCC 1.0 support roadmap to be advised

Support switchover to GovTech in Q4 22

Viewing Bing Wan GovTech's...

Introduction to Singapore Government Tech Stack (SGTS)

🟩 Live 🟨 Work in Progress 🟦 Planned



Singapore Government Tech Stack (SGTS)

Service Layer

- **Analytics**: 🟨 Personalise; 🟩 WOGAA
- **Design**: 🟩 SG Design System
- **Digital Identity**: 🟩 SingPass Login; 🟨 Authorise; 🟩 Corppass; 🟨 Notify; 🟩 MyInfo; 🟨 Identiface; 🟩 Verify; 🟨 Sign
- **IoT**: 🟩 DECADA IoT Stack
- **Data Science**: 🟨 Transcribe; 🟨 GovText; 🟨 Fraud Detect; 🟨 Video Analytics
- **Data Transfer**: 🟨 Cloud File Transfer; 🟨 Video Exchange

Base Layer

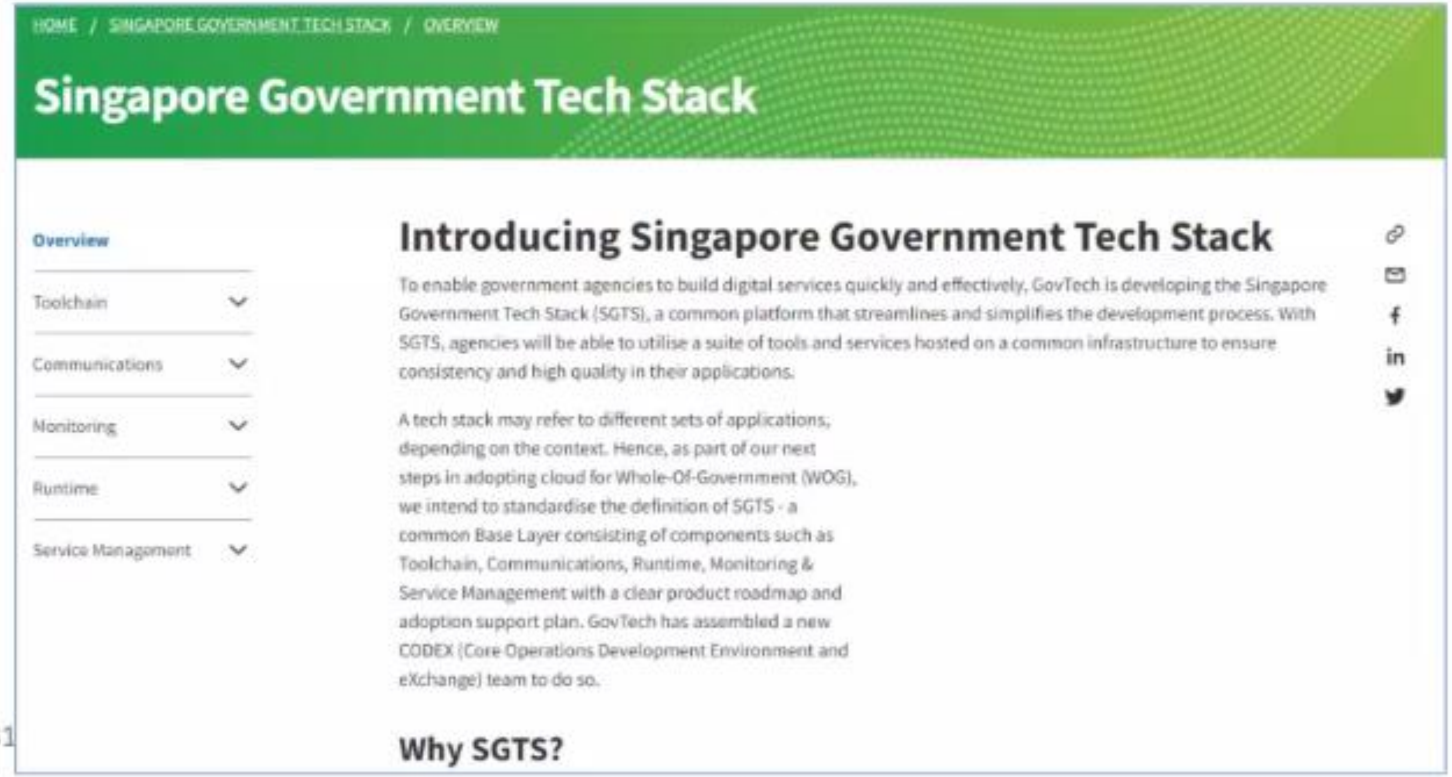
- **Communications**: 🟩 APEX on Prem; 🟨 APEX Cloud; 🟨 APEX Marketplace; 🟩 ADEX(SDX)
- **Toolchain**: 🟩 SHIP-HATS
- **Runtime**: 🟨 Container Stack; 🟨 IaC
- **Monitoring**: 🟩 StackOps; 🟦 Cloudscape; 🟦 Gov Cyber Sec Ops Centre; 🟩 Endpoint Det & Res
- **Service Management**: 🟩 Developer Portal; 🟨 SEED & TechPass; 🟨 Tech Biz

Hosting: On premise; Govt on Commercial Cloud (GCC)

WoG Services: WoG (A)AD; Privileged Access; Secrets Manager

Open Documentation on
Singapore Government Developer Portal

For Technical documentation, Code snippets, Use cases



HOME / SINGAPORE GOVERNMENT TECH STACK / OVERVIEW

Singapore Government Tech Stack

Introducing Singapore Government Tech Stack

To enable government agencies to build digital services quickly and effectively, GovTech is developing the Singapore Government Tech Stack (SGTS), a common platform that streamlines and simplifies the development process. With SGTS, agencies will be able to utilise a suite of tools and services hosted on a common infrastructure to ensure consistency and high quality in their applications.

A tech stack may refer to different sets of applications, depending on the context. Hence, as part of our next steps in adopting cloud for Whole-Of-Government (WOG), we intend to standardise the definition of SGTS - a common Base Layer consisting of components such as Toolchain, Communications, Runtime, Monitoring & Service Management with a clear product roadmap and adoption support plan. GovTech has assembled a new CODEX (Core Operations Development Environment and eXchange) team to do so.

Why SGTS?