Strategic Command
Defence Digital

MODCLOUD

MODCloud SECRET Early Market Engagement

Version: 1.1

29TH April 2021

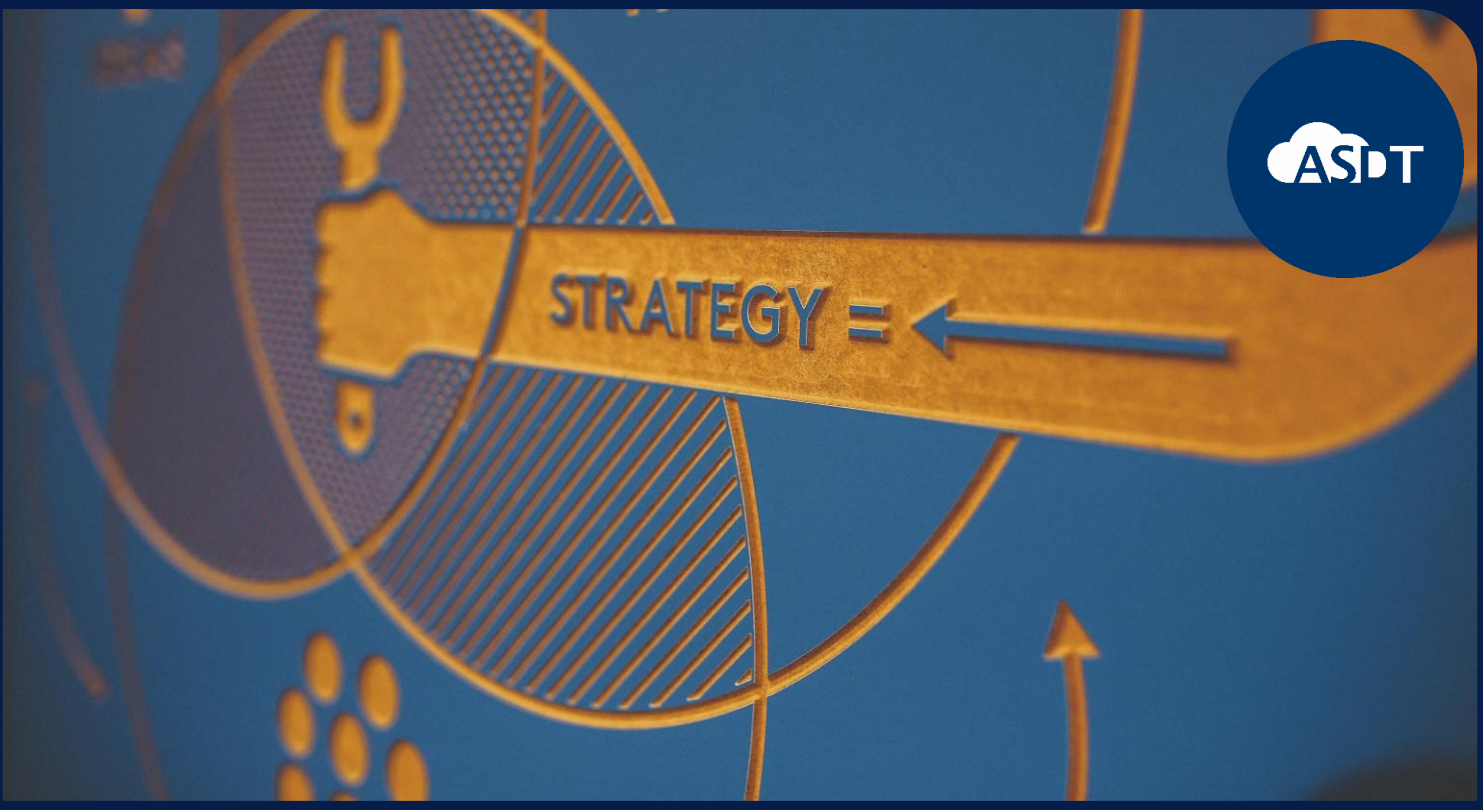


Table of Contents

List of Figures

Summary

The MOD wishes to expand on the current MODCloud ecosystem and make a managed private Cloud with security level of 'SECRET' available to the wider MOD community to:

- Replace legacy infrastructure and address obsolescence.
- Provide a modern platform with Cloud capabilities (scalable/elastic), while future proofing for future Cloud services.

The MODCloud SECRET platform will be engineered and run to the highest-common security standards, thereby offering no barrier to adoption for business areas that have particularly challenging security requirements.

It is expected that during the life of MODCloud SECRET it will evolve in scale, capability and functionality to meet the challenging demands of Defence.

The information provided in response to this request may be used to inform the options for conducting a possible subsequent competition. The provided information will not be used in the assessment of any proposal from Industry. It should be noted that all responses released in relation to this Request for Information (RFI) is released on a subject to contract basis, is subject to change and does not signal the start of a formal procurement process. Your response to this RFI should consist of a completed soft copy in Adobe PDF or MS Word format. To keep the response size manageable, you are requested to limit your response to no more than 2500 words (font Arial, size 11) excluding diagrams.

Responses to this RFI are requested by no later than 1200 on 14 May 21. Any response provided is voluntary and does not start the official procurement process for delivering a Cloud-like capability. Please send your responses to ISSComrcl-ASDT-Multiuser@mod.gov.uk and CC ISSDel-ASDT-EMP-UV@mod.gov.uk.

Outcome

No later than August 2022; The MOD MUST have an operational private Cloud delivering live Cloud Services at SECRET.

This Cloud must:

- Support the complete and successful migration of all previously mentioned C4ISR (Command Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) applications.
- Support the delivery of PREDA.
- Be delivered with a Shared Responsibility Model.
- Have a Service Wrap required to support its customers.

- Have a billing solution in place.
- Have SCN connectivity with MOD assurance/ATO (Authority to Operate).

Alpha

The MOD wishes to meet an Alpha at the earliest possible opportunity, this will consist of the following:

- A C4ISR container-based application connected to the production SECRET Core Network (SCN).
- The application consumption must be measured sufficiently for billing purposes.
- Must meet MOD assurance/ATO.

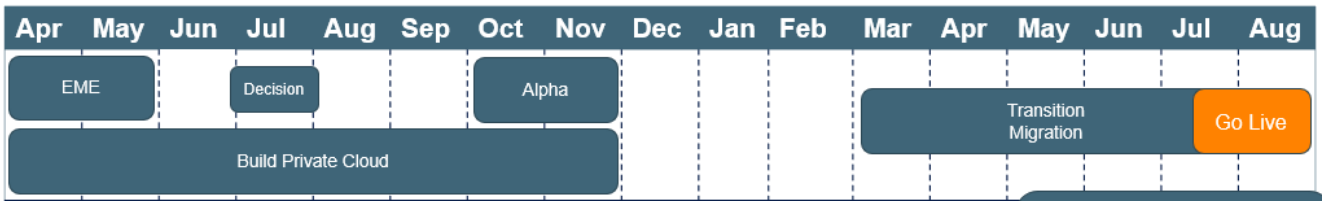


Figure 1: High level overview of Project Plan

Route to Delivery

- The MOD are already building and delivering a small private Cloud to deliver an Alpha by November 2021. The Cloud will have the capability for hosting workloads that have the security marking of 'SECRET'.
- The future of the MOD-owned Cloud environment will be dependent on the outcome of these Early Market Engagement (EME) discussions, with a decision expected by July 2021.
- Following commercial activities and Contract Award, Industry will on-board to take ownership and operation of the private Cloud.
- C4ISR applications will migrate across to the new Cloud, no later than August 2022.
- The MOD currently have three possible courses of actions (COAs) which are available and are expected to meet MOD timelines.
- The COAs are not exhaustive. MOD wishes Industry to assess COAs and provide any alternate COAs that can deliver the Outcome sooner (with cost/risk reductions).

Outcome Assumptions

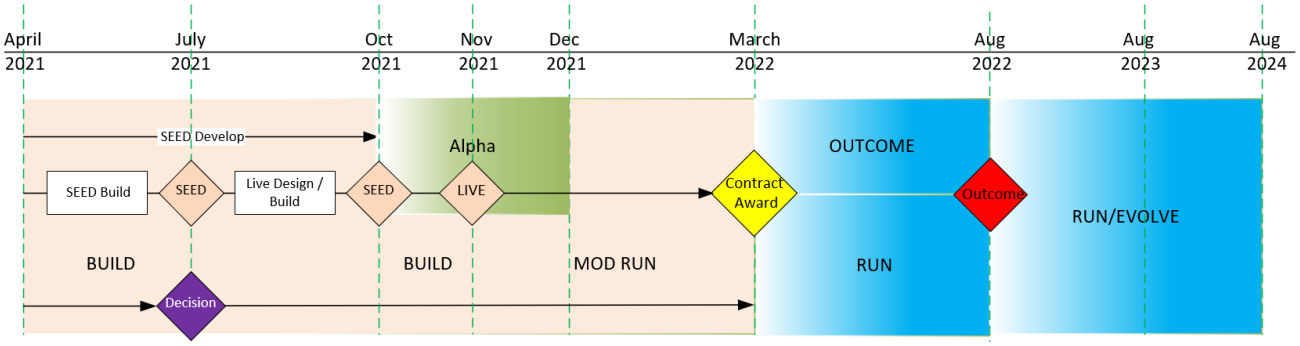
The MOD wishes to highlight the following assumptions that will need to be satisfied:

- Nodes will be managed within a hybrid of Data Centers; MOD, Crown/Industry.
    - The solution will comprise of at least two physical nodes, separated across at least two geographic locations chosen by MOD within UK.

- Ability to deploy nodes to support Tactical Edge and to support currently deployed nodes overseas.
- The nodes must be evergreened.
- Ownership of MOD hardware will be transitioned to service provider.
- There must be 24/7 UK-based support to the platform.
- There must be 24/7 Security Monitoring that can provide full stack monitoring.
- The solution must be able to provide IaaS, PaaS and SaaS.

COA 1 – Build, Run, Evolve

COA1 defines the proposed route to delivery (*Figure 1*) of the outcome, no later than August 2022, through Build, Run and Evolve phases.



- SEED - Environment for Engineering and Design
- LIVE – SECRET Live
- Decision - EME and Commercial activities have identified that COA1 is the chosen route for delivery.
- Contract Award – Following Commercial activities.

Figure 2: The proposed timeline for COA1

Build

The Build phase (April 2021 – November 2021) will include:

- The MOD will Design/Build/Run a private Cloud to meet the Alpha as described.
- The private Cloud will be MOD assured (JSP604 IATO as a minimum) and connected to the production SCN.
- The MOD will manage and operate the Cloud as an interim until Industry on-board.
- The build will comprise of the following environments (SEED Appendix 1, LIVE Appendix 2)

Run

For the Run phase of COA1, the MOD require:

- Industry to on-board and take ownership and operation of the Cloud.

- Industry to provide a fully managed Cloud Service, supporting multiple MOD DevOps Teams at SECRET.
- Industry to manage the Cloud utilising the Shared Responsibility Model.
- A Service Wrap to support its customers.
- A billing solution in place.
- Industry to deliver the Outcome, no later than August 2022.
- The ongoing provision for current and future apps, including but not limited to;
  - C4ISR
  - PREDA
  - NATO/allied
  - Future Cloud hosting requirements.
- Options for Application support.
- An availability of 99.99% (Target)
- 24/7 support to the platform (UK). (1st line support provided by MOD Single Point of Contact (SPOC)).
- 24/7 Security Operating Center (SOC) support (for both threat and prevention at 24/7/365)
- An Evergreen platform and a transition of Initially MOD owned hardware/software/licenses, to Industry owned/provisioned hardware/software/licenses.

Run/Evolve

The MOD require Industry to provide Cloud Transformation delivering enhanced services, turning the small private Cloud into something that is scalable and sustainable for the demand of Defence.

Such deliveries may include:

- Delivery of catalogue services available to customers (e.g., DBaaS, SaaS, FaaS, PaaS, IaaS Workflows).
- Secure Application Program Interface (API) access
- Enhancement of the services (Pay as you Go, Metered Billing, Serverless Technologies)
- Elastic/ Scalable
- On-demand services e.g. Request VM, Spin-Up/Down, via a portal, or code (with a common API interface)

COA2 – Design/Implement and Run

COA2 (*Figure 2*) proposes an initial design/implement phase, followed by a run phase, to meet the outcome of August 2022.

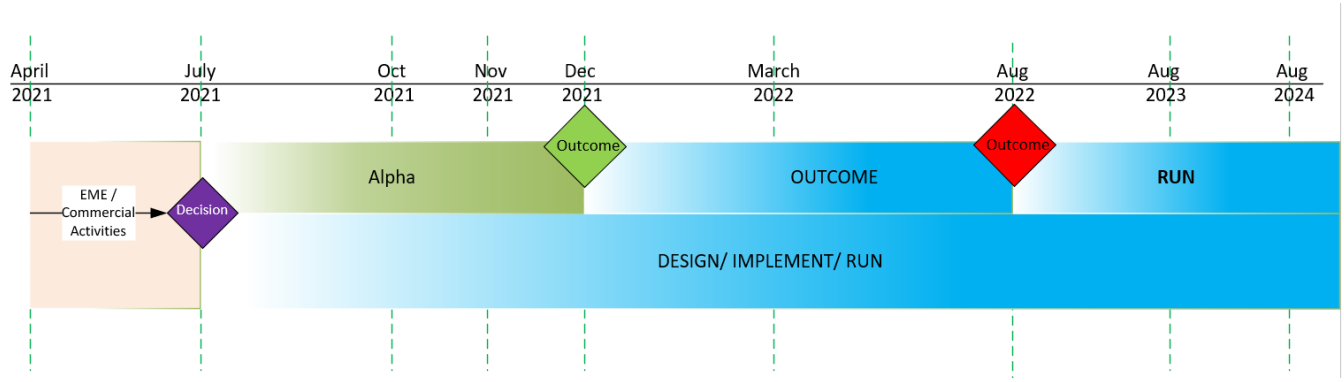


Figure 3: The proposed timeline for COA2

Design/Implement

The Design/Implement phase of COA2 will see Industry provide MOD with the design and build of an assured private Cloud, connected to the SCN and capable for hosting workloads that have the security marking of 'SECRET'.

The private Cloud will provide an Alpha go-live as soon as it can be delivered.

The following are high level the requirements for the private Cloud (this list is not exhaustive list):

- Cloud-like service provision
  - Virtual Machines
    - Automated Build Scripts
    - Catalogue Gold Images
    - Quarantined VMs (apps running on older OS)
  - Enterprise Containers
  - GUI and API driven workflows
- Network virtualisation / Micro-segmentation
- Interface connections i.e. SCN
- GPU Compute / VDI
- Encryption at Rest, Encryption in Transit
- Elasticity, ability to scale Hardware from standard software template
- Identity Management
- Multi-Tenancy
  - Tenant Billing
  - Tenant controlled SDN, Firewalling, Load Balancing
  - Tenant controlled Identity Management
  - Workload Separation (Hardware and Software)
- Multi-Site Hosting (Possible OOC)
- On-Demand Self Service
  - IaaS, PaaS

- A zero-trust network model
- Network security architecture including network virtualisation/micro-segmentation
- Resilience against a wide range of threats and failure modes
- Application of NIST 800-53 high threat profile in a multi supplier environment
- Multifactor Authentication
- Two Person Workflow Controls
- PKI As a Service
- Shared Services
    - DNS, NTP, OS Repositories (YUM, WSUS)
- Shared VDI Capability (VDI AS A Service)
- Underlying Cloud Monitoring and Logging

Run

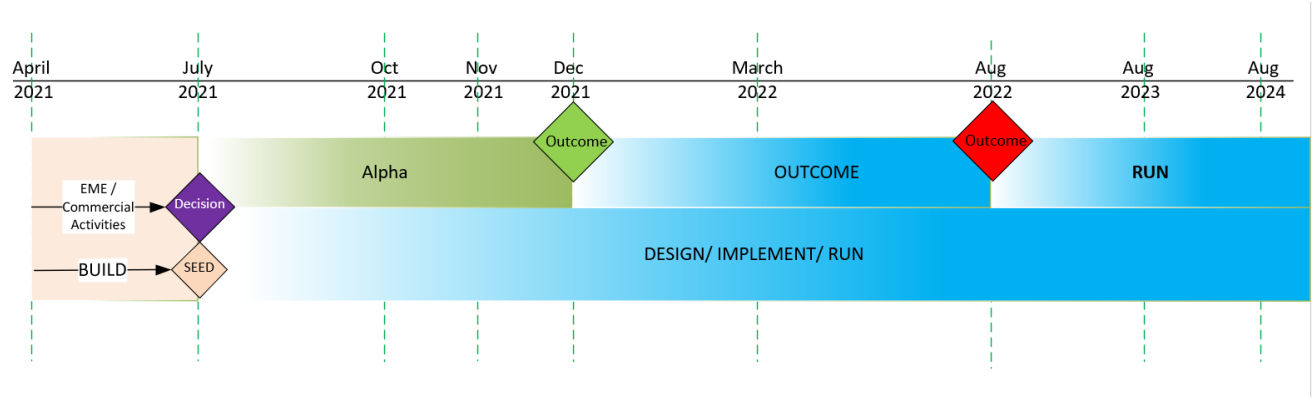
The Run phase of COA2 must be completed no later than August 2022. The MOD require:

- Industry to provide a fully managed Cloud Service, supporting multiple MOD DevOps Teams at SECRET.
- Industry to manage the Cloud utilising the Shared Responsibility Model.
- A Service Wrap to support its customers.
- A billing solution in place.
- Industry to deliver the Outcome, no later than August 2022.
- The ongoing provision for current and future apps, including but not limited to;
    - C4ISR
    - PREDA
    - NATO/allied
    - Future Cloud hosting requirements.
- Options for Application support.
- Availability of 99.99% (Target)
- 24/7 UK support to the platform. (1st line support provided by MOD SPOC).
- 24/7 UK SOC support (for both threat and prevention at 24/7/365)
- Evergreen platform and a transition of Initially MOD owned hardware/software/licenses, to use Industry owned/provisioned hardware/software/licenses.
- Industry through a series of continual improvements to provide Cloud transformation, delivering a Cloud that is scalable and sustainable for the demand of Defence. Such deliveries may include;
    - To deliver catalogue services available to customers (e.g., DBaaS, SaaS, FaaS, PaS, IaaS Workflows).
    - Secure API access

- To enhance the services (Pay as you Go, Metered Billing, Serverless Technologies)
- Elastic/ Scalable
- On-demand, customers can create VMs, storage, services etc. via a portal, or code (with a common API interface)

COA3 – Build, Design/Implement, Run

COA3 (*Figure 3*) proposes an initial build phase, followed by design/build and run, also to be delivered by August 2022.



- SEED - Environment for Engineering and Design
- Decision - EME and Commercial activities have identified that COA3 is the chosen route for delivery.
- SEED - handed over to Industry as GFX or payment consideration.

Figure 4: The proposed timeline for COA3

Build

- MOD continue to build the SEED environment in line with COA1.
- MOD handover ownership of SEED hardware to Industry as GFX of payment consideration.
- SEED contains the following cloud elements (Appendix 1)

Design/Implement

- To mirror COA2 (see above)

Run

- To mirror COA2 (see above)

Questions

1. MOD requests Industry to assess COA1 and feedback on their feasibility (capability and capacity to deliver). Please also provide a ROM cost for this option.
2. MOD requests Industry to assess COA2 and feedback on their feasibility (capability and capacity to deliver). Please also provide a ROM cost for this option.
3. MOD requests Industry to assess COA3 and feedback on their feasibility (capability and capacity to deliver). Please also provide a ROM cost for this option.
4. MOD requests Industry identify any additional COAs available to meet the MOD Outcome sooner? (Suggest different technology/ timelines, and cost reductions) Please also provide a ROM cost for these options.
5. If Industry were to take ownership of MOD small scale private Cloud, how would industry turn this Cloud into something that is scalable and sustainable for the demand of Defence?
6. Would industry be interested in taking ownership of the SEED hardware, and would there be options for negotiation with regards to the continued use of hardware assets, to build out suppliers existing IAAS or to create their own private cloud?
7. Can Industry provide options available to MOD for application migration, support and management?
8. In a scenario where some apps aren't suitable for a modern Cloud (e.g., dependency on old operating systems) what interim support and upgrade/migration services would you recommend?
9. What challenges do you foresee with managing nodes based in UK (on and off premises), overseas and at the tactical edge?

Appendix 1

SEED - Environment for Engineering and Design

The SEED environment will be deployed within the 'SECRET' tier to provide the necessary tooling to undertake all design and development activities for the MOD Cloud SECRET environment to deploy, control, access and Test the overarching MOD Cloud SECRET Live Deployment (*Figure 4*).

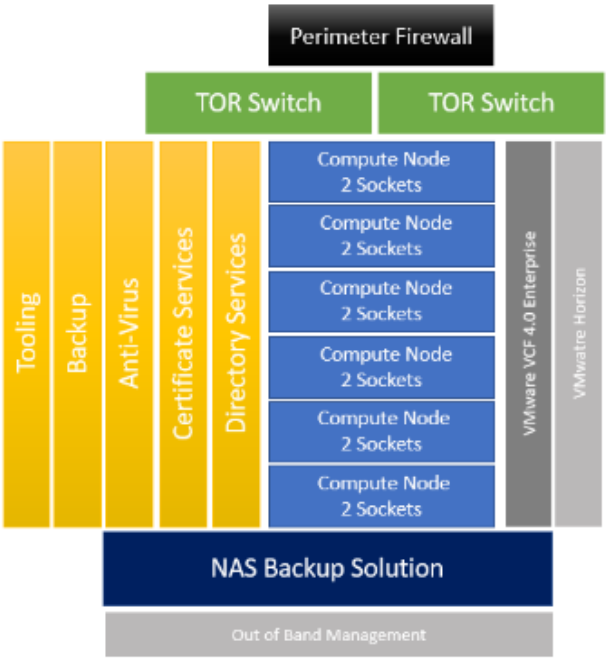


Figure 5: SECRET live deployment

The SEED capability will include a customised VMWare VCF implementation utilising primarily Dell VXRAIL infrastructure component set. This environment will be connected to the SCN and made available for DevOps and design collaboration.

The SEED environment will meet the following functionality:

- Cloud-like service provision
  - Virtual Machines
    - Automated Build Scripts (IAC)
    - Catalogue Gold Images
  - DevOps Containers
  - GUI and API driven workflows
- Network virtualisation / Micro-segmentation
- GPU Compute / VDI
- Application of NIST 800-53 high threat profile in a multi supplier environment
- Multifactor Authentication
- Underlying Cloud Monitoring and Logging

Appendix 2

SECRET LIVE

The live private Cloud will be SCN connected, delivering live workloads providing hosting for SCN connected applications operating at SECRET only. The MOD is targeting an initial Alpha within the live environment for November 2021 (or as soon as it can be realised), and the Outcome delivered no later than August 2022.

It will comprise of two physical nodes, separated across two geographic locations (*Figure 5*) for both resilience and performance. The exact locations of the sites are still TBC but under the current assumption, the primary located within the Corsham ARK, with the secondary located either within Northwood ARK or within MOD controlled MOD Farnborough (exact location TBC).

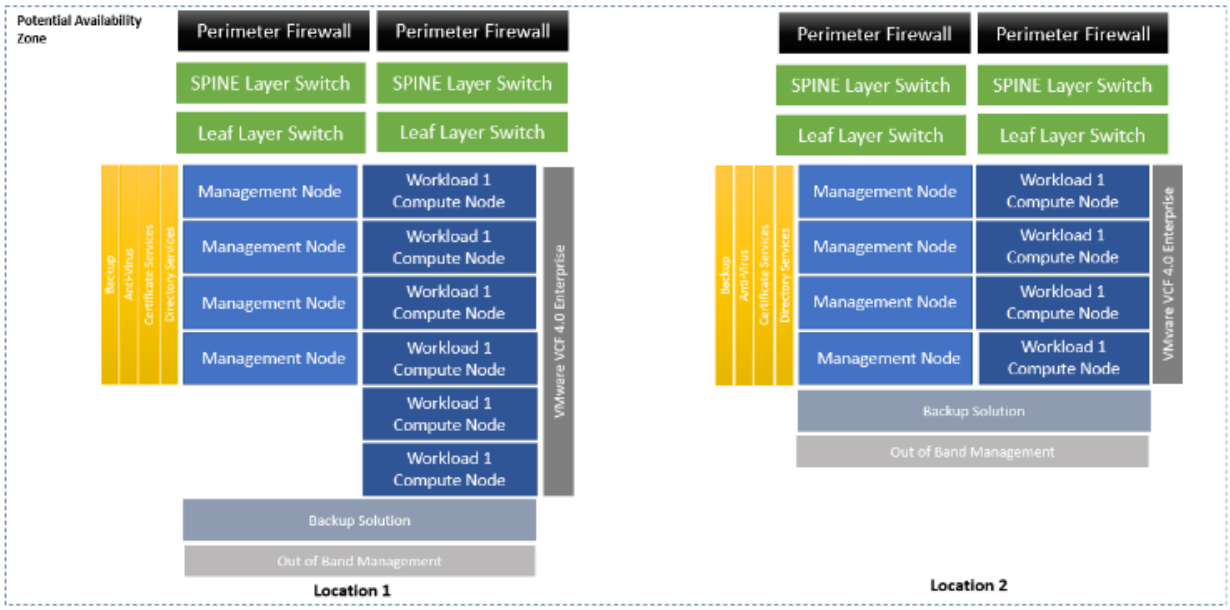


Figure 6: The potential availability zone of Location 1 and 2

Subject to confirmation, a further NODE located within the Falklands will be included within the scope of the delivery, including its maintenance and support.

The MODCloud SECRET Live environment will meet the following functionality:

- Cloud-like service provision
  - Virtual Machines
    - Automated Build Scripts
    - Catalogue Gold Images
    - Quarantined VMs (apps running on older OS)
  - Enterprise Containers

    - GUI and API driven workflows
- Network virtualisation / Micro-segmentation
- Interface connections i.e. SCN
- GPU Compute / VDI
- Encryption at Rest, Encryption in Transit
- Elasticity, ability to scale Hardware from standard software template
- Identity Management
- Multi-Tenancy
    - Tenant Billing
    - Tenant controlled SDN, Firewalling, Load Balancing
    - Tenant controlled Identity Management
    - Workload Separation (Hardware and Software)
- Multi-Site Hosting (Possible OOC)
- On-Demand Self Service
    - IaaS/ PaaS
- A zero-trust network model
- Network security architecture including network virtualisation/micro-segmentation
- Resilience against a wide range of threats and failure modes
- Application of NIST 800-53 high threat profile in a multi supplier environment
- Multifactor Authentication
- Two Person Workflow Controls
- PKI As a Service
- Shared Services
    - DNS, NTP, OS Repositories (YUM, WSUS)
- Shared VDI Capability (VDI AS A Service)
- Underlying Cloud Monitoring and Logging