SCOTTISH GOVERNMENT HOSTING IMPLEMENTATION

Hosting Implementation

06 – STAGE 2 – CLARIFICATION SUBMISSION

IBM Response – 24th April 2018

Scottish Government
Riaghaltas na h-Alba
gov.scot

IBM

Exec Summary to our response to your Hosting Implementation Clarification Submission

We believe our unique value proposition is the building of accredited Government application stacks of similar complexity and security standards on AWS at a wide range of Public Sector clients. From deploying critical national infrastructure at DWP and HMRC to supporting cloud platform delivery on the Home Office's most strategic programmes. This experience puts us at the forefront in the UK Public Sector of building secure, automated infrastructure services to be operated in the long term by in house client capability.

In addition to this we have in-depth knowledge of the SPM product and deployment and have developed a strong understanding of the culture and delivery model within your delivery teams during the first few months of our delivery of the Low Income Benefits service. All of this will enable you to have more certainty of delivery to the required timelines and quality of the service, which will enable a successful go-live of the first of the Low Income Benefits.

We have in-depth knowledge of how to build the necessary infrastructure, integrate and operate Applications that underpin the UK Welfare Estate (CIS, DRS and CPS, HMRC Child Tax Credits) and we can ensure you meet your objectives for the successful delivery of a production hosting service accredited to Official Sensitive workloads, by leveraging the resource, knowledge and experience gained in deploying infrastructure as code hosting services that underpin some of the UK's Critical National Infrastructure (CNI).

We propose the use of a proven products and services within UK government e.g. Ansible, Terraform, AWS and we've gained over 10-person years' experience deploying accredited hosting on AWS enabling us to be confident that we can help you quickly deploy your hosting service on time for the dates required. We will then iterate the solution together with you through the required testing and security validation period to create a secure accredited hosting platform.

Our experience can help you deploy a "secure by design" service using Infrastructure as Code, working with your team and the National Cyber Security Centre. We will commit to the delivery of building you a repeatable, fully automated, hosting service and ensure we provide support to your teams as we transition the live support of the hosting service back to Scottish Government. In addition, we've read, experienced first-hand and successfully navigated your Digital First Service Standard and will use it as a permanent guide to focus our delivery activities on what matters to your wider teams.

We believe in the short time we have worked together, we have demonstrated our commitment to you, the Scottish people and are committed to making this delivery a success.

We look forward to helping transform the lives of your citizens and working with you on this exciting journey!

1. (a) Confirm and provide assurance that you will meet the requirements in terms of deadlines for the environment deliverables, plan adoption, and resource modelling with assurance that the delivery dates of 31 July and 31 August 2018 will be met. Refer to the "What" section of the SOR

Our response to this question is broken down in the following sections (coloured with blue headings) and can be found by clicking on the following document links to help navigate this answer:

Our proposal for building the Pre-Production and Production hosting service is predicated on maximising re-use and a phased delivery to provide assurance that we can meet the July 31st and 31st August dates with ongoing improvements through to the October 2018 go-live.

Our approach will:

- Use an agile delivery method to quickly iterate services with demonstrable outcomes
- Leverage Infrastructure as Code throughout for the automated provision of environments
- Maximise the use of AWS services to de-risk delivery
- Leverage the team, skills and experience of delivering cloud hosting services for CNI
- Provides value through the sharing of infrastructure as code assets IBM has established
- Re-use of the secure cloud hosted Application Development services currently used for LIB
- Use a tried and tested approach for knowledge transfer and handing the service back to SG

This approach helps us:

- Put your users' needs first, tailoring the service to support your principles
- Reduce risk and provide certainty in the delivery of the Hosting Service
- **Provide confidence** when working with OGDs as you are partnering with a trusted DWP and HMRC partner
- Deliver greater value more quickly to the Scottish people
- **Leverage** cost effective **secure Cloud** hosting
- Become self-sufficient more quickly

Summary

Our understanding of principles, timeline and what's important to you

There is a need for the newly formed Scottish Social Security Directorate to establish a secure production hosting service in which to host the recently contracted delivery of the Low-Income Benefit platform which launches to the Scottish public in Autumn 2018. In order to complete this, Scottish Government need to build and deploy a set of security and infrastructure Foundation Services.

We understand that you are looking to establish a secure accredited production service to be deployed by building a set of security services that:

- Are fundamental to the secure operation of Social Security Directorate (SSD) Cloud hosted systems;
- Are fundamental for the proper execution of application processing or the lack of which will stop processing occurring;
- Are services, required for the proper operation by more than one application or device type.

This secure service requires elements that would be considered "Foundation Services" and are comprised of the following high-level capabilities:

- Platform and Security Management
- Security Information Event Management (SIEM)
- Perimeter and Network Security
- Data and Communications Security
- Identity and Access Management
- Threat and Vulnerability Management
- Privileged User Access Management

Alongside these security needs we understand that creating this service using Infrastructure as Code (IaC) and automated infrastructure principles is key to developing a platform which is cost effective, flexible and highly maintainable to cater to your future infrastructure demands. Through both DevOps tooling, methods and process this service should enable you to deliver rapidly to support the demanding programme of project delivery you have in the coming years.

Delivery timeline

In order to meet the delivery milestones outlined in the Statement of Requirements, we propose adopting a phased delivery approach to maintain credible but acceptable delivery timescales. We propose to deliver the environments in 3 key stages:

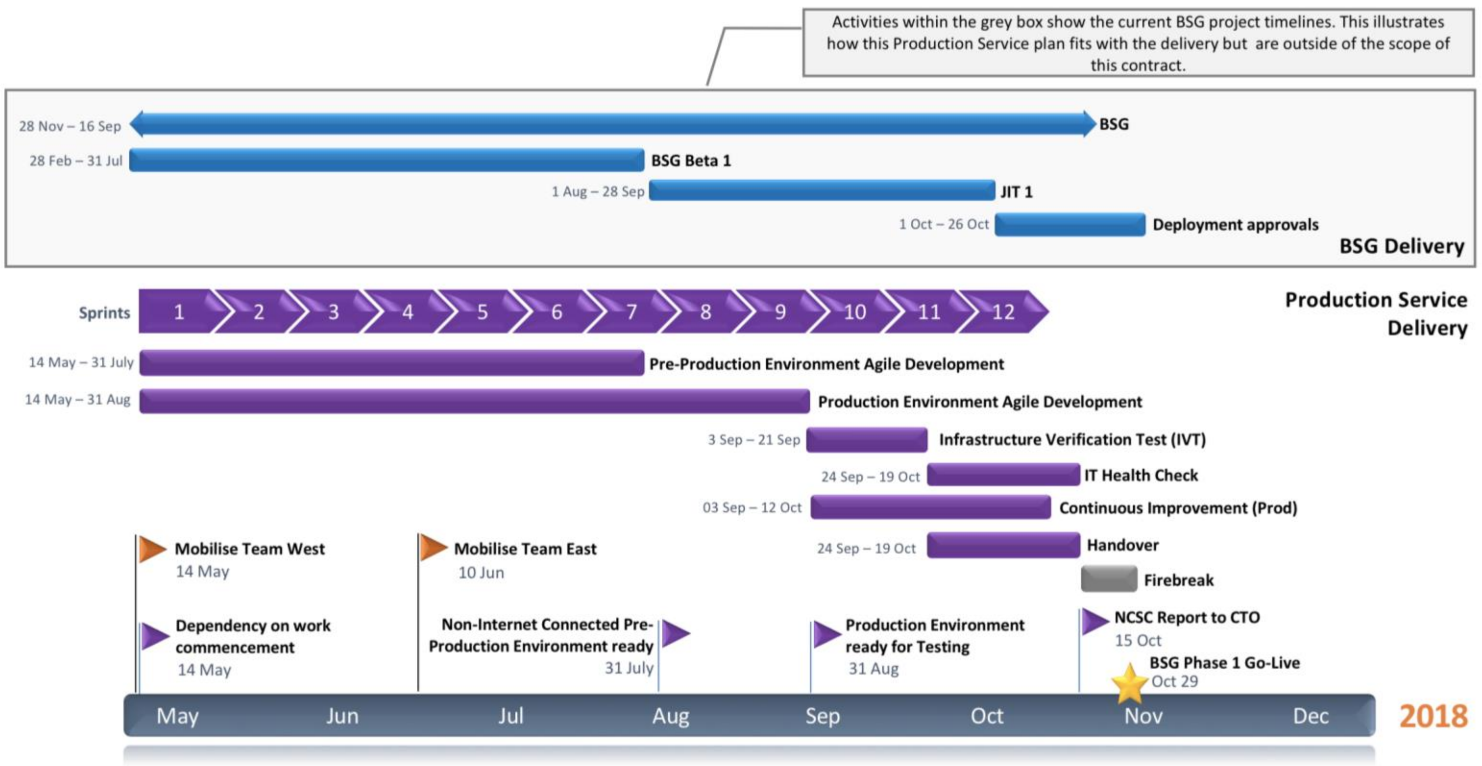
1. A non-internet connected pre-production environment by 31st July ready to start a joint System Integration Test for Best Start Grant
2. A production environment with 80% automation complete by 31st August, ready for further testing and IT Health Check
3. A fully automated production environment ready by 19th October

By adopting this phased delivery approach, we can prioritise the product backlog and apply early focus on achieving the critical outcomes in order to complete the IT Health Check and have a production environment ready for the Best Start Grant (BSG) go-live in October.

This approach also enables the team to focus on delivering the Minimum Viable Product (MVP) required to build the production environment and move into the IT Health Check with a level of automation completed, while providing some additional time for the team to complete continued improvements in parallel to the IT Health Check to deliver a fully automated production environment ahead of the BSG go-live.

Within the Agile sprints, the team will incrementally produce Level 2, 3 and 4 designs as each service is built on a sprint by sprint basis alongside development and test, including Performance Testing completed in-sprint. A separate Infrastructure Verification Test phase and IT Health Check will follow the build of the production environment on 31st August to ensure the environment is ready ahead of the go-live.

The plan below outlines how the delivery for the production service will link in to the your current BSG delivery plan and shows the major milestones and dates over the 6 month duration.



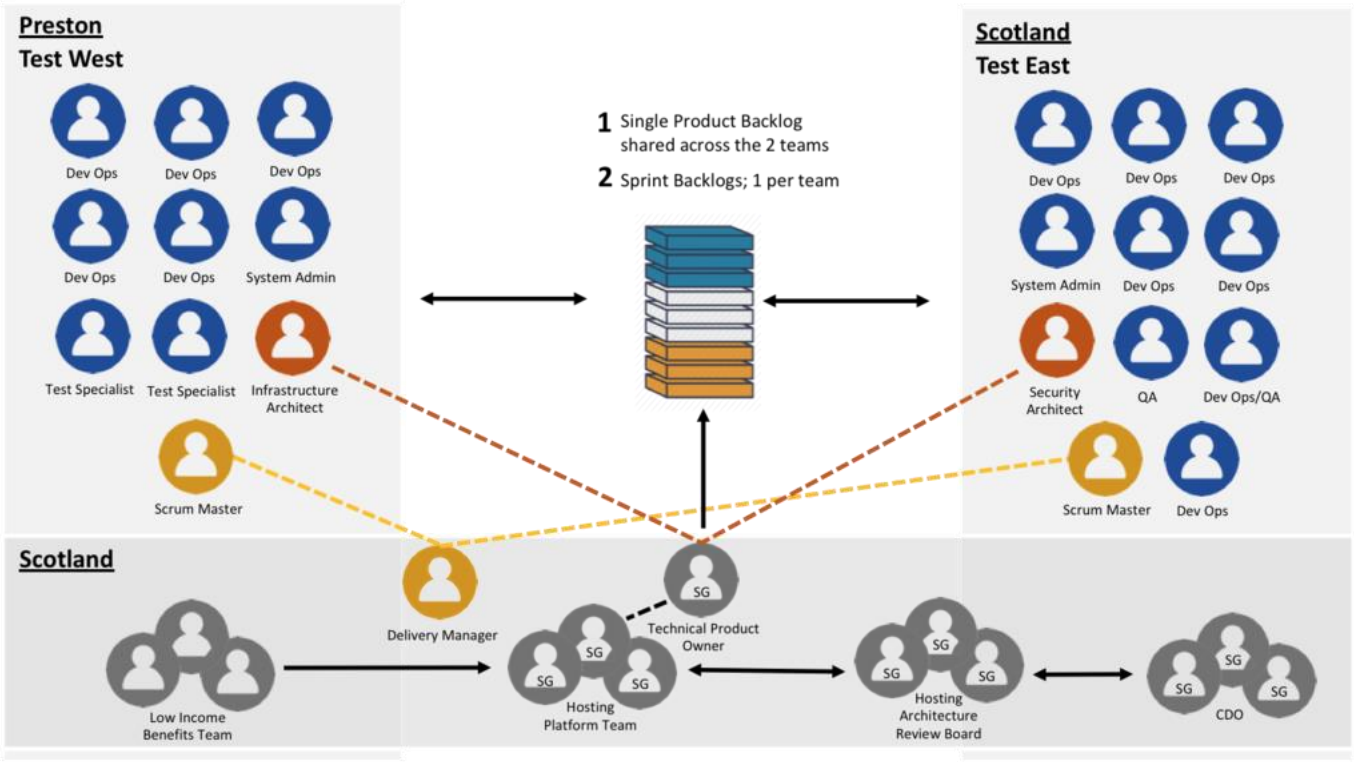
Proposed resource profile

In support of achieving the delivery timelines, we plan to mobilise the first team to start in May and commence work for the first 2 sprints, building up the backlog and kicking off the delivery before bringing on a second team. We will then mobilise the second team in June to start running the Agile delivery at scale adopting the LeSS Agile framework from Sprint 3 onwards. By adopting this approach, we will enable a steady ramp-up of the team, bringing in a second team once we have set-up a defined backlog and agreed the ways of working with the Hosting Platform team. The proposed resource profile is illustrated in the image below, which highlights the resource ramp-up and ramp-down points. We also propose that the Scottish Government operational support team ramps up ahead of September to enable a handover period as highlighted in the plan above.

Team	Role	18-May-18	25-May-18	01-Jun-18	08-Jun-18	15-Jun-18	22-Jun-18	29-Jun-18	06-Jul-18	13-Jul-18	20-Jul-18	27-Jul-18	03-Aug-18	10-Aug-18	17-Aug-18	24-Aug-18	31-Aug-18	07-Sep-18	14-Sep-18	21-Sep-18	28-Sep-18	05-Oct-18	12-Oct-18	19-Oct-18	26-Oct-18
ALL	Delivery Manager	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
ALL	Infrastructure/Security Architect	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
ALL	Infrastructure/Security Architect	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5					
East	Scrum Master	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
East	Sys Admin	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
East	DevOps	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
East	DevOps	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5								
East	DevOps	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5								
East	DevOps	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5								
East	DevOps	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5								
East	Quality Assurance Analyst	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
East	Quality Assurance Analyst	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
West	Scrum Master					5	5	5	5	5	5	5	5	5	5	5	5								
West	Sys Admin					5	5	5	5	5	5	5	5	5	5	5	5								
West	DevOps					5	5	5	5	5	5	5	5	5	5	5	5								
West	DevOps					5	5	5	5	5	5	5	5	5	5	5	5								
West	DevOps					5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
West	DevOps					5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
West	DevOps					5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
West	DevOps					5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
West	DevOps/QA					5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5		
West	Quality Assurance Analyst					5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5				

Adopting the LeSS approach to scaled Agile delivery, we will hold 1 single backlog shared across the two scrum teams ensuring both teams are sprinting towards the same goal to build a pre-production environment and a production environment by the dates required. We will follow a converge and diverge principle across the two scrum teams. This is where they will converge at the start and end of each sprint to review the single shared backlog and agree priorities with the Product Owner and Hosting Platform Team, interlocking with the LIB and CDO teams to ensure a fully prioritised backlog managing the dependencies both on other deliveries and on this delivery.

Once the teams have identified the key priorities for the backlog for the upcoming sprint, the teams will then diverge to run with their own individual sprint backlogs, with the Scrum Masters making sure to coordinate any key dependencies between the two teams, holding a scrum of scrums twice a week to ensure sufficient communication between the teams and blockers removed.



What does Dev/Test provide today?

[redacted]

[redacted]

What is needed to extend Dev/Test into Production

We propose extending the existing Dev/Test Infrastructure as Code (IaC) platform, building an AWS hosted, repeatable, fully automated set of secure infrastructure security services delivered as Infrastructure as Code for Pre-Production and Production Hosting use. Our phased delivery approach will enable you to implement infrastructure, supporting services and network integration for the pre-production environment by July 31st, 2018 in order to perform a joined-up system integration test for the LIB platform. Through a combination of shared AMI's, distributed source code and package repositories and VPC peering, our approach means we can safely move Dev/Test into your own AWS accounts.

With our phased approach we will work with you to deploy the production environment and all supporting services and external network integration by August 31st, 2018.

As part of our phased approach, the hosting services will mature at pace to enable full functionality and the successful completion of specified operational readiness tests in time for the October 2018 go live date. Given the aggressive timescales, our phased approach will place emphasis on completion of activities that enable operational acceptable service is delivered on time, and any "non-operational essential" services delivered following successful service acceptance.

To maximise value and de-risk delivery, our approach will make use of a range of AWS infrastructure, security and network services to enable, support, disaster recovery, the securing and management of the overall cloud infrastructure. Where NCSC deems a AWS service is not fit for purpose we will automate the deployment of a suitable service or component installed on standard AWS Infrastructure utilising Infrastructure-as-a-Service top ology or by leveraging solutions on the AWS marketplace.

Proposed high level deployment architecture

[redacted]

To de-risk delivery we will use NCSC approved AWS services and enable early deployment of a Production environment. These services will be integrated and deployed using Infrastructure as Code in a object orientated development enabling SG over time (if there is a desire to) replace AWS services with cloud agnostic security and infrastructure services in line with SG, GDS and OGD best practice.

Over ~30 services will need to be installed, automated, deployed and tested as part of the Production Architecture deployment helping SG secure the future LIB go-live and providing a common framework for the future roll-out of additional benefits including disability.

The tables that follow provide products that need to be deployed in order to create a secure Production service and support SSD applications deployed in AWS.

Ref.	Service	Service Description
1	Directory Service	AWS Active Directory will be used to administer features, such as Group Policy and single sign-on (SSO). AD will be configured to join EC2 instances to the domain and use AWS Enterprise IT applications such as AWS workspaces with Active Directory users and groups.
2	DNS	AWS DNS will be used as the main DNS service allowing easier integration options with hybrid infrastructure and AWS services. AWS Route 53 will used to resolve namespace of all AWS services such as ELBs.
3	DHCP	Each VPC created in AWS has a corresponding DHCP scope attached allowing options such as DNS server IP, namespace suffix and NTP IP to be set of the subnets within the VPC.
4	Time Service	AWS NTP time services will be utilised to synchronise time within the environment.
5	Backup	AWS Snapshots will be scheduled and created for each resource deployed. Snapshots are stored in AWS S3.
6	Archive	AWS s3 will be used for all long term storage such as backups with lifecycle policies configured to transfer the data to AWS Glacier (AWS cold, low cost storage).
7	Centralised Logging	Logs will be saved to AWS Cloudwatch logs initially and then extended to a more strategic logging service e.g. ELK stack.
8	System Monitoring and Alerting	AWS Cloudwatch will be configured initially to monitor key system metrics with alerts configured to trigger on key thresholds.
9	Application Monitoring and Alerting	Our solution re-uses the secure accredited platforms and delivery model that is used for both DWP and HMRC. This fully complies with all 14 of the National Cyber Security Centres Cloud Security Principles and we would work with you to determine the right services needed to link in to your deployed applications.
10	Scheduling Tool	AWS Lamda will be used for AWS scheduling use cases. Cron jobs will be used for batch type transfers until a strategic solution is identified.
11	System Patching	AWS RHUI for RedHat, WSUS for Windows and Repo mirror for CentOS will be configured and deployed to manage system patching.
12	Application Patching	We will test updates in route to Live environment and promote to live when satisfied using a set of services we determine with you during the delivery.
13	Bastion	Bastion server used as jump box (linux – ssh) or Windows administration box (RDP). Only available from trusted routes (Scottish Government networks) with AD authentication. Key authentication also required for SSH sessions.
14	OS	All OS to be authenticated against AD. All users\admins to authenticate with AD. AMIs to be created to appropriate patch and hardening level before used in environments. AMIs versions to be managed and deployed in environments on a regular schedule which we will agree with you during the agile sprints.

Ref.	Service	Service Description
15	Key Management Services	Leverage AWS KMS to produce, store and manage issuance and revocation of encryption keys to encrypt data at rest in EC2 instance EBS and S3 volumes.
16	Certificate Services	Use Scottish Government certificates for external facing components signed with trusted external CA. Leverage AWS certificate services for internal transport layer encryption for services such as TLS certificate deployed on internal ELBs.
17	Critical Security Patching	AWS RHUI for RedHat, WSUS for Windows and Repo mirror for CentOS will be configured and deployed to manage system patching.
18	Security Scanning	SaaS AV solution. Available on AWS Marketplace. Agent deployment on EC2 instances. Secure console (MFA) to manage environment.
19	Vulnerability Scanning	Deploy Nessus either directly or as part of the Security Onion distro to support real time vulnerability scanning.
20	Intrusion Detection System	Deploy Snort either directly or as part of the Security Onion distro to support real time ID scanning.
21	Security Logs	Security Logs to be hived off to secure area with limited access using a combination of ELK stack, BEATS and Security Onion.
22	Layer 7 Inspection	All internet traffic to be filtered through WAF for layer 7 inspection.
23	Internal Firewall	Subnets entry\exit controlled using AWS NACL (course grain). AWS Security Groups will be used on each instance or service to provide fine grained access (IP Layer).
24	DDOS	AWS Shield service utilised for DDOS protection. Other good practice to be adopted such as using WAF sandwich (ELB-WAF-ELB) for all internet layer 7 entry and exposing minimum attack surface.
25	SSO	An external identity broker such as Microsoft ADFS will be used in combination with AWS STS for federated access for Scottish Government users
26	Privilege Access Management	Access will be controlled at multiple layers – OS and application access will be controlled using a combination of AWS IAM and AWS Active Directory groups. AWS console access controlled using MFA, users, groups and roles.
27	Integration with SCOTS	Assumed SCOTS network will be integrated with AWS service using VPN IPSEC tunnel. All traffic to be routed through this link. (SG responsible for all SCOTS desktop work).
28	Integration with DWP	Assumed DWP network will be integrated with SGs AWS cloud service using VPN IPSEC tunnel. All traffic to be routed through this link.
29	SSD DevOps MAC Laptop integration	Assumed Mac users can use standard network interface. Possible separate SSID (wifi) and NAC on copper based on certificates stored on Mac. SCOTS network will allow route through to AWS via internet of VPN tunnel. (SG responsible for all desktop work).

Ref.	Service	Service Description
30	SSD Standard User integration	Assumed SSD users can use the same desktop as Scottish Government – TBC. (SG responsible for all desktop work).
31	Load Balancing	Utilise AWS ELB services. Region wide load balancing service.

What the final service will look like

Once deployed, the hosting service will provide SSD with a set of Infrastructure as Code assets that can enable the production roll-out of future SSD benefits. The Production service will adhere to the following principles:

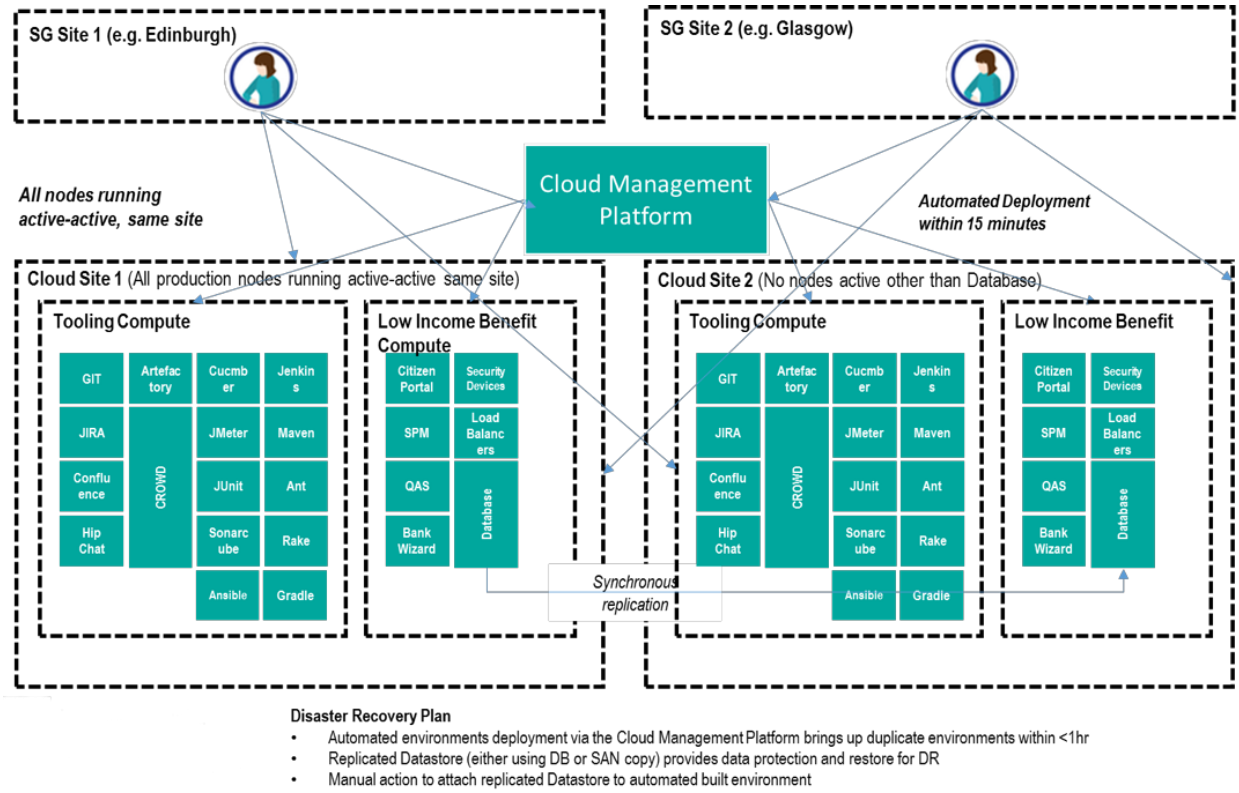
Enabling cost effective, efficient disaster recovery

Utilising a range of AWS infrastructure, security and network services combined with infrastructure as code and database replication to enable, support and deliver and efficient, effective disaster recovery solution.

Our solution will replicate the management VPC across 2 AWS London region data centres which will provide value for money as there will be no need to run entire Production environments as active-active.

Instead, the active-active management tooling will enable SG to automate the full production environment roll-out in the event of disaster. This will then be re-connected to any database instances where active-active log shopping / mirroring is in place.

The diagram below shows this design at a summary level.



Disaster Recovery Plan

- Automated environments deployment via the Cloud Management Platform brings up duplicate environments within <1hr
- Replicated Datastore (either using DB or SAN copy) provides data protection and restore for DR
- Manual action to attach replicated Datastore to automated built environment

Our proposal for the build of the pre-production / production hosting solution in terms of Disaster Recovery is to build this in two parts. The first is utilising automation technologies such as Ansible to define all components of the system as code. This enables us to deploy a full production instance in <1hr. This means that we do not have to build and have running a second DR site. This reduces the cost of hosting for you.

The only item that will exist in the second site is a replica of any Production databases. These databases will be configured in a HADR (High Availability Disaster Recovery) configuration. We will use either database log shipping, or database / storage replication depending on your RTO and RPO objectives. The decision as to which method is used will also be impacted by latency on the network links between SG hosted and externally hosted systems. If the latency is >3.5-5ms, the solution will not be suitable for replication and will have to use database log shipping.

1. (a) (ii) Describe any caveats, assumptions and dependencies that apply to Question 1. (a) above.

Our solution and approach to building the pre-production and production service is based off the planned delivery dates. By planning out what needs to be done by when, the following assumptions and dependencies need to be met to keep the plan on track.

#	Assumption / Dependency	Type	Rationale
1	We assume that AWS is the agreed cloud hosting facility	A	Leveraging AWS will save time testing migration and operation with other cloud providers as the Dev/Test platform currently resides in AWS today
2	[redacted]	D	Without this in place within 12 weeks, the July date for pre-production will not be possible
3	We are dependent on SG procuring AWS accounts and provide access to IBM prior to team landing	D	The team will begin deployment work on Day 1. Access to a SG AWS account structure will help establish the early segregation of duties design and the policies that will control all SG AWS accounts and VPC's
4	[redacted]	A	[redacted]
5	We are dependent on SSD to provide DevOps laptops to connect to a SG owned AWS account by contract signature	D	The plan requires that we have all equipment and access to AWS environments on day 1 following contract signature. Any delay could impact the plan and risk the July pre-production dates
6	We assume that SSD will be utilising the existing SCOTS services for network, desktop, email, internet, file and print	A	No desktop services are to be provided (other than access)
7	We assume that there is no need to take decisions to TDA if an AWS service is being leveraged.	A	Delay in product selections will ultimately delay the overall plan and increase cost and add risk to delivery
8	We assume that Cloud PaaS and SaaS services can be utilised wherever possible in order to meet timescales	A	AWS s3 will be used for all long-term storage such as backups with lifecycle policies configured to transfer the data to AWS Glacier (AWS cold, low cost storage).
9	We assume that SG will be responsible for all desktop services and developer laptop builds and configuration	A	There is no effort in the price / plan for IBM to undertake this work

#	Assumption / Dependency	Type	Rationale
10	We assume that we will co-locate only relevant staff and may with SG agreement complete some build aspects remotely. This is for expedience, efficiency, productivity and to leverage SME skills where necessary. This will be done transparently and in agreement with SG.	A	Since this is an aggressive plan, we will risk delays to the delivery if the team are distracted by technical discussions. The price at present assumes reduced travel.
11	We are dependent on SG agreeing a network connectivity design with DWP and for DWP to commit to delivering their end of the connection within 12 weeks of contract signature	D	This dependency is in line with the Capita Direct Connect lead time. Without this in place within 12 weeks, the July date for pre-production will not be possible
12	We assume that all services will be built using IaC, but there will be no concept of self service.	A	No time has been factored into building a Self-Service Portal that non-technical users can use for provisioning environments.
13	We assume that a phased delivery approach is acceptable.	A	The timelines are aggressive and it is not possible to have a fully automated Internet Facing -> Trusted environment ready for July 31st.
14	IBM will provide our IBM AWS assets (the AWS automated Dev/Test scripts for building an accreditation compliant Dev/Test environment) on a Royalty Free license on the assumption that this will not be shared with other suppliers	A	IBM has invested heavily in creating these assets and it provides our Public Sector clients with the ability to deliver these types of projects in shortened timescales. To lose this to a competitor would severely impact IBM's ability to compete across all sectors.
15	We are dependent on SG proving relevant skilled technical SMEs in parallel to this delivery in order to enable an iterative handover approach	D	Once a service has been automated and tested, we intend handing this over to SG resource for any further configuration. e.g. AWS Directory Services – we will automate the deployment and configure the outline Organisation Units and permissions, but would hand this service over to SG for the SG Hosting Platform Team to administer additional SG users. Our estimate assumes a similar approach for all other services.
16	Our estimate is dependent on the scope of this work being fixed to the 32 services requested in the Statement of Requirements	D	No additional effort has been factored in for change. Any change will require an impact assessment on both the delivery plan and the estimate.
17	We assume that ITHC will be carried out following successful automated deployment of Pre-Production after 31st July 2018.	A	There is not enough time in the plan to undertake an ITHC prior to this date.
18	We assume that ITHC will be carried out following successful automated	A	There is not enough time in the plan to undertake an ITHC prior to this date.

#	Assumption / Dependency	Type	Rationale
	deployment of Production after 31st August 2018.		
19	We assume that the High-Level Design is an SSD responsibility in line with the Statement of Requirements and is already approved at TDA.	A	The estimates are based on the current High-Level Design. Any changes will be subject to an impact assessment.
20	We assume that all resources will require BPSS clearance	A	There is no requirement for SC clearance for any of the team as the team will not have any access to Secret or Top Secret information
21	We assume that the IBM team will not have any access to Production Data	A	This will impact the IBM GDPR compliance for any future contract which has not been factored into the estimates.
22	We are dependent on SG providing resilient, and high performing wireless connectivity by 11th June to the Internet in order to meet the deadlines.	D	Without access to the Internet, the second team (which we are planning to co-locate with you) will not be able to complete their work within the given timescales.
23	We are dependent on iTECS implementing the Scots side of the VPN within 5 days of the SWAN Capita link implementation.	D	If this is not possible, then the plan will be impacted and there is a risk of delay to the overall timeline.
24	We are dependent on SG and DWP agreeing and implementing any SG-DWP network connectivity within 5 days of the SWAN Capita link implementation.	D	If this is not possible, then the plan will be impacted and there is a risk of delay to the overall timeline.
25	We assume that ongoing support is out of scope of this contract	A	We have not estimated for on-going support as part of this estimate. This is included as part of the optional requirement B

1. (b) Confirm and provide assurance that you will meet the requirements in terms of the "How" section of the SOR.

Our response to this question is broken down in the following sections (coloured with blue headings) and can be found by clicking on the following document links to help navigate this answer:

- Delivering in line with the NCSC Cloud principles (here)
- Ensuring data is processed in line with policies for Official-Sensitive classification (here)
- Using our Infrastructure as Code and Automated Infrastructure expertise (here)
- How we will provide the DevOps tools within the AWS London Region (here)
- How we will work in collaboration with your team and broader partners (here)

Delivering in line with the NCSC Cloud Principles

We fully understand the 14 NCSC cloud principles and have significant experience applying them having built the Home Office DevOps platform with all digital projects being automated as Infrastructure as Code with literally 100s of digital projects successfully delivered on AWS using secure cloud principles combined with a DevOps / IAC approach. We have successfully deployed CIS for DWP and again our approach was aligned to the 14 principles below. We partnered with HMRC for the AWS production roll-out for the Customs Declaration System (CDS). Our approach for SG will ensure that the provision of any and all environments, components and services are delivered in alignment with the UK NCSC Cloud Security Principles, evidenced via a formal report to the Chief Digital Officer at least 14 days before go-live. The table below shows how.

#	NCSC Cloud Principle	How we will adhere / meet the principle
1	Data in transit protection	[redacted]
2	Asset protection and resilience	User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. This will be implemented through the use of accredited UK hosted AWS data centres
3	Separation between users	This will be achieved at a number of levels through a combination of: AWS accounts for Pre-production and Production IAM roles segregating system administrator rights and privileges AWS Directory Users and Computers using a combination of OU's, Group Policy, Security Groups and Permissions to restrict access on a specific needs basis
4	Governance framework	As part of our overall delivery and through the use of level 4 runbooks we will document a security governance that provides: A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. A documented framework for security governance, with policies governing key aspects of information security relevant to the service. Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. Processes to identify and ensure compliance with applicable legal and regulatory requirements.
5	Operational security	Good operational security will be implemented that is simple, yet effective with clear processes that successfully manage:

#	NCSC Cloud Principle	How we will adhere / meet the principle
		Configuration and change management –changes to the system will be properly tested and authorised through a combination of automated testing and workflow. [redacted] Incident management – through re-use of our service management model at DWP and HMRC we will use a tried and tested incident management service to respond to incidents and recover a secure, available service whilst being developed and until hand over to SG
6	Personnel security	AWS s3 will be used for all long-term storage such as backups with lifecycle policies configured to transfer the data to AWS Glacier (AWS cold, low cost storage).
7	Secure development	This will be achieved by utilising our existing secure accredited Dev/Test environment on which LIB is currently being developed
8	Supply chain security	We will ensure that all security controls and measures that are deemed necessary to maintain alignment to the cloud principles are filtered through any 3rd party supply chain as we do today for DWP, HMRC and SG
9	Secure user management	[redacted]
10	Identity and authentication	[redacted]
11	External interface protection	[redacted]
12	Secure service administration	[redacted]

#	NCSC Cloud Principle	How we will adhere / meet the principle
13	Audit information for users	Our approach utilises the proven AWS cloud watch services for audit and logging. These logs will be directed to the SG SOC and NOC for consumption. We can also supplement these logs with Security Onion and Elk stack logs if Cloudwatch does not meet your requirements
14	Secure use of the service	Our approach will follow strict "infrastructure as a code" and "immutability" principles (i.e. no change and configuration management in production or user login is allowed, with the exception of break-glass security and forensic procedures). This minimises the risk of human error and/or accidental access or loss of data

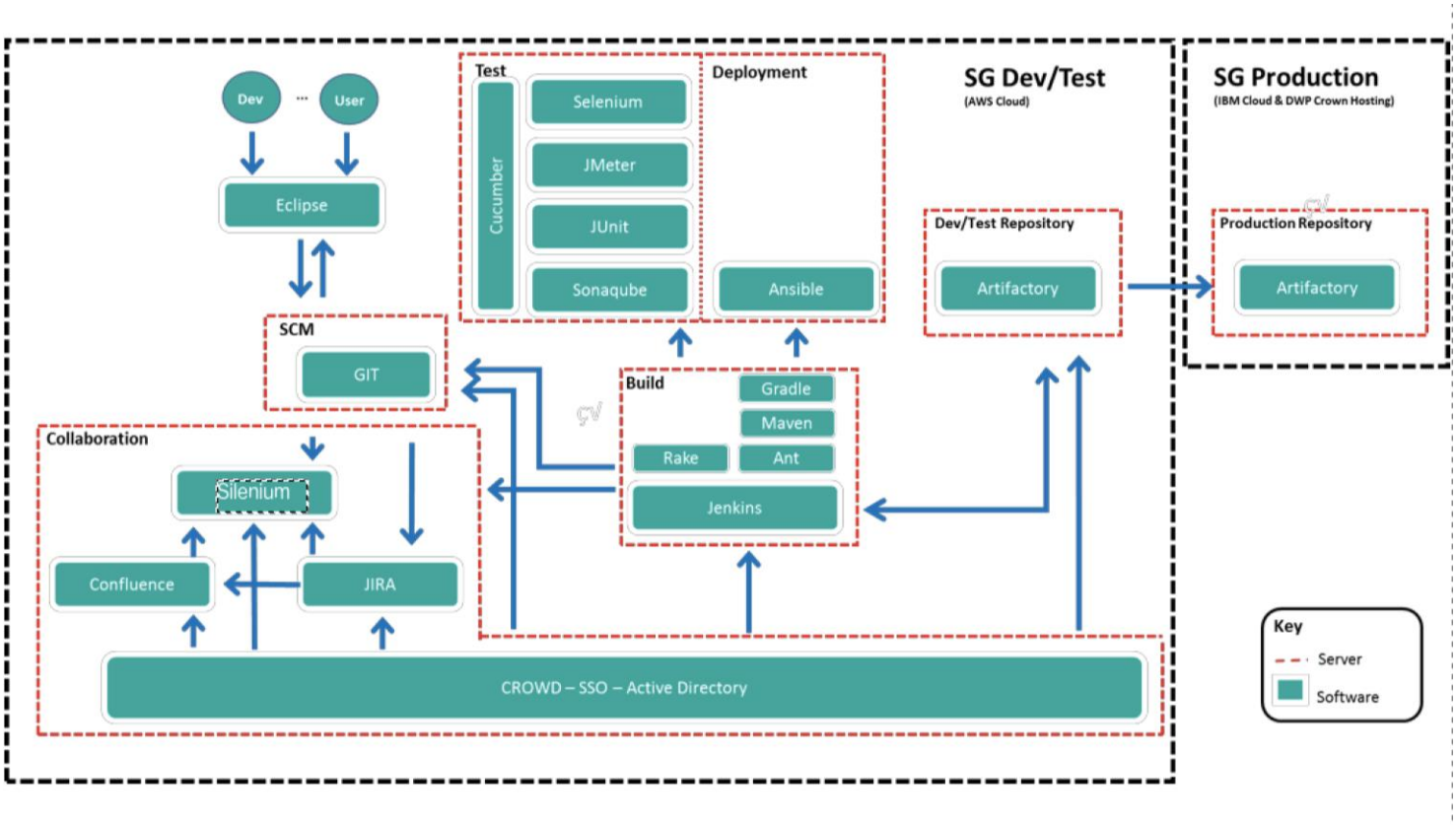
Ensuring data is processed in line with policies for Official-Sensitive classification

Data processed during this engagement will be handled in line with requirements of the Government Security Classification policy, specifically the requirement for OFFICIAL-SENSITIVE. All our team members will have as a minimum BPSS clearance. By extending our accredited Dev/Test environment (which is already accredited for hosting OFFICIAL-SENSITIVE workload) combined with our existing ISO27001 handling measures and with appropriate security testing of the proposed hosting service, will ensure that this handling requirement is fully met prior to go-live.

Using our Infrastructure as Code and Automated Infrastructure expertise

Our approach for your hosting solution utilises 'Infrastructure as Code' and 'Automated Infrastructure' techniques and is central to our delivery approach, creating the capability to automate and replicate for the efficient delivery of non-production environments from the delivered instances.

This means that all parts of the stack from software components, through to integration assets, interfaces, network and security devices as well as compute is all defined as code. This enables us to rapidly, in an automated manner, move quickly from story / backlog through Development, automated testing, package build and test and deployment into the Cloud. To place a quality control gate prior to production release, we utilise Artifactory replication and user testing sign off workflow to support the promotion of code from Dev to Live as can be seen below:



How we will provide the DevOps tools within the AWS London Region

With our proposal, all of the tooling above is already available in the AWS London region and being used for your current LIB delivery. This means that from Day1, developers and sysadmins can begin developing the pre-production / production hosting solution and utilise the stack above as part of an Agile development approach. By extending the existing Dev/test service used for LIB, we will provide the necessary DevOps tools and processes to support the migration from the IBM Test and Development environments through to the new Pre-production and Production environments.

How we will work in collaboration with your team and broader partners

By co-locating one of our scrum teams with you in Scotland we can provide a highly collaborative approach where we can work directly and effectively with SSD staff throughout the lifetime of the contract. This would include integrating in to the existing SSD Hosting team and CDO as part of the architectural governance and to enable knowledge transfer of the environments over to the Hosting Platform Team for live operations.

Working collaboratively as part of a number of Agile ceremonies and through Prince2 Lite governance, we will ensure we work with your other delivery partners such as iTECS for SCOTS integration, SWAN Capita for VPN integration, the LIB delivery team and other parts of the Social Security Programme who are developing common components and services for the agency.

As part of our agile delivery, we will hold fortnightly Show N' Tells, demonstrating to the hosting platform team the work that has been completed so far and providing them early opportunity to understand the architecture, design and IaC assets. We will provide the Hosting Platform Team with the necessary hands on time through a combination of shadowing, documentation and opportunity to "play" with aspects of the service deployed into Dev/Test. For the Hosting Platform Team to be able to fully support the service we will ensure thorough documentation and knowledge transfer material and specific KT (Knowledge Transfer) sessions. This will ensure the receiving team will be able to effectively and efficiently support the service and be assume ultimate responsibility for its live operation.

1. (c) Confirm and provide assurance that you will meet the requirements in terms of the design and test approach

Our response to this question is broken down in the following sections (coloured with blue headings) and can be found by clicking on the following document links to help navigate this answer:

Summary

Our approach to testing is to provide as much coverage through automated testing as possible within the timescales to provide the SG Hosting Architecture Board and Hosting Platform team with the confidence that the hosting platform performs as expected.

Proposed in scope testing

- IVT (Infrastructure Verification Testing) / Build testing where new infrastructure is deployed and configured in the respective availability zones for use
- Security vulnerability assessment on the infrastructure builds
- Operational Acceptance Test (which SG Hosting Platform will be responsible for receiving)

Out of scope testing

- Performance testing (of any SG application)
- Batch testing (of any SG application)

Test objectives

The objective of the Hosting test phases is to ensure that the target environment is fit for handing over to the next project phase by having delivered into it all infrastructure, connectivity and software as defined by the 'SG Production Hosting Design' document.

The core objectives are:

- To verify that the infrastructure has been installed and service activated as IaC
- To verify that the required network connections have been established as IaC
- To verify that applications have been deployed to the Target environment during the period July 31st to October 1st
- To verify that applications have been integrated with other systems and software to satisfy business and testing requirements

Focus areas of Testing

Areas of infrastructure testing that will be applicable specifically for the Pre-Production and Production hosting build. Our proposed Testing scope will only cover non-functional i.e. no application testing will be performed. The following table provides a summary of test focus:

Test Area	Description	Example
Internal Interfaces	The new location of the application platform and associated IP address range change will need to be tested within the context of existing internal system	Database and application servers referenced by the systems and applications being deployed are changed.
External Interfaces	The new location of the application platform and associated IP address range change will need to be tested within the context of existing External system interfaces	Other applications, DMZ, 3rd party applications and changes to Firewall rules.
Performance	This attribute may be affected by the migration due to increased latency or a change in the host platform or disk subsystem performance	May include; Load, Stress and Volume testing. These may be documented within the Service Level Agreements. Must also consider Network Capacity and Latency Changes to the network performance against the network requirement based on the traffic estimated. Verifies the system and application speed across WAN links.
User Access	The method used by the business user to access to the application may change.	Citrix (thin-client), new Infrastructure, location of login script or .exe file etc. need to check; remote access, negative testing, firewalls
User Roles	Each level of role access and privileges incl. negative testing	Are we introducing changes to user roles that have an impact on infrastructure or the application?
Monitoring and Alerting	Checking IT processes and procedures executed.	System Monitoring: Changes to the monitoring Applications or framework in system level (e.g., CPU Utilization, free disk space, memory paging, memory availability, system response, operating system and database performance, network I/O, exceptions and failures), Application Monitoring: Changes to the implementation of application monitoring clients and jobs with failure scenarios simulated. e.g. alert on critical events, etc. and Network Monitoring: Changes to the client and implementation of monitoring work on network components with failure scenario simulated. e.g. alert on critical events, etc.
Failover	Checking IT processes and procedures executed	Failover within a cluster, server to server failover.
Security	Changes to the system security setup, application vulnerability, interface security and security key generation based on policies.	Are IBM ISEC standards met or SOX or regulatory standards?
Load Balancing	Balanced load, server down-rerouting requests, sticky sessions	Are we implanting a new load-balancing technology?

Test Area	Description	Example
Backup /Restore	Changes to the system's capability to perform; Network backup operational, local archive, backup and restore facilities operational	New Back-Up Application and Cycle implementation. Local and/or Remote backups processes tested.
Container / infrastructure change	Changes to the operating system, platform hardware etc	Patch updates.
Disaster Recovery	The disaster recovery solution implemented post-migration may change and it is vital to make sure that the agreed RTO and RPO are met and the step-by-step DR procedures	Changing the disaster recovery solution and the implications on recovery time and point objectives. Are and changes necessary to the TRP and SRP documentation post migration based on any changes that may have taken place during the migration.
Availability	The level of resilience may change, and/or the solution implemented to provide resilience may change. This can be broken down into System Resilience and Network Resilience.	System Resilience (such as high availability, load balancing or database clustering in order to ensure the resiliency is working properly according the design. Any changes to the procedures required to achieve the resilience should be verified during the test. The fail-over time, session's stickiness and data integrity after fail-over will be observed) and Network Resilience (such as high availability, load balancing or database clustering in order to ensure the resiliency is working properly according the design. Any changes to the procedures required to achieve the resilience should be verified during the test. The fail-over time, session's stickiness and data integrity after fail-over will be observed)
Operations, Maintenance and Stability	Failures that endanger continuing operation, including, patches and upgrades, Failures that take down the system too frequently enough or keep it down too long. Personnel without much know-how on the system should be able to use the procedures to build the system.	For a new environment, careful considerations should be made to the systems availability (time-up) and reliability.
Compatibility	Failures with certain supported browsers, networks, operating systems and other environmental elements/components	Ensuring application and infrastructure components and versions are aligned.

Three deliverable / work products will be produced in support of testing during the test phases: -

- Detailed (Event) Test Plan
- Test Completion Report
- Repository of test scripts, test results and defects.

The table below sets out the outputs that will be generated by test phase.

	IVT	System	OAT	AVT
DTP	Y	Y	Y	Y
TCR	Y	Y	Y	Y
Scripts	N	Y	Y	Y
Results	Y	Y	Y	Y
Defects (locally)	Y	Y	N	N
Defects in test tool	N	Y	Y	Y

Infrastructure Verification Testing (IVT), System and Operational Acceptance Testing will be undertaken as part of this delivery. Application Verification Testing would be the responsibility of SG or your other suppliers but required to ensure a holistic set of tests is performed.

Infrastructure Verification Testing

IVT will be completed to ensure the installation of Operating Systems and Services are completed as per Design including automated installs and configuration management they are deployed with. Tests will then be completed to ensure they integrate with the wider shared services within the Infrastructure.

The following conditions be considered when defining the commission test:

- Initial Power on Tests
- Local Admin settings and access
- Reboot of devices
- Network and Storage connectivity tests and resilience
- Operating System Installation as per Design
- Provision of Services for Server deployment
- Configuration Management of Operating Systems
- Access controls to the Server
- Connectivity to and resolution of Policy from Monitoring/Systems Management Server
- Automated Installation of the Service
- Access Controls for the Service
- Functional Testing of the Service
- Resilience Testing of the Service
- Reboot and recovery of Service
- Audit of Service
- Server Backup and Restore
- Server Monitoring
- Server Alerting

Entry Criteria	Exit Criteria
• Relevant plans and documentation prepared, agreed and resourced • All resources confirmed and aligned with the test schedule • Relevant plans and documentation prepared, agreed and resourced	• Test cases passed • Test Completion Report issued • No Severity 1 or 2 defect outstanding

• All resources confirmed and aligned with the test schedule • Foundation services to support build complete • Raid log and defect log up to date	

IT Health Check

IT Health Check provides an independent assessment on the Production environment build activities to adhere to the security considerations for maintaining a secure and robust hosting service. It is assumed that SG will arrange for a 3rd party IT health check. Our proposal ensures that there are SME's available to remediate any part of the service following IT Health Check.

Suspension and resumption criteria

Testing will be suspended on each individual component when a major defect prevents further tests being performed within a system test phase. Testing will be resumed when the defect has been fixed and has been proved by any subsequent re-testing.

Testing will be suspended if any of the following scenarios occurs:

- Testing proves the solution contains severe problems that affect the infrastructure and applications to the extent that it is no longer useful to continue testing
- Performance deteriorates to the extent that no progress can be made against the test plan, and the validity of the tests is being called in to question.

While each test activity has its own specific considerations for test suspension & resumption, the principles are:

- Suspension of testing activity can occur at three primary levels:
    1. All test effort is suspended as the defect / fault prevents further test effort
    2. Test effort in a particular area of the application/infrastructure is suspended, but testing of other areas can continue while the issue is resolved
    3. Testing of a particular function/feature is suspended, but testing of other functions/features can continue
- Resumption on resolution of the defect / fault will be identified according to the nature of suspension. It will include a statement of the possible delay in the completion of the test effort/activity, and an estimate of the amount of additional test effort required on resumption of testing (e.g. repeat x amount of testing, time to re-set up test environment, etc.).
- The decision to suspend or resume testing of a single component will be made by the IBM QA's. The decision to suspend or resume testing will be proposed by the IBM QA to the SG Hosting Project Manager, SG Hosting Lead Architect, IBM Delivery Manager, IBM Lead Architect and other interested parties.
- The suspension and resumption of testing will need quantifying with SG to understand resource retention and possible financial impact incurred for any periods of inactivity.

Definition of Done

Following the approach that has already been agreed within the LIB delivery, we would propose using the same agreed definition of done to bound our delivery commitment shown in the bullets below:

- Code written
- Code peer reviewed
- Manual tests ran
- Acceptance criteria met
- Automated tests scripted & ran
- Bugs resolved
- Updated in Jira

2. (a) Provide assurance of availability and ability to supply the optimal core team and supplementary resources at pace.

Our response to this question is broken down in the following sections (coloured with blue headings) and can be found by clicking on the following document links to help navigate this answer:

- Summary (here)
- Skills required to complete the work (here)
- Resources required to successfully deliver at pace (here)
- Breakdown of outcomes by team (here)

Summary

Our proposal for the building the Pre-Production and Production hosting service is predicated on providing the optimal core team. Our approach will:

- Involve **teams** of highly skilled **DevOps** engineers **experienced** in **AWS** and **IaC**
- Leverage **individuals** with **skills** and **experience** in delivering **AWS** cloud hosted services for **CNI**
- Ensure appropriate interlock with SG Hosting Architecture Board
- Ensure smooth handover to the newly formed SG Hosting Platform Team

This approach will enable us to help SG:

- Deliver at pace
- Reduce risk and provide certainty in the delivery of the Hosting Service
- When working with OGDs as you are **partnering** with a **trusted DWP** and **HMRC partner**
- Deliver greater value more quickly to the Scottish people
- Become self-sufficient more quickly

Skills required to complete the work

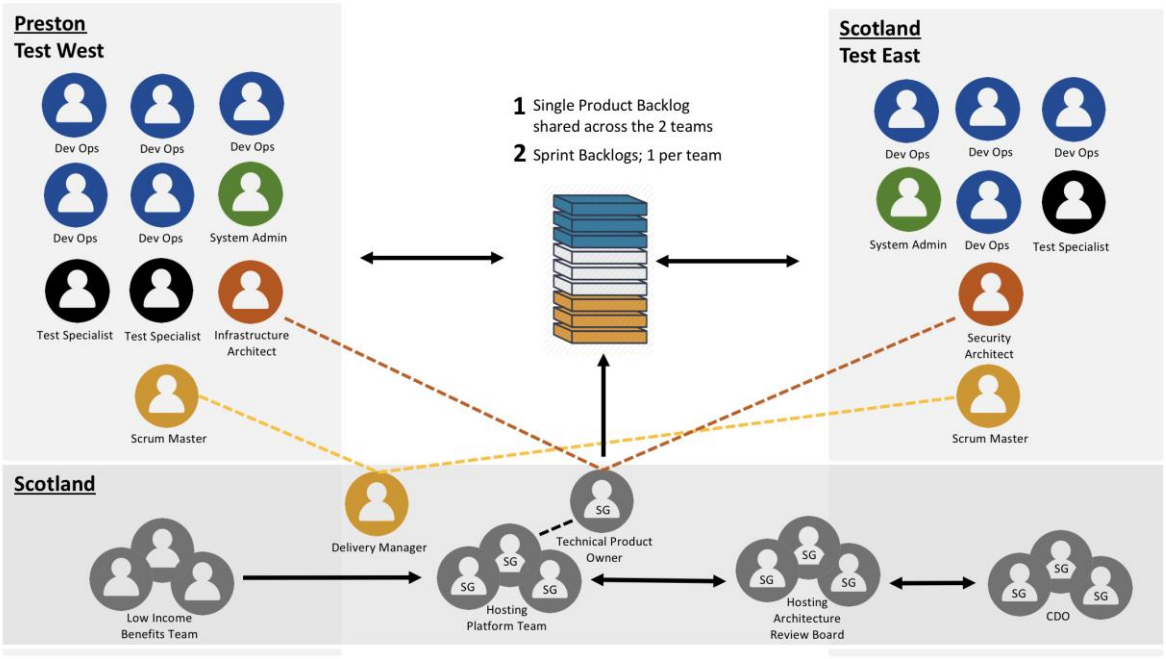
To complete the work within the timescales, we are going to need a high performing team with skills across AWS, IaC, Infrastructure and Security Architecture, DevOps, Systems administration, Quality Assurance and agile. The matrix below shows the role-skills alignment required to complete this type of work.

Role	Technical Skills												General Skills						
	AWS	Infrastructur	Security	Network	IaS	Ansible	GIT	Complex SI	Agile	Agile at scale	Artifactory	SonarQube	Test Driven	Automated	Self-	Dedicated	Team player	Conscientiou	Communicati
Delivery Manager								■	■						■	■	■	■	■
Scrum Master									■	■					■	■	■	■	■
Infrastructure Architect	■	■	■	■		■	■								■	■	■	■	■
Security Architect	■	■	■	■											■	■	■	■	■
DevOps Engineer	■	■		■	■	■	■				■	■	■		■	■	■	■	■
Systems Admin	■	■		■	■	■	■				■	■			■	■	■	■	■
QA	■					■	■						■	■	■	■	■	■	■

Please see provided Pen-Pics in Question 3A which evidences our team's skills and experience against the above skills matrix.

Resources required to successfully deliver at pace

We've sourced the key skills required to deliver this solution and plan to mobilise the team over 2 phases. Our proposed team has proven experience of automating the deployment of Critical National Infrastructure (CNI). To deliver the work at pace we are proposing 2 scrum teams working from one back log. To maximise value, the Infrastructure and Security Architects will play an overarching role across both scrum teams and will have regular interlock with the Product Owner and Hosting Architecture Review Board. The Delivery Manager will also play an overarching role for this delivery, managing the dependencies across both scrum teams, ensuring the backlog is sufficiently prioritised and burn-up on track for the delivery milestones, while also managing the dependencies across third parties and the Low-Income Benefits programme to align the backlog priorities with the LIB delivery timelines.



By having one team within an IBM location, it provides access to a wider pool of resources and skills enabling the team to focus on driving the delivery forward at pace. Fortnightly Show N' Tells will be provided to the SG Hosting Architecture Review Board and Hosting Platform Teams in a SG location.

To facilitate an effective and efficient delivery maximising the outcomes during a tight delivery timescale, we propose to adopt a scaled agile approach using the less framework. A link to the framework can be found here: https://less.works.

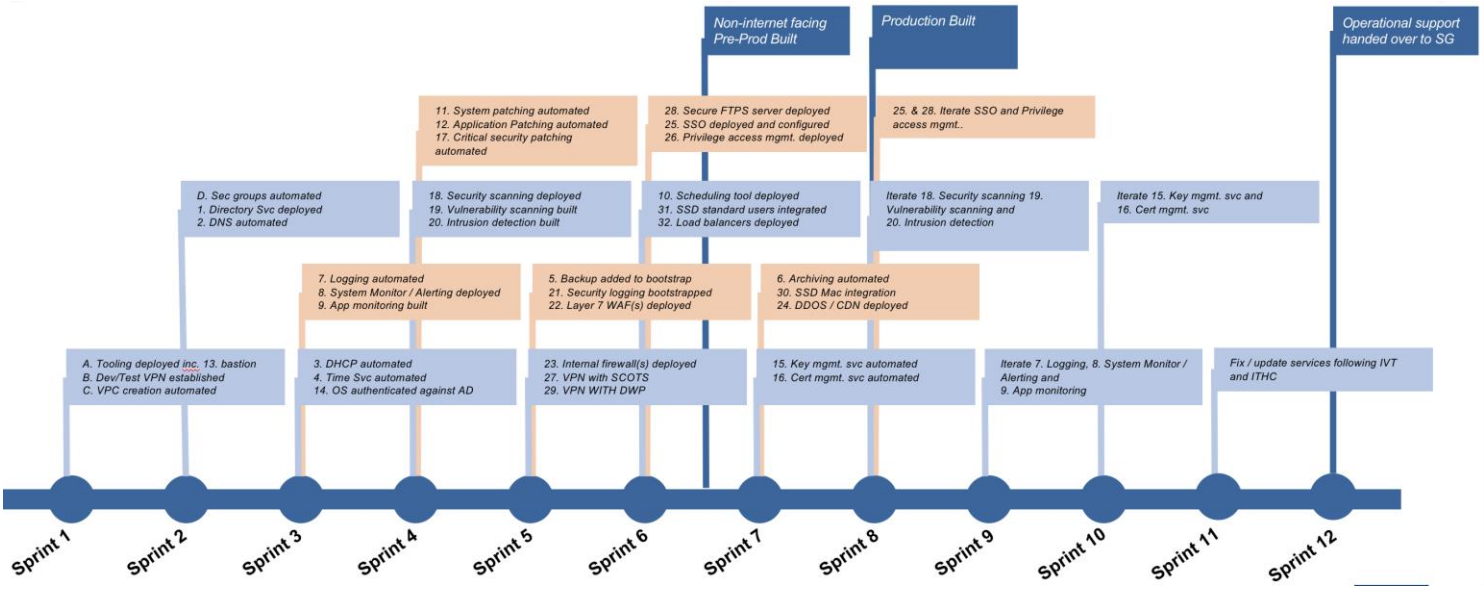
The diagram above demonstrates how we will work to this framework by having a single shared Product Backlog between two teams, which is prioritised by the Technical Product Owner with input from the two teams. Each team will then have a separate sprint backlog to focus on delivering incremental change. Following a diverge and converge approach, the Scrum teams will diverge at the start of a Sprint to deliver at pace within their individual teams, holding separate stand-ups and managing an independent Sprint Backlog where the Scrum Masters will ensure coordination across the teams, managing the inter-dependencies and planning ahead for the next sprint. At the end of each Sprint, the teams will start to converge again, where Sprint reviews will be held in unison, enabling a team to provide an overarching demonstration of the latest Product increment.

Breakdown of outcomes by Team

There are over 30 services that to be automated in order to be deployed. These services will not act on their own but will need to be integrated with one another and in addition, each environment will need to be defined as Infrastructure as Code, implementing each of the ~30 relevant services that will need to be deployed to make up an environment. Furthermore, additional automation scripts will need to be developed to open up static routes, ports and other services to finally provide and e2e Pre-Production and Production environment. This is a highly complex, high risk delivery (given the aggressive timescales).

To meet the demanding work schedule, we propose a two-scrum team approach jointly consisting of 11 DevOps engineers, 2 Infrastructure / Security architects, 2 Scrum Masters and a Delivery Manager with overall responsibility for the successful e2e delivery of the Pre-Production and Production hosting environments. We have proposed a breakdown of the expected outcomes by team in the diagram below to demonstrate how we will ensure the teams can deliver at pace to maximise the

outcomes on the sprint by sprint basis. By following this approach and splitting the workload across two teams, this 2-team approach de-risks the delivery timescales and enables the team to deliver the key outcomes required to meet the Pre-Production and Production environment milestones.



3. (a) Please provide evidence of your 'infrastructure as code' and 'automated infrastructure' expertise in your proposed team.

Summary

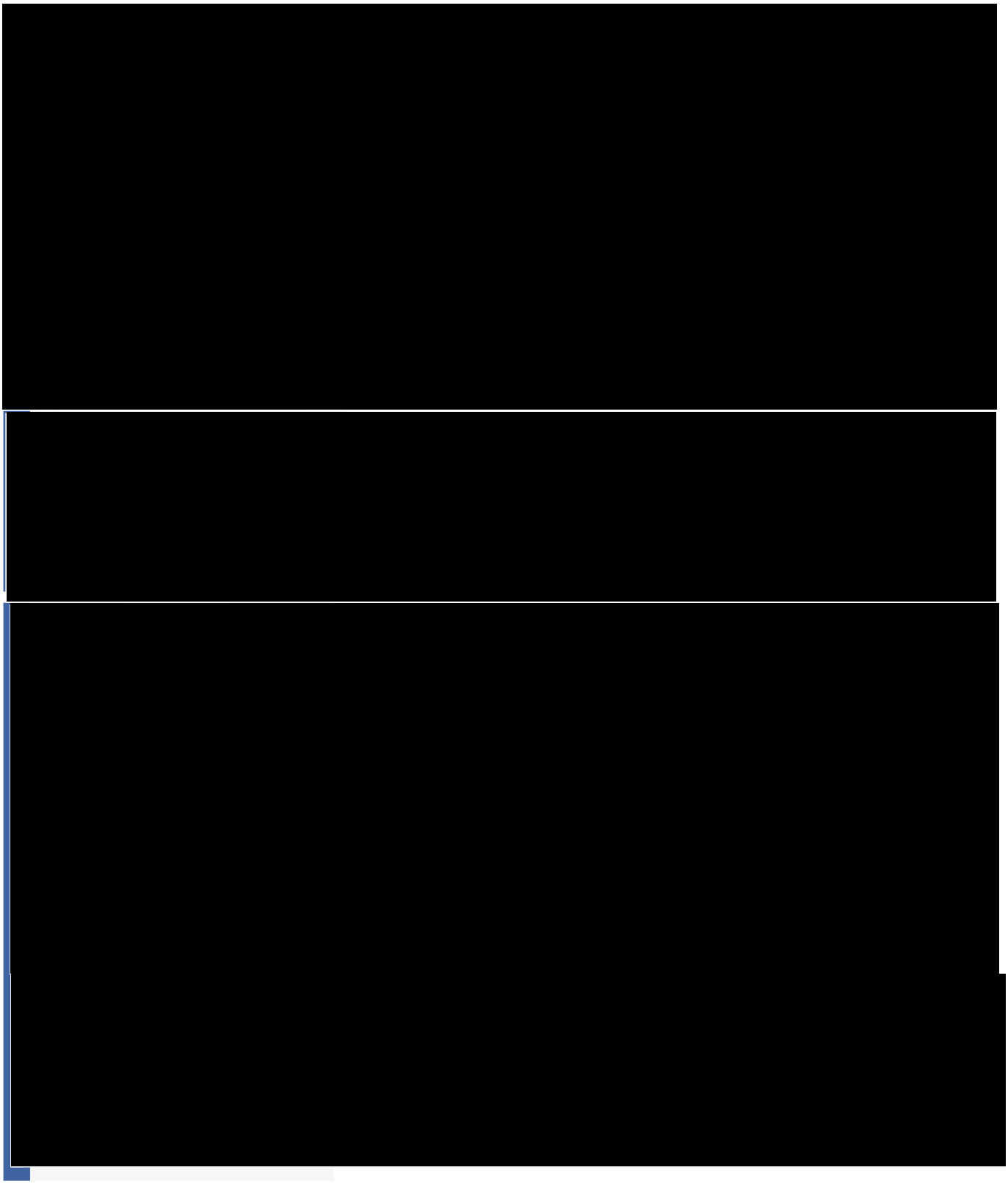
We've sourced the key skills required to deliver this solution and plan to mobilise the team over 2 phases. Our proposed team has proven experience of 'infrastructure as code' and 'automated infrastructure'.

Please see the following Pen Pics which provides an overview of some of our proposed team and the skills they have in automating the deployments in AWS and with CNI.

[redacted]

Work Experience

[redacted]



[redacted]

3. (b) Please provide 2 examples of your recent experience of similar delivery (demonstrating how you used techniques described in the How section of the SOR) including dates, project details, client name and deliverables.

[redacted]

- [redacted]

Florida Department of Children and Families (DCF), Florida Safe Families Network Programme

Apr 2017 – Dec 2017

Insight:

Florida's Department of Children and Families were running a number of web-based applications on traditional On-Premise hosting using manually built and deployed to infrastructure. These are highly critical services that provide the backbone for the welfare of children across the state and any outages or poor operational service can put the lives of vulnerable children at risk.

The manual deployment and management of environments created a very high cost infrastructure service, was inflexible to any increase in workload demands and difficult to ensure security compliance by the third-party providers. It also created a very rigid deployment and software upgrade lifecycle which was limiting the Department getting changes out to users at pace and putting services and children in danger.

Idea:

We worked collaboratively with the respective platform owners with the Department to create a cost-effective automated infrastructure solution with better agility and deployment life cycle without compromising the highly demanding performance SLAs.

This solution is using range of AWS services such as AWS EC2, ALB, Route 53, S3, Lambda, Cloudwatch along with Chef Automate service for installation and configuration automation.

Specifically, it provided DCF with:

- Ability to leverage AWS services to created highly available multi-availability zone environments with cross region replication of databases in warm standby mode to minimize hardware foot print and application downtime.
- Separated AWS accounts and security controls to manage Protected Health Information (PHI) and Non-PHI workload for increased governance and assurance
- Automated security services deployment and improved security monitoring and tracking to ensure highly regulated HIPPA compliance is achieved.
- Automated components installation and configuration management using Infrastructure as Code principles and a Chef Automate service. This was supported by application deployment automation using third party open source tool where needed to manage the diverse range of DCF software.
- Automated monitoring utilising AWS native services to track and maintain any respective changes through the application infrastructure and raise appropriate alarms based predefined conditions.

Impact:

The solution has saved the Department a significant amount of annual cost to maintain the Florida Safe Families Network application infrastructure and provided them with the high degree of resilience they need to manage their time sensitive work.

Though the Chef Automation service we are enabling faster environment deployment and ongoing management & re-creation as needed to ensure a seamless production service. By automating a range of application component deployment such Oracle Weblogic, IBM DB2 and SAP Business Objects we are providing the DevOps tooling needed to provide quick and error free release process through test and in to production.

We have also worked hard to ensure this is a highly optimised deployment leveraging AWS cloud features and automating resource utilisation and application optimisation through proactive monitoring of resource metrics and real time reallocation of the infrastructure.

We believe these case studies confirm our ability to deliver on your set of requirements and how we have been at the heart of building automated infrastructure to handle truly critical workloads at the heart of our Public Sector clients. This is underlined by our work at the Department for Work and Pensions where we have been fundamental to the success of automating environment and application deployments for key critical national infrastructure such as CIS. Our collaboratively approach with DWP sees us being actively engaged in helping the client shape their standards, policies and frameworks so that they can successfully manage the automated environments in the long term with their in-house teams.

3. (c) Methodology – provide assurance that you will meet the "Do So By" section of the SOR.

Our response to this question is broken down in the following sections (coloured with blue headings) and can be found by clicking on the following document links to help navigate this answer:

- Summary (here)
- Utilising the Amazon Market Place (here)
- Our Experience and tools alignment (here)
- Confirmation of our ability to resource and deliver at pace (here)
- Ensuring appropriate and effective Governance (here)

Summary

We can confirm and provide assurance that we will meet the "Do So By" section of the SOR. We will do so by:

- Ensuring **no manual** or **hand configuration** will take place – it will **all** be developed as **IaC**
- Involving **agile teams** of highly skilled **DevOps** engineers **experienced** in **AWS** and **IaC**
- Leverage **individuals** with **skills** and **experience** in delivering **AWS** cloud hosted services for **CNI**
- Ensure appropriate interlock with SG Hosting Architecture Board through Prince2 Light project management
- Ensure **smooth handover** of code, designs and documentation to the newly formed **SG Hosting Platform Team**

This approach will enable us to help SG:

- Deliver at pace
- Reduce risk and provide certainty in the delivery of the Hosting Service
- When working with OGDs as you are **partnering** with a **trusted DWP** and **HMRC partner**
- Deliver greater value more quickly to the Scottish people
- Become self-sufficient more quickly

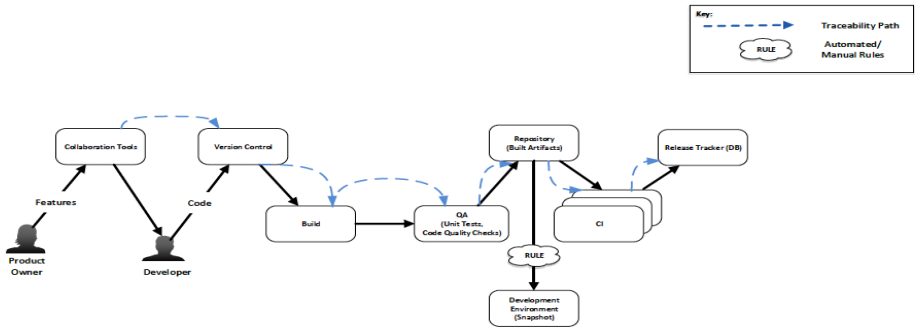
Utilising the Amazon Market Place

We will work with SSD to utilise the Amazon Market Place where effective to do so, working with SSD to incorporate where relevant and practical Scottish and Central Government IT guidance with a priority focus on pace, enabling delivery within the timescales described. This is evidenced in our response in 1a where we provide our commitment to the delivery timescales in our proposed timeline. We will provide expert level knowledge and guidance to SSD in applicable subject areas and work with SSD to adhere to the relevant SD/CDO policies and standards. We will ensure we handover responsibility for support and continued infrastructure development (with appropriate design and configuration documentation) to SSD nominated support staff.

Our Experience and tools alignment

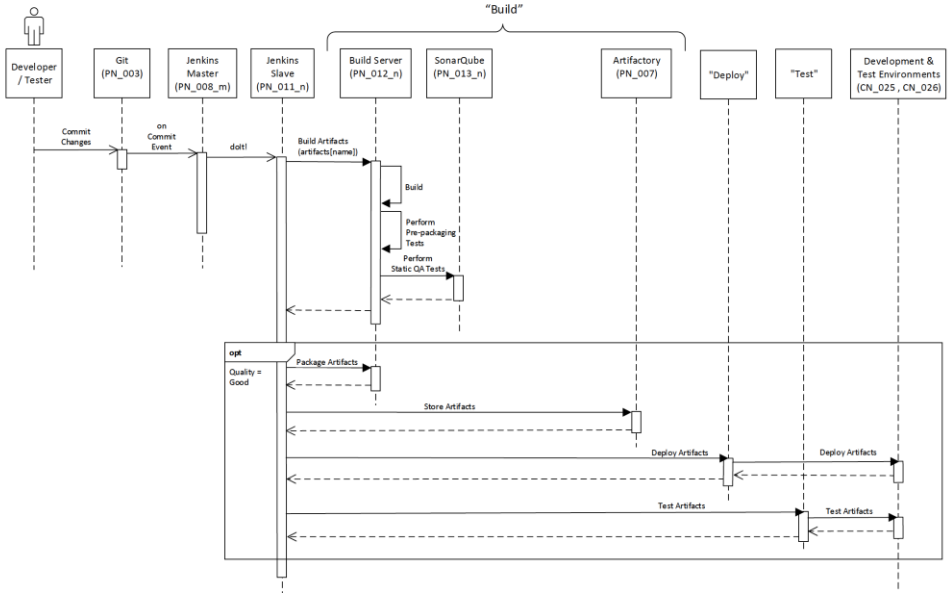
We will leverage our previous relevant experience of deploying Critical National Infrastructure as 'infrastructure as code' and 'automated infrastructure'. The diagram(s) below will provide a e2e overview of how we propose this working.

The diagram below shows the CI/CD overview we currently utilise for SG as part of our LIB delivery. Using the current set of SG collaboration tooling, the Technical Product owner will prioritise the fixed backlog from SOR. The DevOps engineers will use the appropriate development tooling – GIT, Artifactory, Jenkins, SonarQube and Ansible to automate the provision of infrastructure services as Infrastructure as Code, stored in the GIT source code repository.



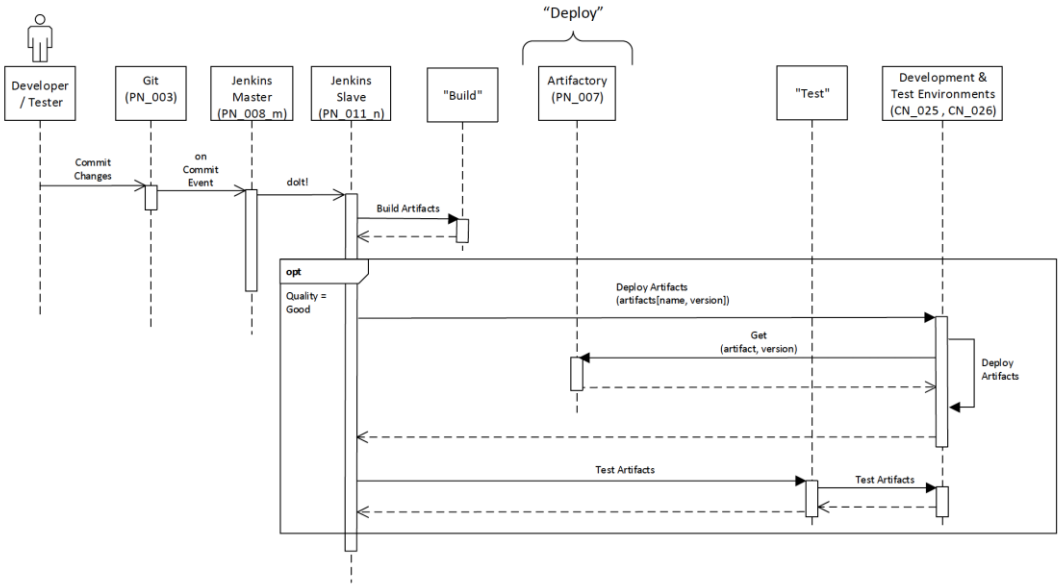
The diagram below shows the proposed IaC Build process for SG hosting services. Once the DevOps engineer has written the Ansible playbooks, any changes will be committed to GIT. Build jobs will be coded and stored in Jenkins. Our Git – Jenkins integration is already in place and used as part of our LIB delivery. Using this integration Jenkins jobs execute once it identifies a new check-in operation on a GIT branch. The Jenkins Master server will then orchestrate build requests via the Jenkins Slave server which in turn will execute the build request (including any pulls of packages and executables stored in the Artifactory repository) in the given environment (Dev/Test, Pre-Production or Production).

Sequence Diagram – Pipeline - "Build" - Physical Nodes (Scalable Build)



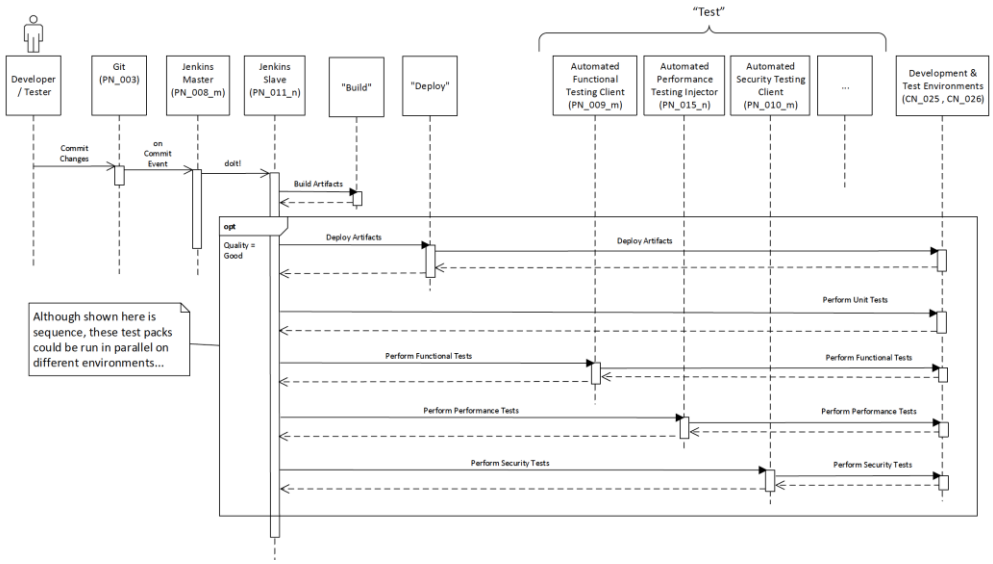
The diagram below shows the proposed IaS Deploy interactions for SG hosting services. Through a combination of Ansible roles, Ansible playbooks and orchestration with Artifactory, Jenkins will deliver builds into the new environment. As part of the Get and Deploy artefacts process, automated tests are executed to ensure each IaC component and the whole IaC release are tested.

Sequence Diagram – Pipeline - "Deploy" - Physical Nodes (Scalable Build)

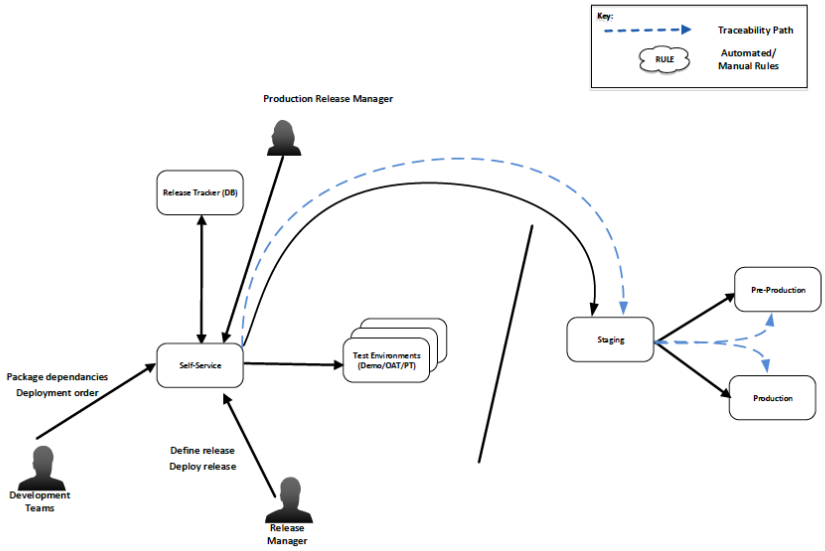


The diagram below shows the proposed IaC Test process for SG hosting services. Our test tooling will leverage tools like Junit, JMeter, SonarQube, Selenium and Cucumber to name a few. Depending on the type of test being executed, different test tools will be leveraged. The testing will also be written as code and will perform a combination of Functional, Performance and Security Testing.

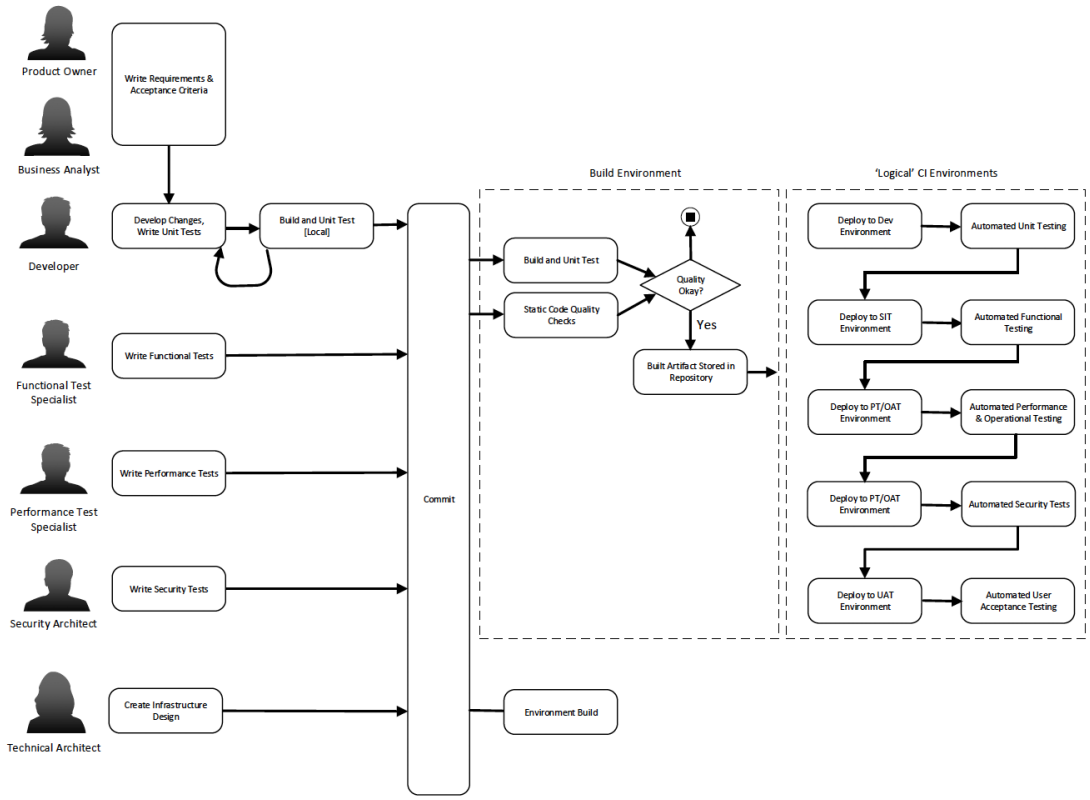
Sequence Diagram – Pipeline - "Test" - Physical Nodes (Scalable Build)



Finally, once the tests have completed successfully, workflow will be established that enables the Production Release Manager to release the tested code into the next stage environment. The diagram below shows the proposed IaC Release process for SG hosting services.



The final diagram below shows an overview of each of the key actors within our proposed approach and the role they play in preparing and delivering automated tests scripts.



We can assist with the implementation of processes to prevent environment drift via manual changes that are not within code. As part of the functional tests and as part of the Ansible roles and playbooks we can execute the playbook with the ***- - check*** option. This enables the IaC that was used to build the environment to be run again (but making no deployment updates and reporting back any changes in the build from the IaC.

Confirmation of our ability to resource and deliver at pace

We can confirm we have the capacity and capability to mobilise the skilled resource and capabilities to meet the defined timescales, in particular the 31 July 2018 date. We've sourced the key skills required to deliver this solution and plan to mobilise the team over 2 phases. Our proposed team has proven experience of automating the deployment of Critical National Infrastructure (CNI). To deliver the work at pace we are proposing 2 scrum teams working from one back log. To maximise

value, the Infrastructure and Security Architects will play an overarching role across both scrum teams and will have regular interlock with the Product Owner and Hosting Architecture Review Board. The Delivery Manager will also play an overarching role for this delivery, managing the dependencies across both scrum teams, ensuring the backlog is sufficiently prioritised and burn-up on track for the delivery milestones, while also managing the dependencies across third parties and the Low-Income Benefits programme to align the backlog priorities with the LIB delivery timelines.

Ensuring appropriate and effective Governance

Our Delivery Manager will help govern the overall delivery using a Prince2 Lite method ensuring appropriate interlock with the SG TDA, BDA, Hosting Architecture Board and Hosting Platform Teams. We will use Agile methods to deliver the actual build of the required live service. To facilitate an effective and efficient delivery maximising the outcomes during a tight delivery timescale, we propose to adopt a scaled agile approach using the less framework. A link to the framework can be found here: https://less.works.

We will work to this framework by having a single shared Product Backlog between two teams, which is prioritised by the Technical Product Owner with input from the two teams. Each team will then have a separate sprint backlog to focus on delivering incremental change. Following a diverge and converge approach, the Scrum teams will diverge at the start of a Sprint to deliver at pace within their individual teams, holding separate stand-ups and managing an independent Sprint Backlog where the Scrum Masters will ensure coordination across the teams, managing the inter-dependencies and planning ahead for the next sprint. At the end of each Sprint, the teams will start to converge again, where Sprint reviews will be held in unison, enabling a team to provide an overarching demonstration of the latest Product increment.

We will accept delegated responsibility for delivery while aligning with SSD Governance ensuring appropriate interlock with TDA and Hosting Architecture Review Board so as to ensure the service is fit for purpose and “secure by design”.

Through a combination of providing SG with our Dev/Test assets (which has taken 6-person years to develop) combined with leveraging a team with the necessary experience in AWS CNI deployments, we will ensure implementation and delivery costs are demonstrably value for money.

Finally, in terms of IPR in line with the GCloud framework call off contract we would grant you a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the IPR created on the Project and to any Background IPRs embedded within the IPR created on the project for use in your business activities.

We only ask that assets we are providing at the outset of this work to enable a rapid start are not passed onto any commercially interested 3rd party as we have invested heavily at our own cost to establish these assets but are happy to provide them to you as part of this delivery with no restrictions on your usage.

4. (a) Option A - Development, test and training environments. Please confirm that you are able to meet this requirement if the option is needed. Details of resources and pricing do not need to be provided here as they should be provided within the pricing schedule.

Summary

Yes, we can confirm that we can meet the requirement to provide develop, test and training environments by 28th September 2018. By building the pre-production and production environments using Infrastructure as Code, this will enable us to quickly replicate the environment at Scottish Government's request.

We can make a replica environment rapidly available within a week of the request due to the automated nature of our core delivery. We would recommend providing an additional FTE to sit alongside the two scrum teams for a fixed 2 sprint period to support any deployments or fixes and co-ordinate the requirements and integration points required in the training envionment.

This resource will be dedicated to supporting the additional training environments to avoid creating a distraction in the two scrum teams who will be delivering continuous improvements and further automations to the pre-prod and production environments to enable to scrum teams to successfully deliver the fully automated requirements ahead of go-live in October 2018.

We assume both of the following will be SG responsibilities,

- User Access (Providing / Adding users to the training system)
- Establishing Active and Appropriate Test Data Sets

We have detailed our suggested support days in the pricing schedule for Option A. By providing a capped Time and Materials support model, if this additional full-time resource is not required for the duration of the fixed 2 sprint deploy and support phase, we can ramp down earlier to offer cost savings.

4. (b) Option B - Operational Support. Please confirm that you are able to meet this requirement if the option is needed. Please also state where the support resources will be located. For the avoidance of doubt we will require UK based personnel due to the sensitivity of some of the data being managed and co-located with the hosting build support and in-house teams would also be a strong preference for the majority of the operational support solution.

Our response to this question is broken down in the following sections (coloured with blue headings) and can be found by clicking on the following document links to help navigate this answer:

- Summary (here)
- The support process (here)
- The proposed team (here)
- Escalation routes (here)
- Fair work practices (here)

Summary

We have a wealth of experience managing services in production, providing 'around the sun' support for our products so we can build an operational support model providing 24/7, 365 cover. The escalation route defined in our response below will facilitate a rapid response for operational support, and tapping into rich experience and a network of resources who work with and provide fixes for the same technology.

To help build and maintain an Agile programme, we propose to introduce an Agile operational support model that will empower the Product Owner within the Hosting Platform team to prioritise both new features and problem fixes and enable the creators of the product, the Scrum team, to maintain the service and continuously enhance the product by adopting a 'one-team, one-backlog' approach.

The Support Process

We would propose a Level 1 SG-owned business and techinical helpdesk function acts as the first line support desk to provide an early triage of the incidents raised to support end-users in raising and resolving Incident tickets and Service Requests. We can build dashboards and provide training and knowledge transfer to facilitate the capability build of this team, empowering them to route the incidents to the approriate support teams from Day 1. Once the Level 1 Support team routes hosting incidents to the Hosting Platform team, an in-depth triage exercise will be completed as part of the Level 2 Support to confirm the incident is indeed infrastructure related and identify the route cause for resolution.

Our Level 2 Service Manager will act as a first line of action for the support team and will monitor all incidents raised in the queue and will assess their criticality before prioritising the incident within the backlog and alerting the Product Owner to any major incidents. We would expect SG to provide a Service Manager or Product Owner to act as single point of contact for the IBM service desk to work collaboratively with the IBM Service Manager during the triage process.

By adopting this model, it enables the SG Product Owner and IBM support team to manage the problem backlog collaboratively. If the level of incidents is low in any given day, we would propose that the support team can be used during core hours to support the introduction of new features in line with the Product Owner and Hosting Platform Team's priorities. To enable this flex within the team to support both incidents and new features, the product backlog can be broken out into individual epics in relation to whether the ticket item is a new feature story or a live service problem with emphasis on live service problems and support stories being top priority to support fixes.

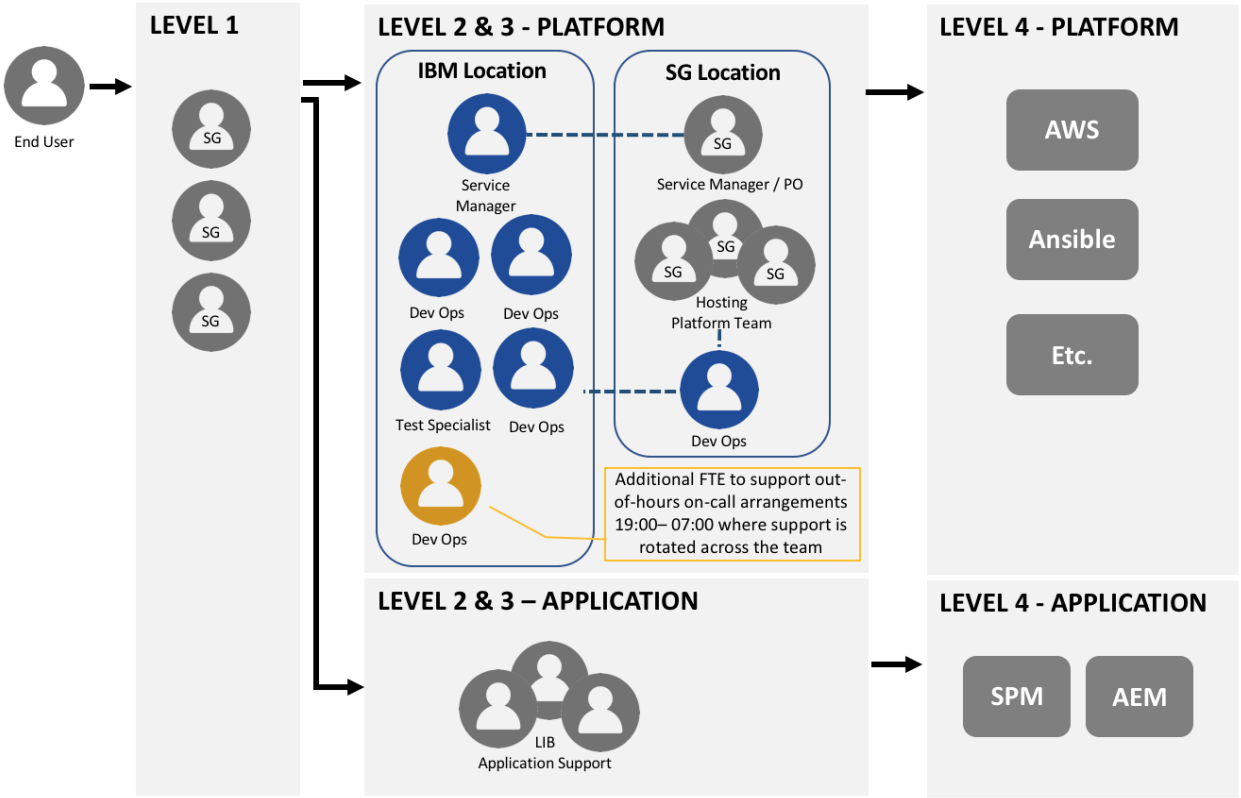
The Proposed Team

Our proposed support model covers a team to provide full-time support during core hours of 07:00 to 19:00, Monday to Friday, with on call arrangements in place outside of these core hours to provide 24/7 support. In order to provide this 'around the sun' support model, we have structured our proposed team to include 3 dev ops engineers and 1 QA analyst full time during core hours where the majority of service impacting incidents are expected to occur.

This is then backed up with an out-of-hours call-out model, supported in the first instance by the team above, who know the service but with access to a wider pool of skills within IBM UK. To maximise the efficiencies and access to the IBM pool of skills and expertise, we propose the team will be based out of an IBM office, while ensuring all resources have BPSS clearance and SG has regular access to the team through regular checkpoints with the Service Manager.

By adopting this model of having the team based in an IBM office, this enables us to maximise the use of a wide set of expertise within IBM by calling on a pool of shared resources depending on the nature of the support required, which can be assessed on a case-by-case basis to call on the necessary skill for the job.

While a team will be based in an IBM office, we also suggest that an additional FTE is embedded withint the Hosting Platform Team, operating out of the SG office to ensure regular interlock with SG and the Hosting Architecture Review Board, which will also enable a handover of the service from the point when SG are ready to take on the service completely from IBM.



Escalation Routes

We are committed to making sure the service is running smoothly in production 24/7, 365. In the event that you should wish for further assistance beyond the scrum team, we will offer a direct escalation route to the Executive Partner, who will work closely with you to ensure that problems and incidents are resolved and to resume BAU operational support. Prior to commencement of the Live service, we will propose an introductory meeting with the IBM UKI General Manager, providing you with the chance to meet and greet our team who form our escalation route. Therefore, should further support and escalation be required, the Executive Partner will personally involve the IBM UKI General Manager.

Fair Work

1. (a) Are you a Living Wage Employer as defined at http://scottishlivingwage.org/?

IBM is committed to paying its employees competitively. We regularly conduct bench marking exercises to ensure our salaries are consistent with what are paid in the marketplace. Pay competitiveness is a key component of our salary increase programmes.

1. (b) Have you signed or are you considering signing the Scottish Business Pledge?

IBM, as a UK Government Green Status supplier (Crown Commercial Service - Cross Government Strategic Supplier Assessment) meets or exceeds most of the shared ambition objectives of the Scottish Business Pledge. At this moment in time, IBM is not a signatory to the Pledge, however IBM will be delighted to engage with you on how we might sign up to this in the future. As an international company that operates in over 100 countries globally, there are some clarification questions that we would have in relation to the "internationalism" section, but we are confident that with a pragmatic approach on both sides, we will be able to proceed with the vast majority of the pledges ambition.

1. (c) Will the living wage will be paid to all employees engaged in the delivery of this contract?

Yes, the living wage will be paid to all employees engaged in the delivery of this contract. IBM is committed to paying its employees competitively.

1. (d) Please describe how you will commit to fair work practices for workers (including any agency or sub-contractor workers) engaged in the delivery of this contract. Examples are provided below

IBM operates with a robust fair work policy. We are committed to paying all employees competitively and operates a flexible working environment to support work life balance for its employees. IBM is also committed to providing a welcoming environment for employees, nurturing talent to support the development of employees to fulfil their potential across a number of talent programmes and training development plans. Examples of these programmes include the IBM Graduate and Apprenticeship schemes, designed to support the development of our early professionals to guide them to their desired career paths.

Hosting Build Support

Clarification Response Document

This document is provided for clarification purposes for a requirement for Hosting Build Support for Scottish Ministers acting through the Scottish Government.

The Crown Commercial Services G-Cloud Framework is the applicable procurement route.

Please refer to the Statement of Requirements (SOR) and 7 other supporting documents (issued separately under cover of a Non-Disclosure Agreement) when completing this document.

Instructions

1. Suppliers MUST complete their responses using this document and submit final responses via the Public Contracts Scotland portal no later than 10am on Wednesday 25 April 2018. Any questions regarding the requirements must also be submitted through the portal.

   https://www.publiccontractsscotland.gov.uk/Authority/SupplierSearch/DetailsSearch.aspx

2. Suppliers must provide their responses to the Questions in the sections provided. There is no word limit but information provided should be clear and concise. Each box can be increased in size to accommodate the information being provided.

3. This document will be used by the evaluation panel to review each Supplier's response.

4. If you have any other queries regarding this document, please email [redacted]

Questions

1. Technical merit and functional fit: coverage, network capacity and performance as specified in relevant service levels

1. (a) Confirm and provide assurance that you will meet the requirements in terms of deadlines for the environment deliverables, plan adoption, and resource modelling with assurance that the delivery dates of 31 July and 31 August 2018 will be met. Refer to the "What" section of the SOR.

1. (a) (i) Describe any caveats, assumptions and dependencies that apply to Question 1. (a) above.

1. (b) Confirm and provide assurance that you will meet the requirements in terms of the “How” section of the SOR.

1. (c) Confirm and provide assurance that you will meet the requirements in terms of the design and test approach.

2. After-sales service management: helpdesk, account management function and assurance of supply of a range of services

2. (a) Provide assurance of availability and ability to supply the optimal core team and supplementary resources at pace.

3. Non-functional characteristics

3. (a) Please provide evidence of your ‘infrastructure as code’ and ‘automated infrastructure’ expertise in your proposed core team.

3. (b) Please provide 2 examples of your recent experience of similar delivery (demonstrating how you used techniques described in the How section of the SOR) including dates, project details, client name and deliverables.

3. (c) Methodology – provide assurance that you will meet the “Do So By” section of the SOR.

4. Information Relating to Options in Section 7 of the SOR

4. (a) Option A - Development, test and training environments. Please confirm that you are able to meet this requirement if the option is needed. Details of resources and pricing do not need to be provided here as they should be provided within the pricing schedule.

4. (b) Option B - Operational Support. Please confirm that you are able to meet this requirement if the option is needed. Please also state where the support resources will be located. For the avoidance of doubt we will require UK based personnel due to the sensitivity of some of the data being managed and co-located with the hosting build support and in-house teams would also be a strong preference for the majority of the operational support solution. Further details of resources and pricing do not need to be provided here as they should be provided within the pricing schedule.

PRICING

There are 3 elements to pricing for this opportunity.

1. Fixed Price for the initial 6 month period
2. Indicative Price (capped time & materials) for Option A - Development, test and training environments
3. Indicative Price (capped time & materials) for Option B - Operational Support

A pricing schedule has been provided within the portal for each element.

Suppliers must enter details for every question/ section in the Pricing Schedules.

A fixed price is required for the initial 6 month period. From the point that delivery is complete we may require to flex the team into a support and implementation model.

There is an option to extend by up to 6 months with a further option to extend by up to 3 months with the contract anticipated to commence on 30 April 2018.

An indicative price is requested for the 2 options within Section 7 of the SOR:

A. Development, test and training environments;
B. Operational Support.

Separate pricing schedules are provided for each option. A capped time and materials model would be applied to these periods of support, subject to value for money and our governance.

An indicative methodology is not required for these 2 options at this stage but if SG chooses to take up either or both of the options we will expect a separate response on how you propose to deliver these options including methodology and a revised resource profile and price. The rates that will apply to any extension period will be those of the Supplier's G-Cloud 9 service offering at the time the call-off contact was let.

All prices appropriate to the proposal, including all overheads, travel and subsistence and other expenses, must be included within the overall price. Prices which appear elsewhere in the proposal but which are not summarised here will be presumed to have been waived. All prices are to be exclusive of VAT.

The total price for the 6 month period will be the price used for comparison purposes and will be the fixed price for the initial period of the contract.

Pricing Schedule

The tables within the attached excel spreadsheets, within the portal must be completed and returned with the other parts of your submission. The pricing schedules must be submitted as separate documents and prices shall not appear elsewhere within your submission. This is to ensure that the technical evaluation is undertaken independently of the commercial evaluation.

Payment Terms

On appointment of the successful Supplier, 80% of the fixed price, quoted within the submission, will be split into 6 payments, paid monthly in arrears, with a final payment of 20% at the end, on successful completion of the contract.

Payment for any extension period will be made monthly, in arrears, subject to successful completion of the deliverables for the extension period.

Hosting Build Support - Questions and Answers 2

Questions on Scope & Timelines

- Are you comfortable with an phased delivery approach where we can ensure the services required for ITHC are in place by 31 August and all services will be automated for go-live during a continuous improvement phase?

  Answer > A phased approach is acceptable.

- Capita SWAN direct connect link has a 12 week lead time. Can you confirm that the order has been placed to enable a 31 July delivery of the pre-production environment?

  Answer > DX hosted connections order is in progress however site to site Internet VPN connections have also been requested as contingency.

- We assume that a connection to DWP will take an equivalent amount of time as Capita SWAN of 12 weeks. Has a network design been agreed with DWP and have DWP confirmed their lead times?

  Answer > Communication with DWP on integration is underway. DWP have produced an integration approach for online (Internet to API Gateway) and batch (GFTS) connections. Note that DWP have not confirmed lead times and these designs need to be detailed and agreed

- Is it fair to assume that iTECS can implement the VPN over direct connect to Scots within 24 hours of the completion of the Direct Connect?

  Answer > Assume 5 days for iTecs requests. Note that design discussions and requests have started. It is hoped that site to site internet VPN will be available for use in the coming weeks with DX hosted connections to follow (approx. 12 weeks)

- Would it be acceptable if part of the team is not co-located to enable concentration on the delivery, such as working from another location?

  Answer > Content where it works as this will be Agile delivery can the Supplier please define e.g. 10% - 95% not co-located. The team must be UK based.

- Can we assume that an IT Health Check is only required for the Production environment, and not required for Pre-production or training environments?

  Answer > No – all environments will be security assessed to some extent

- Can we assume that Scottish Government will line up a third party pen tester and NCSC to complete the Security Accreditation?

  Answer > Yes

- Does the Scottish Government have an existing contract with a Content Delivery Network, for example, Akamai, that can be used for this delivery?

  Answer > No

- Will the High Level Design be completed and approved by the appropriate Technical Design Authority (TDA) / Social Security Board by contract signature? Can we assume that only key changes to the current design will be taken back through TDA?

  Answer > Agreed. Note that a hosting ARB will be in operation to manage hosting platform related design changes, however, any major deviations to agreed HLD will need to be approved at TDA

- Is there a Design and Test Approach that can be shared, referenced in question 1C?

  Answer > Expectations that the build team will test as they deploy but it is assumed that there will be an official test approach (systems and security test phase and associate acceptance criteria).

  Information provided previously (issued 20 April 2018) >

  Design Approach

  The supplier is expected to produce design artefacts for each component and service deployed. High level design information outlining functional solution, integration, deployment approach, security and infrastructure required in order to progress deployment. Detailed design collateral will be required that describes the service including infrastructure, interfaces, batch, security elements, etc.

  Test Approach

  The hosting platform will service business applications and processes with agreed NFRs. The supplier is expected to continuously integrate each component and any supporting service (including deployment) within the hosting infrastructure to ensure they can also adhere to these NFRs.

  An example of this is the agreed RTO of less than 4 hours and an RPO of last committed transaction for the business services. The hosting infrastructure must also be deployed in a way that is highly available and resilient to ensure they don't impact the business applications. The supplier is expected to test each component to ensure it is highly available and resilient and can support these business NFRs.

Questions on Option B - Operational Support

- What are the expected hours of support in relation to the optional requirement Option B to provide operational support?

  Answer > Expected model similar to core hours 07:00 to 19:00 Mon to Fri with on call arrangements in place outside these hours.

- In relation to the optional requirement Option B to provide operational support:

- a) what are the defined SLAs and expected number of users?

  Answer > Internally there will be up to 2000 users phased in over the next 3 years.

  Indicative service level targets as per below for incident management:

  Priority 1: Response: 15min, Resolution: 3hrs

  System unavailable causing significant disruption to citizens;

  Main site (or sites) without connectivity;

  Significant threat to the service, e.g. security, reputational

  Priority 2: Response: 30min, Resolution: 5hrs

  - System or connectivity unavailable to a group of users without causing significant disruption to citizens;

  Priority 3: Response: 1hr, Resolution: 8hrs

  - Degraded service or performance on non-critical processes
  - Individual staff member without system access

  Priority 4: Response: 8hr, Resolution: 48 hrs

  - Minor incident which has a known workaround in place;
  - Incident with minimal impact;

  b) can we provide support from a different UK office?

  Answer > Yes

  c) what are the defined service management processes?

  Answer > The detailed service management processes are being developed in alignment with ITIL 2011. The Service Management Strategy is attached. An Incident Manager and Change & Configuration Manager are being recruited to finish defining those processes and subsequently implement them.

  d) what help desk tooling is expected to be used?

  Answer > Short listed service management tooling options are currently being assessed for the Technical Design Authority recommendation.