



Crown
Commercial
Service

DIGITAL SERVICES RM1043ii CALL-OFF CONTRACT

Part A - Order Form, Specific Terms

Part B - Schedules

PART A – ORDER FORM

PROJECT REFERENCE: DS02-012 Lot 2

This Order Form is issued in accordance with the provisions of the Digital Services- RM1043ii, Part B - The Schedules and Part C - Call-Off Terms and Conditions.

The Supplier agrees to supply Digital Services specified below and subject to the terms of this Contract and for the avoidance of doubt this Contract consists of the terms set out in this Part A - Order Form, Part B - The Schedules, any executed Statement of Works, together with Part C - Call-Off Terms and Conditions.

NB: in the case of a Central Government Contracting Body, the Call-Off Contract will be entered into by the Authority acting as an agent on behalf of that Central Government Contracting Body but thereafter the rights and obligations of the Customer hereunder shall be the responsibility of the Customer

DATE: 02/11/2015

PURCHASE ORDER NUMBER: PO022149

FROM: the “Customer”

Crown Commercial Service (CCS)

Rosebery Court, St Andrews Business Park, Norwich NR7 0HS

Acting as an agent on behalf of the departmental customer:

Innovate UK

North Star House, North Star Avenue, Swindon SN2 1UE

TO: the “Supplier”

Nomensa Ltd

King William House, 13 Queen Street, Bristol,

Avon, BS1 4NT

TOGETHER: the “Parties”

PRINCIPAL CONTACT DETAILS:

For the Customer:	Name:	[REDACTED]
	Title:	[REDACTED]
	Email:	[REDACTED]
	Phone Number:	[REDACTED]
For the Supplier:	Name:	[REDACTED]
	Title:	[REDACTED]
	Email:	[REDACTED]
	Phone Number:	[REDACTED]

1. CALL-OFF CONTRACT TERM

- | | | |
|-----|---|---------------|
| 1.1 | Commencement Date: | 02/11/2015 |
| 1.2 | Term of Call-Off Contract: | Up to 2 years |
| 1.3 | Date the Customer served an Order Form for Services on the Supplier: | 02/11/2015 |

2. CUSTOMER CONTRACTUAL REQUIREMENTS

- | | | |
|------|---|--|
| 2.1 | Digital Services required: | For the provision of technical expertise and delivery of a user-centred accessible digital service as described in the 'Beta planning requirements Sept15' document under the DS02-IFS project |
| 2.2 | Warranty Period: | 90 Days date of customer acceptance of release |
| 2.3 | Location(s)/Premises: | Swindon – Innovate UK offices |
| 2.4 | Relevant Convictions: | NOT USED |
| 2.5 | Staff Vetting Procedures: | NOT USED To be listed explicitly as a deliverable in the SOW. |
| 2.6 | Security Requirements:
(including details of Security Policy and any additional Customer security requirements) | Appropriate for Government Body. |
| 2.7 | Protection of Customer Data: | |
| 2.8 | Standards: | Digital by Default Service Standard |
| 2.9 | Business Continuity and Disaster Recovery: | To be addressed as part of the development planning. |
| 2.10 | Liability: | £1,000,000 |
| 2.11 | Insurance: | As per Clause 16 of the framework Agreement RM1043ii:
<i>"liability insurance, in respect to amounts that the Supplier would be legally liable to pay as damages, including claimant's costs and expenses, in respect of (i) accidental death or bodily injury and/or (ii) loss of or damage to property, with a minimum limit of five million pounds sterling (£5,000,000)" "Professional indemnity insurance with a minimum limit of indemnity of one million pounds sterling (£1,000,000) for each individual claim"</i> |

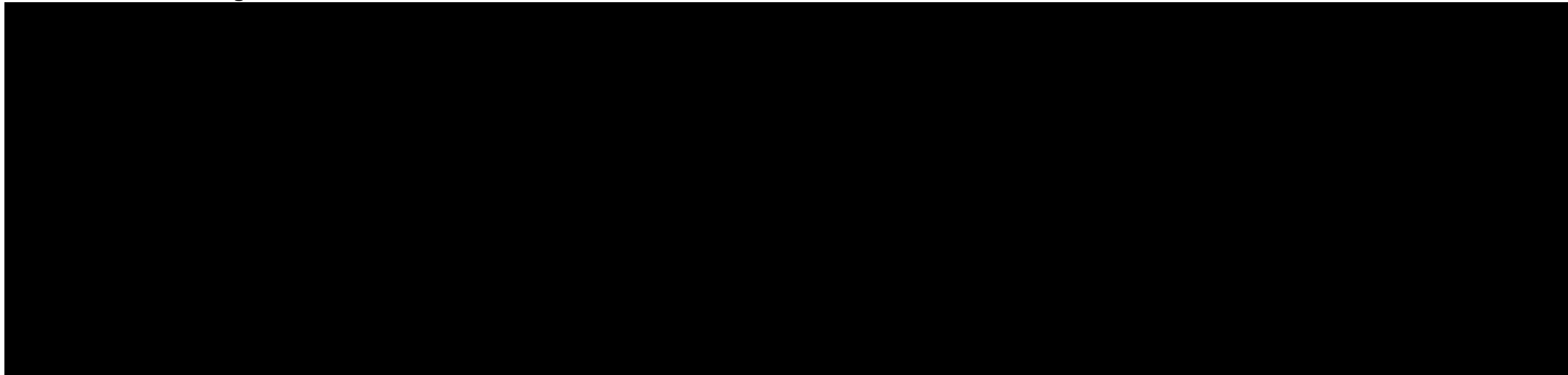
3. SUPPLIER'S INFORMATION

- | | | |
|-----|--|--|
| 3.1 | Supplier Software and Licences: | Not Used |
| 3.2 | Commercially Sensitive Information: | Any pricing information, methodologies and CVs |
| 3.3 | Key Sub-Contractors/Partners: | Not Used |

4. CONTRACT CHARGES AND PAYMENT

- | | | |
|-------|---|--|
| 4.1 | The method of payment for the Contract Charges (GPC or BACS) | BACS |
| 4.1 | Invoice details | |
| 4.1.1 | Who and where to send invoices: | ██ |
| 4.1.2 | Invoice information required – e.g. PO, Project ref, etc. | ████████████████ |
| 4.2 | Invoice Frequency | As per deliverables listed in SOW |
| 4.3 | Contract Value: | £223,890.00 |

4.4 Contract Charges:



5. ADDITIONAL AND/OR ALTERNATIVE CLAUSES

5.1 **Supplemental requirements in addition to the Call-Off Terms** Not Used

5.2 **Customer Specific Amendments to/refinements of the Call-Off Terms** Not Used

5.3 SPECIFIC TERMS:

Clause	Heading	Minimum Number of days held within the Call-Off Agreement
4	WARRANTIES AND REPRESENTATIONS	Remains Ninety (90) Days date of customer acceptance of release
17	SUPPLIER ASSISTANCE AT RETENDERING	Remains Ten (10) Working days
23	FORCE MAJEURE	Remains Fifteen (15) consecutive Calendar Days
28	CHANGES TO CONTRACT	Remains Five (5) Working Days
36	DISPUTE RESOLUTION	Remains Various shown within the Call-Off Terms
37	LIABILITY	Remains Various shown within the Call-Off Terms
38	TERMINATION EVENTS	Remains Fifteen (15) consecutive Calendar Days

6. FORMATION OF CONTRACT

- 6.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter a Call-Off Contract under Digital Services – RM1043ii with the Customer to provide the Services.
- 6.2 The Parties hereby acknowledge and agree that they have read the Part A - Order Form and the Call-Off Terms and by signing below agree to be bound by this Contract.
- 6.3 In accordance with paragraph S-9 of framework Schedule 4 (Call-Off Procedure), the Parties hereby acknowledge and agree that this Contract shall be formed when the Customer acknowledges the receipt of the signed copy of the Order Form from the Supplier within two (2) Working Days from receipt (the "Call-Off Effective Date").
- 6.4 The Call-Off Contract outlines the deliverables and expectations of the Agreement. Order Form outlines any Terms and Conditions amended within the Call-Off Contract. The terms and conditions of the Call-Off Order Form and will supersede those of the Call-Off Standard Terms and Conditions

7. RECITAL

- (A) The Authority undertook a procurement as a central purchasing body on behalf of public sector bodies, to select suppliers, including the Supplier, to provide Digital Services ("the Services")
- (B) The Supplier is a provider of Digital Services and undertook to provide such Services under the terms set out in framework agreement number RM1043ii ("framework Agreement").
- (C) The Customer is entitled to enter into this Contract under the framework Agreement and has completed an Order Form ("Order Form") served by the Customer on the Supplier
- (D) The Customer served an Order Form for Services on the Supplier on the Date Served as stated in the Call-Off Contract clause 1.3 Call-Off Contract Term
- (E) The Supplier confirmed its agreement to the terms of the Order Form and its acceptance of the Order Form and the Parties hereby duly execute this Contract.
- (F) The Parties wish to establish a flexible Call-Off Contract which reflects the Digital Service Design methodologies (<https://www.gov.uk/service-manual>), and close co-operation that will be adopted by the Parties in the delivery of the Services. The intention of the Parties is that the Contract can be terminated by the Customer at short notice without liability for costs of termination and similarly, the Contract will automatically expire if the Parties do not agree to execute a further Statement of Work (SoW).

- (G) The Parties intend that specific instructions and requirements in respect of each Release (or other adhoc Services under this Contract) shall be issued and shall have contractual effect on the execution of an SoW and as agreed by the Parties in the SoW and that payment for Services shall only become due as set out in an executed SoW.

SIGNED:

Name:
Title:
Signature:
Date:

DIGITAL SERVICES RM1043ii

PART B – THE SCHEDULES

PART B – THE SCHEDULES

The following schedules are an amalgamation of the Customer's Requirements and the Supplier's submission.

Once agreed and signed by the Parties, CCS will redact any Commercially Sensitive information and publish the contract to Contracts Finder.

SCHEDULE 1 – REQUIREMENTS

CURRENT SITUATION/ BACKGROUND:

We are seeking a supplier to deliver the technical expertise for a Beta phase of our Innovation Funding Service, a user-centred accessible digital service.

Following a successful Discovery and Alpha phase and working within Governments Digital by Default Service Standard, we are looking to establish a technical team who will take the Alpha 'thin slice' version of our Innovation Funding Service and help work with us through a Beta phase with the aim of putting the service online by February 2016. Alpha code has been developed as 'Beta ready product' and so we will expect to re-use these built components within our Beta product. We would expect the team to consist of (but are not restricted to) a UX researcher, Front-End Developer/s, Back-End Developer/s, Business Analyst and Tester with the potential for an architectural and environments team member/s. This procurement has been divided into two separate lots and so if a bid is received to Lot 2 only (User Research), the supplier should indicate how they would interact and work with Suppliers from Lot 1 (Software Engineering and Ongoing Support AND Agile Product Design and Delivery). As the time-line for a Beta product is aggressive, we would envisage suppliers suggesting the running of parallel working teams however Innovate UK does not want to be prescriptive about how a supplier should set the team up in order to meet this ultimate goal. It is expected that members of the Innovate UK team will work as part of the delivery team with the ultimate aim of moving the expertise in-house. With this in mind, knowledge transfer is an essential part of the supplier remit. Co-location within the Innovate UK offices is also essential.

Longer-term, the Innovation Funding Service is intended to support the digitisation of all other types of funding that Innovate UK offer.

Innovate UK is the new name for the Technology Strategy Board – we're the UK's innovation agency, accelerating economic growth.

Innovators whether small, medium or large, see the world as full of problems - they have the ideas and talents to fix society's challenges. We know that taking a new idea to market is a challenge. We fund, support and connect innovative businesses through a unique mix of people and programmes to accelerate sustainable economic growth.

As Innovate UK has grown in strength and maturity, we have developed a range of highly effective tools, products and services to support business and accelerate innovation. However, a significant number are still dependent upon legacy systems with outdated and awkward functions and operation, or via a combination of applications, e.g. MS Word, MS Excel and MS Access. This situation impacts our ability to scale -up our operations efficiently.

In response, Innovate UK has launched the Innovation Funding Service work-stream with the aim of moving all of our end-to-end transaction services on-line. We aim to operate a "Digital by Default" business model designed to meet the government Digital by Default Service Standards, leveraging the benefits of cloud computing, in line with the Government's digital strategy.

The first end-to-end service to be migrated under this work-stream relates to the application process for Collaborative Research and Development (CR&D) funding projects. It forms a large part of Innovate UK's grant funding and is currently not on-line. This represents operational inefficiencies and a poor customer experience.

Business Scenario

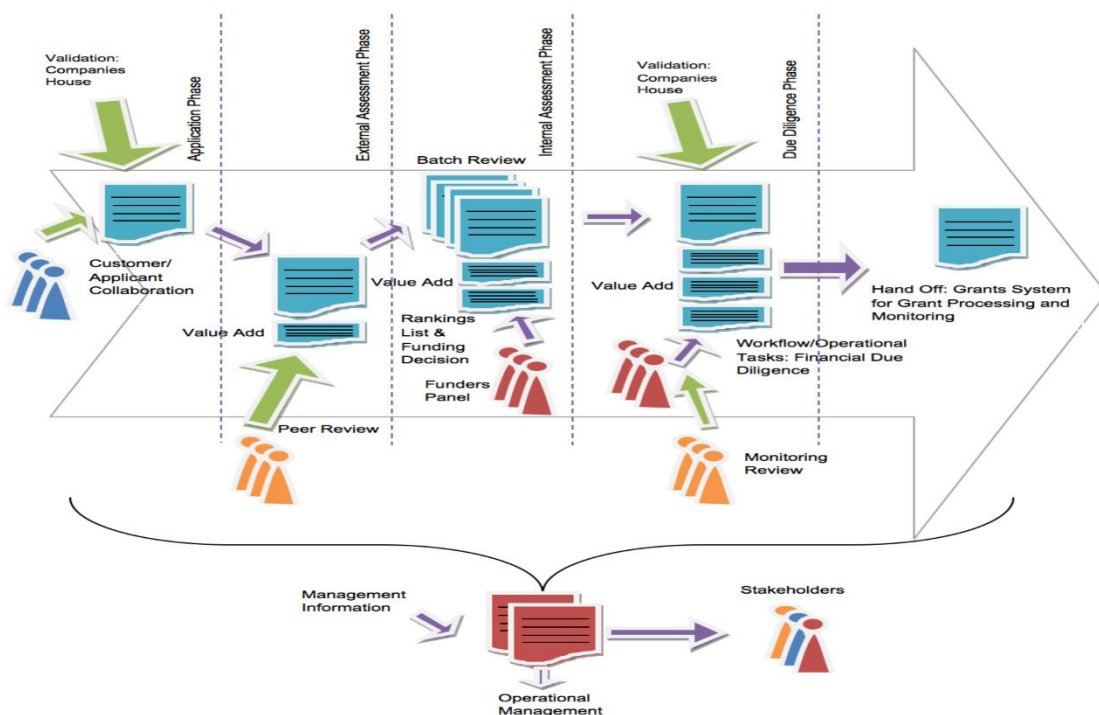
Collaborative research and development (R&D) encourages businesses and researchers to work together on innovative projects in strategically important areas of science, engineering and technology – from which successful new products, processes and services can emerge, contributing to business and economic growth. Each £1 we invest in collaborative R&D typically returns around £7 in GVA (Gross Value Added).

By co-funding projects involving partnerships between businesses and between business and academia, collaborative R&D reduces financial and technical risk and encourages knowledge exchange, supply chain development and parallel working on complex challenges.

We hold frequent competitions for collaborative R&D project funding, in a wide range of areas covering specific technical or societal challenges.

Business Process 'As Is'

The current business process is represented in the following diagram:



This is described in more detail below:

Application Phase

1. The lead or single applicant registers for a Competition in order to receive a username, password and a unique application ID and form.
2. Once registered for the Competition, they receive an email containing an application form, a username, password and a secure URL.
3. They upload their completed documentation to our upload secure site.

External Assessment Phase

1. Once the Competition submission deadline is reached, all applications submitted to the competition are sent for assessment. Applications are assessed independently by experts taken from both business and academia (known as Assessors).
2. Each application is assessed by up to five Assessors and against the same set of gateway and criteria questions.
3. Each Assessor is required to complete and submit a score-sheet with comments for each application they are assigned to assess. If the Assessor has a conflict of interest they must notify our Competitions Team who will reallocate the application to another Assessor.
4. A report is compiled to identify ranked order of all applications. Within this ranked list are all the Assessor comments and score given to each question.
5. Where there is a second stage to the Competition, successful applications are invited to the second stage of the Competition in strict order from the top of the ranked list as recommended by the Assessors.
6. At the final stage of a Competition an assessment panel is convened to discuss any applications that require clarification around scope, quality, feasibility or fundability. The assessment panel recommends a ranked list of applications to be funded by Innovate UK.

Internal Assessment Phase

1. The final recommended panel list is presented to the Funders Panel of Innovate UK to obtain final approval for funding.
2. Once all applications have been assessed and checked for completeness, the applicant or the lead applicant will be informed of the decision by email.
3. Feedback from assessors who reviewed the application is collated. The applicant or the lead applicant can access the feedback from the assessors who reviewed the application by logging on to the secure website where they uploaded their application documents.

Due Diligence Phase

1. The applicant or the lead applicant is sent a Conditional Grant Offer Letter following the email notification. They are asked to accept and return all required documentation within the stated timeframes.

The following are examples of documents that may be requested in the Conditional Offer Letter:

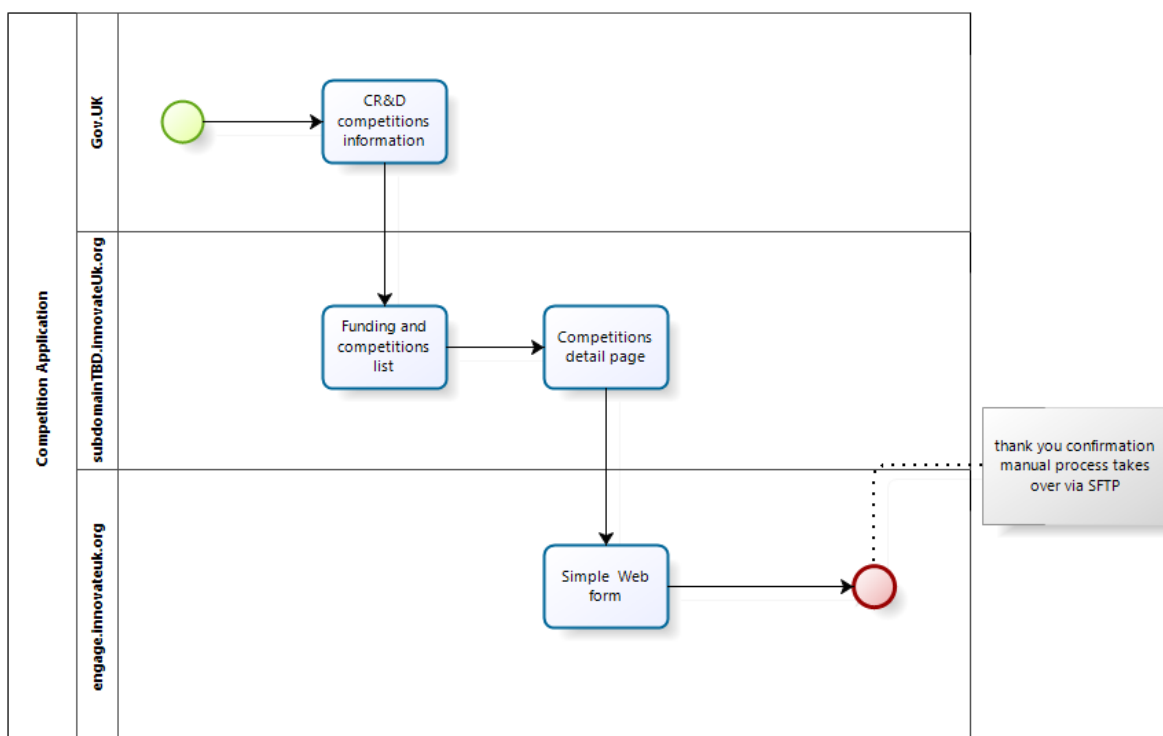
- Collaboration Agreement, for collaborative projects, duly signed by all participants.
 - An initial Financial Forecast for each project participant / consortium member showing the anticipated spend split quarterly throughout the life of the project.
 - A letter on company headed paper confirming BACS details for payment purposes.
 - A detailed Project Plan splitting the original project proposal into individual work packages.
 - A Milestone and Risk Register for the whole project showing key milestones with an allocation of the project costs assigned to each milestone, the key risks and how these will be managed during the project.
 - An Exploitation Plan for your project, containing further information where possible from that provided in the original application, setting out how the project team will exploit the results of the project.
2. After the Conditional Offer Letter has been sent, Innovate UK will undertake costs review and financial checks on each of the project participants:

- The cost review is to ensure that the project costs comply with the rules for the Competition and the State Aid requirements. A member of the finance team may contact applicants for further information on the detail in the finance forms; the project will not be able to start until this review has been completed satisfactorily.
 - The financial viability checks are based on the latest accounts filed at Companies House, but we may ask for additional financial information if a participant has not filed accounts recently. If an organisation fails one or more of the financial viability test criteria, or if specific funding ratios cannot be ascertained because of limited information or abbreviated accounts, or if they are not required to file accounts with Companies House, then additional information may be requested directly from them.
 - Once all checks are completed and passed, and all the required documentation received, Innovate UK will issue a Grant Confirmation Letter detailing the contract between Innovate UK and the recipient organisation(s). This must be signed and returned to us before the grant for the project can be claimed.
3. They are required to attend a new project workshop and if they are in a consortium one representative from each partner will need to attend with them. This workshop is compulsory before the project starts as it provides them with an opportunity to:
- Find out about the project start-up process.
 - Understand our expectations of you once the project is underway.
 - Meet their project assigned Monitoring Officer who will attend project meetings as well as report progress and issues to Innovate UK. Like Assessors above, Monitoring Officers are not employees of Innovate UK. Monitoring Officers also assist in the 'start up' phase of a project, helping them with all key documentation and ensuring the project starts off smoothly.

Hand Off: Grants System for Grant Processing & Monitoring

- Participants can only claim for eligible costs incurred AND paid between the project start and end dates. Any costs incurred or paid outside the project dates are ineligible.
- Depending on the size of grant awarded, claims will be subject to an independent audit to confirm that the costs claimed are in line with the terms and conditions of the offer. The audit requirement will be stated in the Conditional Offer Letter.
- All grants are claimable quarterly in arrears (unless otherwise stated in the grant confirmation letter) and will only be paid once the necessary reporting and audits have been completed. Claims are paid directly to each participant. It is important that you plan your cash flow requirements to ensure you can accommodate the funding required for the project.

Web flow 'As Is'



Technology 'As Is'

The existing business process is run via a combination of applications:

- Secure FTP
- MS Word
- MS Excel
- MS Access
- Email

There is some limited automation to migrate/import data between MS Access and Excel. We aim to migrate our existing disconnected process into one, integrated web-application.

PROJECT SCOPE

The scope of the overall project is to create a digital service for the application process from the point of initiation of the application to the transfer of information into the grant system to enable grant claiming. We need to consider the wider business context when designing this service however, as it must co-exist with other Innovate UK services to enable a seamless user journey across all our services.

A Discovery and Alpha phase of this project have been successfully completed where a 'thin slice' of the technology and user experience has been proven to work with the technologies selected. It is now the role of the Beta phase to complete the backlog tasks associated with Alpha and complete the entire user experience.

The scope of this specific engagement covers the Beta phase of our Innovation Funding Service Project.

CURRENT ROLES AND RESPONSIBILITIES:

Role	Responsibilities
------	------------------

Service Manager – [REDACTED]	Overall responsibility for the project. To interpret user insight and performance data to drive service design and iterative operational improvements for digital and assisted digital service channels. Will engage with the supplier's technical staff to define the best system and platform configurations to achieve business/user objectives.
Delivery Manager – [REDACTED]	To run the project on a day to day basis. Will manage the customer side of the engagement and the interfaces with the supplier on a day to day basis. This includes ensuring user input and existing collateral are available to the supplier as per the agreed schedule.
Technical Architect – [REDACTED]	Provide hands-on technical leadership, in the development, operation and ongoing improvement of complex, transformational digital services serving millions of users.
Development Manager - [REDACTED]	To provide assurance of the low level technical design.
Test Manager - [REDACTED]	To provide assurance of the testing process and transition to UAT.
Business Analyst – [REDACTED]	To support the project by analysing propositions and defining and mapping requirements. Will validate and maintain requirements internally.
Business Improvement Specialist – [REDACTED]	To ensure any new processes developed are fully aligned to the meet all business requirements. Will lead on any business process re-engineering required to implement the new service and on the implementation of change management within the business.

REQUIRED OUTCOMES:

To establish a technical team who will take the Alpha 'thin slice' version of our Innovation Funding Service and help work with us through a Beta phase with the aim of putting the service online by February 2016.

Beta

The purpose of Beta is to:

- Complete the backlog tasks from the Alpha phase with the aim of achieving an online service that can be launched as a private Beta from February 2016.
- Establish the basis for measuring the success of the new service

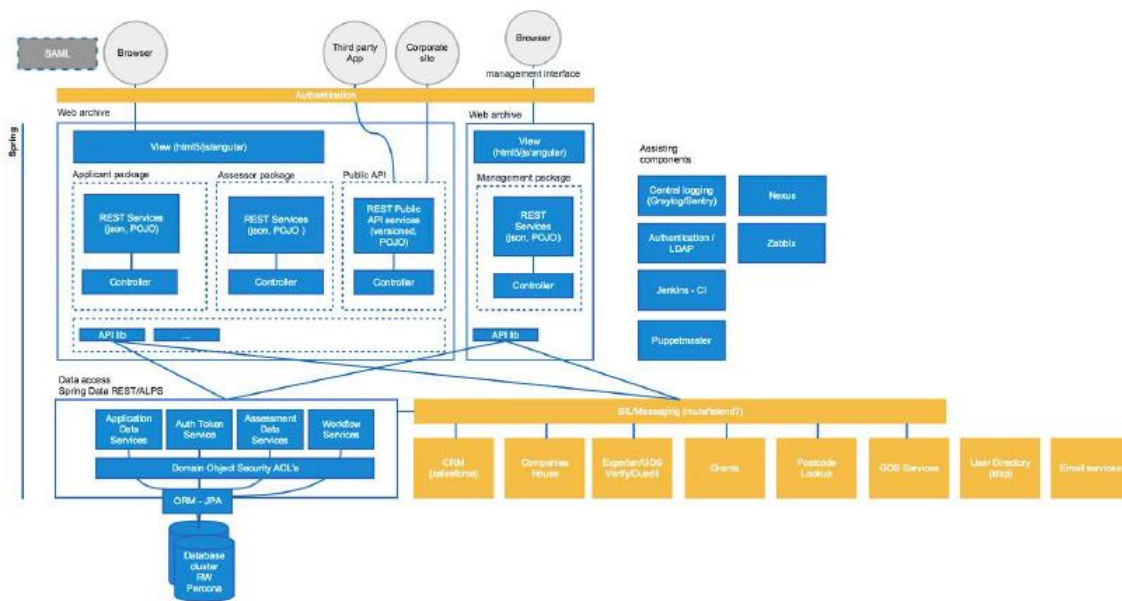
HIGH LEVEL REQUIREMENTS

We have some high level business and technical requirements as inputs to the Discovery phase. These are outlined below:

Target Architecture

The following information explains the higher level design we are looking to achieve:

Development View, Module level



Key elements in the development view

- The top layer of the application will be deployed in one archive, containing multiple packages.
- The management interface will be developed as part of the same system, but will be prepared for deployment separately from the other services.
- We will package controllers and rest services in a logical way together. Some shared libraries will be packaged separately so they can be used by all other packages. An example of this is the API library which is used to contact the data access and SIL services.

The controllers will receive a user interface call like 'getApplicationStatusOverview(...)' and will pass this on to multiple calls to the backend to retrieve the needed data. The data will be combined to then include competition deadlines and application progress into one set of data that is returned to the client.

- The database will be exposed to the rest of the system by a set of REST services. This decouples the database from the other application modules and allows us to implement domain object security ACL's at this level.

Using REST services to access the database in a stateless environment has an impact on the performance, we advise to include load tests to assess the impact.

- We recognise there will be a set of devops components that are not part of the 'system' but do delivery the day-to-day deployment, testing, build and continuous integration environment (shown on the right side of the diagram).

Technology decisions

- Innovate UK has a working setup for SSO based on Open AM. This SSO system can be used in front of the IFS system to authenticate. We do not introduce new authentication mechanisms or user database with the introduction of IFS.

Since the system consists of stateless services, we plan to work with a token based system where the end user holds a security token that gives access to the required data (token service). The details of the SSO process and the combination with the LDAP repository needs to be included in the detailed technical design when this feature is delivered.

- We have selected Spring framework to deliver the custom Java based modules in the system. The Spring system framework provides a big part of the needed security features. Spring is a proven enterprise ready

framework with a good track record and userbase, and delivers the needed REST and microservice modularities.

- For the frontend we have selected an HTML5/CSS/Javascript based setup. These components will deliver the one page application feel for the end user and we are also able to deliver the required accessibility standards.
- We use an out of box ORM layer like JPA/Hibernate to access the database.
- Email services will need to address anti-spam features like SPF records and backlist prevention techniques. We foresee an external email service to handle email sending and managing bounces and anti-spam.
- The java application will run on Apache Tomcat.
- The workflow service will expose methods to the application to update the state of the process of objects in the system (like an application).

Workflow

The applications are running through several processes before they become actual projects. There are several steps where different parties have to perform actions e.g. submitting of the application, assessing, etc. This process for CR&D is predefined and will not change.

The workflow solution will be positioned centrally and close to the data layer, such that the different components can make use of this module if necessary. For the current CR&D application process the following requirements should be met in terms of the workflow process:

- It should accommodate in following the process and step through the process, by transitioning from one state to another.
- During the process the different tasks should be able to be assigned to a certain role.
- Only certain users can perform certain transitions, permissions must be evaluated.
- Transitions are not only initiated by users, but can also be triggered by batch processes or set moment by an event mechanism.
- The different state changes should be logged.
- Longer processes during the transition (e.g. mailing many people or processing documents, etc.) should take place asynchronously.
- Workflow elements should be reusable and flexible.
- The workflow component needs to be able to be configured up to a certain level – for instance switch on or off steps for a competition.
- Preconditions for certain workflow transitions are part of the business logic of the application and need to be enforced to ensure data integrity.

At this moment these are just basic requirements and therefore we have not chosen to start with an off-the-shelf workflow engine like JBPM or Activiti. The following has been considered for when you do need to consider using a workflow engine:

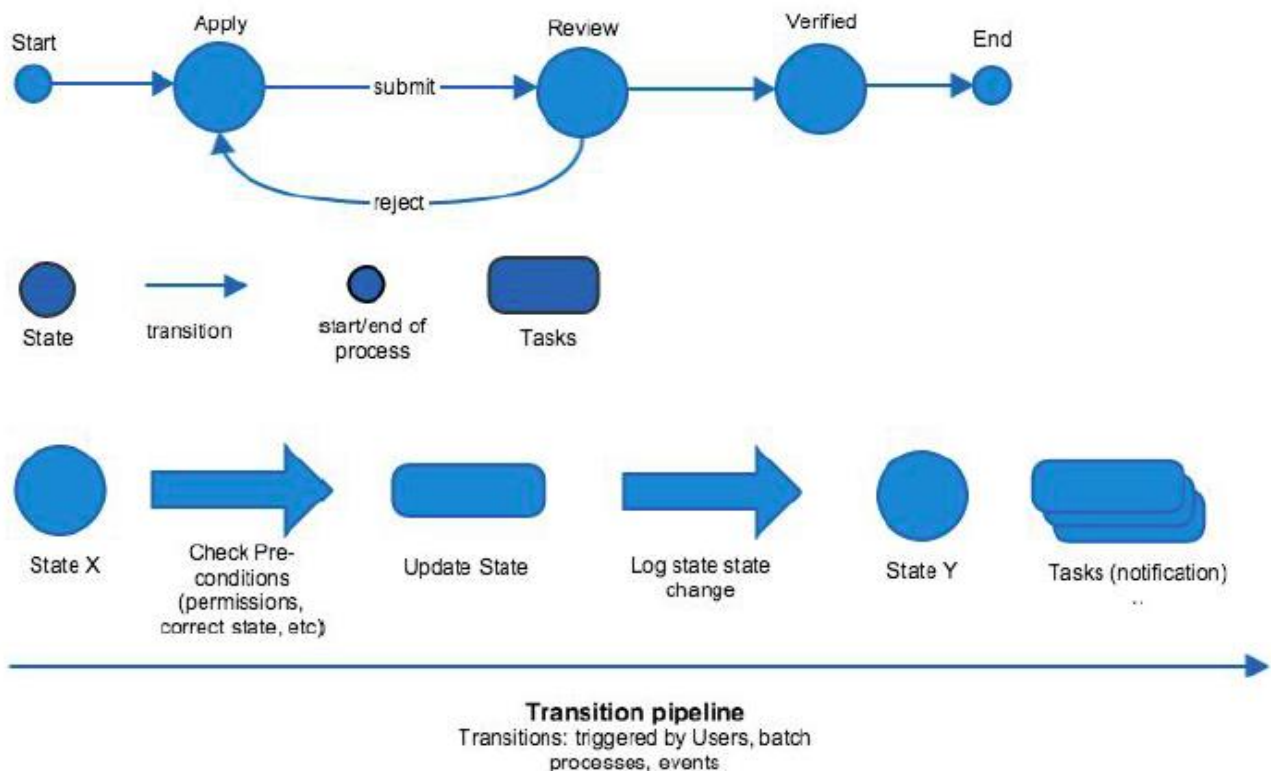
- The workflow needs to be able to be changed by the business.
- Visualisation of the workflow / modelling is required.
- If you expect the workflow to change often, and want non-devs to be able to make the adjustments – go workflow engine.
- If you need rich workflow features later in the applications lifecycle, you can have all of these out of the box in the engine (like forking, merging, rule based decisions etc.)

The reasons not to choose a workflow engine is that it is quite a large component to introduce where it does more than (in this case) we need, which might result in issues that are not easily resolved and a steep learning curve.

The following elements will be introduced for the CR&D process:

- Workflow supertype, with CR&D Workflow as one variant.
- It consists of transitions and states and tasks.

- States are stored in the domain object concerned (application, or competition or assessment invite).
- Tasks are reusable units like informApplicant, updateState.
- Transitions have preconditions which check if the object is allowed to make the transition, the right user is requesting the transition etc. At the end of the transition, the state has changed.
- Transitions have permissions. Only certain users can perform certain transitions.
- Transitions are running in a transaction – so they are atomic.
- Transitions are logged in the audit log.
- Transitions can be triggered by end users (with the right permission), by batch processes or triggered at set moments by an event mechanism.
- If a transition is dependent on multiple preconditions, we listen to these events to execute the preconditions.
- Longer running processes may run asynchronously so the user does not have to wait for these to finish while his request runs.



Due to the flexibility of the workflow, the different states are not calling each other, since you may want steps to be reused multiple times in different combinations. The workflow holds decisions which way to go. Based on states, certain actions are enabled. We define a limited set of states per object.

For the CR&D process the following workflows are currently identified:

- Project setup (a set of tasks to be completed by one or more parties) – per application. (Listener on save event for a certain object – evaluate if an automatic transition is needed).
- Competition timeline (adjusts the state of the competition – driven by set timelines and data in the competition) (con process driven which may run a transition at set times) – alternative is a logical order, all previous states have been completed.
- Application state workflow (previously submitted, submitted, in progress, open, awaiting assessment (waiting for deadline to pass, precondition), successful, unsuccessful) (user interface might trigger the transition)

- Assessor allocation (invited, accepted)

We have considered various issues around locking, concurrent updates and race conditions in the workflow:

- We do not use locking on a database level.
- We use transaction for workflow transitions. A check of the current state of the workflow during the state change will be part of the transition. If two people transition the workflow at the same time, only one will succeed and the other will be rolled back.
- We don't expect concurrent updated to be a significant issue, due to the fact that only one user can change application state at a time.

Integrating with systems outside of the IFS (System Integration Layer)

- One of the modules might need to retried data from one of the systems connected to the SIL – to do a postcode lookup for an end user to auto-fill an address. The module will get in contact with the SIL by means of an API/SIL library that is included and provides the methods to do so.
- It is also possible that a process where no users are involved directly needs to get data from the SIL. It can do so by contacting the SIL through the same library by the process.
- Sharing data with the SIL can be done on a data level (with every crud operation) if the SIL is interested to subscribe to these events.

Application Security

Security is a big topic and to be effective it needs to be addressed in all layers of the solution stack – not just in the application. For example: datacenter, network and OS security needs to be addressed as well, but is not in the scope of this document.

Main security risks identified

Security starts with identifying the risks involved.

- Logged in users of the system being able to access data that they should not have access to.
- Anonymous users getting access to confidential data
- An individual getting access to someone else's user account (potentially an assessor or someone with extended permissions).
- An individual making changes based on unauthorised access.

Application security

- No local password storage, we use a central login facility providing SSO / SAML. The application will use a token provided by the central facility.
- We secure data access as close to the data as possible – in the model. The data layer is called using a usertoken that only gives access to the required items.
- We limit the attack surface by making sure there is a separate management interface. The other interfaces will only have access to a small portion of the data in the system.
- We use ACL security level for domain object security, implementing Spring Security.
- We apply the Spring security module providing (among other) CSRF protection.
- Spring SAML plugin for authentication and central user management.

- We did consider encrypting whole filesystem, db or fields. In those situations the system would need to store the key to get access to the data, which defeats part of the purpose. For now we have decided against encryption of the whole database or filesystem.

Secure coding practices

- We advise using a security checklist for web development like:
<https://www.certifiedsecure.com/checklists/cs-web-application-secure-developmen.pdf>
- We advise using OWASP tooling to check the application for security flaws.
- Escape at the leafs. We escape in the places it is necessary, for instance on the output for XSS prevention, or on the query for injection prevention. All types of XSS will be covered.
- The spring data binding needs to be configured correctly to prevent security issues. We advise to implement specific automated tests to ensure this sensitivity does not cause issues.

Authentication

We envision the final solution to be placed behind a proven authentication solution like CAS, Shibboleth, OpenAM or a central government authentication solution. We plan using Springs SAML plugin to allow authentication and central user management.

For special roles (roles that give access to multiple applicants' data) we foresee two factor authentication.

For Public API Access, we implement that OAuth2 mechanism that Spring Security supports.

Authorisation

We will apply Springs Security framework to implement interceptor that do pre-invocation authorisation on methods, and domain access security control before accessing objects.

In some cases also post-invocation security methods can be applied to filter data before it is returned to the end user.

For the support purposed special security controls may be applied that allow support users to get access to end users records for a limited amount of time. The authorisation checks are set up on a deny by default basis – access is only granted when this is explicitly done in the required methods and domain ACLs.

Data validation

Data will be filtered for malicious activity:

- Escaping, injection of SQL/JS. This will limit XSS risks.
- We will use Spring Security CSRF protection to include random security tokens in form submissions, file uploads and ajax requests. This will ensure the request is coming from the trusted application.
- File uploads will be checked on data type and will be virus checked.

Data will be validated on three levels:

- On a domain object using Springs annotations, making sure the users data that has been entered is valid.
- In the controllers, checking if the user input and activity is valid in the context of the object.
- On a state change in the workflow, checking if the object has a consistent state. This will ensure an application only get to a certain state (for instance 'accepted' in the case it complies with all the rules that have been set for the state.

Auditing and Logging

We foresee using a Spring aspect to apply audit logging to all relevant methods logging date/time, user, access permission, IP address, and the object involved. This way it is possible to trace back changes that have been made. In the case of a compromised user account, the changes made can be traced back to the account.

Application exception Management and Monitoring

Application exceptions are logged and this log is monitored. Suspicious activity is often started with trying to do invalid things which can be logged and spotted by monitoring the logs.

Data protection in storage and transit

- Domain Object Security – Spring ACL
- When an application is completed (either accepted or rejected), access permission on sensitive data will be removed, limiting the access to archived data completely.
- User Passwords will not be stored in the solution, but in the central authentication system. This solution will ensure the password complexity requirements.

Since the SIL is still in development, security in combination with the SIL is not yet designed.

REQUIRED CAPABILITIES AND OUTCOMES OF THE SUPPLIER:

Required Capabilities and Outcomes of the Supplier	
Capabilities	Outcomes
Agile Product Design & Delivery	Scrum-master and project management skills (to be able to answer resourcing based questions and understand planning)
Software Engineering and Ongoing Support	Developer to work alongside User Researcher and turn UX design into Front-end code. Back-end developers also required. Understanding of different testing environments, code deployment and maintenance.
User Research (UX Design)	Ability to work with Front-end developer to turn sketches into real-life code that can be tested with users. User testing skills essential.

THE METHODOLOGY:

We would expect Supplier to work within an Agile Methodology as per the GDS Service Design Manual.

GOVERNANCE:

Expected meetings/reporting:

Daily scrums

Sprint checkpoint reviews

Sprint reviews

Sprint retrospectives

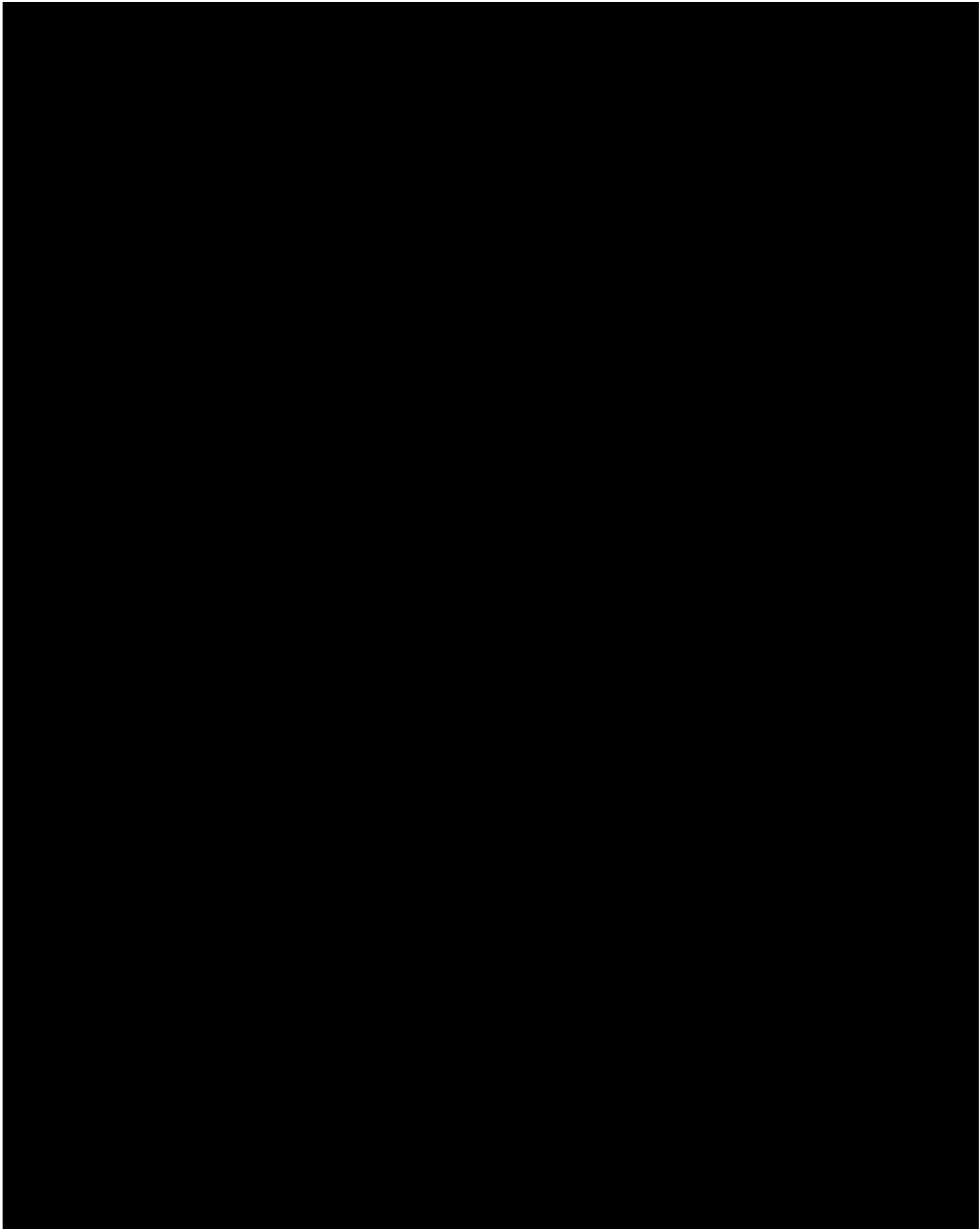
Sprint planning sessions

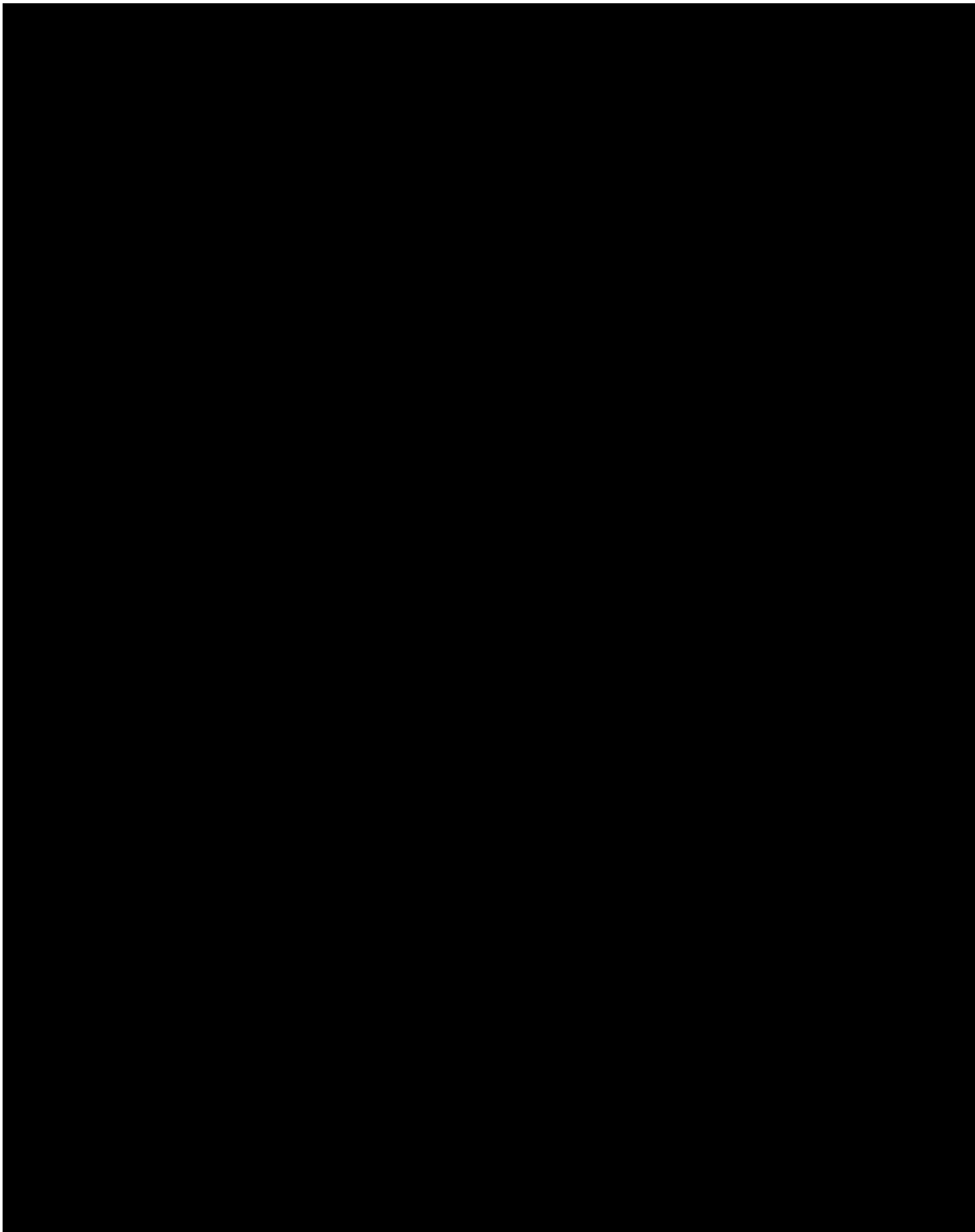
Highlight reports – TBC (frequency TBC also)

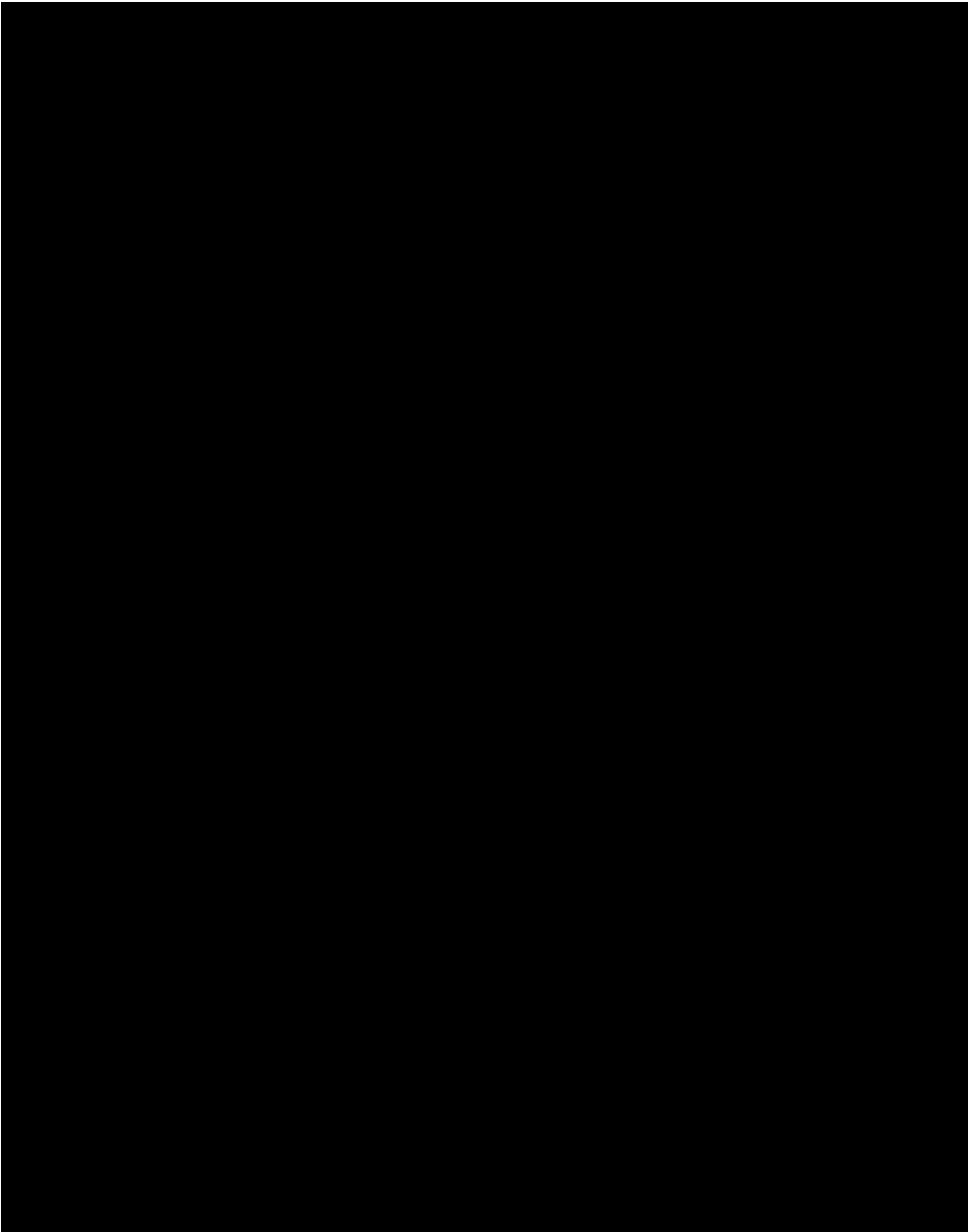
Senior Stakeholder team meeting if required, to discuss high level progress and mitigate any risks/issues.

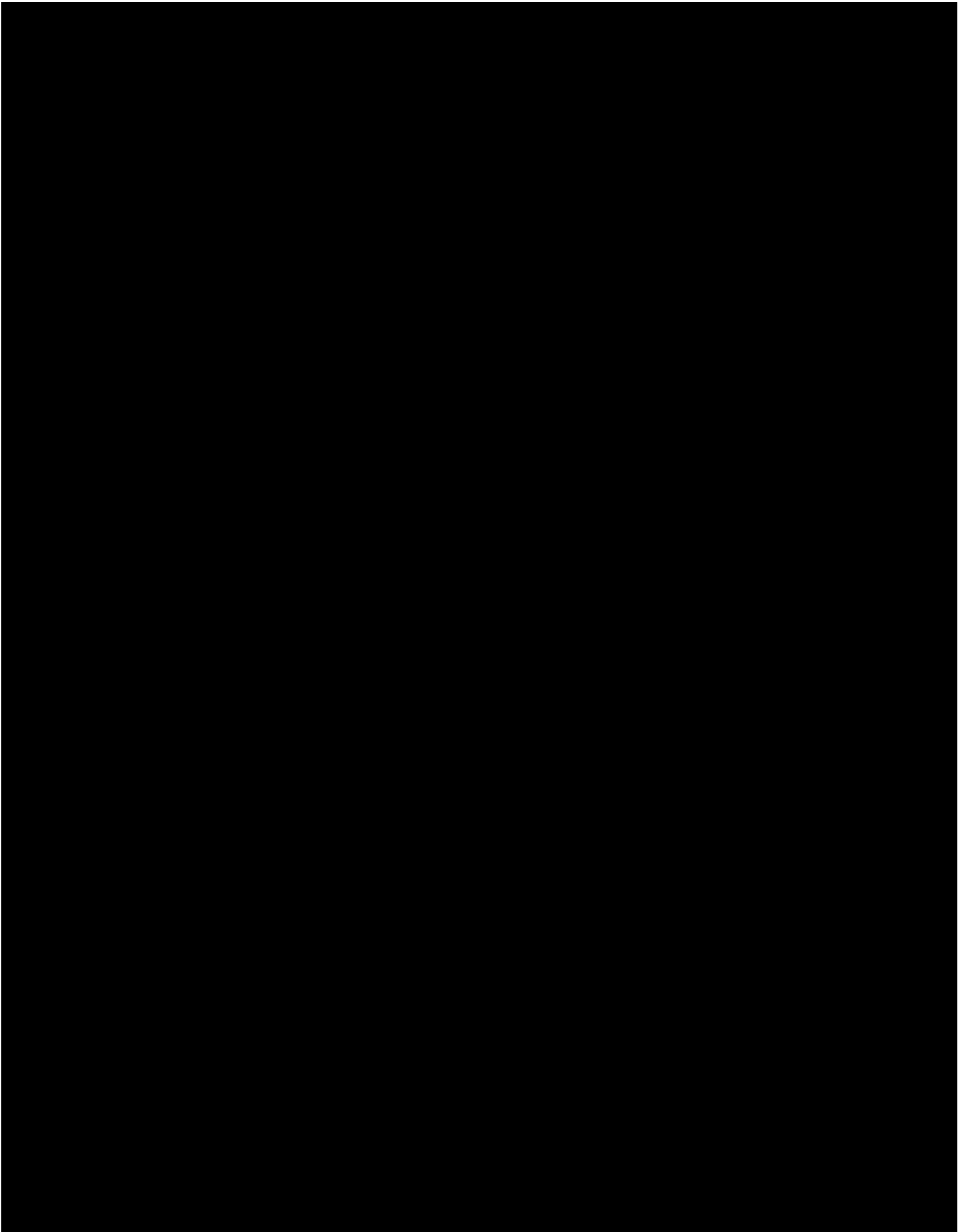
BIS assessment – checkpoint review required ahead of moving into private beta in February 2016.

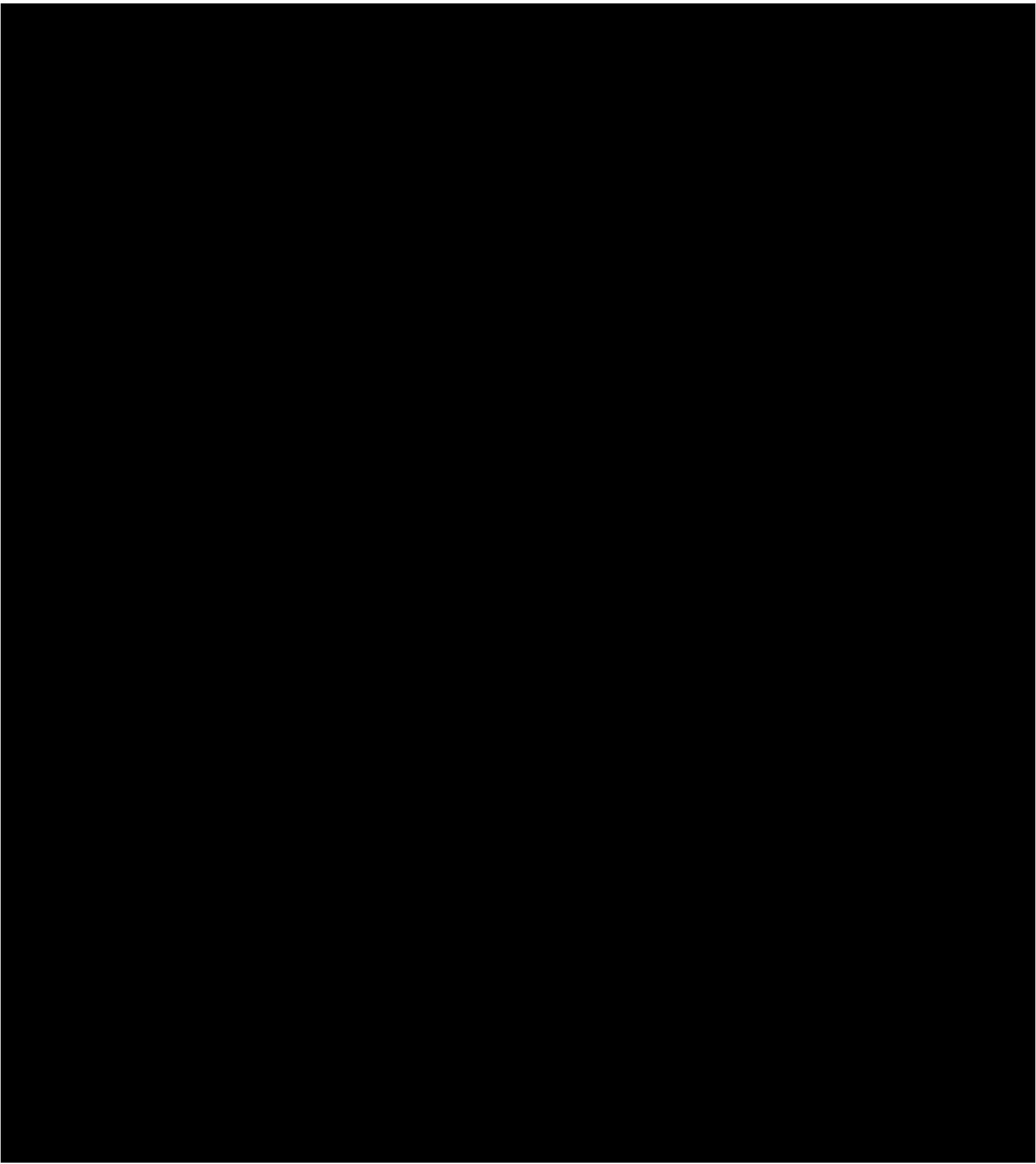
SCHEDULE 2 – SUPPLIER’S RESPONSE











SCHEDULE 3 – ADDITIONAL CUSTOMER TERMS

1. RELEVANT CONVICTIONS

- 1.1 This Clause shall apply if the Customer has so specified in the Order Form.
- 1.2 The Supplier shall ensure that no person who discloses that he has a Relevant Conviction, or who is found to have any Relevant Convictions (whether as a result of a police check or through the Criminal Records Bureau procedures or otherwise), is employed or engaged in any part of the provision of the Services without Approval.
- 1.3 For each member of Supplier Staff who, in providing the Services, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Customer owes a special duty of care, the Supplier shall (and shall procure that the relevant Sub-Contractor shall):
 - 1.3.1 carry out a check with the records held by the Department for Education (DfE);
 - 1.3.2 conduct thorough questioning regarding any Relevant Convictions; and
 - 1.3.3 ensure a police check is completed and such other checks as may be carried out through the Criminal Records Bureau,
 - 1.3.4 and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Services any person who has a Relevant Conviction or an inappropriate record.

2. ADDITIONAL STAFFING SECURITY

- 2.1 This Clause 2 shall apply if the Customer has so stipulated in the Order Form.
- 2.2 The Supplier shall comply with the Staff Vetting Procedures in respect of all or part of the Supplier Staff (as specified by the Customer) and/or any other relevant instruction, guidance or procedure issued by the Customer that will be used to specify the level of staffing security required and to vet the Supplier Staff (or part of the Supplier Staff).
- 2.3 The Supplier confirms that, at the Commencement Date, the Supplier Staff were vetted and recruited on a basis that is equivalent to and no less strict than the Staff Vetting Procedures and/or any other relevant instruction, guidance or procedure as specified by the Customer.

SCHEDULE 4 – STATEMENT OF WORK (SoW)

1. SOW DETAILS

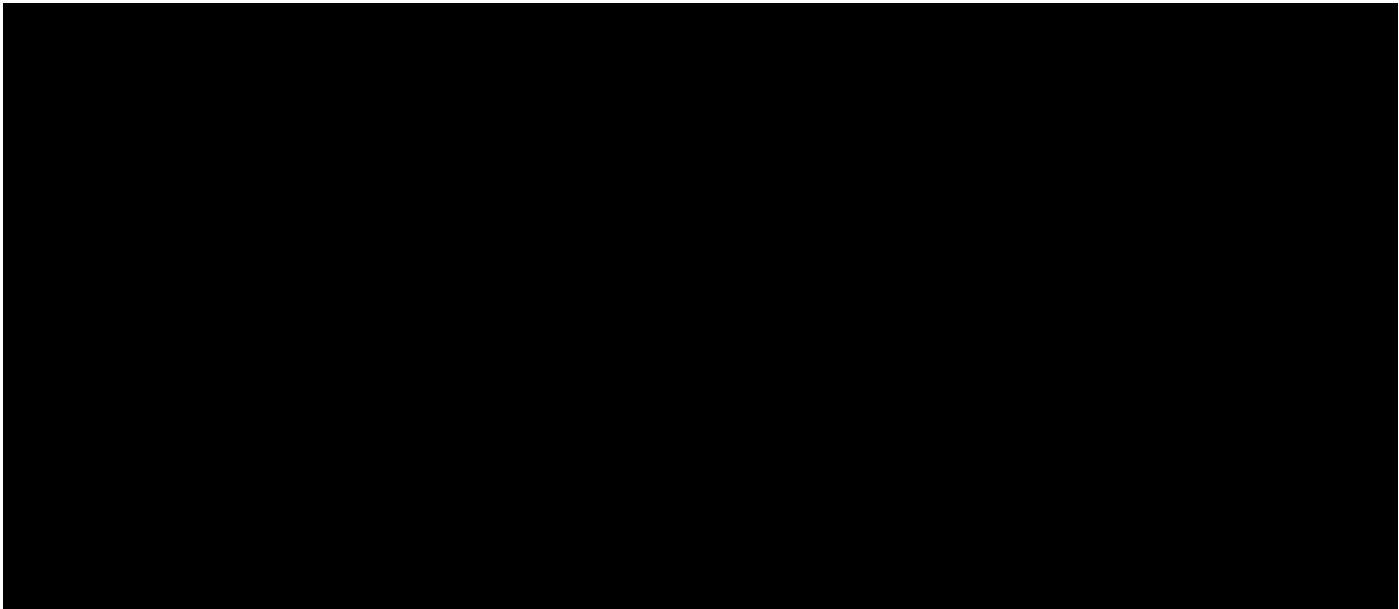
Date of SoW:	02/11/2015
SoW Reference:	DS02-012.1
Departmental customer:	Innovate UK
Supplier:	Nomensa Ltd
Release Type(s):	Delivery
Phase(s) of Development:	Beta
Release Completion Date:	05/04/2016
Duration of SoW	Between 20 and 89 working days depending on role
Charging Mechanism(s) for this Release:	Capped Time and Materials

- 1.1 The Parties shall execute a SoW for each Release. Note that Inception Stage, Calibration Stage and any ad-hoc Service requirements are to be treated as individual Releases in their own right (in addition to the Releases at the Delivery Stage); and the Parties should execute a separate SoW in respect of each.
- 1.2 The rights, obligations and details agreed by the Parties and set out in this SoW apply only in relation to the Services that are to be delivered under this SoW and shall not apply to any other SoW's executed or to be executed under this Contract unless otherwise agreed by the Parties.
- 1.3 The following documents shall be inserted as Annexes to this Schedule as soon as they have been developed and agreed by the Parties:
- 1.3.1 Annex 1: the initial Release Plan developed for this Release;
 - 1.3.2 Annex 2: the Stories which are to form the subject of this Release;
 - 1.3.3 Annex 3: the current Product Backlog; and
 - 1.3.4 Annex 4: High Level Objectives for the Release

2. KEY PERSONNEL

- 2.1 The Parties agree that the Key Personnel in respect of this Project are detailed in the table below.

2.2





3. DELIVERABLES

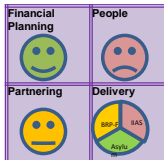
Please note the deliverables will be agreed with the Customer during the kick off, however the following deliverables are anticipated to be required:

- 3.1 [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

4. BALANCED SCORECARD & KPI'S

- 4.1 In addition to the Supplier's performance management obligations set out in the framework Agreement, the Parties have agreed the following Balanced Scorecard & KPIs for this Release. Balanced Scorecard Model:

Balanced Scorecard

<p>KPI – FINANCIAL AND RESOURCE PLANNING</p> <p>Suppliers work with the Authority through planned monthly resourcing meetings and produce a costed resource profile on the standard template provided by the Authority. The forecast resource plans must be credible and capable of maintaining future delivery momentum.</p> <p>Measurement</p> <table><tr><td>Costs are accurate and resource plans are credible.</td><td>Costs and/or resource levels are incorrect but the plan is broadly credible with some minor adjustments.</td><td>Costs and/or profiling do not align with the programme delivery plan and will require substantial reworking to make credible</td></tr></table> <p>Source</p> <p>Project Manager verification of supplier resource profile and plans feedback</p> <p>Owner</p> <p>Commercial with Delivery and Finance support.</p>	Costs are accurate and resource plans are credible.	Costs and/or resource levels are incorrect but the plan is broadly credible with some minor adjustments.	Costs and/or profiling do not align with the programme delivery plan and will require substantial reworking to make credible	<p>ACME Computing</p> 	<p>KPI - PEOPLE</p> <p>Successful recruitment and placement of key resources meets the planned deliverables and contractual obligations; the supplier pro-actively manages their resource skills by identifying skills issues early and in a timely fashion addressing any deficits.</p> <p>Measurement</p> <table><tr><td>Supplier conversion of candidate to placement is not lower than 1:3 and/or placed resources are not substituted at the Authority's request in the month.</td><td>Supplier conversion of candidate to placement is less than 1:3 but no less than 1:6 and/or supplier is asked to swap out at least one resource in the month.</td><td>Supplier conversion of candidate to placement is less than 1:6 and/or is asked to substitute more than one resource in the month.</td></tr></table> <p>Source</p> <p>Project Managers verification of recruitment and retention.</p> <p>Owner</p> <p>Commercial with Delivery support.</p>	Supplier conversion of candidate to placement is not lower than 1:3 and/or placed resources are not substituted at the Authority's request in the month.	Supplier conversion of candidate to placement is less than 1:3 but no less than 1:6 and/or supplier is asked to swap out at least one resource in the month.	Supplier conversion of candidate to placement is less than 1:6 and/or is asked to substitute more than one resource in the month.
Costs are accurate and resource plans are credible.	Costs and/or resource levels are incorrect but the plan is broadly credible with some minor adjustments.	Costs and/or profiling do not align with the programme delivery plan and will require substantial reworking to make credible						
Supplier conversion of candidate to placement is not lower than 1:3 and/or placed resources are not substituted at the Authority's request in the month.	Supplier conversion of candidate to placement is less than 1:3 but no less than 1:6 and/or supplier is asked to swap out at least one resource in the month.	Supplier conversion of candidate to placement is less than 1:6 and/or is asked to substitute more than one resource in the month.						
<p>KPI - PARTNERING BEHAVIOURS AND ADDED VALUE</p> <p>Supplier promotes positive collaborative working relationships within and across team by acting in a transparent manner in line with partnering behaviours.</p> <p>Supplier shows commitment to IPT programme goals through adding value over and above the provision of compensated skilled personnel.</p> <p>Measurement</p> <table><tr><td>- No behavioural problems identified. - IPT workshops (such as pulse, think tank, lessons learned) attended and positive contributions made. - Added Value recognised by the programme above provision of compensated skilled resource</td><td>- Some minor behavioural problems. - Supplier only attends Some workshops or provides minor contributions. - Supplier adds some value above provision of compensated resource but programme do not regard as significant.</td><td>- Significant behavioural problems - Supplier contributions are rare or insignificant and shows little interest in working with other suppliers - no added value contributions recognised by Programme.</td></tr></table> <p>Source</p> <p>Collective feedback on suppliers from both client and other supplier staff.</p> <p>Owner</p> <p>Commercial with Delivery verification.</p>	- No behavioural problems identified. - IPT workshops (such as pulse, think tank, lessons learned) attended and positive contributions made. - Added Value recognised by the programme above provision of compensated skilled resource	- Some minor behavioural problems. - Supplier only attends Some workshops or provides minor contributions. - Supplier adds some value above provision of compensated resource but programme do not regard as significant.	- Significant behavioural problems - Supplier contributions are rare or insignificant and shows little interest in working with other suppliers - no added value contributions recognised by Programme.		<p>KPI - DELIVERY</p> <p>The team in which a supplier is a member has delivered all of the agreed stories in a month (or supplier specific agreed deliverables where the role may not be delivery focused. A supplier will achieve the RAG status of the team.</p> <p>Measurement</p> <table><tr><td>All teams in which a supplier is a member of have delivered 100% of the planned stories for the month.</td><td>Less than 100% of the stories have been achieved by a team.</td><td>Less than 95% of the stories have been achieved by a team</td></tr></table> <p>Source</p> <p>Project Manager verification from retro's.</p> <p>Owner</p> <p>Commercial with Delivery verification.</p>	All teams in which a supplier is a member of have delivered 100% of the planned stories for the month.	Less than 100% of the stories have been achieved by a team.	Less than 95% of the stories have been achieved by a team
- No behavioural problems identified. - IPT workshops (such as pulse, think tank, lessons learned) attended and positive contributions made. - Added Value recognised by the programme above provision of compensated skilled resource	- Some minor behavioural problems. - Supplier only attends Some workshops or provides minor contributions. - Supplier adds some value above provision of compensated resource but programme do not regard as significant.	- Significant behavioural problems - Supplier contributions are rare or insignificant and shows little interest in working with other suppliers - no added value contributions recognised by Programme.						
All teams in which a supplier is a member of have delivered 100% of the planned stories for the month.	Less than 100% of the stories have been achieved by a team.	Less than 95% of the stories have been achieved by a team						

5. CONTRACT CHARGES

5.1 CAPPED TIME AND MATERIAL CHARGES

5.1.1 Where Services for this Release are being delivered on a Capped Time and Materials Basis, the provisions of this paragraph 5.1 and the Time and Material Rates set out at paragraph 5.3.5 shall apply.

The maximum price the Supplier is entitled to charge the departmental customer for Services delivered [REDACTED]

[REDACTED] (“Maximum Price”)

5.1.2 Capped Time and Materials Contract Charges shall be calculated on a daily basis at the respective time and material rates for each Supplier Staff for every day, or pro rata for every part of a day, that the Supplier Staff are actively performing the Services and in accordance with the relevant rates for such Supplier Staff as required to perform such Services.

5.1.3 The Supplier acknowledges and agrees that it shall provide the Services in relation to this Release within the Maximum Price set out at paragraph 5.1.2 above and it shall continue at its own cost and expense to provide the Services even where the price of Services delivered to the departmental customer on a Capped Time and Materials basis has exceeded the Maximum Price.

5.1.4 The departmental customer shall have no obligation or liability to pay for the cost of any Services delivered in respect of this SoW after the Maximum Price has been exceeded.

5.2 PRICE PER STORY POINT CHARGES

Unused

5.3 TIME AND MATERIALS CHARGES

5.3.1 The Time and Materials pricing structure shall apply:

- (a) for Services delivered during the Inception and Calibration Stage(s) (or as agreed otherwise by the Parties); and,
- (b) for other aspects of the Services as agreed by the Parties.

5.3.2 Time and Materials Contract Charges shall be calculated on a daily basis at the respective time and material rates for each Supplier Staff for every day, or pro rata for every part of a day, that the Supplier Staff are actively performing the Services and in accordance with the relevant rates for such Supplier Staff as required to perform such Services as set out at paragraph 5.3.5.

5.3.3 The Supplier shall provide a detailed breakdown of any time and materials Contract Charges with sufficient detail to enable the departmental customer to verify the accuracy of the time and material Contract Charges incurred.

5.3.4 For the avoidance of doubt, no risks or contingencies shall be included in the Contract Charges in relation to the provision of Services for which time and materials Contract Charges apply. The Supplier shall maintain full and accurate records of the time spent by the Supplier Staff in providing the Services and shall produce such records to the departmental customer for inspection at all reasonable times on request.

5.4 FIXED PRICE

Unused
6. **SERVICE CREDITS**
Unused

7. **ADDITIONAL REQUIREMENTS**
Working in Swindon

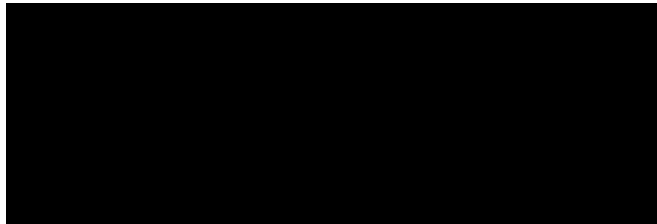
8. **AGREEMENT OF SOW**

8.1 BY SIGNING this SoW, the Parties agree to be bound by the Terms and Conditions set out herein:

For and on behalf of the Supplier:

Name and Title

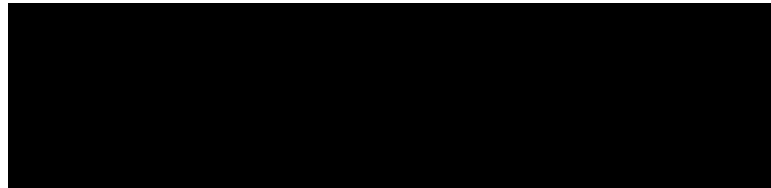
Signature and Date



For and on behalf of the departmental customer:

Name and Title

Signature and Date



Please note that the first SoW is signed by CCS. Any subsequent SoW(s) would require the departmental customer's signature. With a copy sent to CCS for its records.

SCHEDULE 5 - CONTRACT CHANGE NOTE

Order Form reference for the Contract being varied:

PROJECT: DS02-XXX
CCN NUMBER: XX
2015 IPR TERMS USED? YES/NO

BETWEEN: the “Customer”
Crown Commercial Service (CCS)
Acting as an agent on behalf of the departmental customer:
Customer Full Name
the “Supplier”
Supplier Full Name

1. The Contract is varied as follows and shall take effect on the date signed by both Parties:

Reason for the change:

Please enter here

Full Details of the proposed change:

Please enter here

Likely impact of the change on other aspects of the Contract:

Please enter here

Original Contract Value: £ Please enter here

Additional Cost due to change: £ Please enter here

New Contract Value to be: £ Please enter here

2. Words and expressions in this change Contract Note shall have the meanings given to them in the Contract.
3. The Contract, including any previous changes shall remain effective and unaltered except as amended by this change.

For and on behalf of the Supplier:

Name and Title

Signature and Date

X

Click here to enter a date.

For and on behalf of the departmental customer:

Name and Title

Signature and Date

X

Click here to enter a date.