SCHEDULE 2

SERVICES DESCRIPTION

Schedule 2 (*Services Description*)

1. INTRODUCTION

1.1. General

1.1.1. This schedule specifies the intended scope of the Services to be provided by the Supplier under this Agreement and a description of what each of the Services entails.

1.1.2. The requirements for the Services have been categorised under the following headings:

(a) Implementation Services, comprising the elements as set out in Paragraph 2;

(b) Operational Services, comprising the elements as set out in Paragraph 3; and

(c) Optional Services, comprising the elements as set out in Paragraph 4.

1.2. Scope

1.2.1. The capabilities required for this Contract are summarised below:

(a) to implement and cutover to the Supplier Solution in its entirety (the **"Beta"**) within eighteen (18) months of the Effective Date;

(b) to provide the core NFWS functionality for Users within England:

- define (geographic) Operational Boundaries and Target Areas;
- provide a Common Operational Picture by region;
- create Warnings and manage Warnings in force;
- allow Users and Organisations to Register to receive Warnings;
- issue location-based Warnings and other Messages through multiple Contact Channels;
- obtain contact details for Unregistered Users for a region;
- ingest data or publish data to GIS systems, address systems, flood risk mapping systems, telemetry systems, forecasting systems, and data sharing systems.

(c) provide product delivery, user-centered services, IT Service Management and hosting;

(d) provide the capability to introduce future services, such as additional geospatial services, new Contact Channels (e.g. social media, smart devices, mobile app), new flood and/or geospatial related digital services, and new Message types (e.g. environment related incidents, such as drought); and

(e) provide the option for other Defra Group bodies, Risk Management Authorities, and other UK government departments to utilise the Services.

2. IMPLEMENTATION SERVICES

2.1. General

2.1.1. The Supplier shall provide the Implementation Services necessary for the Supplier to:

(a) provide the Operational Services required from Achievement of the ATP Milestone (as set out in Paragraph 3); and

(b) meet the Test Success Criteria for each Test relating to each Milestone as set out in Schedule 14 (*Testing Procedures*) Annex 4 (*Test Success Criteria*).

2.1.2. The ATP Milestone Date shall be no later than eighteen (18) months from the Effective Date and the CPP Milestone Date shall be three (3) months from Achievement of the ATP Milestone. ATP Milestones and major "go-live" activities cannot occur in January, February, March, November, or December.

2.1.3. With the exception of the phased activities set out in Paragraph 2.9.20, the Supplier shall plan for and subsequently implement a single cutover to the remaining Operational Services delivered from the ATP Milestone (as set out in Paragraph 3) that minimises the disruption incurred by Users.

2.2. Outgoing Supplier exit activities

2.2.1. The Supplier shall work with the Outgoing Supplier to agree the detailed sequence of Implementation Services and activities to be documented in the Outgoing Suppliers Exit Plan.

2.2.2. The Supplier shall work with the Outgoing Supplier to ensure:

(a) a smooth transfer of operations and Authority Data from the Outgoing Supplier to the Supplier;

(b) no loss or corruption of Authority Data;

(c) the transfer of "open" work-flow items (e.g. outstanding IT Service Management requests);

(d) the considerate management of Transferring Former Supplier Employees; and

(e) Users are kept informed of the changes.

2.2.3. The Supplier shall obtain all necessary

(a) Authority Data;

(b) Authority Software;

(c) Transferring Assets;

(d) details of Transferring Former Supplier Employees;

(e) any Telephone Operator Data Sharing Agreements held by the Outgoing Supplier which are transferring to the Supplier; and

(f) any other information that the Authority has obtained from the Outgoing Supplier

which are necessary for the Supplier to provide the Operational Services required from the ATP Milestone (as set out in Paragraph 3).

2.3. Unregistered Users solution

2.3.1. The Supplier shall work collaboratively with the Telephone Operators in order to agree technical and operational interfaces, and Telephone Operator Data Sharing Agreements, prior to the Business Readiness and Private Beta Milestone, which enable the Supplier to Ingest contact details for Unregistered Users into the Supplier System. The Supplier shall document this in an Unregistered Users Solution Design.

2.4. User research and user centered design

2.4.1. The Supplier shall review the Authority's User research undertaken to date and be responsible for defining the ongoing User research strategy. The Supplier shall document their findings and their ongoing User research strategy in a User Research Discovery Report.

2.4.2. The Supplier shall be responsible for Testing the developing service throughout the Implementation Phase with likely Users to make sure it meets their needs, and understand and resolve usability issues.

2.4.3. The Supplier shall be responsible for delivering the ongoing User research strategy defined in the User Research Discovery Report and the subsequent External User recruitment (e.g. members of the public and Organisations) that delivers that strategy. This may include but is not limited to:

(a) paid for usability testing;

(b) unmoderated testing;

(c) pop up testing;

(d) attendance at industry events;

(e) provision of lab facilities; and

(f) user recruitment incentivisation schemes

during the Implementation Phase.

2.4.4. The Supplier shall be responsible for defining the service design, interaction design, and content design strategies that will:

(a) trial and test different ideas and concepts and hypotheses;

(b) support A/B testing with Users (citizens and Organisations) to support the Users achieving their goals, desired outcomes, and improve User satisfaction;

(c) highlight where policy could be changed to improve the end-to-end User journey; and

(d) highlight where Message design can influence User behaviour.

2.4.5. The Supplier shall work and collaborate with the Authority's user centered design teams to create a level of design consistency and shared learning.

2.4.6. The Supplier shall produce the relevant user research documents to support design decisions, which may include (but is not limited to) research reports, personas, user journey maps, and storyboards.

2.5. Working with the Authority and Other Suppliers

2.5.1. The Supplier shall work collaboratively with the Floodline Contact Centre (via the Authority) in order to agree the design of the IVR Contact Channel interactions, in accordance with the requirement as set out in WIP034 in Annex B.

2.5.2. The Supplier shall lead a collaborative service design process with the Authority and Other Suppliers to capture and document a common understanding of the roles and responsibilities of all parties within the ITSM model for the Supplier Solution. The Supplier shall document this in an Operational Level Agreement.

2.5.3. The Supplier shall lead a collaborative process with the Authority and Other Suppliers to capture input and document a Joint Statement of Intent.

2.5.4. The Supplier shall work collaboratively with the Authority and Other Suppliers in order to agree technical interfaces between the Supplier Solution and Downstream Systems, in accordance with the requirements as set out in Annex C.

2.5.5. The Supplier shall maintain Documentation related to the Implementation Phase and deliver monthly progress updates against the following items to the Authority before the 15th of each month:

(a) the Detailed Implementation Plan;

(b) a summary of the Charges paid to date and a forecast of future Charges;

(c) a log of all risks, assumptions, issues, and dependencies associated with the Implementation Phase (the **"RAID Log"**).

2.6. Design Documentation

2.6.1. The Supplier shall produce an Integration Specification for the Supplier Solution using the OpenAPI Specification.

2.6.2. The Supplier shall produce a Detailed Design for the Supplier Solution in accordance with the technology architecture standards as set out in Schedule 4 (*Standards*) Paragraph 5 (*Technology Architecture Standards*).

2.6.3. The Supplier shall produce a Data Architecture Design for the Supplier Solution in accordance with the technology architecture standards as set out in Schedule 4 (*Standards*) Paragraph 5 (*Technology Architecture Standards*).

2.7. Build, test and deployment of the Supplier System

2.7.1. The Supplier shall implement the Supplier System in incremental New Releases.

2.7.2. The Supplier shall create and maintain the Product Backlog for the Implementation Phase. The Product Backlog for the Implementation Phase shall be derived from the requirements and associated user stories set out in Annex A, Annex B, and Annex C.

2.7.3. Throughout the Implementation Phase, the Authority's Product Manager(s) and the Supplier shall meet regularly (the **"Sprint Planning Meeting"**) to review the Product Backlog and shall agree a prioritisation for each Deliverable in the Product Backlog.

2.7.4. In support of the Sprint Planning Meeting, the Supplier shall provide an estimate of the effort required to develop each Deliverable in the Product Backlog. The Supplier shall prepare these estimates with appropriate care and skill.

2.7.5. At the Sprint Planning Meeting, the Authority's Product Manager(s) and the Supplier shall identify the Deliverables in the Product Backlog which shall be built, tested, and deployed in the next upcoming set period of time during which specific work has to be completed and made ready for review by the Authority (a **"Sprint"**).

2.7.6. At the Sprint Planning Meeting, the Supplier shall produce the prioritised list of the individual Deliverables which are proposed to be implemented during the upcoming Sprint as agreed by the Authority and the Supplier (the **"Sprint Backlog"**).

2.7.7. The success criteria for each Sprint (the **"Definition of Done"**) shall be agreed between the Parties and documented in the Sprint Backlog. The Definition of Done shall set out:

(a) the agreed Authority Requirements in scope of that Sprint and the tolerance for completion of Authority Requirements;

(b) the levels of Testing coverage required (e.g. automated, manual) for that Sprint;

(c) the types of Testing required (e.g. user acceptance testing, site acceptance testing, integration testing, system testing) for that Sprint;

(d) the Environments to be Tested within for that Sprint;

(e) any Standards that must be complied with for that Sprint;

(f) a set of acceptance criteria for that Sprint; and

(g) the agreed number of Test Issues for each Sprint and the time period for resolving any remaining Test Issues.

2.7.8. Upon satisfying the Authority that the Definition of Done has been met for each Sprint (in whole or in part), the Authority shall issue the Supplier with a Test Certificate.

2.7.9. In the event of a dispute between the Parties regarding the prioritisation of the Sprint Backlog, the Definition of Done, or a Test Certificate, the Parties shall attempt in good faith to resolve the dispute in accordance with the Joint Statement of Intent. If such attempts are not successful within a reasonable period, the Parties shall comply with Paragraph 2 of Schedule 23 (*Dispute Resolution Procedure*) to resolve the dispute.

2.7.10. The Supplier's Testing approach for each Sprint shall be undertaken in accordance with the Test Strategy.

2.8. Data migration

2.8.1. The Supplier shall migrate the following Authority Data to the Supplier Solution prior to the ATP Milestone.

Data type	Volume	Format
Contact details (individuals)	2,500,000	Text
Contact details (Organisations, to include link between Users within the Organisation)	200 Organisations comprising 2,000 Users	Text
Target Area coverage	5,000	Polygon
Target Area attributes (to include link to spatial coverage)	5,000	Text
Geographic coverage of Operational Boundaries	2,500	Polygon
Location data for Organisations	150,000	Point, line or polygon
Account Preferences (link between User details and Target Areas, including preferences for which types of Messages are received)	2,500,000	Text
History of Messages issued for Target Areas (including Message details)	40,000	Text
User details	1,500	Text
Static prompts for IVR	100	Wav
Telephone area codes linked to Target Areas for IVR	10,000	Text
Quickdial codes linked to Target Areas for IVR	5,000	Text
Caller line identification records to associate repeat and registered callers to Target Areas for IVR	100,000	Text

Data type	Volume	Format
Contacts to be excluded from imports of data received from Telephone Operators	100,000	Text

2.9. Business readiness and Private Beta

2.9.1. The Supplier shall follow the Authority's Change Method in the delivery of the Implementation Services.

2.9.2. The Supplier shall appoint a Business Change Lead in the delivery of the Implementation Services.

2.9.3. The Supplier shall support the Authority in producing the materials required for internal communications.

2.9.4. The Supplier shall support the Authority with internal communications between the ATP Milestone Date and the CPP Milestone Date.

2.9.5. The Supplier shall provide support to Internal Users in the first use of the functionality introduced from the ATP Milestone Date for a period of twenty (20) Working Days during Normal Working Hours. For the avoidance of doubt, the provisions of this Paragraph 2.9.5 does not relate to resolution of Service Incidents.

2.9.6. The Supplier shall support the Authority in undertaking Internal User engagement, in the form of system demonstrations and "show and tells".

2.9.7. The Supplier shall support the Authority in producing a User communications campaign that shall enable the following objectives to be achieved:

(a) notify Registered Users that the management of their Accounts is being transferred to the Supplier; and

(b) inform Users of any relevant changes to the manner in which the Services are being provided.

2.9.8. The Supplier shall agree the content of Messages used in each Contact Channel with the Authority prior to the Business Readiness and Private Beta Milestone.

2.9.9. The Supplier shall agree the "look and feel" and content used in each Contact Channel with the Authority prior to the Business Readiness and Private Beta Milestone.

2.9.10. The Supplier shall support the Authority in producing the Training Needs Analysis[1].

2.9.11. The Supplier shall produce a Training Plan for each Internal User group (as set out in Paragraph 2.9.15) and a Training Plan using a Train the Trainer methodology (as set out in Paragraph 2.9.16).

2.9.12. The Supplier shall produce a System Manual, which the Authority can use to develop internal procedural documents.

2.9.13. The Supplier shall prepare simple scenario-based training which allows Internal Users to practice aspects of their role in the Training Environment.

2.9.14. The Supplier shall prepare e-Learning Modules (lasting no more than thirty (30) minutes) which demonstrates how Internal Users use the Supplier Solution.

2.9.15. The Supplier shall provide five (5) virtual (remote) training sessions, assumed to be no more than six (6) hours, on all relevant elements of the Supplier Solution to 50

[redacted]

Internal Users (ten (10) per training session) using a Train the Trainer methodology prior to the Business Readiness and Private Beta Milestone[2].

2.9.16. The Supplier shall provide ten (10) virtual (remote) training sessions, assumed to be no more than two (2) hours, on the Duty Officer elements of the Supplier Solution to ten (10) Internal Users per training session prior to the Business Readiness and Private Beta Milestone[3].

2.9.17. The Supplier shall report on training completion rates to the Authority.

2.9.18. The Supplier shall ensure all training materials comply with any training standards as set out in Schedule 4 (*Standards*).

2.9.19. The Supplier shall support the Authority in producing the materials required for, and participate in, the Beta Service Assessment.

2.9.20. The Supplier shall Test the Supplier Solution with a limited number of Users prior to full deployment (**"Private Beta"**)[4]. The Authority has assumed that Owner Areas can be utilised as an early adopter for the purposes of Private Beta, and that Private Beta could be conducted by Owner Area or catchment, by type of Message (e.g. Operational Message), or by type of User (e.g. Organisations).

2.9.21. The Supplier shall ensure that the Private Beta testing conducted pursuant to Paragraph 2.9.20:

(a) covers an end-to-end journey (e.g. from Account Registration to receipt of a Message);

(b) replicates the post-ATP Live Environment as far as is practicable;

(c) is not dependent on weather or flooding conditions;

(d) doesn't require Internal Users to issue Messages in both the Supplier Solution and the Outgoing Supplier's system;

(e) enables External Users who have Registered for an Account to get Messages they have Registered to receive; and

(f) demonstrates an exercise with Internal Users and External Users to test an end-to-end journey for a wide range of operational scenarios.

3. OPERATIONAL SERVICES

3.1. Non-functional requirements

3.1.1. The non-functional requirements are set out in Annex A.

3.2. Functional requirements

3.2.1. The functional requirements are set out in Annex B.

3.3. Integration requirements

3.3.1. The integration requirements are set out in Annex C.

3.4. Service management requirements

General management

3.4.1. The Supplier shall undertake all the IT Service Management general management practices as set out in ITIL and the Standards in Schedule 4 (*Standards*) Paragraph 7 (*Service Management Software & Standards*) in order to deliver the Operational

[redacted]

Services. The Supplier shall integrate their ITSM activities in accordance with the principles set out in the Authority's Service Run Manual.

3.4.2. The Supplier shall maintain the Documentation (including training materials) throughout the Term to ensure it is consistent with the current version of the Supplier Solution.

3.4.3. The Supplier shall support the Authority in producing the materials required for, and participate in, the Live Service Assessment in the period of eighteen (18) months following the ATP Milestone Date and then support the Authority in producing the materials required for, and participate in, any subsequent Service Assessments required for any major New Releases.

3.4.4. The Supplier shall propose, and the Parties shall agree, a methodology to calculate the "cost per transaction" metric[5] in the Management Reports.

3.4.5. The Supplier shall produce reports, ideally in real time but in any case no less frequent than monthly, which document the usage of the Supplier Solution (the **"Management Reports"**). The Management Reports shall set out, as a minimum:

(a) Cost per transaction;

(b) Completion rate;

(c) Digital take up;

(d) Increase/decrease in the number of Registered Users;

(e) Increase the number of 'active' Users;

(f) Digital take up or channel shift (e.g. moving users from phone to SMS);

(g) Number of Users per Contact Channel;

(h) Number of Registrations per Contact Channel;

(i) Number of Account Preferences updates per Contact Channel;

(j) Number of Account Closures per Contact Channel;

(k) Number of Unregistered Users who have opted in;

(l) Number of Unregistered Users who have opted out;

(m) Number of Warnings issued;

(n) Number of successful and unsuccessful Notifications sent per Contact Channel;

(o) Number of users who go on to find more information from Messages per Contact Channel;

(p) Click throughs;

(q) Bouncebacks;

(r) User satisfaction.

3.4.6. The Supplier shall manage the relevant Telephone Operators in provision of the Services.

3.4.7. The Supplier shall ensure its continual improvement processes and procedures incorporate the requirements of Clause 8 (*Services Improvement*).

3.4.8. The Supplier shall ensure its measurement and reporting processes and procedures incorporate the requirements of Schedule 3 (*Performance Levels*).

[5] https://www.gov.uk/service-manual/measuring-success/measuring-cost-per-transaction

3.4.9. The Supplier shall ensure its information security management processes and procedures incorporate the requirements of Schedule 5 (*Security Management*).

3.4.10. The Supplier shall ensure its service validation and testing processes and procedures incorporate the requirements of Schedule 14 (*Testing Procedures*).

3.4.11. The Supplier shall ensure its financial management processes and procedures incorporate the requirements of Schedule 18 (*Financial Distress*) and Schedule 19 (*Financial Reports and Audit Rights*).

3.4.12. The Supplier shall ensure its knowledge management and records management processes and procedures incorporate the requirements of Schedule 19 (*Financial Reports and Audit Rights*) Part B (*Financial Reports*), Schedule 24 (*Reports and Records Provisions*) and Schedule 25 (Exit Management) Paragraph 2 (*Obligations During the Term to Facilitate Exit*).

3.4.13. The Supplier shall ensure its governance processes and procedures incorporate the requirements of Schedule 21 (*Governance*).

IT Service Management

3.4.14. The Supplier shall undertake all the IT Service Management service management practices as set out in ITIL and the Standards in Schedule 4 (*Standards*) Paragraph 7 (*Service Management Software & Standards*) in order to deliver the Operational Services.

3.4.15. The Supplier shall provide Second Line Support and Third Line Support for the Supplier Solution. The Authority shall provide First Line Support for the Supplier Solution as set out in Schedule 7 (*Authority Responsibilities*).

3.4.16. The Supplier shall provide an English speaking Help Desk aligned to the Standards in Schedule 4 (*Standards*) Paragraph 7 (*Service Management Software & Standards*), accessible as a minimum via phone and email, which shall serve as a single point of contact for First Line Support for all queries relating to support of the Supplier Solution.

3.4.17. The Supplier shall have an appropriate number of suitably skilled and experienced Supplier Personnel to operate the Help Desk during Operational Hours.

3.4.18. The Supplier shall store and maintain records of all communications to the Help Desk including, as a minimum, details and categorisation of what was received or sent, the communications transmitted, the date and time of communications received or sent, and User details.

3.4.19. The Supplier shall operate an access control regime for the Supplier System (as set out in Schedule 5 (*Security Management*) Annex 1 Paragraph 5 (*Identify, Authentication and Access Control*)) and notify Users within two (2) Working Days of any such access being granted. The Authority shall provide and maintain the list of the Authority's staff who are authorised by the Authority to access certain parts of the Supplier Solution as set out in Schedule 7 (*Authority Responsibilities*).

3.4.20. The Supplier shall inform the Authority of any Permitted Maintenance with ten (10) Working Days advance notification, in accordance with the Maintenance Schedule and Clause 9.4 to 9.6 (*Maintenance*). The Suppler shall facilitate a go/no-go discussion with the Authority on the day of the Permitted Maintenance so that major incidents (such as flooding or a disease outbreak) can be considered.

3.4.21. The Supplier shall undertake IT Change Management in accordance with ITIL and the Authority's Service Run Manual.

3.4.22. The Supplier shall monitor and manage the Supplier System.

3.4.23. The Supplier shall log software application errors in the Supplier Solution through an IT Service Management process that is controlled from receipt of the initial fault report to fix of the Supplier System.

3.4.24. The Supplier shall ensure that all Service Incidents, Problems and any associated Upgrades, Updates or New Releases are logged with the Help Desk.

3.4.25. The Supplier shall provide configuration documentation and release notes for each Upgrade, Update or New Release.

3.4.26. The Supplier shall operate an ITSM Toolset in delivery of its IT Service Management activities and provide access to the ITSM Toolset to the Authority. The ITSM Toolset shall be capable of integration with the Authority's ITSM Toolset (currently ServiceNow).

3.4.27. The Supplier shall ensure that the ITSM Toolset is able to segregate the Authority's data and metadata from the Supplier's other client's data and metadata captured using the same ITSM Toolset.

3.4.28. The Supplier shall ensure that the ITSM Toolset is able to track when Service Incidents, Problems, or other entries in the ITSM Toolset are set to breach a Performance Indicator.

3.4.29. The Supplier shall produce Knowledge Articles and record Knowledge Articles within the ITSM Toolset.

3.4.30. The Supplier shall ensure that the ITSM Toolset provides the capability to log and track and report issues, questions and User feedback in a structured and consistent format.

3.4.31. The Supplier shall produce Help Articles and record Help Articles within the Supplier System.

3.4.32. The Supplier shall keep all the Supplier Solution components within support in accordance with Clause 5.5(c).

3.4.33. The Supplier shall ensure its IT asset management processes and procedures incorporate the requirements of Clause 9.4 to 9.6 (*Maintenance*), Schedule 12 (*Software*) Paragraph 1 (*The Software*), and Schedule 32 (*Intellectual Property Rights*) Paragraph 1.6 and Paragraph 4 (*Open Source Publication*).

3.4.34. The Supplier shall ensure its service continuity management processes and procedures incorporate the requirements of Schedule 26 (*Service Continuity Plan*).

Technical management

3.4.35. The Supplier shall undertake all the IT Service Management technical management practices as set out in ITIL and the Standards in Schedule 4 (*Standards*) Paragraph 7 (*Service Management Software & Standards*) in order to deliver the Operational Services.

3.4.36. The Supplier shall use Training Environments and Testing Environments that simulate functionality of the Live Environment.

3.4.37. The Supplier shall minimise the use of Personal Data within the Testing Environments and the Training Environments.

3.4.38. The Supplier shall utilise a Testing Environment and a Training Environment that are distinct and separate from the Live Environment. For the avoidance of doubt, the Training Environment shall be Available during Operational Hours but the Supplier's performance against Subsidiary Performance Indicator 1 (SPI1) (Service Availability of the Training Environment) shall only be measured during Normal Working Hours. Should additional support be required for the Training Environment outside Normal Working Hours, then this shall be agreed in accordance with the Change Control Procedure and be charged in accordance with the principles set out in Schedule 15 (*Charges and Invoicing*).

3.4.39. The Supplier shall conduct training in the Training Environment and shall not use the Live Environment for conducting training.

3.4.40. The Supplier's Training Environments and Testing Environments shall be updated no later than seven (7) elapsed days to represent the relevant elements of the Live Environment and shall include any test harnesses, simulators and hardware/or software Upgrades, Updates or New Releases required in accordance with the Test Strategy.

3.4.41. The Supplier's Testing Environments shall use Good Industry Practice test automation tools to reduce the cost of Testing defined in Schedule 14 (*Testing Procedures*).

3.4.42. The Supplier's Testing Environments shall be correctly configured and available on an ongoing basis from the date of the first Test for the testing activities defined in the Test Strategy.

3.4.43. The Supplier's Testing Environments shall be maintained so as to generate consistent results from Tests (in accordance with the Test Strategy) that will allow new outputs to be comparable to baseline results.

3.4.44. The Supplier shall provide Users access to the Testing Environments to support Testing in accordance with Schedule 14 (*Testing Procedures*).

3.4.45. The Supplier shall make available sufficient business and operational IT equipment (hardware and software), IT processing power, IT storage and IT bandwidth to deliver the Services.

3.4.46. The Supplier shall manage and control the implementation activities and deployment event(s) of Software enhancements, Upgrades, Updates or New Releases to the Supplier Solution in accordance with ITIL Change Management and release and deployment management.

3.5. Product Backlog management

3.5.1. The Supplier shall create and maintain the Product Backlog for the Operational Phase. The Authority shall provide the initial list of Deliverables for the Product Backlog for the Operational Phase.

3.5.2. Throughout the Operational Phase, the Authority's Product Manager(s) and the Supplier shall conduct regular Sprint Planning Meetings to review the Product Backlog and shall agree a prioritisation for each Deliverable in the Product Backlog. In the event of a disagreement between the Parties regarding the prioritisation of the Product Backlog during the Operational Phase, the Authority's Product Manager shall provide the final decision.

3.5.3. In support of the Sprint Planning Meeting, the Supplier shall provide an estimate of the effort required to develop each Deliverable in the Product Backlog. The Supplier shall prepare these estimates with appropriate care and skill.

3.5.4. At the Sprint Planning Meetings, the Authority's Product Manager(s) and the Supplier shall identify the Deliverables in the Product Backlog which shall be delivered in the next Sprint.

3.5.5. Should the Authority want to commission a Sprint or a set of Sprints (each an **"Improvement Project"**), this shall be agreed in accordance with the Change Control Procedure. To support any Change Request, the Supplier shall produce the Sprint Backlog, which shall include the Definition of Done.

3.5.6. For the avoidance of doubt, each Improvement Project shall align with the scope as set out in Paragraph 1.2 and (unless otherwise agreed by the Authority in writing in the relevant Change Request) each Improvement Project shall:

(a) comply with the non-functional requirements as set out in Annex A;

(b) be incorporated into the IT Service Management regime as set out in Paragraph 3.4, upon completion of the Improvement Project until the expiry of the Term;

(c) be incorporated into the performance monitoring regime as set out in Schedule 3 (*Performance Levels*), upon completion of the Improvement Project until the expiry of the Term;

(d) comply with the Standards as set out in Schedule 4 (*Standards*);

(e) be incorporated into the security monitoring regime, and comply with the associated security requirements, as set out in Schedule 5 (*Security Management*), upon completion of the Improvement Project until the expiry of the Term;

(f) be designed, built, and tested in accordance with the principles as set out in the Test Strategy;

(g) be charged in accordance with the principles as set out in Schedule 15 (*Charges and Invoicing*);

(h) produce Documentation which is deposited in the Virtual Library and incorporated into the knowledge management and records management processes and procedures outlined in Schedule 24 (*Reports and Records Provisions*) and Schedule 25 (Exit Management) Paragraph 2 (*Obligations During the Term to Facilitate Exit*), upon completion of the Improvement Project until the expiry of the Term;

(i) be incorporated into any annual update to the Exit Plan as set out in Schedule 25 (*Exit Management*) Paragraph 5 (*Exit Plan*), upon completion of the Improvement Project until the expiry of the Term; and

(j) be incorporated into the service continuity planning regime as set out in Schedule 26 (*Service Continuity Planning*), upon completion of the Improvement Project until the expiry of the Term.

3.6. Social Value requirements

3.6.1. The Supplier shall implement measures in order to support the following Social Value policy outcomes:

Create new businesses, new jobs and new skills

(a) create opportunities for entrepreneurship and help new organisations to grow, supporting economic growth and business creation.

(b) create employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas, and for people in industries with known skills shortages or in high growth sectors.

(c) support educational attainment relevant to the contract, including training schemes that address skills gaps and result in recognised qualifications.

Effective stewardship of the environment

(d) deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions.

(e) influence staff, suppliers, customers and communities through the delivery of the contract to support environmental protection and improvement.

Tackle workforce inequality

(f) demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce.

(g) support in-work progression to help people, including those from disadvantaged or minority groups, to move into higher paid work by developing new skills relevant to the contract.

(h) demonstrate action to identify and manage the risks of modern slavery in the delivery of the contract, including in the supply chain.

Improve health and wellbeing

(i) demonstrate action to support health and wellbeing, including physical and mental health, in the contract workforce.

(j) influence staff, suppliers, customers and communities through the delivery of the contract to support health and wellbeing, including physical and mental health.

4. OPTIONAL SERVICES

4.1. A list of requirements to be delivered as part of the Optional Services is shown in Annex E.

Annex A – Non-Functional Requirements[6]

Group	ID	Requirement
		The Supplier shall ensure that the Supplier Solution
Compatibility	NF1	uses APIs which are based on RESTful or JSON, conforming to "API technical and data standards" where relevant (as set out in Schedule 4 (*Standards*)).
Compatibility	NF2	complies with industry open standards.
Compatibility	NF3	exposes its main functions as services.
Compatibility	NF4	exposes, uses and integrates services provided by other (external) systems.
Compatibility	NF5	has a flexible and open software architecture.
Compatibility	NF6	modules provide services that are published using the OpenAPI Specification (as set out in Schedule 4 (*Standards*)).
Compatibility	NF7	modules provide services that are described in such a way so they can be used by an (expert) third party.
Compatibility	NF8	shall be designed and built-in order to work with mobile devices for External Users.
Compatibility	NF9	provides the capability to enable interoperability of components.
Compatibility	NF10	has provisions for legacy integration using mechanisms such as an adapter framework.
Functional suitability	NF11	retains daily back ups of Authority Data for thirty-five (35) days and then archived with a retention period of seven (7) years, as set out in Schedule 24 (*Records and Reports Provisions*) Paragraph 3 (*Records*).
Functional suitability	NF12	disposes of Authority Data in accordance with Schedule 5 (*Security Management*) Annex 1 (*Security Requirements*) Paragraph 5 (*Data Destruction or Deletion*).
Functional suitability	NF13	retains back ups of Authority Data for non-Live Environments in a similar manner to that taken for Live Environments with a retention period of six (6) months.
Functional suitability	NF14	is designed in accordance with the standards and policies listed in Schedule 4 (*Standards*).
Functional suitability	NF15	adheres to the open standards requirements as set out in Schedule 4 (*Standards*) Paragraph 4 (*Open Data Standards and Standards Hub*).
Functional suitability	NF16	complies with Authority's password policy.
Functional suitability	NF17	can use version management for Source Code and Documentation.
Maintainability	NF18	provides the capability to enable maintainability of components without a disproportionate impact on other components.
Maintainability	NF19	provides the capability to enable enhancement of components without disproportionate effort.
Maintainability	NF20	provides the capability to enable re-usability of components.
Performance efficiency	NF21	is designed to minimise the total ongoing running cost of the Supplier Solution, including operating and maintenance costs.
Performance efficiency	NF22	has the minimum capacity to support the following number of concurrent Users: (a) 100 Duty Officers; (b) 20 Flood Resilience Officers;

[6] The quality model within ISO 25010 has been used to categorise the non-functional requirements.

Group	ID	Requirement
		The Supplier shall ensure that the Supplier Solution
		(c) 10 System Administrators; (d) 20 Floodline Contact Centre Agents; (e) 1,000 External Users including the support for at least 6,000 Account Registrations per day at a maximum rate of 1,500 Account Registrations per hour. For the avoidance of doubt, if additional capacity is required then the Charges shall be recovered from the Authority in arrears in accordance with the Change Control Procedure and be charged in accordance with the principles set out in Schedule 15 (Charges and Invoicing).
Performance efficiency	NF23	is resilient in the event of peaks in demand.
Performance efficiency	NF24	is resilient to the volume of stored Authority Data without degradation of the Services during peaks in demand.
Performance efficiency	NF25	shall be scalable, not requiring disproportionate effort to meet changing Authority requirements.
Performance efficiency	NF26	has the initial storage capacity to support the following numbers of records: (a) 10,000,000 Messages (email, phone call and SMS); (b) 10,000 operational Target Areas[7]; (c) 20,000 deactivated Target Areas; (d) 4,000 Partner operational boundary polygons; (e) 500,000 User locations (point, line, polygon); (f) 3,000,000 telephone numbers; (g) 3,000,000 email address; (h) 3,000,000 text numbers; (i) 3,000,000 addresses; (j) 680 Duty Officers; (k) 190 Flood Resilience Officers; (l) 20 System Administrators; (m) 140 Floodline Contact Centre Agents; (n) 1,500,000 External Users.
Performance efficiency	NF27	has the capacity to create 5,000 Messages and issue 75,000 Notifications per hour.
Performance efficiency	NF28	has the capacity to process 100,000 changes to Unregistered Users to per week.
Performance efficiency	NF29	can provide bandwidth to support the equivalent calling capacity of a minimum of 750 connections which can be increased to 2,000 connections as required which will be shared with IVR and must support VOIP.
Performance efficiency	NF30	can designate a minimum 10% of the connections to be made available to IVR as a default which can then be increased as required.
Performance efficiency	NF31	shall take no more than 10 seconds from an Internal User logging in to being fully available.

[7] The cumulative storage capacity for Target Areas shall not exceed 20GB. For the avoidance of doubt, if additional capacity is required then this shall be agreed in accordance with the Change Control Procedure and be charged in accordance with the principles set out in Schedule 15 (*Charges and Invoicing*).

Group	ID	Requirement
		The Supplier shall ensure that the Supplier Solution
Performance efficiency	NF32	is able to issue a Notification within 3 minutes of an Internal User logging in and that the Notification must be available on all supported Contact Channels at the same time as it is issued.
Performance efficiency	NF33	can make its first contact attempt (to the Users preferred Contact Channel) within 15 minutes of a Notification being issued for 95% of all Users, measured within a 24 hour period and based on a 60 second message. The remaining 5% to be dealt with within the following hour.
Performance efficiency	NF34	has the capacity to issue the following number of Notifications per annum via each Contact Channel: (a) SMS (text) = 3,000,000. (b) E-mail = Unlimited. (c) Audio (Text-to-Speech) = 2,000,000[8]. (d) Calls made to the IVR = 45,000. (e) Messages published to the IVR = 35,000. and shall be expandable to meet future needs. For the avoidance of doubt, if additional capacity is required then this shall be agreed in accordance with the Change Control Procedure and be charged in accordance with the principles set out in Schedule 15 (*Charges and Invoicing*).
Performance efficiency	NF35	provides latency that is acceptable to Users (at a minimum, response time to be no greater than 3 seconds).
Performance efficiency	NF36	shall index data for fast searching.
Performance efficiency	NF37	provides adequate bandwidth to enable satisfactory User experience.
Performance efficiency	NF38	utilises relational data models for storage and retrieval of data.
Performance efficiency	NF39	shall not adversely affect the Authority System.
Portability	NF40	uses Cloud Service Deployment Models to deliver a modern IT platform and more efficient Services.
Portability	NF41	uses Cloud Service Models to deliver a modern IT platform and more efficient Services.
Portability	NF42	consists of discrete pieces of software (modules) that provide application functionality through well-defined services to other modules and applications.
Portability	NF43	modules provide services that impose low consumer coupling and that themselves are decoupled from its surrounding environment.
Portability	NF44	is supplied as a cloud-based software service.
Portability	NF45	provides the capability to enable portability of Authority Data and Specially Written Software to alternative architectures or platforms.
Reliability	NF46	uses a Disaster recovery site which shall be kept at a safe distance in accordance with Good Industry Practice to eliminate the risk of both sites being made unavailable at the same time due to any unforeseen Disaster.
Reliability	NF47	automates monitoring of the Supplier Solution to optimise the delivery of the Services.
Reliability	NF48	provides a Disaster recovery site in accordance with Good Industry Practice and the requirements of Schedule 26 (*Service Continuity Plan*) to allow full recovery of the Services should the primary site fail. For the avoidance of doubt, should the Disaster recovery site be required in any one (1) Service Period then the Charges shall be recovered from the Authority in arrears in accordance with the Change Control Procedure and be charged in accordance with the principles set out in Schedule 15 (Charges and Invoicing).

[redacted]

Group	ID	Requirement
		The Supplier shall ensure that the Supplier Solution
Reliability	NF49	is able to fully restore Authority Data taken for each system component.
Reliability	NF50	will be capable of 'rolling back' to a known working state should the introduction of an Upgrade, Update or New Release be found to be causing Service Incidents and Problems in the Live Environment.
Reliability	NF51	will be resilient to multiple and cascading subsystem failures.
Reliability	NF52	has a function that logs all commands generated by the software applications/modules and Users.
Reliability	NF53	has a back-up regime that complies with the requirements of Clause 18 (*Authority Data and Security Requirements*). The back-up regime shall have no impact on the Live Environment and shall be stored in a secure location separate to the Live Environment.
Reliability	NF54	produces audit logs.
Reliability	NF55	can be recovered with no more than fifteen (15) minutes data loss following a system failure (the **"Recovery Point Objective"** or **"RPO"**).
Reliability	NF56	will have a maximum time to recovery (the **"Recovery Time Objective"** or **"RTO"**) of sixty (60) minutes or less.
Security	NF57	enables effective use of role-based access control and measures (such as those set out in Schedule 5 (*Security Management*) Annex 1 Paragraph 5 (*Identity, Authentication and Access Controls*)), such as Single Sign-on to remove any need for Internal Users to re-authenticate needlessly. The Supplier Solution shall allow Internal Users to be assigned multiple roles.
Security	NF58	automatically logs Users out of the service after 29 minutes of inactivity, unless the User's permissions have been set to a different period of inactivity.
Security	NF59	NOT USED
Security	NF60	creates a new session every time a User logs into the Supplier Solution.
Security	NF61	allows a logged in User to be in more than one active session at the same time.
Security	NF62	will record all system activity (e.g. who has accessed the system, record creation and amendment dates etc.) and for this to be recorded in the audit log.
Security	NF63	complies with the security requirements set out in Schedule 5 (Security Management).
Security	NF64	applies the 'principle of least privilege' and uses role-based access control to minimise visibility of Authority Data and Personal Data (e.g. anonymisation of Unregistered Users contact details).
Usability	NF65	provides the capability to provide access to all Services and Environments through an appropriate User Interface.
Usability	NF66	uses colour in presentation of information to support Users in the processes of completing the required operational task.
Usability	NF67	has a screen lay-out which supports Users in the processes of completing the required operational task.
Usability	NF68	has a User Interface which is consistent as to the design of controls, warnings, indicators and layout of presentation elements.
Usability	NF69	has a User Interface which draws the natural focus of Users to the place where attention is required to complete the required operational task.
Usability	NF70	is accessible to Users who have communication difficulties stemming from a protected characteristic as set out in the Equality Act, with the outcome not being inferior in terms of quality or standard.

Group	ID	Requirement
		The Supplier shall ensure that the Supplier Solution
Usability	NF71	has a User Interface for External Users which meets (or exceeds) the accessibility standards as set out in Schedule 4 (*Standards*) Paragraph 6 (*Accessible Digital Standards*). The Supplier shall use reasonable endeavours to ensure that the Supplier Solution has a User Interface for Internal Users that works towards the principles contained in the same accessibility standards.
Usability	NF72	has a User Interface which supports the avoidance of erroneous input (e.g. using data validation, on screen tips and context dependent Help Articles being available, standard validation rules to prevent entry of any special characters other than letters). Currently known exceptions are listed below: (a) Welsh characters; (b) apostrophes; (c) dashes; (d) ampersand (not permitted in name fields); (e) normal brackets (not permitted in name fields); (f) number 0-9 (not permitted in name fields).
Usability	NF73	has a User Interface which supports experienced Users by providing quick entry input means.
Usability	NF74	has a User Interface which supports the overall objective for efficiency by providing an efficient experience for Users to minimise the delays in performing tasks. This shall include as a minimum: a) consideration of the number of clicks to carry out processes; b) presentation of information as to be readily identifiable as to its relevance; c) grouping of related functions to simplify processes; d) pre-filling of screens as Users progress through standard workflows; e) use of auto-complete; f) consistency.
Usability	NF75	enables persistence of User settings between sessions.
Usability	NF76	will ensure no User side software installation is required.
Usability	NF77	is capable of integration with the Authority's identity management service for Single Sign-on purposes (currently based on Active Directory).
Usability	NF78	provides an ergonomic User Interface.
Usability	NF79	provides latency that is acceptable to Users.
Usability	NF80	is designed and built to allow Users to access the Supplier Solution using the internet on their own device.
Usability	NF81	includes full, on-line and fully searchable user centred Help Articles within the Supplier System.
Usability	NF82	has a User Interface which includes context specific on-screen Help Articles.
Usability	NF83	Uses error messages which are meaningful, appropriate to the User and clearly displayed.
Usability	NF84	is designed and built to operate correctly on the list of browsers and devices included within "Designing for different browsers and devices" as set out in Schedule 4 (*Standards*).

Group	ID	Requirement
		The Supplier shall ensure that the Supplier Solution
Usability	NF85	User Interface used by External Users is designed and built in accordance with the GOV.UK Design System as set out in Schedule 4 (*Standards*).

Annex B – Functional Requirements

ID	Theme	Requirement The Supplier shall provide the capability	Corresponding user story[9]
WIP001	Public facing flood warning service	to increase the presence of the Services.	As a Citizen or Organisation, I need to know that there is a service so that I can decide if I want to use the service
WIP002	Public facing flood warning service	to allow Users to understand what the Supplier Solution offers.	As a Citizen or Organisation that is thinking about registering to use the service, I need information so that I can understand what I need from the flood warning service
WIP003	Public facing flood warning service	to allow Users to choose which Location(s) they want to get Messages for.	As a Citizen or Organisation, I need to choose locations so that I can receive warning messages for those locations
WIP003.1	Public facing flood warning service	to allow Users to register and manage a single address Location they want to get Messages for.	As a Citizen or Organisation, I need to register a single address location so that I can receive warning messages for my address location
WIP003.2	Public facing flood warning service	to allow Users to register and manage multiple address Location(s) they want to get Messages for.	As a Citizen or Organisation, I need to register multiple address locations so that I can receive warning messages for my address locations
WIP003.4	Public facing flood warning service	to allow Users to register and manage non address Location(s) they want to get Messages for.	As a Citizen or Organisation, I need to register a non-addressable location so that I can receive warning messages for my commute, my horse in a field or any other non-property related location
WIP003.5	Public facing flood warning service	to allow Users to register and manage an Operational Boundary they want to get Messages for.	As a Citizen or Organisation, I need to register operational boundary so that I can receive warning messages for my operational boundary
WIP004	Public facing flood warning service	to allow Users to Register for a single Account in order to get Messages via their preferred Contact Channel(s).	As a Citizen or Organisation, I need to provide relevant details so that I have a single registration for the service and will receive warning messages for my locations via my specified channels.
WIP004.1	Public facing flood warning service	for a User to Register Nominated Contact(s)to receive Messages on their behalf.	As a Citizen I need to register Nominated contact(s) to receive notifications on my behalf so that friends and family know when I'm at risk and can help me take action
WIP004.2	Public facing flood warning service	for a User to receive confirmation of Registration via their preferred Contact Channel following Account Registration.	As a Citizen or Organisation, I need to receive confirmation, following signing up so that I know I've successfully signed up to receive notifications when there is flood risk.
WIP004.3	Public facing flood warning service	for a User to be told that they already hold an Account and not allow an e-mail address or telephone number to be registered to more than one Account.	As a Citizen or Organisation, I need to know if I already have an account so that I don't create duplicate accounts when I subscribe
WIP004.6	Public facing flood warning service	for a User to see a summary of their chosen Messages for their Account.	As a Citizen I need to see a summary of what I have subscribed to receive so that I understand what I have subscribed to and can amend if I need to
WIP004.7	Public facing flood warning service	for a User to sign out of the Supplier Solution.	As a Citizen or Organisation, I need to sign out of the service so that I know I have finished my journey
WIP004.8	Public facing flood warning service	for a User to indicate whether they are a member of the public, a Public Sector Organisation, or a Non-Public Sector Organisation in the Account Registration process.	As a Citizen or Organisation, I need to specify if I am a citizen or organisation so that I am registering as the correct customer type
WIP004.11	Public facing flood warning service	for a User to register multiple Nominated Contacts within their Organisation to receive Messages.	As an Organisation I need to register multiple contacts to receive warnings so that all the contacts in my organisation are registered and can receive the same warnings

[9] These user stories have intentionally not been aligned to contractual definitions in order to provide contextual information to the contractual requirement.

ID	Theme	Requirement **The Supplier shall provide the capability**	Corresponding user story[9]
WIP005	Public facing flood warning service	to authenticate Users (and their contact details) through the lifecycle of an Account (e.g. from Account Registration to Account Closure).	As a Citizen or Organisation, that is registering to use the service I need to authenticate during registration so that I can be sure it will be me that will receive warning messages
WIP006	Public facing flood warning service	to allow Users to personalise their Account Preferences during Account Registration.	As a Citizen or Organisation, I need to customise options during registration so that I can receive warning messages appropriate to my needs
WIP007	Public facing flood warning service	for the Authority to provide an Assisted Digital capability.	As a Citizen or Organisation, that requires assisted digital or non-digital user support I need to be provided with assisted digital options so that I can sign up to be warned about the risk of flooding, update my account or leave the service
WIP008	Public facing flood warning service	to allow Users to receive Messages for multiple Locations.	As a Citizen or Organisation, I need to manage multiple locations and assets so that I can receive warning messages for those locations
WIP009	Public facing flood warning service	to Notify Users of any possible or imminent Risk of Flooding.	As a Citizen or Organisation, I need to be warned if there is imminent real risk to my locations or assets so that I can make relevant preparations
WIP010	Duty officer services	for Duty Officers to create a Message for a Target Area(s).	As a Duty officer I need to create the appropriate severity warning message containing the most accurate information for the locations identified so that I can publish the message as a warning
WIP010.3	Duty officer services	for Duty Officers to create a Message using a Message Template.	As a Duty Officer I need to create a warning message that contains both static and the latest situational information so that citizens and organisations have relevant advice and guidance
WIP010.4	Duty officer services	to allow Duty Officers to preview the Message as it will appear to Users before it is sent.	As a Duty Officer I need to see the full message before it's sent so that I can QA the message before its sent
WIP010.7	Duty officer services	to allow Duty Officers to create, edit, save and cancel a draft version of the Message.	As a Duty Officer I need to be able to create, edit, save and cancel a draft of the message so that they are sent out when required (e.g. in advance of a warning) or canceled if not needed
WIP010.9	Duty officer services	to allow Duty Officers to add additional information to the Message which will only be seen by selected Users (e.g. emergency partners).	As a Duty Officer I need to be able to enter additional sensitive information that is sent in a message to our partners only so that members of the public do not see this sensitive information, but our partners are aware of it
WIP010.11	Duty officer services	to allow Duty Officers to create a Message that is phonetically correct for IVR and voice Contact Channels (using text to speech technology).	As a Duty Officer I need to be able to create messages that will be sent phonetically to telephone and IVR so that messages will be delivered clear and phonetically correct to the recipient
WIP010.13	Duty officer services	to allow Duty Officers to view the number of Users that the Message will be sent to before they send the Message.	As a Duty Officer I need to have information about the number of subscribed users the message will be sent to so that I can understand the impact when I send the message out
WIP010.14	Duty officer services	to store different pronunciations of place names which can be used when a Duty Officer sends a Message involving that Location.	As a Duty Officer I need the system to store local dialect versions of a place name word (i.e. a local phonetic dictionary) so that these are used when the message is read out over the phone so the local citizens understand what area could be affected by flooding

ID	Theme	Requirement **The Supplier shall provide the capability**	Corresponding user story[9]
WIP010.15	Duty officer services	to allow Duty Officers to view Messages previously issued to that Target Area and use that Message content as an initial Message Template.	As a Duty Officer I need to be able to view previously sent messages for the target area so that I am not starting with a blank sheet of paper for each message I create and can use a previous message as an initial template
WIP010.20	Duty officer services	to notify a Duty Officer if a Message is being issued out of sequence, (e.g. if a Remove Message is being issued before a Warning).	As a Duty Officer I need to follow current "sequencing" logic when selecting or sending warnings and alerts so that messages aren't sent incorrectly
WIP011	Public facing flood warning service	to issue a Message(s) to Users and Downstream Systems.	As the Environment Agency we need to send the warning message via the relevant channels so that systems, citizens and organisations will receive the message I created
WIP011.2	Public facing flood warning service	to allow Duty Officers to understand the progress of a Message, how many Notifications have been sent, how many are in progress, and when all Notifications have been sent	As a Duty Officer I need confirmation that the message has been sent, is in progress and when it has reached its end point so that I don't need to manually check the message has been sent.
WIP011.5	Public facing flood warning service	to attempt Notification of all Messages immediately with the most urgent Messages prioritised in accordance with the Message Priority.	As a Duty Officer I need all messages to be sent immediately but if there is any delay the most urgent and/or severe messages to be sent as priority so that the most urgent messages are sent out first
WIP011.7	Public facing flood warning service	to re-send Notifications if the original Notification has not been successfully sent or delivered/received based on an agreed methodology.	As a Duty Officer I need if a message was not sent successfully to re-try to send that message based on an agreed methodology so that messages are re-sent if they did not get through successfully (e.g. phone was engaged when originally sent) and the user gets the message
WIP011.8	Public facing flood warning service	for Duty Officers to view the Notification delivery status rates for each Contact Channel.	As a Duty Officer I need to be able to view the message delivery success rates for telephone, text and email so that a decision can be made as to whether the message needs to be re-issued
WIP011.10	Public facing flood warning service	for Duty Offices to issue a Message if the if the Authority System is unavailable (e.g. due to a failure of the Authority's Active Directory, end user devices, network etc.).	As a Duty Officer I need to be able to issue a message even if the EA network is unavailable so that citizens and organisations receive the message
WIP012	Duty officer services	to allow Duty Officers to update Warnings with the latest Situational Information available and issue a Message(s) to Users and Downstream Systems.	As a Duty Officer I need to update published warning messages so that citizens and organisations have the most up to date information
WIP012.8	Duty officer services	for Duty Officers to view Messages that are currently in force that have been issued across England and specific Target Areas.	As a Duty Officer I need to see the warnings that have been issued across England and for specific areas so that I know the warnings I'm currently responsible for updating
WIP013	Duty officer services	to allow Duty Offices to remove Warnings when there is no longer a Risk of Flooding or remove Messages when a Message has been issued in error.	As a Duty Officer I need to remove published warning messages when they are no longer in force so that citizens and organisations know the risk of flooding has passed
WIP014	Public facing flood warning service	to ensure that Messages the Authority sends to Users are relevant to their needs and are meaningful to Users.	As a Citizen or Organisation I need to receive flood warning notifications that are relevant and accurate so that I am aware of the risk of flooding
WIP014.11	Public facing flood warning service	to issue a Welcome Message to any new Unregistered Users in current Target Areas with options to allow them to Register or "opt out" of further Notifications.	As the Environment Agency I need to send a welcome text message to all new unregistered mobile contacts and a telephone message to all new unregistered landline contacts so that new unregistered contacts in current target areas are aware of the service and have the option to register or cancel

ID	Theme	Requirement The Supplier shall provide the capability	Corresponding user story[9]
WIP014.12	Public facing flood warning service	to identify new contact details in cooperation with Telephone Operators for Unregistered Users so that a Welcome Message can be sent.	As the Environment Agency I need to identify all new contacts in existing Target Areas so that all new contacts added that month receive a welcome text message
WIP014.13	Public facing flood warning service	to issue a Welcome Message to new Unregistered Users when a Target Area is updated or created with options to allow them to Register or "opt out" of further Notifications.	As the Environment Agency I need to send out a welcome message to all new unregistered contacts when Target Areas are updated or created so that all new unregistered contacts receive a welcome message and given the option to opt out
WIP014.14	Public facing flood warning service	ensure the Welcome Message content can be configured.	As the Environment Agency I need to include information about the service in the welcome message so that all new contacts can learn about the flood warning service
WIP015	Public facing flood warning service	for Users to give feedback.	As a Citizen or Organisation I need a mechanism to provide feedback about the service and quality of the messages so that the Environment Agency can take steps to improve the service
WIP015.6	Public facing flood warning service	for Users to give (optional) feedback on what action a User has taken after receiving the Notification.	As the Environment Agency I need a mechanism to measure what action a user took after receiving a flood warning or alert so that the Environment Agency can measure if the service is a success and take steps to improve the service
WIP016	Public facing flood warning service	for Users to manage their Account Preferences from Account Registration to Account Closure.	As a Citizen or Organisation I need to be able to update my account information so that my details are up to date
WIP017	Internal services	to create or Ingest, maintain, export, and Publish Target Areas. For the avoidance of doubt the Supplier Solution will be the authoritative source of Target Area data (both text and geographic).	As a Flood Resilience Officer I need to be able to maintain target areas so that they can be published for consumption by flood services
WIP017.1	Internal services	to ensure that Target Area data (i.e. shapefiles) created outside of the Supplier Solution can be Ingested into the Supplier Solution.	As a Flood resilience team member I need the ability to upload target area data (e.g. shapefile) if created outside of the system so that I have the relevant target area data in the system to use as required
WIP017.2	Internal services	to ensure that Target Area data can be exported and Published, using the relevant standard(s), to all Downstream Systems that currently use the Target Area data (including for use in desktop GIS) using a combination of automated processes and manual export as appropriate.	As a Flood resilience team member I need Target Areas to be published for export to systems so that all systems using Target Area data have the latest information
WIP017.4	Internal services	to define the status of Target Areas to enable any follow-on process.	As a Flood resilience team member I need to be able to set a status for Target Areas and view this so that I know the relevant status of any target area to know what I may need to do next (e.g. which ones are due for publication next from an update)
WIP017.7	Internal services	to allow Flood Resilience Officers to add Target Areas to requests to update contact details for Unregistered Public Users.	As a Flood resilience team member I need to know that all active target areas submitted to request contact details of unregistered users will be populated with up to date contacts so that the process can continue with the correct target area data
WIP017.14	Internal services	to add new data to the Supplier Solution for testing, user research and Private Beta.	As a Service for private beta I need to have fixed set of data for target areas during initial private beta phase (Possibly the current API) so that we can link contact data to location data during private beta
WIP017.15	Internal services	to allow Duty Officers to view the Target Area for the Message on a map when the Message is being created.	As a Duty Officer I need to be able to view target area data on a map when preparing to issue a warning so that I can be sure I am issuing a warning to the correct target area

ID	Theme	Requirement **The Supplier shall provide the capability**	Corresponding user story[9]
WIP017.16	Internal services	to create and store Target Area standard information which can be used when Duty Officers are creating the Message.	As a Duty Officer I need to be able to create and have a store of target area standard information which can be used when creating messages so that I can save time when creating the message and have the text at hand I can use.
WIP017.17	Internal services	to create and store Location specific information (e.g. code, name etc.) which will then be available for inclusion in Messages and on Downstream Systems.	As a Flood resilience team member I need to populate and store location specific information for a target area so that relevant information is available for inclusion in messages and on downstream systems
WIP017.20	Internal services	to ensure that any Internal User updating or creating a Target Area can identify the number of External Users that may receive Notifications.	As a Flood resilience team member I need to be able to identify who may receive messages from any target area I create or update so that I can understand the impacts of any changes I make
WIP017.21	Internal services	for Messages to be prepared for issue together for pre-defined groups of Target Areas.	As a Flood resilience team member I need to be able to pre-define a group of target areas that can be prepared for issue together so that duty officers can efficiently issue to an appropriate group of target areas.
WIP017.22	Internal services	to ensure that each Target Area has a designated Owner Area.	As a System Admin I need to ensure that each target area has a designated owner area so that ownership and maintenance responsibilities are clear
WIP018	Internal services	to issue Messages to Unregistered Users in a Target Area.	As a Service Manager I need to ensure business rules and requirements are followed so that messages can be sent to unregistered users
WIP019	Internal services	for System Administrators to manage Accounts throughout their lifecycle (e.g. from Account Registration to Account Closure).	As the Environment Agency we need administration functionality to create, update and remove accounts for internal and external users so that the system is up to date with the latest information
WIP019.7	Internal services	to allow access to the Supplier Solution to permitted Organisations, provided they are an authenticated User.	As an External partner organisation I need access to the service so that I can log in to the service as an authenticated user to my account
WIP020	Internal services	for System Administrators to have functionality in order to maintain and configure the Supplier System (e.g. new roles, new permissions, new business rules, Target Areas, Message Templates,).	As the Environment Agency we need functionality for any system administration required so that the system is up to date and has relevant information and business rules to run smoothly
WIP020.4	Internal services	to ensure Unregistered Users contact data is not visible to any Users without the relevant permissions.	As the Environment Agency we need all unregistered user contacts to not be visible to staff so that contact numbers are not visible in the system
WIP020.13	Internal services	to allow System Administrators to update Users with important notifications when they log into the Supplier Solution.	As a Admin I need to be able to update users with important notifications when they log into the system so that users are aware of any notifications that they need to be aware of
WIP021	Internal services	to interrogate Authority Data held within the Supplier System, create ad-hoc reports, and run standard reports and dashboards.	As the Environment Agency we need reporting and dashboard functionality so that we can understand the number of warnings, warning information, users, etc
WIP021.7	Internal services	to allow permitted Internal Users to run reports on the level of user satisfaction with the Supplier Solution.	As the Environment Agency I need to see user satisfaction with the service so that we can evaluate performance
WIP021.8	Internal services	to allow permitted Internal Users to run reports on the cost per transaction (subject to Paragraph 3.4.4) to use the Supplier Solution.	As the Environment Agency I need to see cost per transaction so that we can evaluate performance

ID	Theme	Requirement	Corresponding user story[9]
		The Supplier shall provide the capability	
WIP021.9	Internal services	to allow permitted Internal Users to run reports on journey completion rates for External Users of the Supplier Solution.	As the Environment Agency I need to see completion rate for user journeys so that we can evaluate performance
WIP021.10	Internal services	to allow permitted Internal Users to run reports to understand the digital take up of the Supplier Solution.	As the Environment Agency I need to understand the level of digital take up for the service so that we can evaluate performance
WIP022	Internal services	create and maintain Help Articles in the Supplier Solution.	As Environment Agency users we need access to information to give advice and guidance on creating messages, target areas or other functionality and for system admins to be able to create and amend that guidance so that we are aware of the correct procedures to follow
WIP023	Internal services	to allow Users to practice and train on use of the Supplier Solution within a Training Environment.	As Environment Agency users we need a system to allow us to practice and train new duty officers so that users know how to use the system before they use it in real time
WIP024	Internal services	to monitor the performance of the Services.	As the Supplier we need to monitor the performance of the services so that we are aware of any errors or issues that need to be resolved
WIP025	Internal services	to integrate the Authority System with the Supplier Solution, as set out in Annex C.	As the Environment Agency we need to ensure all systems are integrated so that the whole service works properly across the flood estate
WIP026	Internal services	for System Administrators and Floodline Contact Centre Agents to manage Account Preferences on behalf of Users.	As the Environment Agency we need to ensure Area Advisor users can manage the service in order to meet internal business needs and processes
WIP027	Public facing flood warning service	for Users to understand the Common Operational Picture for their Locations.	As an organisation user I need reporting functionality so that I can understand the number of locations, warnings, users, for my organisation
WIP027.9	Public facing flood warning service	for an Organisation to view information showing previous activity within the Supplier Solution for the Organisation.	As an Organisation user I need to see a report that shows all previous activity for locations for an organisation so that I can review the flood risk and make appropriate response plans
WIP028	Internal services	for Internal Users to understand the Common Operational Picture for Organisations.	As the Environment Agency we need reporting functionality so that we can understand the number of warnings, warning information, users, for any (or all) organisations
WIP028.9	Internal services	for the Authority to view or produce reports showing all activity for any or all Organisation(s).	As a System Admin I need to view or produce reports that shows all previous activity for any or all organisation(s) so that I can review activity on the service
WIP030	Public facing flood warning service	to allow Users to Close their Account.	As a Citizen or Organisation I need to be able to remove my account information so that my details are up to date
WIP032	Public facing flood warning service	to operate the following outbound Contact Channels (which enables the Message types to be sent as set out in Annex D), as a minimum: (a) SMS (text); (b) e-mail; (c) audio (**"Text-to-Speech"**); (d) website; (e) CAP XML;	As the Environment Agency I need a set of contact channels for the service so that citizens and organisations can sign up to the contact channels, notifications are sent via those channels and the service can operate using those channels

ID	Theme	Requirement **The Supplier shall provide the capability**	Corresponding user story[9]
		(f) IVR; (g) post.	
WIP033	Internal services	for Internal Users to issue an Emergency Alert.	As the Environment Agency I need to create the emergency alert message containing relevant information to send to the emergency alert service so that the message can be sent to the general public in the Emergency Alert area
WIP033.6	Internal services	for Internal Users to cancel an Emergency Alert.	As the Environment Agency I need to cancel the emergency alert message so that the message will not longer be sent to the general public in the Emergency Alert area
WIP033.5	Internal services	to create and send a simplified polygon of the Target Area to the Downstream Systems that require this e.g. Emergency Alerts.	As a Duty Officer I need to create and send a simplified polygon of the target area to the service that will issue the Emergency Alert (i.e.Notify) so that citizens and organisations will get the Emergency Alert for the affected target areas
WIP034	Public facing flood warning service	for an IVR service to provide real time flooding information to Users.	As a Citizen or Organisation I need access to an IVR service so that I can get flood warning information in order to take action
WIP031.8	Public facing flood warning service	to direct Users from the Supplier's IVR to the Floodline Contact Centre IVR when Users of the Supplier's IVR choose the option to get further assistance.	As the Environment Agency I need to be able direct users from the suppliers IVR to Floodline Contact Centre IVA so that users can get further assistance as required
WIP034.3	Public facing flood warning service	to automatically recognise an External User through the phone number of the User calling the IVR service and for that External User to be offered information relevant to them.	As a Citizen I need to be automatically recognised through my phone number when calling the IVR so that I am offered to be played flood warning information relevant to me
WIP034.4	Public facing flood warning service	to ensure External Users can access information via the IVR specific to that External User from the links within the Notification without needing to navigate any call plan routing.	As a Citizen I need to be able to access IVR information as easily as possible using links within the message I have received so that I can take appropriate action during an event
WIP034.5	Public facing flood warning service	to allow External Users to access information via the IVR using their existing Quickdial code.	As a Citizen I need to be able to access IVR information using my existing Quickdial code so that I am offered to be played flood warning information relevant to me
WIP034.6	Public facing flood warning service	to allow External Users to find and access information via the IVR using a self-service search functionality.	As a Citizen I need to be able to find and access IVR information using a self-service search functionality so that I am offered to be played flood warning information relevant to me
WIP035	Internal services	for System Administrators to create and maintain Message Templates for different Message types.	As the Environment Agency we need administration users to have functionality in order to maintain and configure message templates for different type of message so that messages are well formatted and nationally consistent
WIP036	Internal services	to enable the Authority to communicate to Users about their Account.	As the Environment Agency we need functionality in order to communicate to our registered users so that we can keep our records updated and keep users informed about the service
WIP037	Internal services	for Internal Users to send Operational Messages.	As the Environment Agency I need to create the appropriate operational message containing the relevant information so that it can be sent as an operational message to relevant users
WIP038	Public facing flood warning service	to automatically issue Messages when a specific threshold has been exceeded.	As a Duty Officer I need a warning to be issued automatically when a threshold is exceeded so that the lead time to warn a community is reduced

Annex C – Integration Requirements

ID	Requirement
	The Supplier shall provide the capability
INT001	to Ingest Ordnance Survey address data[10].
INT002	to Ingest automated Forecast Alarms from the Authority's flood forecasting system (**"IMFS"**).
INT003	to Ingest details of Unregistered Users (filtering out Unregistered Users who have previously "opted out") from Telephone Operators on a weekly basis as a minimum.
INT004	to Ingest Flood Risk Categories from the Authority's flood risk assessment system (**"NaFRA"**)[11].
INT005	to Publish Messages, Target Areas and other Authority Data via an API to third party systems in accordance with the Integration Specification.
INT006	to Publish Messages to FWIS.
INT007	to Ingest suitable digital map layers e.g. Ordnance Survey Mastermap[12].
INT008	to Publish Messages via the Common Alerting Protocol[13].
INT009	to Publish Messages to GOV.UK Notify Emergency Alerts[14].

INT002 – Current message content

This is the XML that IMFS posts to FWS in the body of an HTTP request when a warning needs to be sent.


```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>any unique reference</identifier>
  <sender>www.gov.uk/environment-agency</sender>
  <sent>sentDateTime eg 2018-06-19T15:30:00</sent>
  <status>System</status>
  <msgType>Alert</msgType>
  <source>IMFS</source>
  <scope>Restricted</scope>
  <restriction>For systems involved in England and Wales automated flood warnings</restriction>
  <code>triggerCode</code>
</alert>
```


===

There is also authentication in the request header:

===

[10] https://osdatahub.os.uk/docs/places/overview
[11] https://environment.data.gov.uk/dataset/8dcf3570-d465-11e4-a0f0-f0def148f590
[12] https://osdatahub.os.uk/docs/wmts/overview
[13] https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html
[14] https://docs.publishing.service.gov.uk/manual/notify-emergency-alerts.html

Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

======

Notes:

- There is functionality in the current Flood Warning System (FWS) that allows an administrative user to associate a message to send with a community to send that message to, and to then save that message-community combination, with unique reference code, as an "automation rule".
- There are currently over 4,000 such automation rules configured in FWS, each with a unique reference code (commonly referred to as the "trigger code").
- To instruct FWS to send a message, the triggering system (e.g., IMFS) posts an HTTP(S) request to an endpoint URL with the above XML in the request body/payload. The reference ("trigger") code of the automation rule that needs to be triggered is placed in the XML's <code> element. For security, the HTTP request needs to contain an API key in the request header (see above).
- (At present, IMFS takes no further action, regardless of the status or response-body content of the HTTP response from FWS.)
- The XML itself is adapted from the CAP XML standard – mainly because CAP XML was the design-standard for the transmission of XML within the EA at the time the API was developed. In reality, only the values in the <identifier>, <sent> and <code> elements are used by FWS, and a much simpler XML schema could have achieved the desired outcome. We are currently, however, committed to the XML in its current form, as this is what IMFS has been developed to transmit.
- There are also scripts in FWS that allow the 4,000+ automation rules to be bulk-created, activated, deactivated and deleted (to avoid these things having to be done manually).

INT006 – Current message content, published via HTTPs push, currently via the Flood Warning Information System (FWIS).


```
<?xml version="1.0" encoding="UTF-8"?>
<WarningMessage xmlns="http://www.environment-agency.gov.uk/XMLSchemas/EAFWD" approved="$<System Calender Day>/$<System Calendar Month>/$<System Year> $<System Time Hours (24hrs)>" requestId="" language="$<Target Area Language>">
        <TargetAreaCode><![CDATA[$<Target Area Code>]]></TargetAreaCode>
        <SeverityLevel>1</SeverityLevel>
        <InternetSituation><![CDATA[${Situation}]]></InternetSituation>
        <FWISGroupedTACodes><![CDATA[]]></FWISGroupedTACodes>
</WarningMessage>
```


INT008 – Current message content, published via HTTPs push to Common Alerting Protocol.


```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
    <identifier>$<Message Request ID></identifier>
    <sender>www.gov.uk/environment-agency</sender>
    <sent>$<System Date Time TZ (W3C)></sent>
    <status>Actual</status>
    <msgType>Alert</msgType>
    <source>Flood warning service</source>
    <scope>Public</scope>
    <info>
        <language>en-GB</language>
        <category>Met</category>
        <event><![CDATA[$<Message Set Name>]]></event>
        <urgency>Immediate</urgency>
```

```
        <severity>Minor</severity>
        <certainty>Likely</certainty>
        <expires>$<CAP XML Expiry Date +10days></expires>
        <senderName>Environment Agency</senderName>
        <description>A flood alert has been issued. <![CDATA[${Situation}]]></description>
        <instruction><![CDATA[# To check the latest information for your area

- Visit [GOV.UK](https://check-for-flooding.service.gov.uk) to see the current flood warnings, view river and sea levels or check the 5-day flood risk forecast: https://check-for-flooding.service.gov.uk
- Follow [@EnvAgency](https://twitter.com/EnvAgency) and [#floodaware](https://twitter.com/hashtag/floodaware) on Twitter.
- Tune into weather, news and travel bulletins on local television and radio.
- For access to flood warning information offline call Floodline on 0345 988 1188 using quickdial code: $<Target Area Quickdial>.

# What you should consider doing now

- Monitor local water levels and weather conditions.
- Get ready to act on your flood plan if you have one.
- Move your car or other vehicles to higher ground, if it is safe to do so.
- Prepare a flood kit of essential items including a torch with spare batteries, mobile phone and charger, warm clothes, home insurance documents, water, food, first aid kit and any prescription medicines or baby care items you may need.
- Check that you know how to turn off your gas, electricity and water mains supplies.
- In rural locations, farmers should consider moving livestock and equipment away from areas likely to flood.
- Avoid walking, cycling or driving through flood water - 30 cm of fast-flowing water can move a car and 6 inches can knock an adult off their feet.
- Flood water is dangerous and may be polluted. Wash your hands thoroughly if you’ve been in contact with it.

##### Businesses

- Keep your staff and customers informed about the situation.

For media enquiries please contact our media teams: https://www.gov.uk/government/organisations/environment-agency/about/media-enquiries]]>
        </instruction>
        <web>https://check-for-flooding.service.gov.uk</web>
        <contact>0345 988 1188</contact>
        <area>
            <areaDesc><![CDATA[$<Short TA Name>]]></areaDesc>
            <!-- variable below will create (possibly several) matching "polygon" tags -->
            $<Target Area Shape (simplified)>
            <geocode>
```

```
                <valueName>TargetAreaCode</valueName>
                    <value><![CDATA[$<Target Area Code>]]></value>
                </geocode>
            </area>
        </info>
</alert>
```

Annex D – Message types by Contact Channel

Message Type	Contact Channel							
	SMS (text)	E-mail	Audio (Text-to-Speech)	Website	CAP XML	IVR	Post	Emergency Alert via API
Welcome Message	Yes	No	Yes	No	No	No	No	No
Operational Message	Yes	Yes	Yes	No	No	Yes	No	No
Severe Flood Warning	Yes	Yes	Yes	Yes	Yes	Yes	No	Some
Flood Warning	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Flood Alert	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Remove Message	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Account Registration	Yes	Yes	Yes	No	No	No	Yes	No

Annex E – Optional Services

ID	Requirement
	The Supplier shall provide the capability
OPT001	to Ingest automated Telemetry Alarms from the Authority's telemetry system (**"FoNT"**).
OPT002	for data to be updated and received in real-time from third parties for Unregistered Users.
OPT003 (WIP16.5)	for Users to receive confirmation of changes made to their Account Preferences via their preferred Contact Channel(s).
OPT004	to operate the following additional outbound Contact Channels: (a) social media (b) virtual assistants;
OPT005	to explore how Users could receive Messages in other languages.
OPT006 (WIP029)	to notify the Authority when an Organisation is required to pay a Fee.
OPT007 (WIP029)	to record in the Supplier Solution as to whether an Organisation has paid their Fee or not.
OPT008 (WIP029)	to provide an enhanced level of service when an Organisation has paid their Fee.
OPT009	for Internal Users to use the Supplier Solution on mobile devices.