Ministry of Housing,
Communities &
Local Government

Schedule 1 - Services (Buyer Requirements)

Title: Business Continuity Management Software and Mass Notification System

Reference No: CPD4121111

March 2021

1. Introduction

1.1 The Cabinet Office requires MHCLG, along with other central government departments to maintain arrangements for business continuity (BC). The BC arrangements are designed to enable MHCLG to manage the immediate consequences of a major disruptive incident, maintain business critical services, and plan an orderly return to business as usual.

1.2 The MHCLG Security Team is responsible for oversight of BC activities in MHCLG.

2. Background

2.1 Adequate management of MHCLG BC arrangements depends on mainlining suitable, up to date information about MHCLG's directorates, including critical roles and functions and activities, business impact assessments, minimum requirements to deliver key workstreams, outline BC plans and key contact details. Central management of this information allows the Security Team to develop a holistic understanding of business-critical activities, ensure that BC plans are realistic/aligned, and can contact key staff quickly in the event of an incident.

2.2 The Security Team currently uses the main MHCLG file structure to store copies of this information and manually manages the processes of planning, advising, reviewing and auditing the BC plans.

2.3 Plans are written by Directorate plan leaders, who have minimal knowledge of Business Continuity, and signed off by Directorate plan owners (Senior Civil Servant level staff). The front end of the software needs to be user-centric and simple to input data into and report out of. A current BC plan template and guidance document are attached to allow for a customised demonstration and response.

3. Current landscape

3.1 Where are we now

- The current system does not provide the full range of functionality that business continuity work requires.
- The current process is labour intensive, cumbersome and time costly to team members.
- MHCLG has no independent means of instant communications with all staff in the event of an incident which is linked to specific BC plans.

4. Outputs and deliverables

4.1 The key requirements of a suitable BC Management System for MHCLG are as follows:

4.2 A web-based tool which is accessible independently from the MHCLG network with circa 80-120 users and:

- Ability for ‘super-users’ and ‘key-users’ to instantly message, via SMS, all staff in the immediate aftermath of an incident, with secondary means of communication available;
- Ability to store other information relating to business-critical operations. Generally, in the form of free text description of what these operations are, along with numerical scores indicating criticality in terms of regulatory compliance, customer need etc;
- Ability to store .pdf, .doc(x), .xls, .txt, .jpg and related and similar documents within data areas. Ability to retrieve and view them (although editing not required);
- Ability to structure plans and data stored by grouping and hierarchies and to limit access to groupings and hierarchies on a user-by-user basis;
- Ability to extract data by means of standard and also custom reports. Extraction to cover data on loss of estate, IT tools, people difficulties and the failure of contracts. Generally, in the form of free text description of impacts -and information relating to business continuity plans, generally in the form of free text and numerical data in structured fields;
- Ability for a MHCLG ‘super-user’ to manage permissions to allow access to data and reporting tools, add docs, update plans etc;
- Ability for other ‘key-users’ to edit data and ‘all users’ to view;
- Ability to access tool via 2FA;
- Ability to access database from non-MHCLG hardware and software with full access to functionality. Compatible with MHCLG use of VPN;
- Continuing support to deal with any system-build and IT issues and deliver enhancements and be available through mobile phones and laptops;
- 24/7 phone or webchat helpdesk support and update development and delivery options available;
- Virtual classroom based training, train the trainer videos and support documentation (e.g. FAQ’s) for both users and super users, with the option of more bespoke training if required;

- App meeting relevant ISO and UK Government security, BC and information management standards.

4.3 The expected milestones are below:

1)	Introductory meeting to clarify requirements – to include Security team, Digital colleagues, Procurement contact and others as required	Within 1 week of the contract being awarded
2)	Weekly progress updates – email updates to Security team procurement contact	Throughout the duration of the project
3)	Initial iteration of the software tool – to be trialled by Security team and other key stakeholders	Within 6 weeks of the contract being awarded
4)	Workshop/session with MHCLG about how to use/maintain – circa 2 hours for super users	Within 8 weeks of the contract being awarded
5)	Feedback on initial iteration – formal request to be made to super users that attended the workshop	Within 2 weeks of the workshop
6)	Revisions to the software (if required)	Within 4 weeks of the previous workshop
7)	Further workshop/session with MHCLG about how to use/maintain and update – circa 2 hours with super users and users	Within 4 weeks of the previous workshop
8)	Draft documentation (guide on how it works for both the user and super user with FAQ's) – sent to Security team for review	Within 12 weeks of the contract being awarded
9)	Further iterations and improvements (if required)	Within 16 weeks of the contract being awarded
10)	Final version & documentation sign off – signed off by Security team and Digital colleagues	Within 16 weeks of the contract being awarded
11)	Commencement of the live service	Within 18 weeks of the contract being awarded