6.3.5.3.1. failure or disruption scenarios and assessments of risk, impact and probability for each identified Major Incident;

6.3.5.3.2. identification of any single points of failure within the Services and associated risk management processes;

6.3.5.3.3. identification of risks arising from the interfaces of the Services with any provided by a Third Party; and

6.3.5.3.4. a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

6.3.5.4. a description of all methods, processes and procedures and other actions and sequences to be followed in managing and responding to Major Incidents such as:

6.3.5.4.1. identifying the start and finish of Major Incidents;

6.3.5.4.2. categorisation of each Major Incident identified;

6.3.5.4.3. notifying and liaising with the Authority, end users, and Third Parties;

6.3.5.4.4. agreeing with the Authority who should lead the management of a Major Incident and ensuring clarity of responsibility;

6.3.5.4.5. the assignment of Service Provider Key Personnel and tasks;

6.3.5.4.6. processes and procedures to be adopted;

6.3.5.4.7. using or recalling backups or storage;

6.3.5.4.8. recovering, re-entering or correcting Data; and

6.3.5.4.9. deploying additional Service Provider personnel, processes or procedures;

6.3.5.5. management and review activities including:

6.3.5.5.1. the escalation process for each Major Incident category as set out in Appendix 3 (Major Incident List);

6.3.5.5.2. a communications plan (including declaration of the Major Incident and verification of recovery and restoration of the Services); and

6.3.5.5.3. the arrangements for preparing and training Service Provider personnel to deal with Major Incidents;

6.3.5.6. details of contingency plans;

6.3.5.7. the Major Incident List; and

6.3.5.8. how the Service Provider shall manage Major Incidents involving Third Parties.

6.3.6. The Service Provider acknowledges that Category 1 Major Incidents would have a greater impact upon end users and/or the operation of the Services and shall ensure that the Major Incident Plan reflects the materiality of such Major Incidents.

6.3.7. The Service Provider shall ensure that the Major Incident Plan is designed in such a way to ensure that:

6.3.7.1. it does not depend on any other Third Party adjusting their hardware, software or systems as a result of any Major Incident unless this has been agreed in writing by the Authority;

6.3.7.2. appropriate measures are adopted to ensure that the security of the Services are not compromised where possible and, where this is not possible, that any associated risk is properly managed; and

6.3.7.3. its objective is to allow the Services to be provided by the Service Provider in accordance with the Service Levels and to mitigate the adverse impact of a Major Incident.

6.4. Notification of Major Incidents

6.4.1. Category 1 Major Incidents must be notified to the Authority within 15 minutes and all other Major Incidents within one hour:-

6.4.1.1. of the commencement of the Major Incident; or

6.4.1.2. (if earlier) from when the Service Provider becomes aware that the Major Incident will occur.

6.5. Review of the Major Incident List and the Major Incident Plan

6.5.1. The Parties shall meet at the request of either Party within ten (10) Business Days' prior written notice to review the Major Incident List and agree any amendments reasonably required by the Authority to ensure that the objectives described in paragraph 6.1.1 are achieved. As a minimum, the Major Incident List shall be reviewed annually on the anniversary of the Contract Commencement Date.

6.5.2. The Service Provider shall prepare and submit a draft updated Major Incident Plan to the Authority for Assurance:-

6.5.2.1. following any amendment to the Major Incident List;

6.5.2.2. after any Major Incident has occurred (incorporating lessons learned from any Major Incident); and

6.5.2.3. if and as new Services, new systems and other Variations and Changes are introduced and shall issue to the Authority for approval.

6.5.3. The provisions of paragraphs 6.3.2 and 6.3.3 shall apply in the same way to any draft updated Major Incident Plan as to the original draft Major Incident Plan.

6.5.4. If the Service Provider fails to comply with its obligations pursuant to this paragraph 6.5, then a Corrective Action Notice may be issued to the Service Provider by the Authority

6.6. Testing

6.6.1. The Major Incident Plan shall include the Service Provider's proposals for periodic testing to be undertaken to Assure the Authority that appropriate and sufficient arrangements have been put in place to manage those Major Incidents (the **"Preparedness Tests"**).

6.6.2. The scope and timing of the Preparedness Tests shall be developed with the Authority, and shall include a planned 'fail over' test to be carried out on the Services on a date agreed by the Parties.

6.6.3. The Service Provider shall undertake and manage the Preparedness Tests in full consultation with the Authority and/or any Third Party nominated by the Authority and will liaise with the Authority in respect of the planning, performance and review of each Preparedness Test.

6.7. Reports and Meetings for Major Incidents

6.7.1. Following the resolution of a Major Incident, the Service Provider shall prepare a report (a **"Major Incident Report"**) which shall include but shall not be limited to:

6.7.1.1. details of the trigger(s) for the Major Incident;

6.7.1.2. details of the Major Incident (e.g. duration, scope of Services affected, cause of the incident etc.);

6.7.1.3. an explanation of the solution deployed by the Service Provider and a summary statement as to how well (or otherwise) the Service Provider handled the Major Incident;

6.7.1.4. the lessons learned by the Service Provider as a result of the Major Incident;

6.7.1.5. any proposed changes to the Service Provider's procedures and the Major Incident Plan; and if appropriate, the Major Incident List

6.7.1.6. proposed amendments to Third Party procedures, systems and plans in the event that the Service Provider's investigations into the trigger for the Major Incident reveal that the Major Incident was caused as the result of an act or omission of a Third Party.

6.7.2. A draft of the Major Incident Report shall be prepared and submitted to the Authority within five (5) Business Days of any Major Incident having been resolved and in the event that the Service Provider fails to do so a Corrective Action Notice may be issued to the Service Provider by the Authority.

6.7.3. the Service Provider shall meet to discuss the draft Major Incident Report within five (5) Business Days of its submission and the Service Provider shall finalise the Major Incident Report within a further five (5) Business Days of such meeting.

6.7.4. The Service Provider shall include a summary of all Major Incidents in the Service Performance Report as per Appendix 2 (Service Performance Reports).

7. Problem Management

7.1. Overview

7.1.1. Problem Management is defined as the process used to determine the root cause of one or more Incidents and to develop workarounds and/or permanent fixes in order to minimise the frequency and/or impact of the Incidents

7.2. Requirements

7.2.1. Upon request from the Authority the Service Provider shall initiate or assist in a Problem investigation for a particular Incident or set of Incidents.

7.2.2. As part of any Problem investigation, if requested, the Service Provider shall produce a Problem Report, for each Problem, containing a description of the Incidents, a trend analysis or timeline of the Incidents, the root cause of the Incidents, potential workarounds, and potential permanent fixes.

7.2.3. The Service Provider shall provide the Problem Report to the Authority within the Service Levels in Appendix 1 (Service Levels).

7.2.4. The Service Provider shall, upon agreement with the Authority, schedule and implement the workaround and/or permanent fix and apply the Change Management process if required.

8. Service Performance Report

8.1. The Service Provider shall prepare and submit to the Authority a Service Performance Report. The Service Provider acknowledges that the timely submission of the Service Performance Report following the end of each Period and properly addressing any comments made by the Authority is essential to the processing of the invoice for the Period by the Authority. Any delay in the submission of the Service Performance Report shall extend the period set out in Clause 11.4 (Payment Procedures and Approvals) for review of any associated Invoice by an equivalent period of time.

8.2. The Service Provider shall deliver a report which details the Service Provider's performance of the Services (the "**Service Performance Report**") each Period by 8:00 of 2nd Business Day following the end of each Period. The structure and contents of the report is detailed in Appendix 2 (Service Performance Reports). Additionally, the Service Provider shall provide information in an Excel format or as agreed by the Authority by 8:00 of 2nd Business Day of the Period end showing the overall performance against each Service Level of the Contract.

8.3. The Authority may apply Service Credits (and, where applicable, Service Bonuses) according to clause 5.3 (Performance Regime) based on the data, including raw supporting data, provided by the Service Provider as part of the Service Performance Report which demonstrates the Service Provider's compliance with the Service Levels specified in Appendix 1 (Service Levels).

8.4. The Authority may, at the Service Review Meeting, advise the Service Provider of any items contained in the Service Performance Report that require correction. The Service Provider shall ensure that agreed corrections are communicated to the Authority.

9. Service Review Meetings

9.1. Overview

9.1.1. The purpose of the Service Review Meeting is to review the performance of the Service Provider over the previous Period to ensure the best quality and standards of performance in the provision of the Services.

9.1.2. A Periodic Service Review Meeting shall be held within five (5) Business Days of Period end, unless otherwise agreed between the Parties.

9.2. Requirements

9.2.1. The Service Provider shall send suitably qualified Service Provider Personnel to attend a Periodic Service Review Meeting with the Authority which shall be held at an Authority Premises in London, unless otherwise agreed by the Authority.

9.2.2. The agenda for the Service Review Meeting shall initially cover:

9.2.2.1. the previous minutes;

9.2.2.2. a review of the Service Provider's Service Performance Report;

9.2.2.3. other matters as jointly agreed;

9.2.2.4. Service operation, Contract performance and Contract compliance where appropriate;

9.2.2.5. Assurance feedback; and

9.2.2.6. Transition, where applicable.

9.2.3. The Authority shall be responsible for the creation and distribution of the agenda and meeting minutes.

9.2.4. The Service Provider shall attend scheduled and ad-hoc operational meetings as reasonably requested by the Authority.

10. Asset Management

10.1. Overview

10.1.1. The Authority may make available Authority Assets to the Service Provider to use on their premises for the sole purpose of performing the Service. The use of Authority Assets may require the Service Provider to assist the Authority and its sub-contractor(s) in maintaining the Authority Assets in accordance with the requirements in this paragraph.

10.2. Requirements

10.2.1. The Service Provider shall provide access, at no charge, to the Authority Personnel for the purpose of planned maintenance, repairs or replacement of any Authority Assets held on the Service Provider's premises.