SCHEDULE M

BUSINESS CONTINUITY

The Business Continuity Plan should, as a minimum, address the following issues and be in compliance with JSP 503 (*MoD Business Continuity Management*):

1. PURPOSE AND CONTENT:

1.1 An outline of the scope of the Business Continuity Plan and its relationship to other plans (e.g. the Programme Management Plan).

2. DOCUMENT OWNERSHIP AND MAINTENANCE:

2.1 Who owns the Business Continuity Plan and who is responsible for reviewing amending and updating it and how often these reviews, amendments and updates must occur?

3. ROLES & RESPONSIBILITIES:

3.1 A list of key roles and responsibilities of Engaged Personnel in implementing the Business Continuity Plan.

4. PLAN MECHANICS:

4.1 How will the Business Continuity Plan be invoked?

4.1.1 What is the model for how Engaged Personnel will be contacted in the event of an incident (e.g. will a phone tree be used)? How will this model be maintained throughout the Term?

4.2 Which Engaged Personnel or people at the Authority have the authority to invoke the Business Continuity Plan and under what circumstances may this authority be exercised?

4.3 What is the plan for mobilising Engaged Personnel and demobilising Engaged Personnel in the event the Business Continuity Plans is involved?

4.4 What is the anticipated effect of invoking the Business Continuity Plan on the Services?

4.4.1 What are the alternative processes (including business processes) and responsibilities required if the Business Continuity Plan is invoked, and how will the processes will be returned to 'normal'?

5. CONTACT DETAILS:

5.1 Essential contact details in the event of a disruption to the Service.

6. INCIDENT MANAGEMENT:

6.1 Response required to manage the initial incident and to ascertain who is responsible.

6.2 Site Evacuation.

6.3 On-going Engaged Personnel care

7. BUSINESS CONTINUITY AND RECOVERY STRATEGY:

7.1 Set out activities that are critical to the recovery timescale.

7.2 Set out how to carry out an evaluation of the strategic importance of each part of the Service, and how any re-mobilisation will be prioritised.

7.3 Set out the recovery options available for different parts of the Service.

8. BUSINESS CONTINUITY RISK ASSESSMENT & MITIGATIONS:

8.1 Physical / cyber security risks to off-site accommodation and IT.

8.2 Sub-contractor solvency issues.

9. IDENTIFICATION OF AUTHORITY DEPENDENCIES

APPENDIX 1

DRAFT BUSINESS CONTINUITY PLAN

Draft Business Continuity Plan from the Contractor's ITN response is included on the following pages:

Business Continuity Plan

Introduction

The aim of Business Continuity (BC) is to put in place a series of procedures, mitigations and actions which allow Aurora to continue delivering to the MOD, with minimal disruption, in the event of a serious incident.

The EDP Business Continuity Plan (BCP) provides overall guidance in responding to any significant incident that threatens to interrupt normal operations across all areas of the business over an extended period of time

It is designed to provide immediate response and subsequent recovery from any unplanned business interruption and thereby satisfy the EDP's BC Management requirements.

Purpose of the BCP

The purpose of the BCP is to provide arrangements to address the response, recovery and resumption phases of an incident when escalated to the EDP Leadership Team.

Exclusions from this BCP

This Annex does not cover any incident or loss related to DE&S IT, infrastructure or people.

Incidents related to the delivery of the engineering services themselves, either through the EDP companies or the Provider Network, will be addressed by the BCPs of the companies delivering those services.

BCP Incidents

An incident may occur in one of the following areas impacting the provision of Engineering Services;

- Incident or loss related to the IT/Aurora Cloud;
- Incident or loss of electronic data or artefacts held by the EDP;
- Incident or loss of critical infrastructure at an approved Contractor Group location, such as the Engineering Hub;
- Incident or loss involving Aurora Engineering Hub team members or Critical Resource Augmentees embedded within DE&S;
- Incident or loss of IT or critical infrastructure owned by the Provider Network.

BCP Ownership and Review

The EDP BCP will be agreed with DE&S and communicated to and understood by the EDP Leadership Team who, under the leadership of the Managing Director, is responsible for initiating and managing the plan.

The BCP is an integral part of the Programme Management and Project Controls approach. The BC Strategy and Plan are owned by the Aurora Delivery Director, and will be reviewed by the EDP Leadership Board, which has overall responsibility for the implementation of the strategic direction provided by the Alliance Board, as well as for monitoring and controlling the engineering services outputs and outcomes delivered and coordinated through the Engineering Hub.

The Leadership Team, and the EDP Leadership Board, are further described within Annex B: Governance and Organisation.

SCHEDULE M: BUSINESS CONTINUITY

This BCP has been developed to be aligned to the BCPs of DE&S and each of the EDP companies, QinetiQ, Atkins and BMT. It focuses on safety and security, clear communications, resilience and built-in redundancy of systems and people.

BCP Activation

Based on the incidents outlined in section 0, the plan may be activated by the following parties:

Nature of Incident	Plan Activation
IT	Aurora / QinetiQ (as IT host)
Infrastructure	Aurora / QinetiQ (as Contractor location)
Personnel	DE&S / Aurora / Partner company

Table 1: Summary of BCP Activation Incidents

Method of activation

An Aurora BC WhatsApp group is used to communicate to the EDP Leadership Team in the event of an incident at any time. Communications are initiated by the Delivery Director. The message alerts members to the incident and provides information on the next steps to be taken, such as;

- Whether BC team members need to physically convene, or dial into a teleconference bridge;
- How relevant back-up systems can be accessed;
- Notify any interim changes to personnel roles and responsibilities;
- Outline of next steps.

BC Team Roles and Responsibilities

Once the BCP is activated, the EDP Managing Director is responsible for chairing any required response meetings.

The actions and resolution activities resulting from the response meetings are owned by the Delivery Director, who is responsible for the successful resolution of all incidents that activate the EDP BCP.

Liaison with Aurora partner companies

Where liaison with the appropriate Crisis Management Teams within each of the EDP companies is needed, this is the responsibility of the EDP Managing Director, or nominated deputy.

Incidents activating the Plan

Incidents or loss related to IT/Aurora Cloud

Aurora IS provision will initially be achieved through the adoption of existing tools, already available within the EDP Alliance and operating in delivery of MOD engineering services.

The primary tool, the Collaborative Working Environment, is based on the Enterprise On- Line (EOL) system, adopted from the QinetiQ Strategic Enterprise for Air Technical Services. EOL provides functionality to support many of the EDP processes and workflows, including task management, change management, contract management, GFX management, document library, resource management, supply chain management.

EOL is hosted within a secure CWE provided by QinetiQ and is consequently delivered from within the QinetiQ IS Service Delivery model, in accordance with QinetiQ Group IS/IT policy and procedure.

As the Aurora IS is fully hosted by QinetiQ, any incident related to failure in the Aurora IS will be automatically passed into QinetiQ by the Managing Director. Under QinetiQ's BC Plan, the majority of events or incidents are managed by the local leadership teams with the relevant Business or Functional MD acting as the Chairman or strategic commander for that particular event or incident. Any cyber incident is managed by QinetiQ's Incident Response Centre, based in Malvern.

Full details on Aurora's Information Systems is provided in Annex G: Information Management.

Incident or loss of electronic data or artefacts held by Aurora

As the Aurora IS is fully hosted by QinetiQ, any incident related to the loss of electronic data is automatically passed into QinetiQ by the Managing Director.

Incident or loss of critical infrastructure

Aurora will establish an Engineering Hub, the working environment and focal point for all of the day to day activities of the Alliance Engineering Hub. The Engineering Hub is based in existing List X certified office space within Building 240, Bristol Business Park, BS16 1FJ, which is leased by QinetiQ.

As the Engineering Hub is the base office for all Aurora staff, any incident related to failure in the Aurora infrastructure is automatically passed into QinetiQ by the Managing Director.

Incident or loss involving Personnel

Notification of incidents relating to any Personnel may be received from the Provider Network, an EDP company, DE&S or the Emergency Services.

Any member of the EDP Leadership Team receiving notification of an incident relating to Personnel is responsible for informing the Delivery Director, who will initiate the BCP and control the follow-on activities.

These incidents may relate to the following two scenarios;

- **Critical Resource Augmentation (CRA)**: where Aurora provides Critical Resource Augmentation (CRA) into DE&S, either through the Provider Network or the Alliance partners, those individuals will be embedded into DE&S.
- **Engineering Hub personnel**: Any member of the Aurora Engineering Partnership working within the Engineering Hub

Incident or loss of IT or critical infrastructure owned by the Provider Network

Notification of incidents relating to the IT or critical infrastructure belonging to the Provider Network trigger the activation of the EDP BCP. Such notifications may be received from the Provider Network, an EDP company or DE&S.

Once notification of an incident is received, the EDP Delivery Director will activate the EDP BCP and control the follow-on activities. To resolve an incident related to the Provider Network IT or critical infrastructure, there are three possible options;

1. If the nature of the incident can be resolved immediately by the Provider Network company, no EDP intervention is required.
2. If the Provider Network company is not able to resolve the incident, the EDP BCP will be activated and the EDP will provide interim support during the recovery phase.
3. In the event that the incident cannot be resolved through interim support, the Engineering Delivery Partner will step in to fulfil the Provider Network requirement.

Contacts

SCHEDULE M: BUSINESS CONTINUITY

A full list of emergency contacts for all companies is stored and managed by the Engineering Delivery Partner.