

ANNEX B TO CONTRACT ISSCCT/0239

STATEMENT OF CORE SERVICES

**FOR THE DEFENCE LEARNING MANAGEMENT
CAPABILITY (DLMC) BRIDGING CAPABILITY**

1. This Statement of the Services defines the activities the Contractor shall undertake to deliver the Core Services. The Contractor shall deliver the Core Services on a standard Business Day other than where specifically described in this Annex B to the Contract.

THE REQUIREMENT

2. The Contractor shall deliver Core Services in the following main areas:

TECHNICAL INFRASTRUCTURE SUPPORT

- a. Maintain Technical Infrastructure
- b. Maintain Connectivity with RLI
- c. Technology Changes
- d. Maintain compatibility with DII and MODNet
- e. Maintain Local Area Network (LAN)
- f. System Integration
- g. Managed Hosting Service
- h. Software Management
- i. Manage Interfaces
- j. System Maintenance
- k. System Testing

SERVICE MANAGEMENT

- a. Management of Services
- b. Help Desk Support Services
- c. User Administration
- d. Service Code of Practice
- e. Data Patching
- f. Key Roles
- g. Management of Software Licences
- h. Information Technology Infrastructure Library (ITIL)
- i. Risk Management
- j. Technical Documentation Maintenance

USER TRAINING

- a. Provide user training courses and course materials

DISASTER RECOVERY

- a. Disaster Recovery Services

SECURITY

- a. Security Services

BUSINESS SUPPORT SERVICES

- a. Site Support Services
- b. Business Intelligence Support Services (Army Only)

Further details on each of these are as follows:

TECHNICAL INFRASTRUCTURE SUPPORT

Maintain Technical Infrastructure.

3. The Contractor shall maintain the Technical Infrastructure (namely the hardware and software) used in delivering the Core Services as follows:

- a. IT hardware in the Upavon server room used for hosting the Core Services up to but not including the Service Delivery Point (SDP);
- b. IT hardware at the Contractor's premises used to support the Core Services up to but not including the SDP;
- c. Software required to provide the Core Services.

4. The Contractor shall maintain the Service Levels as set out in Annex C to the Contract and comply with MOD security policies by:

- a. Repair and replacement of hardware;
- b. Installation of routine software updates and security patches;
- c. Provision of software and software licences including those of 3rd Parties.

5. The Contractor shall monitor the performance of the Technical Infrastructure on a daily basis and shall take pre-emptive action to ensure that Service Levels are achieved.

6. The Contractor shall review the Technical Infrastructure capacities against demand to ensure that growth in transactions and data volumes is supported.

7. Defective Technical Infrastructure shall be repaired or replaced at the Contractor's own expense as part of the Core Service. The Authority shall be responsible for the cost of rectifying any defective Technical Infrastructure which is defective as a result of damage caused by the Authority or other third parties engaged by the Authority.

Maintain Connectivity with RLI.

8. The Contractor shall monitor RLI availability, bandwidth capacity and usage, to identify problems in respect of the Core Services requiring action and ensure that Service Levels are achieved.

9. The Contractor shall pass problems that are found not to be associated with the Contractor's Technical Infrastructure to HQ ARTD with recommendations on resolution.

10. The Contractor shall provide recommendations involving additional bandwidth and such recommendations shall be accompanied by capacity/usage figures.

Technology Changes.

11. The Contractor shall, while taking account of technology trends and changes, identify changes required to the Technical Infrastructure over the Period of the Contract to maintain the Service Levels and plan the required changes, including upgrades to COTS and bespoke software. The Contractor shall identify any planned or known hardware or software obsolescence issues to the Authority's Project Manager.

12. On the anniversary of Effective Date of the Contract, the Contractor shall submit a plan to the Authority's Project Manager for agreement, identifying technical products that are reaching obsolescence. The Parties shall discuss technology changes recommendations and agree a reasonable common plan.

Maintain compatibility with DII and MODNet.

13. To ensure that action is taken to maintain compatibility and interoperability in the event of changes to DII, MODNet and Core Services the Contractor shall:

- a. Review each issue of the Applications Development Guides, which are expected to be issued by MOD quarterly, taking note of planned changes to the DII and MODnet UAD builds and expected time frames for implementation;
- b. Attend the MOD run Applications Working Groups for further information on planned upgrades to UAD builds;
- c. Liaise with ISS on DII and MODNet to gain insight into potential changes;
- d. Maintain a view of vendor product road maps relevant to the DII and MODNet builds and raise any impact on the Core Service for discussion with the Authority's Project Manager;
- e. Conduct confidence testing of Core Services products against planned builds using the GFA, namely ACE2, MODNet test rigs or other facilities as may be made available to the Contractor by the Authority for compatibility testing purposes.

14. Using information from actions described in paragraph 13 the Contractor shall use reasonable endeavours to ensure that planned or known changes that impact or may impact on Core Services are notified to the Authority's Project Manager so that they can be fully addressed in a suitable timeframe to ensure continuity of the Core Service.

Maintain Local Area Network (LAN).

15. The Contractor shall ensure that the LAN facilities used in delivering the Core Services at the Upavon server farm are maintained and supported as required to meet the Service Levels.

16. The Contractor shall advise the Authority's Project Manager on recommendations for additional infrastructure and infrastructure changes.

Systems Integration.

17. The Contractor shall integrate new and changed hardware and software components into the Technical Infrastructure, including components or changes that have been provided by third parties.

18. System integration activities resulting from defective Technical Infrastructure shall be completed by the Contractor at his own cost.

Managed Hosting Service.

19. The Contractor shall continue to support and maintain the hosting platform for all Core Services IT Services, for access from any compatible UAD connected to RLI. This should include hosting for Core Services Web applications and legacy systems, databases, file and print Services, Core Services Windows applications, SharePoint, and a Citrix capability to access Windows applications across RLI.

20. The Contractor shall ensure that all Authority data held on the Core Services database is backed up on a daily basis. The Contractor shall ensure that data should be restored within 24 hours of an incident resulting in the need for a restore.

Software Management

21. The Contractor shall maintain all source code and associated technical design documentation as required to meet the Service Levels. All routine maintenance activity shall be carried out as part of the Core Service.

22. Defective software shall be fixed at the Contractor's cost.



24. The Core Service is based on a maximum incident rate of a 50 calls a day. In the event of a sustained increase above the threshold of 50 calls a day, that are not as a result of a fault that is the responsibility of the Contractor, the parties shall enter into good faith negotiations to address the increase in workload.

25. The Contractor shall continue to lodge source code in escrow at the National Computing Centre (NCC) or by other arrangement as agreed with the Authority.

Manage Interfaces

26. The Contractor shall maintain and administer interfaces with JPA and TAFMIS Recruiting Services including:

- a. Monitoring and controlling interface data transfers;
- b. Resolving errors;
- c. Raising business issues with the Authority's Project Manager;
- d. Maintain consistent reference data and mapping of reference data.

27. The existing interfaces at the Effective Date of Contract are agreed as being fit for purpose.

28. Defects shall be repaired or replaced at the Contractor's cost. The Contractor shall not be liable for the cost of investigating repairing or replacing defects in the interface infrastructure which were not caused by the Contractor.

29. The Contractor shall develop data interfaces with RPP and the Army Data Warehouse (ADW) when required. Scope and timings of the required development and support are currently unconfirmed. When requirements are confirmed, the Authority shall raise a contract change requesting the Contractor to provide proposals on additional Technical Infrastructure and Technical Infrastructure changes including any additional impacts.

System Maintenance

30. The Contractor shall create and maintain a rolling maintenance schedule with regard to the Core Service to be agreed with the Authority's Project Manager.

31. When the Contractor wishes to carry out any routine maintenance to the Core Service (other than emergency maintenance), he shall ensure that:

- a. The timing of the planned maintenance is in accordance with the requirements of the agreed maintenance schedule or is as otherwise agreed in writing with the Authority's Project Manager at least 14 (fourteen) Business Days in advance;
- b. It is not carried out during 08:00 to 18:00 Mon to Fri;
- c. Once agreed with the Authority's Project Manager the permitted maintenance is forthwith entered onto the agreed maintenance schedule; and
- d. The permitted maintenance is subsequently carried out in accordance with the agreed maintenance schedule.

32. The Contractor shall carry out any necessary maintenance where it reasonably suspects that the Core Services or any part thereof, has or may have developed a fault. The Contractor shall give as much notice as is reasonably practicable to the Authority's Project Manager prior to carrying out such emergency maintenance.

System Testing

33. The Contractor shall provide full system testing in response to changes to the Core Services and external factors that impact on the Core Services for which the Contractor is responsible. This includes:

Internal

- a. Unit, system, integration and regression testing of specially-written software;
- b. Testing of software, data patches, roll-out procedures;

- c. Performance testing as required to verify Service Levels.

External

- a. Critical Design Reviews;
- b. Critical Implementation Reviews;
- c. System Trials;
- d. Testing interoperability with external systems (e.g. JPA, RPP and DII).

34. Testing as a result of routine maintenance and Contractor generated change is part of the Core Service.

35. System testing activities resulting from defective Technical Infrastructure shall be conducted at the Contractor's cost.

SERVICE MANAGEMENT

Management of Services

36. The Contractor shall manage all aspects of the delivery of the Core Services and work closely with and support the HQ ARTD informed (intelligent customer cell) function to ensure the delivery of the Core Services in accordance with the Service Levels; to include the following Authority-facing services:

- a. Liaise with HQ ARTD staff and third party contractors as necessary for the day to day delivery of the Core Services;
- d. Implement a process of continuous improvement in conjunction with the Authority's team;
- e. Processing change requests shall be recorded and managed under the Core Service except where significant or complex requirements analysis is required to provide a detailed assessment of the requirements and impact of change.

Help Desk Support Services

37. The Contractor shall set up and resource a help desk service. The first point of contact for users requiring support is the DII Single Point of Contact (SPOC). The Contractor shall support users who access Core Services via DII User Access Devices. Issues that do not relate to DII and that cannot be resolved by the SPOC shall be passed to the Contractor's helpdesk for Contractor 2nd and 3rd line support to resolve.

38. The Contractor shall provide telephone support to Core Services during Working Days to resolve problems and issues in the use of the Services as per the Service Levels via the SPOC. Faults that are raised outside of the Business Day hours for the Core Services that are passed to 2nd and 3rd line support shall be resolved during the Business Day hours..

User Administration

39. The Contractor shall maintain details, provided by the Authority or Core Service users, of all Core Services users contact details, locations, access profiles and usage data.

40. The Contractor shall administer and issue logons and passwords for admin users for each site. These admin users will then use the self-service facilities within the Core Service to administer and issue logons and passwords for new users at the site and changes to users' access requirements. The Contractor shall ensure that user admin accounts are closed when, in consultation with the Authority, it is agreed that they are no longer required. Each request for changes is to be completed within 2 Working Days of receipt. The Authority's Project Manager shall arrange for notification to the Contractor at the earliest possible opportunity of all new requests for admin users. In the event that a local admin user is unavailable, the Core Service user will call the Contractor help service; such instances are expected to be infrequent.

Service Code of Practice (SCOP)

41. The Contractor shall work with HQ ARTD to develop and agree a Service Code of Practice (SCOP) that sets out the relationships, working interfaces and procedures needed for the day-to-day performance of the Core Services to support the practical delivery of the Core Services. The SCOP shall be a working document, but will not take precedence over any other document called up or referred to in the Contract. The SCOP can be varied by mutual agreement at a working level without a formal contract change.

Data Patching

42. The Contractor shall, in addition to routine data corrections carried out as part of database administration activities to rectify system faults and problems, produce data patches at the request of the Authority's Project Manager in accordance with the Service Levels.

43. These shall fall into two categories:

- a. Those relating to all items of data that need to be changed and which for all practical purposes there is no facility for the user to change (for example reference data items);
- b. Those relating to items of data that need amending as a result of user error.

Key Roles

44. The Contractor shall ensure that key roles in the delivery of the Services shall be filled by individuals who have been agreed for the role by the Authority's Project Manager. These roles are:

- a. Delivery Lead or equivalent – responsible for the overall delivery of the Services and being the main point of contact for Authority HQ ARTD Head of MIS Branch;
- b. Service Manager - responsible for day to day management of the Core Services and being the main point of contact for the Authority's HQ ARTD Service manager;
- c. Technical Lead – with overall responsibility for technical aspects of Core Service delivery and the main point of contact for the Authority's HQ ARTD technical design Authority;
- d. Commercial Lead – responsible for liaising with the Authority's Commercial Officer named in box 1 of the Appendix to the Contract (DEFFORM 111).

Management of Software Licences

[REDACTED]

USER TRAINING

User Training Services

51. The Contractor shall work with the Authority's Project Manager, or his authorised representative to develop and periodically review a jointly owned training plan identifying the training requirement over the forthcoming year to address new users, changes in staff, business and system changes and refresher training.
52. The Contractor shall provide user training in the use of the system at the agreed Authority locations; this can be either classroom based or an alternative effective method. The training should be delivered in English using terminology that is understandable by the trainees.
53. The Contractor shall provide electronic copies of all training materials to support classroom-based training for the trainees. Any hard copy training materials required will be printed using printing facilities and supplies at the agreed Authority training locations.
54. The Contractor shall ensure that trainers have and maintain a good situational awareness i.e. up-to-date knowledge of how the system is used on site, to ensure that training reflects workplace practices as well as classroom theory.

DISASTER RECOVERY

Disaster Recovery Service

55. The Contractor shall maintain a secondary managed hosting environment at a separate physical location to the primary installation to provide a disaster recovery capability. This must be carried out in accordance with MOD security standards. The Contractor shall maintain the existing secondary managed hosting environment at the Contractor's premises; for the avoidance of doubt the secondary managed hosting environment does not have the same capacity and performance as the primary managed hosting environment.

56. The Contractor shall replicate some but not all the data managed at the primary managed hosting environment to the secondary managed hosting environment, using a replication approach which relies on the availability and performance of the RLI. Replicated

data includes the Core Services transactional databases, the CTDB, EMIS and TAFMIS Recruiting Services transactional data.

57. In the event of a disaster, the secondary managed hosting environment takes over from the primary managed hosting production environment and the replacement Service will reflect a degraded Core Service.

58. The Contractor shall provide access to all Core Services applications from the alternative environment within 24 hours of requesting the Core Service by the Authority's Project Manager.

SECURITY

Security Services

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

BUSINESS SUPPORT SERVICES

Site Support Services

65. The Contractor shall provide suitably qualified and experienced personnel to deliver business support to enable the Authority to gain maximum benefit from the Core Services. This service must be responsive to and reflect the priorities of the Authority at all times.

66. The Contractor shall provide routine site support at the user level (HQ and training establishments), as agreed at the Business Support Meetings:

- a. To resolve problems and issues in the use of the Core Services identified by users and by the Authority in relation to corporate matters (priorities to be set by business support meetings);
- b. To facilitate and maintain maximum uptake in the use of the Core Services in line with single Service and Defence policies and requirements and priorities in the use of the system.

67. The Contractor shall ensure that routine visits to each of the training establishments using the Core Service should take place as directed by the Business Support Meetings.

Business Intelligence Service (Army Only)

68. The Contractor shall provide support Core Services to be located at Ops Branch in Upavon to cover 3 capabilities:

- a. Information management: responsible for advising and guiding the Recruiting and Training Information Cell (RTIC) on all aspects of data and systems;
- b. Report Production; responsible for advising on data structures and business processes;
- c. Business Data Analytics.

69. Information Management:

- a. Advising the RTIC on all aspects of data and systems in support of ARTD Business Intelligence needs;
- b. Maintaining an oversight of recruiting and training data;
- c. Raising information management issues with HQ ARTD Hd Ops and other stakeholders that may require business intervention;
- d. Assisting with the promulgation of information management policy and procedures;
- e. Assisting with identifying ways of improving data quality;
- f. Assisting with identifying information usage by close liaison with key staff in Op Groups and schools through regular site visits;
- g. Assisting with producing Traffic Light (RAG) Reports to indicate the status of each Premise in relation to data quality and usage of the system;
- h. Assisting site based data managers with rectifying data entry anomalies on a Premise-by-Premise basis;
- i. Assessing reference data changes in conjunction with the Authority's Project Manager.

70. Ad Hoc Report Production:

- a. Advising on the interrelationship between the current recruiting and training business processes and how they influence the MIS;
- b. Developing ad hoc reports as required by HQ ARTD Ops Group;
- c. Production of reports against stipulated requirements;
- d. Building and maintaining liaison with HQ ARTD Ops Group data controllers to progress data inconsistency issues;
- e. Notifying the Business Objects architect of possible universe enhancements or issues; it shall be the architect's decision as to how issues are progressed;
- f. Maintaining the data entry handbook;

- g. Liaising with training establishments in relation to data quality, developing reports and addressing requests for information via the RTIC.

71. Business Data Analytics:

- a. To maintain a resourceful, innovative and flexible, industry standard data analytics capability that is able to provide impartial, insightful and repeatable analysis and narrative, and business processes, able to react swiftly to changing requirements in the recruiting and training domains;
- b. To provide sufficient and appropriate recruiting and training [personnel focused] data and information analytics to provide an agreed and coherent narrative, so producing a common recruiting and training operating picture for ARTD and pan-Army use, supporting effective business decision making and consequence management within ARTD and across the Army;
- c. Through additional analysis and modelling, deliver a high level of data and information assurance and confidence when analysing the effects of change throughout the recruiting and training pipelines, producing forecasts or supporting decision-making to drive Continuous Improvement;
- d. To Service requests for information from external stakeholders, through HQ ARTD providing relevant data, information dashboards and contextual analysis whilst adhering to the emerging Army and ARTD information governance structure/framework/regime;
- e. To enable improvement in recruiting and training Data Quality (DQ)/data completeness by analysing, identifying and reporting DQ issues through the effective use of dashboards and subsequent narrative.

72. To achieve these requirements, it is expected that any such data/information analytics capability shall have an understanding of the MOD and the Army, and knowledge of recruiting and training and its associated data (including the system and the Enhanced Management Information System (EMIS) database in order to undertake such analysis effectively, efficiently and in a timely manner.