A303 Amesbury to Berwick Down (Stonehenge)

Volume 2 – Scope

Part 5 – Digital Construction Requirements

April 2022

Doc Ref: A303-MW-CoD-008-V2-P5 Digital Construction

www.nationalhighways.co.uk

Table of Contents

Section **Page**

1 Information Requirements

1.1 Implementation

1.1.1 The requirements of this document shall be fully implemented by the *Contractor* and subcontractors (at any stage of remoteness from the *Client*).

1.1.2 All the equipment, hardware, software and training shall be provided to enable implementation of the digital processes and digital technologies specified in this document.

1.2 Exchange Information Requirements

1.2.1 Information and services shall be provided in accordance with the *Client's* Employers Information Requirements (EIR) [1] contained in the Data Room [2].

1.2.2 The Appointing Party's Exchange Information Requirements as defined in BS EN ISO 19650 (All Parts) 'Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling.' [3] shall be the EIR [1].

1.2.3 Where the EIR [1] references the Supplier, this shall be the *Contractor*.

1.2.4 Where the EIR [1] references the Employer, this shall be the *Client*.

1.2.5 Asset information shall be provided in accordance with the Asset Data Management Manual (ADMM) [4].

1.2.6 Asset information shall be provided to achieve Completion for the relevant section.

1.2.7 A Project Information Model shall be provided.

1.2.8 Asset information shall be linked to the Project Information Model using a unique identifier.

1.2.9 An individual shall be nominated in the role of Digital Lead.

1.2.10 The Digital Lead shall

- implement consistent processes and standards, including with all subcontractors and
- have previous experience leading digital processes to satisfy Building Information Modelling (BIM) according to the ISO 19650 'Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling.' [3] series or BIM Level 2 to PAS 1192-2 'Specification for information management for the capital/delivery phase of construction projects using building information modelling' [5] on two (2) equivalent major infrastructure projects of comparable scale or complexity.

1.3 Project Information Production Methods & Procedures

1.3.1 Digital processes shall be adopted at all locations in the Working Areas.

1.3.2 Digital processes shall be used for

- accessing live design and construction Information,
- accessing as-built information,
- accessing live monitoring information, including the tunnel boring machine (TBM) location and performance,
- accessing geospatial information,
- accessing the Project Information Model,
- accessing Project Data Analytics,
- accessing the Data Hub,
- reviewing and approving of information,
- the *Contractor's* health and safety system for recording inspections, and other visits, observations and incident events in accordance with requirements contained in Volume 2 Part 1 (General Requirements) of the contract,
- live location monitoring of site workers, plant and equipment,
- recording of archaeological information with geospatial information including drawings, photos, and context sheets,
- 3-Dimensional (3D) digital scanning with geospatial information of archaeological features and material,
- accessing locations of previous and proposed archaeological surveys,
- providing enhanced accessibility to information for all staff,
- toolbox talks and
- health and safety briefings.

1.3.3 Digital technologies shall be used to manage access and egress on the Working Areas including the following

- digital personalised access,
- delivery certification and
- monitoring access and egress of all people, vehicles and goods.

1.3.4 Digital personalised access control technologies Should include biometrics.

1.3.5 Digital technology Should be used to automate the payment of subcontractors.

1.3.6 The Project Information Model shall be used with virtual, immersive and visualisation technologies to support the following activities

- site safety planning,
- on site visualisation of existing utility information,
- on site visualisation of proposed design details,
- design for operation and maintenance,
- design review,
- stakeholder engagement and
- (Science Technology Engineering and Maths) STEM or other educational activities.

1.3.7 The Project Information Model shall be used for

- all design and planning activities,
- all construction and site activities,
- all utility planning, design and construction,
- hazard and risk identification and mitigation,
- environmental management[1],
- all construction planning ("4D BIM"), including time dependant construction sequencing and optimisation,
- cost planning ("5D BIM"),
- sustainable design and carbon reduction and
- operation, maintenance services and activities.

1.3.8 A digital design review and quality process shall be adopted in accordance with BS EN ISO19650-2 'Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling.' [3] to quality assure the design output and collaboratively engage with the *Client* and Others.

1.3.9 Digital processes shall be outlined in a BIM Execution Plan.

1.3.10 The BIM Execution Plan shall include design, construction and operational phases of the Scheme.

1.3.11 The BIM Execution Plan shall be prepared and submitted in accordance with Volume 2 Part 9 (Review and Certification) of the contract

- within twelve (12) weeks of the *starting date* and every six (6) months thereafter and
- upon any change.

1.3.12 All design elements shall be 3D geometrical models.

1.3.13 All drawings which represent any element of the Project Information Model, shall be derived directly from the 3D geometrical model component of the Project Information Model.

1.3.14 The Project Information Model shall include a 3D geometrical ground model.

1.3.15 The below surface elements of the 3D geometrical ground model shall include the interpolated representation of the Geotechnical Data.

1.3.16 Materials Should in general not be printed.

1.3.17 Materials may be printed when any of the following conditions apply

- digital processes are not available to undertake the task,
- digital only processes would incur significant additional expense,
- digital only processes would incur significantly delay,
- digital only processes would incur increased health and safety risk or
- it is the only means of providing the information to Others.

1.3.18 A digital survey of the *works* shall be provided.

[1] Refer to the environmental management plans contained in the OEMP [15].

1.3.19 The digital survey shall comprise

- a topographical survey of the *works*,
- a visual record of the *works* and
- a 3D mesh digital model of the Working Areas with full colour data surface imagery.

1.3.20 The digital survey Should be a fully automated process.

1.3.21 The digital survey of the *works* shall be undertaken within one (1) week of the *access date* of the *works* up to the completion of *section 3A*.

1.3.22 The digital survey of the *works* shall be updated every two (2) weeks.

1.3.23 The digital survey shall be used to

- monitor construction progress,
- support site safety planning and
- support the monitoring, planning and operation of earthworks.

1.3.24 Any incoming paper-based documentation shall be converted and stored in the Portable Document Format (PDF)[2].

1.4 Information and Data Delivery

1.4.1 An information portal shall be provided for the *Client* to view the Project Information Model.

1.4.2 The information portal shall include

- the 3D geometrical model of the design which the viewer can navigate in 3D,
- geospatial information,
- all datasets associated with the 3D geometrical model,
- time dependant construction phasing,
- current construction progress information,
- existing topographical information,
- the 3D geometrical ground model,
- all archaeological information and
- the latest digital survey of the site which permits the 3D and time depended (4D) components of the Project Information Model to be overlaid.

1.4.3 The Employer Common Data Environment (E-CDE) shall be Business Collaborator.

1.4.4 All *Client* Shared Status or Published Status information shall be exchanged with the E-CDE within forty-eight (48) hours.

1.4.5 All Information of Shared Status shall be exchanged with the E-CDE in their native file formats at a maximum of monthly intervals.

1.4.6 The following data shall be exchanged every twenty-four (24) hours to the CIP Data Reporting and Analytics Platform (“Data Hub”)

- data which is created by the *works,*
- project control data in accordance with the requirements contained in Volume 2 Part 8 (Integrated Project Controls) of the contract,
- health and safety management system data in accordance with the requirements contained in Volume 2 Part 1 (General Requirements) of the contract, and
- new versions of any *Client* Shared Status data in the P-CDE including the Project Information Model, with associated linked datasets.

[2] As defined in ISO 32000-2 Document management - Portable document format - Part 2: PDF 2.0 [14]

1.4.7 Data which is created by *the works* shall include where the data is available

- groundwater instrumentation and monitoring,
- construction plant and vehicle telemetry including GPS equipment,
- ground monitoring instrumentation,
- temporary traffic control instrumentation
- any other instrumentation and monitoring.
- surveys,
- site worker GPS equipment,
- the *Contractor's* health and safety system for recording inspections, and other visits, observations and incident events in accordance with requirements contained in Volume 2 Part 1 (General Requirements) of the contract,
- service strikes and
- Smart Assets.

1.4.8 The provision of data to the Data Hub Should be automated.

1.4.9 All data exchanges with the Data Hub shall be as required by the *Project Manager* including

- data source,
- data format,
- sampling size and
- sampling frequency

1.5 Reference Information and Shared Resources

Reference information and shared resources are listed in Volume 5 (Data Room) of the contract.

2 Information Security and Client's Data Handling Requirements

2.1 General Requirements

2.1.1 A failure to comply with this section 2 (Information Security and Client's Data Handling Requirements) is treated as a substantial failure by the *Contractor* to comply with its obligations.

2.1.2 A level of Information Security for the *works* and Equipment shall be provided in accordance with the guidance and recommendations contained in BS EN ISO 19650-5:2020 'Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling Part 5: Security-minded approach to information management' [6].

2.1.3 Unless otherwise agreed with the *Project Manager, the Client*'s data shall not be stored or processed outside of the UK or European Union.

2.1.4 The UK Government Technology Code of Practice [7] shall be complied with.

2.1.5 The *works* and the *Contractor's* information communication and technology systems (including any networks) shall be provided in accordance with the requirements, guidance and recommendations contained in

- BS EN ISO / IEC 27001 'Information Technology - Security Techniques - Information Security Management Systems – Requirements' [8] and
- BS EN ISO/IEC 27002 'Information Technology - Security techniques - Code of practice for information security controls' [9]

2.1.6 The *works* and the *Contractor's* information communication and technology systems (including any networks) shall be protected against cyber-attack in accordance with the requirements, guidance and recommendations

- produced by the UK Government National Cyber Security Centre [10],
- of the UK Government Cyber Essentials Scheme [11] and
- contained in the Cabinet Office Minimum Cyber Security Standard [12].

2.1.7 An Information Security Management System (ISMS) shall be provided for all of the *Contractor*'s System(s).

2.1.8 The ISMS shall be certified by a UKAS registered organisation (or other equivalent European accreditation body full member agreed by the Project Manager) to BS EN ISO 27001 'Information Technology - Security Techniques - Information Security Management Systems – Requirements' [8] within six (6) months of the *starting date* .

2.1.9 An individual shall be appointed as security lead who is to be responsible for the implementation and compliance with the security requirements of the Scope.

2.1.10 An Information Security Management Plan shall be prepared and submitted in accordance with Volume 2 Part 9 (Review and Certification) of the contract which

- complies with the requirements of BS ISO/IEC27001 'Information Technology - Security Techniques - Information Security Management Systems – Requirements' [8] and BS EN ISO/IEC 27002 'Information Technology - Security techniques - Code of practice for information security controls' [9]

- is included in the Quality Management System[3] and
- demonstrates how any system, or equipment which stores the *Client's* data shall be safely and securely disposed of.

2.1.11 The Information Security Management Plan shall include procedures which demonstrate how the *works* and Equipment will be provided to

- comply with Data Protection Legislation,
- protect information against accidental, unauthorised or unlawful processing, destruction, loss, damage or disclosure of *Client's* data,
- prevent unauthorised persons accessing Personal Data in accordance with the requirements contained in Volume 2 Part 1 (General Requirements) of the contract or equipment used to process *Client's* data,
- manage and report Security Incidents,
- prevent the disclosure of confidential or proprietary information,
- protect Systems from viruses, malware and security threats,
- safely and securely back-up and restore System data,
- format of data storage,
- safely and securely dispose of Systems and
- vet Staff[4].

2.1.12 The Information Security Management Plan shall define the following for all *Contractor* System(s)

- Service Level Agreements,
- Recovery Point Objectives and
- Recovery Time Objectives

2.1.13 Information security training for *Contractor* personnel for the provision of the requirements contained in the Information Security Management Plan shall be provided on annual basis.

2.1.14 The Information Security Management Plan shall be prepared and submitted

- within twelve (12) weeks of the *starting date* and annually thereafter and
- upon any change.

2.1.15 All *Client's* data held in any format (electronic or hardcopy) by the *Contractor*, subcontractor, or Sub-Processor at any stage of remoteness, no longer required to provide the *works* shall on Completion of the relevant *section* be

- provided to the *Project Manager* in a format agreed with the *Project Manager,* or if not required by the *Client*,
- disposed of in a safe and secure manner.

2.2 System Management

2.2.1 All *Contractor's* System(s) shall be vendor supported and provided with security updates.

2.2.2 An architecture diagram shall be prepared and maintained which includes

- the connectivity of all Systems and
- network security controls.

2.2.3 The *Contractor's* System(s) Should be configured with tools to

[3] The Quality Management System is defined in Volume 2 Part 1 (General Requirements) of the contract.

[4] in accordance with the *Client's* staff vetting procedures, see Annex C in Volume 2 Part 1 (General Requirements) of the contract.

- automatically deploy security updates,
- permit updates and patches to be applied and
- permit the system to be rolled-back following the application of an update or patch.

2.2.4 Disruption or a failure of the *Contractor's* Systems shall not result in data loss in excess of that set out in the Information Security Management Plan.

2.2.5 The *Contractor's* System(s) shall be backed up

- to achieve the Recovery Point Objective and
- prior to a change and immediately after any successful change to the TCMS (including upgrades or patches).

2.2.6 The *Contractor's* System(s) shall be provided so that operation can be quickly and efficiently restored following a failure of the System to achieve the Recovery Time Objective.

2.2.7 If the *Contractor's* System(s) are provided with Multi-Factor Authentication (MFA), MFA shall be used.

2.3 Security Testing and Vulnerability Management

2.3.1 All *Contractor(s)* System(s) shall be tested for security weaknesses through a security test conducted

- prior to activation and
- annually thereafter.

2.3.2 The scope of the security test for the *Contractor's* System(s) shall be agreed with the *Project Manager*.

2.3.3 The un-abridged version of the *Contractor's* System(s) security test reports and its recommendations shall be provided to the *Project Manager*.

2.3.4 A Remedial Action Plan shall be prepared which proposes how vulnerabilities identified in the *Contractor's* System(s) following security testing shall be mitigated.

2.4 Event Reporting & Incident Management

2.4.1 A log of all Security Incidents shall be made available to the *Project Manager*.

2.4.2 All Security Incidents defined as a Major Security Incident shall be reported to the *Project Manager* as soon as reasonably practicable, but not exceeding forty-eight (48) hours of the *Contractor* becoming aware of the Security Incident.

2.4.3 Any Major Security Incident shall be subject to root cause analysis with a report produced documenting the cause of the Security Incident along with proposed remedial actions which could prevent a recurrence of the Security Incident.

2.5 System Hardening and Configuration

2.5.1 The *Contractor(s)* System(s) used shall not use legacy, or insecure protocols.

2.5.2 Documentation which demonstrates that the network configuration management interface is secured shall be provided in the Information Security Management Plan.

2.5.3 Unused network configuration and management functions on the network devices shall be removed or disabled.

2.5.4 The *Contractor(s)* System(s) shall be provided with the capability for the detection and prevention of malware and other malicious activity.

2.6 Digital Signatures

2.6.1 The *Contractor* shall use digital signatures for all submissions including certificates.

2.6.2 Digital signatures shall be

- obtained from a reputable certificate authority which the *Project Manager* can publicly verify the authenticity and identity of the entity using the digital signature and
- stored securely and password protected such that only the owner of the signature shall have access to its use.

2.6.3 The *Contractor* (and any Consortium Member) shall

- amend (if necessary) its disciplinary procedure and policy to include the misuse of digital signatures (including the sharing of passwords and login details) as a disciplinary matter and
- procure its subcontractors (at any stage of remoteness from the *Client*) do the same.

2.6.4 The use of digital signatures, whether correctly or incorrectly, shall not invalidate the dispute process or relieve the *Contractor* of its obligations to the *Client*.

3 Client’s Information Systems

3.1 General requirements

3.1.1 *Client* and *Contractor* personnel using the *Client’s* information systems shall be trained on the *Client’s* information systems.

3.1.2 The following *Client’s* information systems shall be used by the *Contractor*[5]

- CEMAR,
- Xactium,
- Microsoft Dynamics 365,
- AirsWeb 2,
- Microsoft Office 365,
- Data Hub and
- Business Collaborator.

3.1.3 Licenses for the Microsoft Office 365 A303 Stonehenge tenancy for the *Contractor* shall be provided by the *Client.*

3.1.3a The following systems shall use the Microsoft Office 365 A303 Stonehenge tenancy

- Microsoft Dynamics 365,
- Microsoft Office 365 and
- Data Hub.

3.1.4 Not used.[6]

3.1.5 The *Contractor* shall submit requests for licenses for the Microsoft Office 365 A303 Stonehenge tenancy to the *Project Manager* for acceptance.

3.1.6 A reason for not accepting license requests for the Microsoft Office 365 A303 Stonehenge tenancy is that it

- exceeds maximum of 1500 in any year[7] or
- exceeds a quantity not agreed with the *Project Manager*.

3.2 CEMAR

3.2.1 CEMAR shall be used for the management of all contract communications.

3.2.2 The *Client* shall own and operate CEMAR.

3.2.3 The *Client* shall provide first line support and coordinates any escalation with CEMAR.

3.2.4 A Staff member shall be nominated by the *Contractor* for the role of CEMAR Superuser.

3.2.5 The role of CEMAR Superuser shall be to

- manage user access to CEMAR and
- liaise with the *Client’s* CEMAR users.

3.2.6 CEMAR licenses for the *Contractor* shall be provided by the *Client.*

[5] The *Client’s* information systems also include Prism and Primavera P6. This section provides the format requirements of the *Contractor’s* submissions where they shall be compatible with the *Client’s* Prism and Primavera P6 systems.
[6] Not used.
[7] Licenses are provided on an annual basis.

3.3 XACTIUM

3.3.1 Xactium shall be used for the management of risk in accordance with the requirements contained in Volume 2 Part 1 (General Requirements) of the contract.

3.3.2 The *Client* shall own and operate Xactium.

3.3.3 The *Client* shall provide first line support and coordinates any escalation with Xactium.

3.3.4 A Staff member shall be nominated by the *Contractor* for the role of Xactium Superuser.

3.3.5 The role of Xactium Superuser shall be to

- manage user access to Xactium and
- liaise with the *Client's* Xactium users.

3.3.6 XACTIUM licenses for the *Contractor* shall be provided by the *Client.*

3.4 Primavera P6

3.4.1 The *Client* shall use Primavera P6 as their programme management system.

3.4.2 The *Contractor* shall submit programmes to the *Project Manager*

- in a format agreed with the *Project Manager* (either Oracle XML or XER format)
- compatible with the *Client's* version of Primavera P6 (currently 17.12) and
- in accordance with the requirements of Volume 2 Part 8 (Integrated Project Controls) of the contract.

3.5 Microsoft Dynamics 365

3.5.1 The *Contractor* shall provide an IT Service desk using Microsoft Dynamics.

3.5.2 The IT Service desk shall include

- first line support and
- an IT ticket management system.

3.5.3 The *Contractor* shall provide first line support for Microsoft Dynamics 365 and escalate through the *Client's* solution provider Microsoft Dynamics 365 as necessary.

3.5.4 The *Client* shall provide Microsoft Dynamics 365 for Customer Relationship Management (CRM) for managing all stakeholder and customer correspondence.

3.6 AirsWeb 2

3.6.1 AirsWeb 2 shall be used for Health & Safety Incident Reporting in accordance with the requirements of Volume 2 Part 1 (General Requirements) of the contract.

3.6.2 The *Client* shall own and operate AirsWeb.

3.6.3 The *Client* shall provide first line support and coordinate any escalation with AirsWeb.

3.6.4 AirsWeb 2 licenses for the *Contractor* shall be provided by the *Client.*

3.7 Microsoft Office 365

3.7.1 The A303 Stonehenge Office 365 platform shall be used for the following collaborative services between the *Client*, the *Project Manager*, the *Supervisor* and the *Contractor*

- email and calendaring,
- instant messaging,
- video conferencing,
- workflow automation via MS Power Automate and PowerApps and
- reporting and dashboards via PowerBI.

3.7.2 The *Client* shall own the A303 Stonehenge Office 365 platform.

3.7.3 The *Contractor* shall operate the A303 Stonehenge Office 365 platform.

3.7.4 Not used

3.7.5 The *Contractor* shall provide first and second line support for Microsoft Office 365 and escalate third line support through Microsoft Office 365 support.

3.7.6 The *Contractor* shall provide administration for

- Microsoft Office 365 user accounts, roles, permissions,
- security for the tenancy and
- all Microsoft Office 365 components.

3.7.7 Not used.

3.7.8 Monthly reports on Microsoft Office 365 shall be provided to the *Project Manager*, including

- usage statistics and
- security audits.

3.8 CIP Data reporting and Analytics Platform (“Data Hub”)

3.8.1 The Data Hub shall be used for the Project Data Analytics.

3.8.2 The *Client* shall own the Data Hub.

3.8.3 The *Contractor* shall operate the Data Hub.

3.8.4 The *Contractor* shall provide the Project Data Analytics.

3.8.5 Project Data Analytics shall

- utilise an automated reporting platform to provide live reports via dashboards,
- incorporate third party data, where available, which may contribute to any Scheme data and
- incorporate any data sources at the request of the *Project Manager*.

3.8.6 Project Data Analytics shall be used for the following

- risk identification including: health and safety risks, programme risks, and design risks,
- Scheme Specific Performance Measures (SSPMs) reporting as specified in the Performance Manual and
- reporting requirements as specified in Volume 2 Part 8 (Integrated Project Controls) of the contract.

3.8.7 The Data Hub shall use the Microsoft Azure Data Platform.

3.8.8 Not used[8].

3.8.9 The *Client* shall provide administration of the following Data Hub components

- Azure Data Lake Storage for data storage,
- Azure Data Bricks for data cleaning and transformation,
- Azure Data Factory for data orchestration and movement and
- PowerBI as the reporting and dashboard tool (via Microsoft Office 365).

3.8.10 The *Contractor* shall provide individuals for the following roles

- Data Engineer (s) and
- Data Analyst (s).

3.8.11 The Data Analyst (s) shall design and provide the following processes

- data acquisition,
- data handling,
- data processing,
- data visualisation and
- Microsoft Power BI web service administration.

3.8.12 The Data Analyst (s) shall have the following key skills

- Microsoft Power BI web service administration,
- reporting and data visualisation,
- statistical knowledge,
- user interface design,
- SQL / database knowledge,
- spreadsheet expert,
- basic knowledge of azure resources and
- business analyst skills, including requirement gathering and good communication skills.

3.8.13 The Data Engineer (s) shall

- develop the data architecture,
- test the data architecture and
- maintain data architecture

3.8.14 The data architecture shall include how data is managed in all the data processes and visualisations designed by the Data Analyst.

3.8.15 The Data Engineer (s) shall have the following key skills

- Data Warehousing,
- In-depth data architecture and pipelining,
- In-depth SQL / database design and optimisation,
- Microsoft Power BI web service data flows, gateway and premium analytics and
- spreadsheet expertise.

3.9 Business Collaborator[9]

3.9.1 The *Client* shall own Business Collaborator.

3.9.2 The *Contractor* shall operate Business Collaborator.

[8] Not used.
[9] Business Collaborator means the *Client's* instance of Business Collaborator which is used for the E-CDE.

3.9.3 The *Contractor* shall use Business Collaborator in accordance with the *Client's* "Major Projects Directorate Document Management Manual" [13] contained in the Data Room [2] and the EIR.

3.9.4 Licenses for the *Client's* instance of Business Collaborator for the *Contractor* shall be provided by the *Client*.

3.10 Prism

3.10.1 The *Client* shall use Prism as its core information management system for commercial and integrated project controls management.

3.10.2 The *Contractor* shall submit commercial information in accordance with the requirements of Volume 2 Part 8 (Project Controls) of the contract.

4 Information Services Governance

4.1 Project Information Services Steering Group

4.1.1 An individual shall be nominated by the *Contractor* for the role of Information Services (IS) Lead.

4.1.2 The IS Lead shall attend the CIP IS Leads workshops every six (6) months to facilitate knowledge sharing and coordinate innovations between CIP projects.

4.1.3 The IS Lead and Digital Lead shall attend the Project IS Steering Group (ISG) each month[10].

4.1.4 The IS Lead shall provide the following at each ISG meeting

- update of IS activities and deliverables,
- overview of the IS strategy,
- reports on how the IS Strategy is aligned with wider A303 and CIP strategies and priorities,
- submissions of IS deliverables at project stage gates for review and acceptance and
- assistance with resolving issues and risks.

4.2 Information Services Strategy

4.2.1 The Information Services (IS) Strategy shall be prepared and submitted to the *Project Manager* in accordance with Volume 2 Part 9 (Review and Certification) of the contract

- within twelve (12) weeks of the *starting date* and annually thereafter and
- upon any change.

4.2.2 Any subsequent updates to the IS Strategy following the *Client's* review[11] shall address the *Project Manager's* comments and be resubmitted.

4.2.3 The IS Strategy shall cover all systems in sufficient detail to demonstrate the precise scope and approach to delivering the required outcomes and capabilities.

4.2.4 The IS Strategy shall include

- a description of deliverables and outcomes, including infrastructure, business systems, policies and procedures,
- a Service Delivery Plan specifying Service Level Agreement (SLA) and coordination with *the Contractor* and its subcontractors (at any stage of remoteness from the *Client*),
- demand requirement / change control,
- resource plan,
- knowledge sharing/collaboration with CIP,
- proposed innovation,
- Service Management,
- the use of Project Data Analytics in relation to health, safety and wellbeing,
- the methodology for capturing, managing and reporting data for Scheme Specific Performance Measures and

[10] All Information Services scope, investment and performance shall be governed and monitored by the project IS Steering Group (ISG), chaired by the *Project Manager*.

[11] The *Client's* IS Steering Group has two (2) weeks to review the proposed strategy and notify the *Contractor* of any required changes.

- how the Data Hub will be used to manage data, including an architecture diagram.

Reference List

[1] Highways England, “Employers information Requirements v3.0.4,” 2020.

[2] Highways England, “Data Room,” [Online]. Available: https://a303stonehenge.sharepoint.com/sites/DataRooms/procurement/main-works/Shared%20Documents/Forms/AllItems.aspx. [Accessed April 2020].

[3] British Standards Institution (BSI), “BS EN ISO 19650:2018. Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling.”.

[4] Highways England, “Asset Data Management Manual,” [Online]. Available: https://www.standardsforhighways.co.uk/ha/standards/admm/index.htm. [Accessed April 2020].

[5] British Standards Institution (BSI), “PAS 1192-2 Specification for information management for the capital/delivery phase of construction projects using building information modelling.,” 2013.

[6] British Standards Institution (BSI), “BS EN ISO 19650-5:2020. Information management using building information modelling Part 5: Security-minded approach to information management”.

[7] Government Digital Service, “UK Government Technology Code of Practice,” [Online]. Available: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice. [Accessed April 2020].

[8] British Standards Institution (BSI), “BS EN ISO / IEC 27001 ‘Information Technology - Security Techniques - Information Security Management Systems – Requirements,” 2017.

[9] British Standards Institution (BSI), “BS EN ISO/IEC 27002 ‘Information Technology - Security techniques - Code of practice for information security controls’”.

[10] The National Cyber Security Centre, “The National Cyber Security Centre,” [Online]. Available: https://www.ncsc.gov.uk/.

[11] The National Cyber Security Centre, “National Cyber Security Centre,” [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/.

[12] Cabinet Office, “Minimum Cyber Security Standard,” [Online]. Available: https://www.gov.uk/government/publications/the-minimum-cyber-security-standard .

[13] Highways England, “Major Projects Directorate Document Management Manual Ver 1.3,” 2019.

[14] British Standards Institution (BSI), “BS ISO 32000-2:2017 Document management - Portable document format - Part 2: PDF 2.0”.

[15] Highways England, “A303 Amesbury to Berwick Down: 6.3 Environmental Statement Appendix 2.2 (8) - Outline Environmental Management Plan (OEMP),” 2020. [Online]. Available: https://infrastructure.planninginspectorate.gov.uk/wp-content/ipc/uploads/projects/TR010025/TR010025-001950-6.3%20Appendix%202.2(8)%20%E2%80%93%20Outline%20Environmental%20Management%20Plan%20(OEMP)_FINAL_DfT%20Revision_TRACKED%20CHANGES.pdf.