UK Government BIM Working Group

CDE Sub Group

Asset Information Management - Common Data Environment

Functional Requirements

CONTENTS

Figures

EXECUTIVE SUMMARY

This document describes the functional requirements of a BIM Level 2 Asset Information Management Common Data Environment (AIM CDE).

The purpose of an AIM CDE system is to provide a standards compliant environment to specify, collect, assure, store, present and exploit BIM Level 2 information (structured data, 3D models and documents) about the Development and Operational phases of maintained and operated assets from the point of view of a UK Government Department.

"The AIM CDE shall help manage both project and asset information in accordance with BS1192 best practice."

The aim is to help asset owners and operators to procure information in accordance with industry standards, namely BS 1192:2007+A2:2016, PAS 1192-2:2013, PAS 1192-3:2014, BS 1192-4:2014, PAS 1192-5:2015 BS 8536-1:2015 and BS 8536-2:2015.

The AIM CDE covers the BIM and information procurement process from the Employer's point of view and on the Employer's side of the contract line.

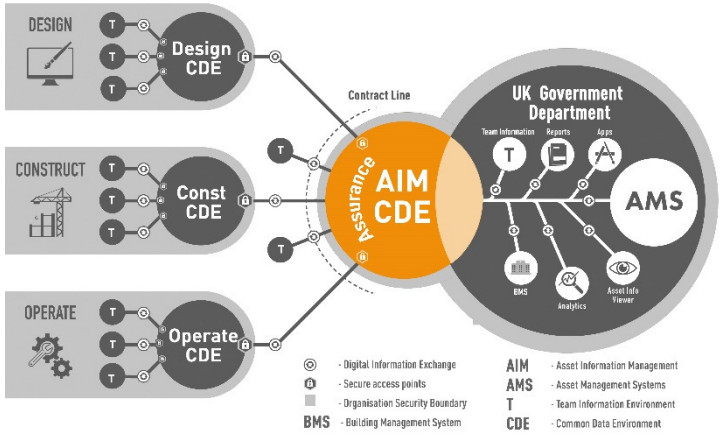

Figure 1 - AIM CDE supports the procurement of assured information

The AIM CDE is a secure online system with dedicated functionality to support the Government Department's role to procure assured information and data to meet their requirements, during not only new build, but also both major and minor refurbishment projects and also operation and maintenance service contracts. The AIM CDE system provides functionality to support information management.

The intention is that the system hosts the required BIM Level 2 information and data about an entire portfolio or estate and represents a reliable assured digital representation of the physical assets themselves.

"An AIM CDE is needed to achieve BIM level 2 benefits which aim to reduce the cost of public sector assets by up to 20%."

The information and data stored shall be sufficient to inform key business decisions at defined gateways or events during capital delivery and operations and inform optimal usage and maintenance strategies.

Digitising an estate with the adoption of BIM Level 2 best practice processes promises to improve the way built and managed assets are delivered, operated and also maintained, significantly reducing capital delivery and operational costs.

In many cases, Government Departments already have systems that store information about their assets. However, these systems often have limited capabilities to procure and assure the information and handle asset information generation across entire portfolios or estates.

Thanks to advances in software, network infrastructure, cloud computing and internet security, there are information management systems available on the market capable of managing asset information in a way that is prescribed in the BIM Level 2 standards.

"An AIM CDE is needed to help achieve the efficiencies required by the Government Construction Strategy: 2016-2020."

The requirements found in the main body of this document are intended for use in Government Department requests for proposals (RFP). The requirements are to be used as selection criteria when assessing the capabilities of AIM CDE vendors and their systems.

Without an AIM CDE system Government Departments will find it difficult to realise the benefits associated with BIM Level 2 and achieve the efficiencies targeted in the Government Construction Strategy: 2016-2020. The UK Government BIM Working Group recommends the procurement and implementation of an AIM CDE for all UK Government Departments that manage built assets.

OVERVIEW

The AIM CDE system shall support the progressive build-up of BIM Level 2 information during the course of a capital delivery project or service supply contract, in accordance with British Standards 1192 series best practice information management standards.

Enabling suppliers to meet their contract information delivery obligations, the AIM CDE system provides Government Departments with more reliable information, procured to answer employer plain language questions (PLQ), in order to make more informed agile decisions.

The AIM CDE system shall manage project and asset information, made up of 3D model files, drawings and documents, and structured data extracted from BS1192-4 data format files.

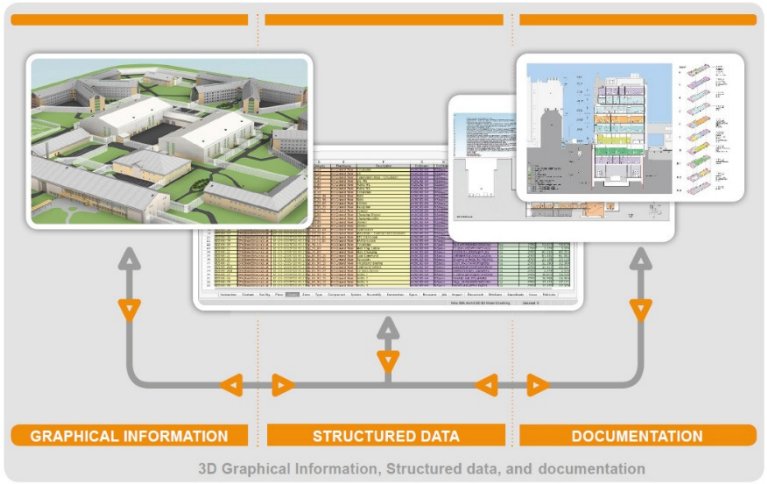

Figure 2 - Graphical Information, Structured data, and documentation

"The AIM CDE manages 3D model files, drawings and documents, and structured data presented in BS1192-4 data format."

Subject to the Departments information requirements the managed information shall represent the physical and functional characteristics of the assets, including extents, regions, facilities, floors, spaces, features, locations, systems and components and their associated characteristics. It also includes supporting information about the assets, such as costs, performance, specifications, operation and maintenance and health and safety information.

Asset information shall be organised in a way which makes it easy to navigate, find and visualize information. Every object, be that a facility, floor, space, zone, system or component shall be connected to another object in a hierarchy and linked to relevant data attributes and documents in the BS1192-4 data structure.

The management of file-based information and extracted data shall be in accordance with the employer CDE process, described in the PAS 1192-3. 'Shared' non-contractual information shall be clearly and separately identified from 'Published' contractual information.

From a 3D geometry view, users shall click on an object and access relevant documents and data. From a tabular data view, users shall be able to view 3D objects and access documents, and from a document list view, users shall navigate back to the data and the 3D geometry.

The AIM CDE system shall be scalable to enable the procurement and management of information on multiple capital delivery projects, refurbishments, minor works projects and operation and maintenance service contracts, at any one time.

"The AIM CDE shall manage information supplied during new capital delivery projects and operation and maintenance service contracts."

Appendix 5 illustrates the implementation of the AIM CDE in context with the BIM Level 2 British Standards.

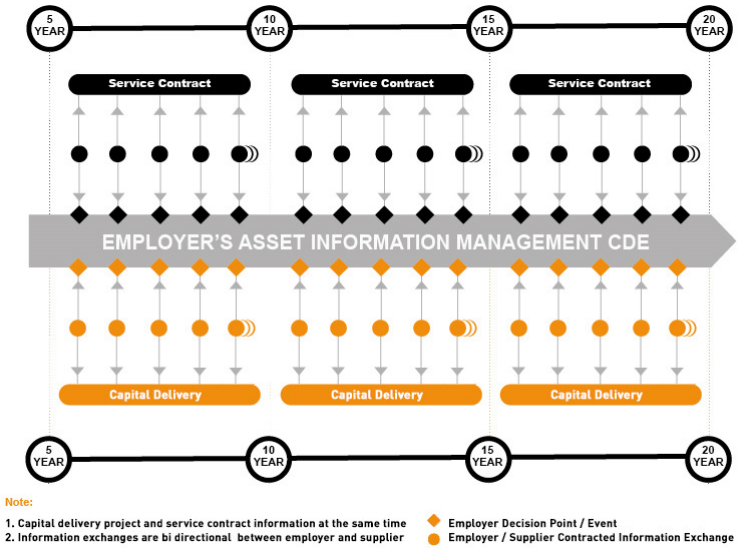

Figure 3 - Concurrent capital delivery and maintenance service contracts

FUNCTIONALITY

The functional requirements for the AIM CDE are organised into five categories, summarized in table below.

"The functional requirements are organised into 5 sections and sub sections as shown in table 1."

1.0	**Information Procurement**
1.1	Defining Information Requirements (Employer)
1.2	Defining information deliverables (Suppliers)
1.3	Information Exchange (Files and Data)
1.4	Information from other Systems
2.0	**Information Assurance**
2.1	Information delivery planning Assurance
2.2	Information Assurance (Files)
2.3	Information Assurance (Data)
2.4	Acceptance and Authorisation Workflows
2.5	Assurance Reporting
3.0	**Storage & Cyber Security**
3.1	File Store
3.2	Data Store
3.3	Cyber Security
4.0	**User Functionality**
4.1	File management
4.2	Model Management
4.3	Data Management
4.4	Collaborative Workflow & Information Reviews
4.5	Navigation and Search in 5
4.6	Project & Asset set up templates
4.7	Viewers
4.8	Audit trail
4.9	Dashboard, Analytics and Reporting
4.10	Tender Management
4.11	Contract Management
4.12	Standard Object Libraries
4.13	Company and user management
5.0	**Information Output**
5.1	Files and Data Download
5.2	Application Program Interfaces (APIs)

Table 1 - Functional Requirement Categories

1. Information Procurement

The AIM CDE shall provide functionality to enable Government Departments to procure information about built and maintained assets during capital delivery projects and on service contracts.

The functionality shall include the capability for the employer or employer's agent to select and define specific information requirements in an information delivery planning tool (IDP). The information requirements shall support key decisions during the course of a capital delivery programme and during operation and maintenance.

The information delivery planning tool shall also include the capability for suppliers to register and schedule file level deliverables against the information requirements. An example of the information delivery planning tool is shown in appendix 2.

"The functionality for Government Departments to select and define specific information requirements in an information delivery planning tool."

1.1 Defining Information Requirements (Employer)

The information delivery planning tool shall provide the necessary functionality for a Government Department to register information requirements at key stages during the capital delivery phase of a project and at events during service contracts.

Project or contract specific information requirements shall be created from master templates which align with the Department Digital Plan of Work and shall be set up to answer Plain Language Questions (PLQ) and support the government department decisions.

During tendering suppliers shall securely register any comments against requirements in the information delivery planning tool. The information planning tool shall also have the ability to import and export information requirements to and from other information planning systems, for example the NBS BIM Tool Kit.

1.2 Defining information deliverables (Suppliers)

"…functionality for suppliers to exchange files and data into the AIM CDE."

The AIM CDE shall provide suppliers with the ability to register and schedule file level information deliverables against corresponding information requirements, in the information delivery planning tool.

Once appointed Suppliers shall be able to define the files and data they plan to supply, registering and scheduling it in the information delivery planning tool. Suppliers shall also be able to update their planned file deliverables during the course of a project.

1.3 Information Exchange (Files and Data)

"Reports to compare planned information deliverables vs actual."

The AIM CDE system shall support a managed exchange of information from suppliers and Government Department teams during a project or service contract. The interfaces for the exchange of information shall be intuitive, handle large file transfers and ensure efficient registration of metadata fields.

Functionality enabling the association of file uploads with scheduled file deliverables in the information delivery planning tool, shall be provided to enable assurance reporting, comparing planned information supply with actual.

The AIM CDE system shall also enable the exchange of BS1192-4 data files which shall be extracted into a Data Store, respecting the necessary assurance, version control and audit trail. See Appendix 3.

"…functionality for data to be provisioned into the AIM CDE from other systems I e.g. an AMS system."

The extracted BS1192-4 data shall link to corresponding files in the file store, and contain appropriate object data with defined bounding box geometry positioning, providing the basis for a structured and linked file and data information model.

1.4 Information from other Systems

Via a reliable data integration, data virtualization service or application program interface (API), it shall be possible to migrate data from other systems into the AIM CDE System. For example, integration with an enterprise the Asset Management System (AMS).

Information supplied via other enterprise systems should be subject to the same authenticity, version control assurance and security considerations as other information delivery.

2. Information Assurance

The AIM CDE shall provide a suitable level of information and data quality assurance to mitigate mistakes and errors and to assure that information supplied meets the requirements in the Information Delivery Planning Tool. See Appendix 2.

The assurance capability shall be provided through a combination of automated digital verification and manual review / sign off validation processes. Together the automated and manual checks shall confirm that the files and data quality are appropriate, within range and meet the Employer's Information Requirements (EIR). This capability is expected to mature over time.

"All information supplied to the AIM CDE will be verified by the system and validated against corresponding information requirements."

Note: the term Information Assurance used in this document applies to the processes used to verify the completeness, consistency, accuracy and integrity of the files and data quality supplied against what is specified and procured, and validate the information procured against the information requirements and Plain Language Questions (PLQ). Also see BS1192-4 cl 4.3.3 and the glossary in Appendix 1.

2.1 Information delivery plannning Assurance

The first assurance step (A) is to confirm that project or contract specific information requirements as selected in information delivery planning tool are justified against a standard Departmental information requirements master template, as a baseline. The AIM CDE shall provide appropriate functionality to report variation and record justification of the variance.

The second step (B) is to confirm individual suppliers' pre-contract delivery proposals against the information requirements. This may form part of tender assessments. The AIM CDE shall provide appropriate functionality to report and compare supplier proposals against the specific information requirements and support supplier selection.

The third step (C) is assurance that the post-contract supplier schedule of proposed file deliverables aligns with the contracted information requirements. The AIM CDE shall provide appropriate functionality to report on incomplete file delivery proposals for each engaged supplier.

2.2 Information Assurance (Files)

"All files uploaded to the AIM CDE shall go through an assurance process."

Formal system checks and workflow should be initiated as soon as files are presented and should include compliance and verification checks on all files, file names and metadata. All non-compliant published information in part or whole shall be rejected.

The fourth assurance step (D) is a check that all files identified in the supplier schedule of proposed file deliverables have been delivered, published and are present in the AIM CDE. Published delivered files shall be reported against the supplier schedule to highlight present, late or missing delivery – green, amber or red.

2.3 Information Assurance (Data)

"All data uploaded to the AIM CDE shall go through an assurance process to ensure the data is compliant and complete."

Steps (E, F G & H) are concerned with data compliance and completeness checks which verify delivered BS1192-4 data. See appendix 3

The verification functionality shall check BS1192-4 data files contain linkages to the other scheduled files, object geometric bounding box data, data format and levels of definition specified in the IDP tool, and against template objects in the object type library, which acts as demand matrices.

2.4 Acceptance and Authorisation Workflows

"All non-compliant published information in part or whole shall be rejected."

Supplied information shall be routed through Shared acceptance or Published workflows, dependent on the suitability status code. The system should include sufficient viewing and mark-up capabilities to ensure read-only review, markup and validation is possible without stand-alone software.

2.5 Assurance Reports

The AIM CDE shall have assurance reports which shall report on each assurance step A to I, again see Appendix 3. Assurance shall be reported via summary and detailed reports with red/amber/green (RAG) status reports.

3. Storage & Cyber Security

"Within the AIM CDE data and information shall be stored in a data store and a file store respectively."

The AIM CDE information shall be stored in both a File Store containing presented native and open standard model, document and BS1192-4 data files, and a Data Store containing extracted BS1192-4 data as information models mapped to the presenting BS1192-4 files. The File and Data Stores shall hold data and linked files as project or service supply contract workspace focused information models. Information shall also be accessible across the whole AIM CDE as a single virtual entity to accommodate alternate virtual view contexts, e.g. mapping or data focused asset portfolio use cases which may cut across the workspace context.

3.1 File store

"The files store shall hold version controlled 'Shared status' and 'Published status' files and metadata."

The File Store shall hold Shared and Published status project and contract files supplied progressively through the course of the asset lifecycle and available for use in subsequent stages. The file store shall be presented as a fully configurable secure electronic document management system, capable of receiving and storing native and open format models, BS1192-4 and open format data files and other native and open format documentation. Documents formats shall include photos and other media files, surveys, commercial and legal documents classified by the IDP deliverable information breakdown structure reference – Delivery Reference.

3.2 Data store

"The data store shall hold structured data compliant with BS1192-4."

The AIM CDE shall store data extracted from Published status structured data BS1192-4 files presented by information suppliers.

Note: the specified BS1192-4 data shall be published as separate deliverable files by suppliers and not embedded in alternate open model format files for extraction after submission. The responsibility to provide appropriate BS1192-4 data lies with the information supplier.

Data shall be subject to an assurance process on presentation before entry into the published state Data Store. Data shall be bound to the delivering file as separate 'model instances' to be viewed in a model viewer complete with linked files & data.

Segregation of information shall align across both File and Data Stores and through either the user or machine (API) interface defined by at

least volume and location strategies.

The AIM CDE shall enable an extraction, transaction and load (ETL) process of authorised published data files, to ensure the secure storage of structured data available for exploitation. It shall be possible to query and view the data store in a user interface including links to information held in remote systems.

3.3 Cyber Security

The security requirements for the AIM CDE system will vary between Government Departments, but in all cases appropriate security and security minded principles shall apply in the context of each project and service contract.

CDE systems typically engage with a broad range of stakeholders and a web based environment is the most effective way of sharing asset information.

While enabling improved collaboration, web based information systems also bring an increased risk of security breaches through widening access to asset information.

"Security risks associated with the internet & web systems mean security measures must be taken when implementing and using an AIM CDE."

The security risks associated with cloud and web-based information systems can be mitigated by taking appropriate security measures. Reference should be made to two key documents, amongst others:

1) The Centre for the Protection of National Infrastructure (CPNI) security guidance for BIM Level 2 Common Data Environments (CDEs).

2) PAS1192-5:2015. The UK specification for security-minded building information modelling, digital built environments and smart asset management.

The CPNI guidance describes 14 cloud security principles that both the Government Departments and System vendors shall adhere to. The application of these principles is covered later in the requirements section.

4. User Functionality

The AIM CDE shall, above all, be easy to use, with information being quick to retrieve. Additionally it shall provide the following key functionality:

"Important criteria when selecting an AIM CDE, include ease of use, speed and reliability."

4.1 File management

The AIM CDE shall support file management and meet the standard requirements in BS1192 2007 A2 2016 such as file naming, document numbering, status fields, document types, revision sequences, location metadata classification

4.2 Model Management

The AIM CDE shall enable the viewing and federation of open format or proprietary models. Users shall be able to navigate around federated models in 3D, click on objects and see associated data and documents.

4.3 Data Management

The AIM CDE shall accept published data submissions through the BIM Level 2 BS1192-4 data file submissions. The AIM CDE shall extract submitted data into a data store where the data can be viewed, checked and analysed, queried and extracted.

4.4 Collaborative Workflow & Information Reviews.

The AIM CDE shall support the collaboration management processes described in BS1192 2007 A2 2016, PAS1192 Part 2 and 3. In particular, the system shall support the PAS1192-3 Shared: accept review and markup, and Publish: verify and validate, acceptance processes.

4.5 Navigation and Search

The AIM CDE shall enable simple searches and a navigation experience to locate projects, assets, document files, model files and data both within a workspace and across workspaces.

"The user functionality requirements cover the features that are expected in the interface of the AIM CDE solution."

The AIM CDE shall provide functionality to allow users to navigate through a model and access documents and data associated with particular objects, navigate through document lists and navigate to associated objects in the model and navigate through a non-geometric view of data and navigate to geometric objects and associated documents.

4.6 Project & Asset set up templates

The AIM CDE shall provide functionality to set up project/contract workspaces to host project and contract information collected through the capital delivery phase of a minor and major works projects (Design, Build and Commission) and service contracts.

4.7 Viewers

The AIM CDE shall include a viewer with the ability to view common industry file formats, negating the need for end users to run native applications to read common files.

4.8 Audit trail

The AIM CDE shall provide full audit reports which shall include tracking events, upload, issue, accessed, read, edited, moved, download and status changed and distributed information and shall include date and by whom the action was carried out by.

4.9 Dashboard, Analytics and Reporting

The AIM CDE shall provide a dashboard interface to alert users of any updates or changes to information and a summary of incoming and outgoing tasks. The AIM CDE shall provide a flexible and configurable report module that allows the employer's staff to deliver bespoke and predefined reports on project and/or assets.

The reports shall be created and named in the AIM CDE by an appropriate level user, and separately called by name only to execute.

4.10 Tender Management

The AIM CDE shall provide the necessary functionality and security to manage the information exchanges and during the tendering process, ensuring tender responses from bidders are segregated and private from competing bidders.

4.11 Contract Management

The AIM CDE Shall provide the functionality to manage contract workflows and the requirements of ACA, ACE, CIC, CIOB, FIDIC, JCT, NEC, PPC and RIBA contracts.

4.12 Standard Object Libraries

The AIM CDE shall provide functionality to store and manage standard object type libraries, along with associated geometry, data and documents.

4.13 Company and user management

The AIM CDE shall provide functionality to set up companies, assign users to their respective companies, to set up users and assign them access to project and or asset workspaces.

The AIM CDE shall provide functionality for users to manage their own details and user access credentials.

5. Information Output

"It is important that the AIM CDE has sufficient functionality to exploit stored data, model files and documents."

The primary purpose of the AIM CDE is to support the controlled procurement and assurance of project and asset information so it can be relied on by stakeholders and re-used by other systems, it is therefore important the AIM CDE has sufficient functionality to exploit the stored assured data and linked files.

Published project and asset information stored in the AIM CDE should be available for use by permitted stakeholders for a range of different purposes, subject to security and access permissions.

The AIM CDE shall enable exposure of data for use in other systems e.g. asset management systems or facility management systems. This can be through a reliable data integration service or application program interface (API).

5.1 Files and Data Download

The AIM CDE shall provide suppliers and staff with access to documents, models and data files to download, subject to full security

and disclosure rules and document marking. Files shall be available to download in bulk.

The export/download of files shall be available with applied renaming rules derived from metadata to meet employer naming policies.

5.2 Application Program Interfaces

The integration interface shall enable secure web services API connectivity to provide query-able data and linked files from the AIM CDE to appropriate connected authorised employer enterprise systems.

The queries shall be created and named in the AIM CDE by an appropriate level user, and separately called by name only from the external party or system.

All calls from external sources to the API or other interfaces shall update the audit trail and be subject to full security and disclosure rules.

FUNCTIONAL REQUIREMENTS

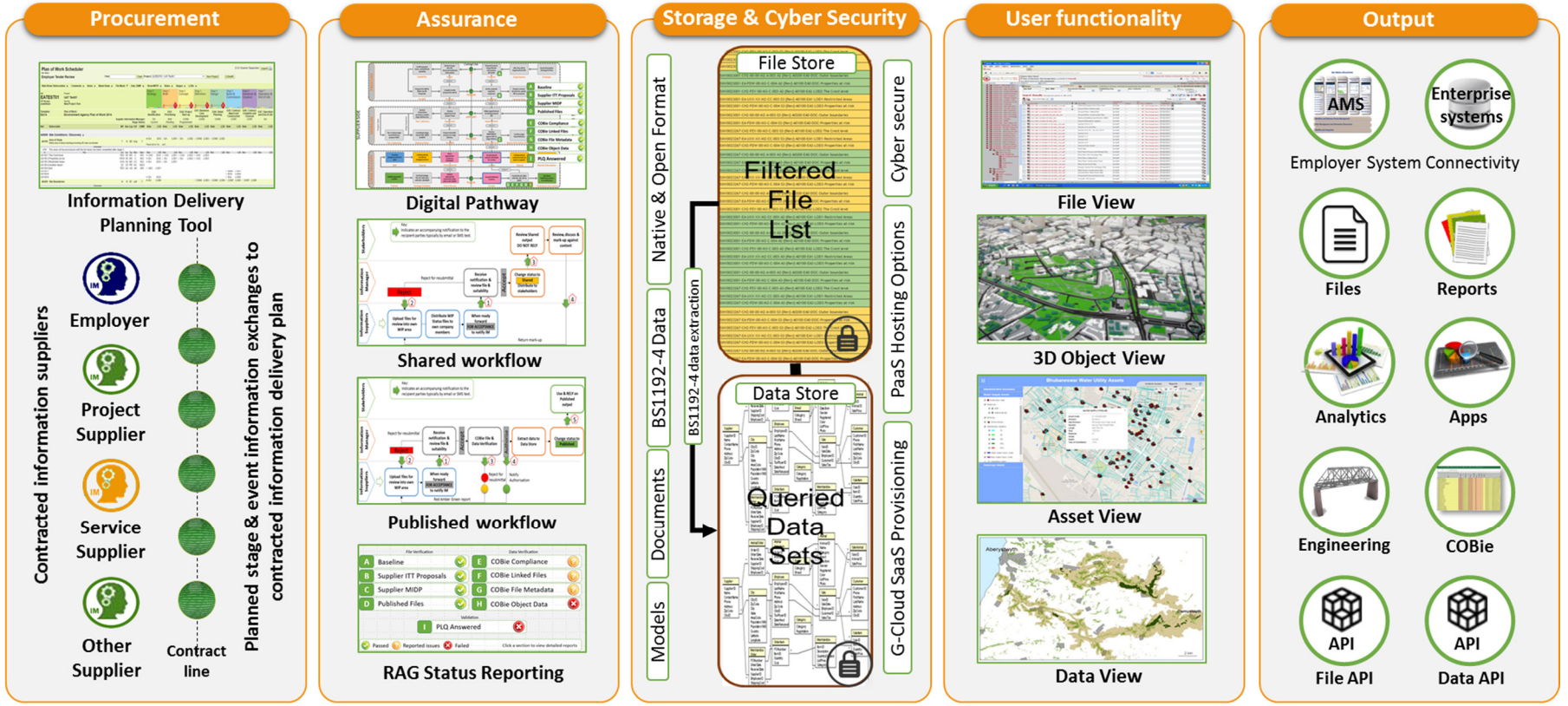

Figure 4 - Functional Requirements Summary

The five tables that follow, present detailed functional requirements in each of the five categories; Information procurement, information assurance, storage, hosting and security, user functionality and information output.

INFORMATION PROCUREMENT

1.0	**General**
The AIM CDE shall provide dedicated functionality to enable Government Departments to define information requirements and procure information from suppliers. The functionality shall include the capability for the employer or employer's agent, to select and define individual information requirements which support plain language questions and key decision making at stage gateways or events. The functionality shall include the capability for suppliers respond to each deliverable requirement at tender stage and to register and schedule individual file deliverables in the against each employer information requirement once appointed.	
1.1	**Defining Information Requirements (Employer)**
1.1.1	The AIM CDE portal shall include the capability to set up, manage and configure information delivery requirements to be selected and form the basis of a project or contract level information delivery plan (IDP).
1.1.2	It shall be possible to define and schedule information delivery requirements, identifying the information scope and formats required, the stage or event when it is required, who is responsible for delivering it, and the required level of information maturity (definition).
1.1.3	The functionality shall enable standard information delivery requirements to be picked from an indexed master template of information delivery requirements, comprising a standard set of information requirements definitions. (To enforce standardisation across projects)
1.1.4	When setting up Information delivery requirement they shall reference specific stage plain language questions to enable project or contract reporting.
1.1.5	The information delivery requirements master list shall be indexed with a standard information breakdown structure/delivery references. The index delivery reference shall be assigned to information as it is uploaded/supplied.
1.1.6	The information requirements master list shall include configurable metadata lists that will be available when registering and scheduling information deliverables. Note, some meta data will need to be configured for each project or service contract e.g. volume and location codes.

1.1.7	The IDP shall also have provision for individual information suppliers to securely add their tender response comments to each information delivery requirement definition. The project or service contract information manager should be able to filter and report on comments. The supplier should be able to only view their own comments.
1.1.8	It shall be possible to import and export the selected project or contract specific information requirements to tools such as the NBS BIM Tool Kit.
1.1.9	If shall be possible to subject changes to the IDP information deliverables post appointment to strict change control.
1.2	**Defining Information Deliverables (Supplier)**
1.2.1	The AIM CDE shall provide appointed suppliers with the ability to register and schedule their planned file level information deliverables (Master Information Delivery Plan) against each IDP information delivery requirement.
1.2.2	When setting up file level information deliverables the supplier shall be prompted to select the appropriate metadata, which will also automatically generate a unique document file name.
1.2.3	The IDP shall be exportable as a BS1192-4 data demand matrix file in a spreadsheet format.
1.2.4	The IDP demand matrix shall be used as the basis of the verification of delivered files and associated data at the identified information exchanges.
1.2.5	While the employer's individual information delivery requirements are contractual and subject to change control post award, the scheduled supplier file deliverables can be changed at any time; however, notifications shall be triggered when this happens.
1.2.6	The IDP tool shall track the actual file upload against the supplier scheduled items in the file store with a RAG status.
1.2.7	It shall be possible to filter the IDP by information types, suppliers, stages etc. For example, it shall be possible to filter by 3D model types to produce a view of models only (the equivalent of the Model Production Delivery Table (MPDT)
1.2.8	The AIM CDE IDP functionality shall include the ability to match IDP information requirements to stage Plain Language Questions, track supplier file level deliverables to each PLQ, and to attach dated notes to each stage PLQ to record the Gateway information validation position.

1. 3	**Information Exchange (Files and Data)**
1.3.1	The AIM CDE shall provide an intuitive mechanism and interfaces for information suppliers to submit the required native & open format model files, BS1192-4 and other required data files, documents, drawings and other file types. Typically, the supplier information exchanges are at, or prior to, prescribed milestones at the end of pre-defined stages or events during the course of capital delivery projects and service supply contracts and
1.3.2	The exchange mechanism shall facilitate the secure reception, registration and storage of multiple files in bulk. The file shall be stored in an electronic document management system (EDMS) – the File Store.
1.3.3	The exchange mechanism shall also facilitate exchange of data in a BS1192-4 data format file. BS1192-4 data spreadsheet files need to be selectively extracted and stored in the Data Store with links maintained to the associated files.
1.3.4	All input of file based information shall pass through an enforced configurable file name profiling and metadata setting process supporting BS1192 file naming standard and extensions. This metadata shall include reference to the appropriate IDP item information breakdown structure code. See appendix 4 for an example.
1.3.5	Only files named in accordance with the naming rules shall be accepted ensuring basic information registration and classification. Where file names are not provided in a compliant format they shall be profiled by the user on submission to select the appropriate metadata before acceptance.
1.3.6	Files shall be added to the system shall be associated with scheduled items in the IDP either by dragging and dropping over the appropriate scheduled item in the IDP or by selecting it from a list, or other mechanism.
1. 4	**Information from other systems**
1.4.1	Via a reliable data integration, data virtualisation service or application program interface (API), it shall be possible to migrate data from other systems into the AIM CDE System. For example, integration with an emterprise the Asset Management System (AMS).
1.4.2	Information supplied via other enterprise systems should be subject to the same authenticity, version control assurance and security considerations as other information delivery.

INFORMATION ASSURANCE

2. 0	**General**
The AIM CDE shall provide a suitable level of information assurance to mitigate mistakes and errors and to assure that information supplied is reliable for use and in line with the Information Delivery Plan (IDP). The assurance capability shall be provided through a combination of automated digital verification and manual review and sign off processes. Together the automated and manual checks shall confirm that the files and data are not only presented but are appropriate, within range and right, and meet the employer's information requirements. This capability is expected to mature over time. The AIM CDE shall support the verification and validation steps aligned to the BIM Working Group '**Digital Pathway**' see Appendix 3. These steps A -H recommend assurance measures to verify and validate the information requirements, information delivery plans and handed over files and data.	
2.1	**Information Delivery Planning Assurance**
2.1.1	The first assurance step (A) shall confirm that project or contract information requirements are justified against the standard Department information requirements and the master template as a baseline. The AIM CDE shall provide appropriate functionality to report and record variation justification.
2.1.2	The second step (B) shall confirm individual supplier's pre-contract delivery proposal against the information requirements. This may form part of a tender assessment. The AIM CDE shall provide appropriate functionality to report and compare supplier proposals against the information requirements and support selection.
2.1.3	The third step (C) shall assure that the post-contract supplier schedule of deliverables files aligns with the contracted information requirements. The AIM CDE shall provide appropriate functionality to report on incomplete file delivery schedules for each engaged supplier.
2.2	**Information Assurance (Files)**

2.2.1	The fourth step (D) shall check that all files identified in the supplier schedule (MIDP) have been delivered, published and are present in the AIM CDE. Published delivered information shall be reported against the supplier schedule to highlight present, incomplete or missing delivery
2.2.2	Information assurance shall be applied to all published information supplied to the AIM CDE. Unless specifically excluded, all non-compliant published information in part or whole shall be rejected.
2.2.3	Reports shall be available to show information supplied versus that planned in the master information delivery plan.
2.2.4	The formal system checks and workflow shall be initiated as soon as information is presented and should include compliance checks on all file names, file metadata and data.
2.2.5	The system shall automate compliance and completeness checks however content validation shall be carried out by the employer or delegated party through content review workflows.
2.3	**Information Assurance (Data)**
2.3.1	The fifth, sixth, seventh & eighth steps (E, F, G & H) are concerned with data standards compliance and completeness checks and shall verify delivered and Published status BS1192-4 data – see appendix 3.
2.3.2	The verification functionality shall check BS1192-4 data file data including file linkages, object geometric bounding box data, data format and is complete compared to the Department object type libraries and/or data demand matrices.
2.3.3	Exchanged published BS1192-4 data files shall be verified to reference all files presented as published, and the variances highlighted.
2.3.4	The formal system checks and workflow shall be initiated as soon as information is presented and should include compliance checks on all file names, file metadata and data.
2.3.5	Content validation or review workflows shall be invoked dependant on status or by the user.
2.4	**Acceptance and Authorisation Workflows**
2.4.1	Supplied information shall be routed through ‘Shared’ acceptance or ‘Published’ workflows, dependent on the suitability status code. The system should include sufficient viewing and mark-up capabilities to ensure this is possible without stand-alone software.

2. 4.2	All information presented as shared status shall be passed through a strict shared-status acceptance workflow that enables the information to be presented to the appropriate employer AIM CDE users for information, or for review and comment back to the information supplier. Shared status information may be non-contractual and cannot be relied upon.
2.4.3	Reviewed comments shall be coordinated back to the information supplier via the project or contract workspace information manager. The system should include sufficient viewing and mark-up capabilities to ensure read-only mark-up is possible without stand-alone software.
2.4.4	Shared status information not subsequently superseded by Published status versions or Archived shall be maintained in the AIM CDE by employer as informative only.
2.4.5	Accepted Shared status information shall be clearly identified as such e.g. colour/icon marked.
2.4.6	All information presented as Published status shall be passed through a strict published-status authorisation workflow that enables the information to be verified and validated before being presented as published.
2.4.7	Published information not passing the verification and validation process in full or in part shall not be presented as published and be archived.
2.4.8	Accepted Published status information should be clearly identified as such: e.g. colour/icon marked.
2.5	**Assurance Reporting**
2.5.1	The AIM CDE shall provide assurance reports which shall report on each assurance steps A to I - see Appendix 3
2.5.2	Information Assurance shall be reported via summary and detailed reports with red/amber/green (RAG) status indicators. RAG reports shall be available to download for action offline. Summary reports shall be in the context of a single workspace or across multiple workspace or other selection criteria.
2.5.3	Report A - IDP ITT vs Baseline - reporting on the variance between the pre-tender IDP deliverables and a baseline standard IDP to confirm and justify completeness & variation. Assurance that the project variation is justified and fully accounted. Promotes the use of standard, repeatable and known deliverable information components. Minimises EIR variations.
2.5.4	Report B – Supplier Proposals vs Information Requirements - reporting on the variance for each contending supplier information deliverable proposals. Enables assessment of tender proposals across the contending parties to assess capability, innovation and assurance, and value information delivery proposal.

2.5.5	Report C – Supplier Delivery Schedule vs Information Requirements - reporting on the supplier deliverable item proposals post-appointment with the appointed IDP. Confirm that all proposed IDP items have sufficient MIDP items, highlight variance - completeness & variation. Enables assessment of supplier item delivery proposals against contractual IDP.
2.5.6	Report D - Presented Files vs Supplier Delivery Schedule - reporting on the presented 'published' files are confirmed against the scheduled supplier items (green) and missing files (red) and presented but not verified (amber). Confirms file delivery against plan, stage/ LOD/ referencing to enable stage PLQ & gateway review, and assessment of ongoing project risk & reserve.
2.5.7	Report E - BS1192-4 data format compliance - reporting on the presented pending BS1192-4 data file(s) compliance to the standard and meets the Department data naming ontology etc. Ensures that the presented information is in the correct format to be processes and act as the basis of presentation as published data.
2.5.8	Report F - Presented Document Tab files - reporting on the variance between the BS1192-4 document tab files and the presented published files and confirm the file linkage to those files. Ensures that the required files are presented and linked into the data set in readiness for extraction into the Published Data Store.
2.5.9	Report G - Presented BS1192-4 Data - reporting on the BS1192-4 data tabs content including document and attribution for the stage/event and LOD, to the Information Requirements.
2.5.10	Report H - Presented BS1192-4 Object Data - reporting on the presence of appropriate BS1192-4 data attribution values for each presented object against the Object Type Library for the stage. Ensure delivered data meets client requirements for each presented object entity before extraction into the Published Data Store.
2.5.11	Report I - Presented Information Answers PLQ - Validation reporting that the specified information as presented, sufficiently answers the employers stage PLQ, including project managers comments. Ensures delivered specified information answers the stage Plain Language Questions to enable fully informed business and stakeholder stage or event gateway decisions based on appropriate reliable information.

STORAGE AND CYBER SECURITY

3.0	**General**
	The AIM CDE system shall host project and asset information, made up of 3D model files, drawings and documents, and structured data extracted from BS1192-4 data format files. Information shall be accessible across the whole AIM CDE and accommodate alternate different views of the information depending on the role and purpose e.g. mapping views by location, asset views by functional breakdown structure, project views by work break down structure or stage etc. The File and Data Stores shall store Shared and Published project and contract information supplied progressively through the course of the asset lifecycle and be made available for re-use. Understanding the vulnerabilities and the nature of controls required to ensure the AIM CDE delivers a secure digital environment for the management of built asset information is essential. As well as describing requirements for file and data storage this section describes the cyber security requirements for the AIM CDE.
3.1	**File Store**
3.1.1	The file store shall be presented as a fully configurable secure electronic document management system, capable of receiving and storing native and open format models, BS1192-4 and open format data files and other native and open format documentation. Documents formats shall include photos and other media files, surveys, commercial and legal documents classified by the IDP deliverable information breakdown structure.
3.1.2	The File Store shall allow the exchange – upload and/or download, of individual or groups of files in a safe and resilient way and store files in a manageable and scalable environment; to allow the efficient search of and retrieval of files; to allow files to be viewed within the system without reliance on third party applications.
3.2	**Data Store**
3.2.1	The Data Store shall be capable of receiving and storing raw data extracted from structured data BS1192-4 data formats including both .xls and .xlsx format spreadsheets.

3.2.2	On upload of a BS1192-4 data format file and subject to an assurance process the contents of the BS1192-4 data file shall be extracted, transformed and loaded into the Data Store.
3.2.3	Any extraction shall maintain an audit trail with links back to the delivering BS1192-4 data file. All data in the data store shall be separate from any link stored in the BS1192-4 data file and used to link the workspace model in the File and Data Stores.
3.2.4	Extracted BS1192-4 data files shall be considered as separate 'model instances' in the Data Store and identified by the presented file name and metadata.
3.2.5	It shall be possible to query and view the data store in a user interface with the query string exportable for use in subsequent API calls.
3.2.6	In many cases data about assets is already held in specific asset management applications. The asset information models shall therefore be able to hold links to information held in remote systems.
3.3	**Cyber Security**
The following should be read in conjunction with the CPNI Guidance for BIM Level 2 Common Data Environments (CDE) Implementation of Cloud Security Principles, which should take precedent.	
3.3.1	**Principle 1. Data in transit protection.**
3.3.1.1	Internet Security Protocols shall be used to encrypt packages of data sent to and from the AIM CDE over the Internet
3.3.1.2	The interface shall be only accessible using HTTPS using the latest version of TLS, currently TLS1.2
3.3.1.3	The interface shall automatically redirect users who visit the HTTP version of your service to the HTTPS version
3.3.1.4	The latest versions of TLS libraries and supporting web frameworks shall be used; implementation issues can introduce vulnerabilities in the libraries which can quickly be exploited if not patched promptly
3.3.1.5	HTTP Strict-Transport-Security (HSTS) shall be used to help the browser secure connections to your service
3.3.1.6	The interface shall add the Strict-Transport-Security HTTP header when the site is accessed over HTTPS - this instructs the browser to only request the HTTPS version in future (until the expiration time in the header elapses)
3.3.1.7	Server certificates shall be acquired from trustworthy and reputable sources
3.3.1.8	A means of revoking compromised certificates shall be available for your interface and services through your chosen Certificate Authority (CA)
3.3.1.9	The interface shall advise users if their web browsers are not supporting a sufficient set of TLS algorithms, and providing them with information on how to upgrade their web browser or operating system if appropriate
3.3.2	**Principle 2. Data & System hosting protection and resilience**

3.3.2.1	Security Measures shall ensure the data centre which hosts the system is physically secure.
3.3.2.2	The legal Jurisdiction of the host data centre shall be the UK where the relevant legislation is understood.
3.3.2.3	Security measures to ensure that the data is encrypted and is physically secure shall be in place.
3.3.2.4	The process of data sanitization including provisioning, migrating or de provisioning resources shall not result in lost or stolen media or unauthorised access of any kind
3.3.2.5	Equipment disposal procedures at end of life shall not compromise the security of the data stored.
3.3.2.6	The levels of resilience and service available shall be guaranteed by the service provider to the satisfaction of the UK Government Department.
3.3.3	**Principle 3. Separation between users**
3.3.3.1	Security measures that shall be taken with the architecture of the system to ensure that a malicious user can not affect the service or data of another user.
3.3.3.2	The interface shall be inherently secure and user access should only be granted on a workspace by workspace basis by the workspace information manager based on the applied workspace information security policy and subject to employer security requirements.
3.3.3.3	Visibility and access to all files, models, views, metadata and data extracted from BS1192-4 data files shall comply with the workspace security policy and the contracted BIM protocol, all in accordance with PAS1192-5. This should be user and role based.
3.3.3.4	Files shall be private and read-only, and only visible to the uploading information supplier, until accepted.
3.3.3.5	An allocated employer information manager role shall have sufficient security authorisation to view files presented for acceptance.
3.3.3.6	Security and visibility of files models and data must be manageable. e.g. through default user, group or roles permissions
3.3.3.7	The AIM CDE shall enable the allocation of permissions based on metadata such as volume and location codes. These access rules can only be set by a suitably authorised employer information manager.
3.3.3.8	It shall be possible to trigger a notification to the workspace information manager of approaching aggregated workspace volume (number) or aggregated workspace storage size set by the workspace information security policy.
3.3.3.9	Security shall be applied so that information volumes, locations, models, files and data and all associated meta data is completely obscured from workspace users with insufficient security levels. This requirement applies to information whether viewed on screen, printed out from the CDE or extracted as files and data.
3.3.4	**Principle 4. Security Governance Framework**

3.3.4.1	The service provider shall have a security governance framework in place, which coordinates and directs its management of the service and information within it.
3.3.5	**Principle 5. Operational security**
3.3.5.1	Security measures shall ensure that the system can be operated and managed securely to minimise the risk of attacks exposing information and data. Measures shall include configuration and change management, vulnerability management, protective monitoring and incident management.
3.3.6	**Principle 6. Personnel security**
3.3.6.1	Where service provider personnel have access to data and systems they shall be subject to security screening and regular security training.
3.3.7	**Principle 7. Secure development**
3.3.7.1	The service provider shall demonstrate that new and evolving threats are reviewed and the service improved in line with them and that development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.
3.3.7.2	Configuration management processes shall be in place to ensure the integrity of the solution through development, testing and deployment.
3.3.7.3	New applications shall be designed to use Content Security Policy, as it can be difficult to retrofit later
3.3.8	**Principle 8. Supply chain security**
3.3.8.1	Security measures shall ensure that the service provider's supply chain fully supports all of the security principles, which the service claims to implement.
3.3.9	**Principle 9. Secure user management**
3.3.9.1	The AIM CDE shall have tools available for appropriately authorised administrators to securely manage user accounts and manage access rights.
3.3.9.2	Security measures shall be in place that ensures the user management service cannot be compromised and accessed by un authorised users. Penetration tests shall be arranged periodically to ensure user management service is only available to privileged users with administration rights.
3.3.10	**Principle 10. Identity and authentication**

3.3.10.1	Access to the AIM CDE and data stored in it, shall be constrained to authenticated and authorised individuals. Authentication should occur over secure channels. Acceptable approaches include: Two factor authentication, TLS client certificate and Identity federation with your existing identity provider.
3.3.10.2	Access to the AIM shall not rely on basic username and password authentication alone. Any compromised credentials can be easily re-used by an attacker to gain access to the service. This is not an acceptable approach for access via the Internet.
3.3.10.3	The service provider may support a combination of approaches, e.g. two factor authentication and/or TLS client certificate, and identity federation.
3.3.10.4	It shall be possible to set user access privileges to be time limited and be revoked unless physically maintained by a suitably cleared and authorised party. This may be for the duration of a task, project or a support maintenance contract.
3.3.11	**Principle 11. External interface protection**
3.3.11.1	To ensure that all external or less trusted interfaces of the service are identified and appropriately defended, the service provider shall provide information about the networks being used to access the service.
3.3.12	**Principle 12. Secure service administration**
3.3.12.1	The security risks associated with the AIM CDE service administration model shall be assessed. Independent assurance from a suitably qualified security architect may be required.
3.3.12.2	An unknown service management architecture represents an unacceptable level of risk for systems processing BIM data and shall not be accepted.
3.3.13	**Principle 13. Audit information for users**
3.3.13.1	Audit records shall be available to monitor access to the AIM CDE and data held within it. The type and scope of audit information available has a direct impact on the ability to detect and respond to inappropriate or malicious activity within reasonable timescales.
3.3.13.2	There shall be a full but secure workspace audit trail of all distribution available to the workspace information manager and allocated workspace auditors.
3.3.14	**Principle 14. Secure use of the service**
3.3.14.1	Security of the CDE will be undermined if the service is accessed or used through poorly configured or compromised end user devices.
3.3.14.2	It shall be possible to restrict access to the AIM CDE to UK Government managed or approved supplier devices. These devices shall be configured securely applying the NCSC End User Devices Security Guidance.

3.3.14.3	For supplier devices, a minimum standard of certification of compliance with the 'Cyber Essentials' shall be contractually required.
3.3.14.4	UK Government security classifications shall be applied to all content including content derived from uploaded file meta-data and extracted data.
3.3.14.5	The default baseline security is OFFICIAL. However, this shall be determined by the application of a contextual information security policy for the particular workspace instance and the application of PAS1192-5 triage process.
3.3.14.6	All points of access - physical, visual and digital including via API access, shall be secure and subject to the same security considerations.
3.3.14.7	It shall be possible to assign and manage individual users or roles security level for a workspace.
3.3.14.8	The allocation and maintenance of user security levels for the workspace shall be assigned to a named and suitably authorised individual or individuals.
3.3.14.9	Only assigned and authorised users shall be able to allocate and maintain user security.

USER FUNCTINALITY

4.0	**General**
4.0.1	The AIM CDE shall be a secure web based portal giving access to data and documents about assets. The portal shall be secure and accessible for authorised users 24hrs a day, 7 days a week 365 days a year.
4.0.2	The AIM CDE shall provide an easy to use and intuitive interface for users to register, schedule, upload, assure and share, review, publish and find model files, documents and structured data.
4.0.3	The AIM CDE shall be fully operable HTML5 compliant using the latest industry standard internet browsers and not require any additional downloads or plugins.
4.0.4	The AIM CDE shall be fully operable through tablet and mobile phone devices as well as Personal Desktop computers and Laptops
4.0.5	The AIM CDE shall ensure all information is backed up and can be retrieved in the event of an incident or perceived information loss
4.0.6	The AIM CDE shall perform well and be scalable to cope with 1000s of accounts, 100s of concurrent users and limitless information storage, covering hundreds of facilities / assets.
4.1	**File management**
4.1.1	The AIM CDE shall support information management requirements in BS1192 2007 A2 2016 such as file naming, document numbering, status fields, document types, revision sequences, location metadata classification
4.1.2	The AIM CDE shall drive the adoption of consistent file naming conventions through measures such as: (a) invalidating files with non-compliant file names (b) auto populating metadata from file names (c) automatically correcting files names based on metadata choices. (d) or other
4.1.3	The AIM CDE interface shall clearly show the status of Information, and clearly differentiate between files that are 'Work in Progress', 'Shared ' 'Published and 'Archived' status.
4.1.4	The AIM CDE shall have appropriate functionality to manage Work in Progress (WIP) information. WIP information shall be visible only to the information supplier and the supplier's own organisation. WIP status information shall be considered as unmanaged and outside the formal AIM CDE process and may be subject to periodic deletion or archive and other restrictions.

4.1.5	The AIM CDE shall have appropriate functionality to manage Shared Status information. Shared status information shall have a special significance in the AIM CDE as un-verified information with unconfirmed governance or unconfirmed provenance where the author is either unknown or does not or cannot accept full responsibility for reliability equivalent to 'site information'. Shared status information shall be uploaded for stakeholder review and mark-up back to the information supplier within the system. Shared status information may be maintained for audit purposes e AIM CDE for the whole life of the asset.
4.1.6	The AIM CDE shall have appropriate functionality to manage Published Status information. Published status information shall have a special significance in the AIM CDE as verified information with confirmed governance and provenance, where the author accepts responsibility for the information and subject to the suitability and purpose at presentation. Published information is equivalent to contractual 'works information'
4.1.7	The AIM CDE shall provide a mechanism to Archive superseded or redundant information ensuring the latest information about the development or operational state of the assets is maintained. Archive information shall be maintained and accessible in the AIM CDE as a complete transaction and version history. Archive status information shall maintain a history of all information activity for knowledge, regulatory and legal requirements. Archive information is of restricted access to those with approved 'need to know' access. Archive information shall be available to the original information supplier or individuals it has been distributed to. Otherwise archive information is obscured, only be available to selected and restricted roles.
4.1.8	The AIM CDE shall enable files to be defined as particular document type from a configurable document type list such as that suggested in BS1192 2007 A2 2016
4.1.9	The AIM CDE shall support revision sequences described in BS1192 2007 A2 2016
4.1.10	The AIM CDE shall enable the allocation of configurable metadata to files. For example, stage, role originator or other specific fields that shall structure the information and make retrieval easier.
4.1.11	The AIM CDE shall enable the assignment of location metadata such as facility, floor, space, system, component which links files to the common BS1192-4 data model.
4.1.12	The AIM CDE shall ensure that all registered and scheduled file deliverables shall be associate with an IDP reference (Delivery Reference)
4.1.13	The AIM CDE shall enable all files to be tagged with an industry classification reference, for example Uniclass 2015

4.1.14	The AIM CDE shall enable the geolocation of all files either directly as metadata, indirectly by association with an asset or indirectly via the BS file name floor/location code that has been geolocated in BS1192-4 data.
4.1.15	The AIM CDE shall ensure that all files uploaded to the system are immutable and cannot be directly edited.
4.1.16	Files and data instances shall be held as a 'read only' state in the AIM CDE only superseded by further presentation by the originator information supplier. It shall not be possible to edit any file or extracted data instance. Superseded information is Archived. Any edit or overwriting shall be added as new instances with the appropriate new originator and instance metadata.
4.1.17	The AIM CDE shall include functionality to automatically set file metadata based on structured file names. The 'file name to metadata' configuration should be flexible enough to support the BS1192 2007 file name conventions and any appropriate extensions. For an example see appendix 4
4.2	**Model Management**
4.2.1	The AIM CDE shall enable the viewing and federation of models extracted from BS1192-4 geo-positioned object files.
4.2.2	The AIM CDE shall enable user to navigate around a model in 3D, click on objects and see associated data and documents.
4.2.3	The AIM CDE shall accept geometric data through model files submissions
4.2.4	The AIM CDE shall provide functionality to identify clashes in the federated model view with configurable tolerances.
4.3	**Data Management**
4.3.1	The AIM CDE shall accept published data submissions through the BIM Level 2 BS1192-4 data file submissions.
4.3.2	The AIM CDE shall extract submitted data into a data store where the data can be viewed, checked and analysed.
4.3.3	Where bounding box data is provided in BS1192-4 files, data shall be viewable in the model viewer and in the geospatial mapping interfaces.
4.3.4	It shall be possible to save the BS1192-4 data views and named asset queries to be visible in the mapping or data API interfaces by name. The created view query string shall be able to be exported as text in a format suitable for using in the data API also by name (text, xml, json).
4.3.5	The BS1192-4 source data files and data extracted from them shall be referenced to the source data file as a single file based information model read only instance.
4.3.6	It shall be possible to view the archive (history) versions of BS1192-4 information models to compare output and federation.
4.4	**Collaborative Workflow & Information Reviews**

4.4.1	The AIM CDE shall support the collaboration management processes described in BS1192 2007 A2 2016, PAS1192 Part 2 and 3. In particular, the system shall support the PAS1192-3 Shared: accept review and mark-up, and Publish: verify and validate, authorise processes which will take priority.
4.4.2	The AIM CDE shall include functionality to select files and distribute to internal staff, partners, and supplier representatives for defined purposes e.g. for information, for review, for authorisation, for acceptance etc.
4.4.3	The AIM CDE shall enable a collaborative review, comment and mark-up functionality on Shared status information. The nature of the files being reviewed shall not be altered during the review process.
4.5	**Navigation and Search**
4.5.1	The AIM CDE shall enable simple browser like searches to locate projects, assets, document files, model files and data
4.5.2	The AIM CDE shall provide an advanced search which shall enable sophisticated refinement of search results by filtering metadata and location.
4.5.3	The AIM CDE shall provide the ability to search the content of files.
4.5.4	The AIM CDE shall provide searches by location. The presentation of information results shall be presented on a map based interface based on bounding box geo positioned of assets, file and attached data.
4.5.5	The AIM CDE shall provide functionality to navigate information both by asset and by project
4.5.6	The AIM CDE shall provide functionality to allow users to navigate through a model and access documents and data associated with particular objects, navigate through document lists and navigate to associated objects in the model and navigate through a non-geometric view of data and navigate to geometric objects and associated documents.
4.5.7	The AIM CDE shall provide a geospatial mapping interface to enable users to navigate easy to both projects and assets
4.5.8	THE AIM CDE shall provide functionality to draw a boundary box and search for all asset information with in and intersects with the selected area.
4.6	**Project & Asset Set-up Templates**
4.6.1	The AIM CDE shall provide functionality to set up project/contract workspaces to host project and contract information collected through the capital delivery phase of a minor and major works projects (Design, Build and Commission) and service contracts. The functionality shall provide a schema to set up the information schema and appropriate standard information delivery plan templates.
4.6.2	The AIM CDE shall provide functionality to set up the definitive list of managed assets within the portfolio or client estate.
4.7	**Viewers**

4.7.1	The AIM CDE shall include a viewer with the ability view common industry formats, negating the need for end users to run native applications to read common files. Formats should include BS1192-4 data and models, dwg/dxf, office (including Open Document) and pdf as a minimum but ideally extended to open geographical formats.
4.7.2	The AIM CDE File viewer shall enable a collaborative review, comment and mark-up features that are integrated with the collaborative information review processes.
4.8	**Audit Trail**
4.8.1	The AIM CDE shall provide full audit reports which shall include, but not be limited to, tracking the following events upload, issue, accessed, read, edited, moved, downloaded and status changed and distributed information and shall include date and by whom the action was carried out by.
4.9	**Dashboard, Analytics and Reporting**
4.9.1	The AIM CDE shall provide a flexible and configurable report module that allows the employer's staff to deliver bespoke and predefined reports on project and/or assets without input required from the AIM CDE supplier.
4.9.2	The AIM CDE shall provide a dashboard interface to alert users of any updates or changes to information and a summary of incoming and outgoing tasks.
4.9.3	A dashboard shall also present users with a summary of approval tasks, notifications and common functions or quick links.
4.9.4	The dashboard interface shall be configurable at system and user level including a user selected default view.
4.9.5	It shall be possible to schedule reports to be run on a time based or other triggers including by remote URI call and for these to be stored in the File Store and notified to workspace user or groups.
4.9.6	Completion of scheduled reports shall be notified with appropriate linkage to the reports held in the File Store.
4.10	**Tender Management**
4.10.1	The AIM CDE shall provide the necessary functionality and security to manage the information exchanges and during the tendering process, ensuring tender responses from bidders are segregated and private from competing bidders.
4.10.2	THE AIM CDE shall provide functionality to manage Public, Private, Confidential, Closed-Envelope tenders or Requests for Quotations (RfQ)
4.10.3	THE AIM CDE shall provide suppliers with the ability to add their own tender proposal notes to each information requirement definition in the employer's information delivery plan.
4.11	**Contract Management**

4.11.1	The AIM CDE Shall provide the functionality to manage workflows and the requirements of NEC, JCT, RIBA, FIDIC, ACA, ACE, CIC, CIOB contracts. Including but not limited to the following Project Manager's Communication Project Manager's Early Warning Notice Project Manager's Request for Quotation Project Manager's Notification of Compensation Event Project Manager's Instruction Supervisor's Communication Contractor's Communication Contractor's Early Warning Notification Contractor's Notification of Compensation Event
4.12	**Standard Object Libraries**
4.12.1	The AIM CDE shall provide functionality to store and manage standard object type libraries, along with associated geometry, data and documents
4.12.2	The AIM CDE shall provide functionality to navigate, search and find standard objects and download them
4.12.3	The AIM object type library shall be formed in BS1192-4 data format objects.
4.13	**Company and User Management**
4.13.1	The AIM CDE shall provide functionality to set up companies and assign users to their respective companies.
4.13.2	The AIM CDE shall provide functionality to set up users and assign them access to project and or asset workspaces.
4.13.3	The AIM CDE shall provide functionality for users to manage their own details and user access credentials

INFORMATION OUTPUT

Information shall be accessible either through a user interface or application program interface (API) for connection of employer enterprise and other systems. Output should be flexible, controllable and secure and profiled for different users and user groups.

5.0	**General**
5.0.1	Asset data shall be provisioned to asset management information systems through a reliable data integration service via a secure file and data application program interface (API).
5.0.2	The integration interface shall enable secure web services API connectivity to provide query-able data and linked files from the AIM CDE to appropriate connected authorised employer enterprise systems. The queries shall be created and named in the AIM CDE and called by name only from the external system.
5.1	**Files and Data Download**
5.1.1	The AIM CDE shall provide suppliers and staff with access to documents, models and data files to download, subject to full security and disclosure rules and marking.
5.1.2	Files shall be available to download to in bulk.
5.1.3	The export/download of files shall be available with applied renaming rules derived from meta data to meet employer naming policies. Files held within the system will be named as the loaded BS1192 standard file name.
5.2	**Application Program Interfaces (APIs)**
5.2.1	The AIM CDE shall enable the provisioning of data into other systems e.g. asset management systems or facility management systems through a reliable data integration service and application program interface (API).
5.2.2	The integration interface shall enable secure web services API connectivity to provide query-able data and linked files from the AIM CDE to appropriate connected authorised employer enterprise systems.
5.2.3	Files stored in the file store shall be available for external query via a secure RESTful APIs subject to full security and disclosure rules.

5.2.4	File API queries shall be created and stored within the system by a suitably authorised role and be sensitive to the security considerations. The ability to run the queries should also be subject to security restrictions above or in addition to the user, role or machine interface authorisation. The API shall resist denial of service or structured query language (SQL) injection attacks.
5.2.5	All calls from external sources to the API or other interfaces shall update the audit trail and be subject to full security and disclosure rules.
5.2.6	Data stored in the data store shall be available for external query via a secure RESTful API, subject to full security and disclosure rules.
5.2.7	The API protocol methods shall include querying files and file based meta-data, and data, based on an SQL-like query returning a selectable output.
5.2.8	The format of the data query shall be selectable in HTML, XLSX, XML or JSON format.

APPENDICES

Appendix 1 - Glossary

Note: this section also covers interpretation of terms in this document relating to the BIM Level 2 standards

AIM CDE	The Asset Information Management Common Data Environment (AIM CDE) is the managed file and linked structured data repository holding the particular Employer whole life information procured from project, contract and other information suppliers and maintained as the virtual BIM Level 2 instance of managed assets in the development and in use state. See PAS1192-3 generally and 4.6 for AIM.
AIM CDE Security Visibility	All information within the AIM CDE shall be subject to strict security based on the user role and role security level. Information visibility can be set by the information supplier, based on the applied Volume Strategy or other agreed file meta-data derived security level. The default security visibility is private and only visible to the information supplier. Information security may be upgraded by the AIM CDE Information Manager dependent on the applied information security policy and volume considerations.
AIM CDE Status	AIM CDE information status, one of Work-In-Progress, Shared, Published or Archive indicating the use and reliance on the file and data information. See individual definitions in this glossary.
AIM Information Manager	Role responsible for managing the information flow and status in the AIM CDE; as a whole or in a workspace area of the AIM CDE; commonly referred to as the employer information manager.
AIR Object Type Library	An Asset Information Requirements (AIR) Object Type Library (OTL). A library of asset entities (e.g. Room or Feature Data Sheets) defining the asset object or entity e.g. Lighting Gantry, and information requirements in a BS1192-4 data structure, at the various stages of the Capital Digital Plan of Work and/or events or triggers across the whole lifecycle of the asset; an information demand matrix used to define the Employer specific information requirements for each required asset entity. Complementary to and defining the asset object data in the IDP BS1192-4 Information Requirements for use by information suppliers in compiling BS1192-4 data for Employer presentation. This may be complementary to and extending specified digital libraries such as the NBS BIM Toolkit.
Asset Management System	Systems used by the Employer or other party to manage the maintenance and operation of assets and the asset estate and its relevant information. These are typically specialist proprietary systems focused on the operational in use phase; including CAFM and AIMS systems, all likely to consume information from the AIM CDE.

API	Application Program Interface: published software interface of inputs, query methods & outputs enabling machine to machine communication and information exchange.
Archive	Historic information status only visible to suitable roles; the information supplier may set WIP or Rejected status information to Archive; an information manager may set Shared or Published information to Archive.
Asset Workspace	Filtered and possibly named view of an asset or assets in the AIM CDE. A logical set of linked file and data viewed from the AIM CDE around an asset object or objects defined by a user created or saved search criteria such as asset, type, location or state e.g. facility, extent, building, region, bounding box, delivery reference, geographic area, condition etc. based on meta or BS1192-4 extracted data. An Asset Workspace may be viewable through a file, model or geographical context interface.
Authorisation	The process of AIM CDE information assurance and extraction of accepted files and BS1192-4 data into the Published status, File and Data Stores. See PAS1192-3
Bounding Box	A model containing a simple 3D geometric wire frame box; bounding the full extent of the geometric object, including working space. Available from the early stage of development and maintained across the full asset lifecycle. May have Employer requirements, design, commissioning and/or operational documents and/or attribute data attached. The minimum geometric content of presented BS1192-4 data sheets. A 2-point orthogonal or 2 point & rotated, 3D geometric wire frame box. For the early stages of the development of infrastructure assets it is common for bounding boxes to be 2D.

Capital Phase	That part of the asset lifecycle where major acquisition, creation or maintenance works are being managed typically through a PAS1192-2 project team collaboration process and external PIM CDE managed by the project information manager and where the asset may be out of service.
CDE	Common Data Environment: In the case of the AIM CDE a PAS1192-3 Employer side information management tool to visibly portray the information load, acceptance, review, verification and extraction process into the File, model & Data stores for stage based decision making and onward exploitation. Note Information is held in one of four states Work-In-Progress, Shared, Published & Archive. The Shared and Published states in the AIM CDE have a special and significant contractual relevance – see specific definitions.
BS1192-4 Data Extraction	The process of extracting – and transforming, presented and verified BS1192-4 data sheets from the File Store into the Data Store. Only successfully verified and extracted data will be presented to the Data Store as a new version of the data set. The individual instance BS1192-4 data sheets should be treated as individual models defined by the BS file name. If no GUID is present, then this will be generated. If mapped into an alternate open model format store, then model extent bounding box should be auto generated to contain the individual model object boxes.
BS1192-4 Data Information Requirements	BS1192-4 Data Information Requirements. A BS1192-4 data demand matrix generated from the IDP defining the project or contract information deliverable requirements and the meta data requirements for each, and the supplier registered information deliverables to the requirements. The BS1192-4 Data IR should also contain the associated

	file field meta data pick lists and applied Volume & Location strategies for use by information suppliers in compiling BS1192-4 data for Employer presentation.
Data Store	Part of the AIM CDE storing BS1192-4 data files as structured data and URI links to files in the file store. The Data Store structure can be based on BS1192-4 data as a Master Data Model or a view onto an Industry Foundation Class model store.
Data Verification	The second stage of AIM CDE verification; focusing on analyzing the presented BS1192-4 data file or files for completeness and compliance of the exchanges stage file set and metadata against the IDP BS1192-4 Data IR, and each object presented for the stage or event against the AIR OTL demand matrix.
Delivery Reference	A unique Information Breakdown Structure code for an information requirement as defined in the AIM information delivery master table. Note, the Delivery Reference is a significant classifier to enable file and derived information management, searching and discovery into the operational phase of asset lifecycles.
Digital Plan of Work	The cross-Government capital project plan of work  in 8 stages and stage gateways – red diamonds, where information is required in the AIM CDE to answer defined Plain Language Questions (PLQ). Also shown are the Information Exchange points – green circles, providing information Shared for review or Published as contractually required, to answer the PLQ at each defined stage procured via the EIR and IDP. Note: information can be Shared with the AIM CDE at any point in a stage. The

	concept is extended into whole life operations to define the information required to meet the PLQ for a planned or reactive event or trigger in a service supply contract.
Discipline models (files)	Models or files authored by a single supplier entity with appropriate provenance, shared or published with a particular status and purpose. Read only in AIM CDE.
EDMS	Electronic Document Management System, see File Store
Extended File Name	The BS1192 and extended metadata data dash delaminated File Name to aid drag and drop file upload of multiple files and decoded into BS1192 files name and metadata on upload.
Employers Information Requirements	As defined in **PAS1192-3 cl 3.21 Employer's Information Requirements (EIR):** pre-tender document setting out the information to be delivered, and the standards and processes to be adopted by the supplier as part of the project delivery process. **For Government Departments with Framework supply chains, this document is split into two parts - the Employers Information Requirements (EIR) a standard minimum technical requirements document bound into the framework contracts an applicable to all projects and service contracts, and a project or contract specific schedule of information requirements contractually engaged as part of supplier's tender proposal. See Information Delivery Plan.**
Federated models	The bringing together or overlaying of separate discipline models or files into a single model for a specific purpose maintaining the discipline model provenance and separation.
File Name	A BS1192:2007 (2016), formal 'dash delaminated' file name used to determine versioning in the File

	Store. File names are set by the Information Supplier on upload and not changeable once in the File Store – read only.
File Store	Part of the AIM CDE storing files – the Electronic Document Management System
File Verification	The first stage of AIM CDE verification; focusing on verifying the pre-procurement IDP against a baseline position, the supplier IDP proposals, and the post appointment IDP proposals and with the delivered files for a stage and supplier.
For Acceptance	An interim status; initiated by the Information Supplier and visible to the information supplier and information manager; notifying the workspace Information Manager of the acceptance request. The workspace Information Manager will triage the request setting the CDE status to Shared, or Rejected, or pass the request on for Authorisation subject to the file suitability and verification policy.
Information Delivery Plan (IDP)	A project or contract profiled plan of information output requirements for each stage/event and supplier selected for a project or contract from the Employer master list. The IDP is created by the Employer or Employer's representative, confirmed by the contending suppliers and forming the basis for contracted information delivery. The IDP shows all contracted information products procured from all information suppliers including Employer supplied deliverables. **The IDP is the specific information requirements portion of the Employers Information Requirements which must be read together. See Employers Information Requirements.**
Information	BIM Level 2 information: 3D models, documents and BS1192-4 data exchanged as files.
Information Supplier	Any party supplying information to the AIM CDE including the Employer and contracted parties.
MIDP	Master Information Delivery Plan: created by an appointed lead supplier to confirm all the specific files to be published to meet the information requirements stage by stage. Note this may be a subset of the supplier project MIDP/TIDP set and targeted at meeting the contracted IDP. See PAS1192- 2 7.3.3.
Model Store	Part of the AIM CDE storing extracted georeferenced asset model files in viewable open data format mapped onto the Data Store.
Naming Ontology	Alternate industry sector naming for BS1192-4 data Tabs and Digital Plan of Work stages, to enable industry assimilation and understanding and acceptance. Data entity relationships are to BS1192-4.
Operational Phase	That part of the asset lifecycle where normal operation and maintenance activities are being managed, undertaken or occurring either through the AIM CDE or outsourced to an Asset or Facility service supplier or Total Facility Manager.
Project Workspace	Named and referenced workspace area of the AIM CDE for the receipt, collection and management of employer specified exchanged information for the purpose of initiating, tracking or managing a project or contract. Typically arms-length to the separate PAS1192-2 collaborative Project Information Model CDE with its own Project Information Manager. An AIM CDE Project Workspace may be viewable through a file, model or geographical context interface.
Published	Published Information: Verified information with confirmed provenance where the owner accepts responsibility for reliability to the stated level of development, purpose and suitability. Information purchased for a purpose – 'Works Information';

	Published information that can be contractually RELIED upon – subject to contract wording.
Rejected	An interim status for files not accepted or failed authorization and passed back to the information supplier.
Security Classification	UK Government Security Classifications should be applied to all content and derived from uploaded file meta-data. The default is OFFICIAL however this should be determined by the application of a contextual information security policy for the particular AIM CDE instance and the application of PAS1192-5. Volume and or Location considerations may upgrade this requirement. *NOTE: the maximum level of classification needed by a particular Department will need to be determined prior to procurement of the system and this will impact hosting and other considerations at a system provision level.*
Shared	AIM Shared Information, Un-verified & un-validated information, or with unconfirmed provenance, or where owner does not or cannot accept full responsibility for reliability – 'Site Information'; Shared information cannot be contractually RELIED upon. Accepted shared suitability files are accepted as Shared status for information or distributed for review and mark-up to suitable workspace members' dependent on policy. Shared information may be maintained in the AIM CDE for the life of the asset.
Verification Reporting	Reporting on the file and data (BS1192-4 data) verification process producing a Red Amber Green (RAG) status reports in summary and in detail and be recorded in the audit log.
Validation vs Verification	The Supplier verifies information output is complete & present to the contracted specification and validates suitability as professionally appointed before exchange. The Employer verifies information is complete & present to the contracted information requirements for a particular stage, and then validates that the specified information meets the stage or event gateway PLQ. *NOTE: The Employer may employ independent verification & validation on information process and security but this is outside the AIM CDE requirements. The results of this external audit process may be presented as a separate line of information delivery handled by the AIM CDE.*
WIP	Work in Progress WIP files are visible only to the uploading information supplier but may be distributed to users in the same supplier organisation. WIP files may be used by any supplier including the employer team prior to distribution within the AIM CDE or to other systems.

Appendix 2 - Information Delivery Planning Tool

The system referenced here is a proof of concept system developed to test the process and information requirements. It has been used with a single serial procuring Government Department to drive over 400 capital projects. As a reference system, it will act as a guide for the expected functionality and the AIM CDE requirement.

Please see the Information Delivery Planning Tool as specific project or contract specific part of the framework level PAS1192-2 Employers Information Requirements in Appendix 1.

The system has the following characteristics

1. The AIM CDE project/contract workspace context is generated from a template with associated information breakdown structure 'master list' and BS1192-4 data requirements, metadata, AIR OTL Library and PLQ templates.
2. The project context will have a single assigned project manager and a number of assigned editors to manage the status and progression, status, roles and assignments of the project.
3. The IDP is a single document accessible by all information suppliers either in the pre-appointment or appointed state.
4. The stage plan can be profiled with information manager, gateway dates and status. The gateway dates are not the project programme, but dates when stage published information should be presented by.
5. The plain language questions, with typical and actual stage deliverables, are available to display for each stage. The display confirms actual delivery and project manager added notes to report on delivery to the stage gateway review.
6. The employer and other stakeholders may also be information suppliers.
7. The full long list of deliverables can be displayed and selected by allocating a role and level of definition information requirement at each required stage.
8. Potential tendering information suppliers may add their own tender proposals to each information deliverable visible to themselves and the project manager/editors who can select tender proposals from one or all to view.
9. Appointed information suppliers can add their own master information delivery plan schedule file delivery items to each of the appointed IDP deliverables linked by delivery reference. The IDP and MIDP tracks actual file delivery stage by stage with a RAG status. Files may be added to the system by dragging and dropping over the appropriate stage MIDP item which will appropriately name the file in the system subject to confirmation of suitability and revision codes.
10. Volume and location strategies can be profiled by information suppliers as part of the MIDP process.
11. A BS1192-4 Data Information Requirements sheet based on the template(s), IDP/MIDP and volume and location strategies can be generated and downloaded for use outside the system, e.g. for transfer to say the NBS Toolkit.

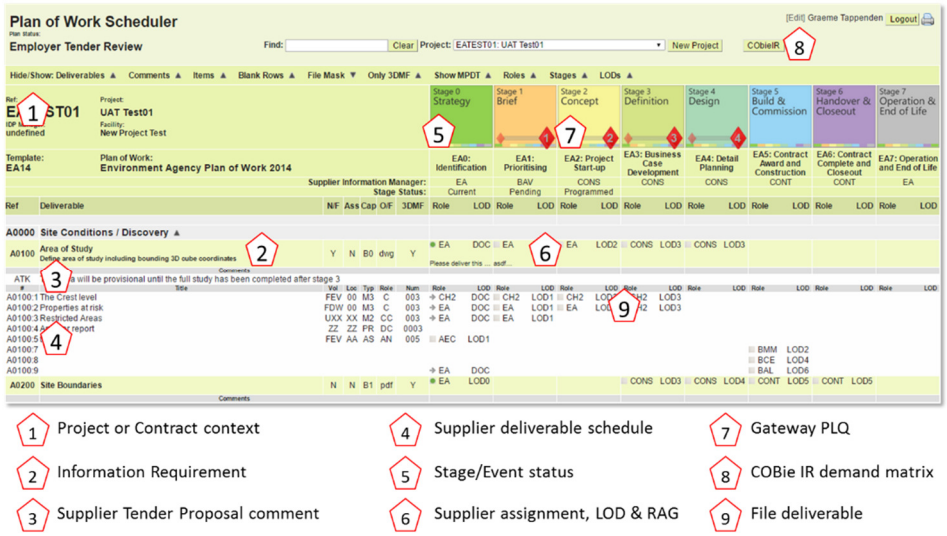

Figure 5 - Proof of Concept Information Delivery Plan Tool

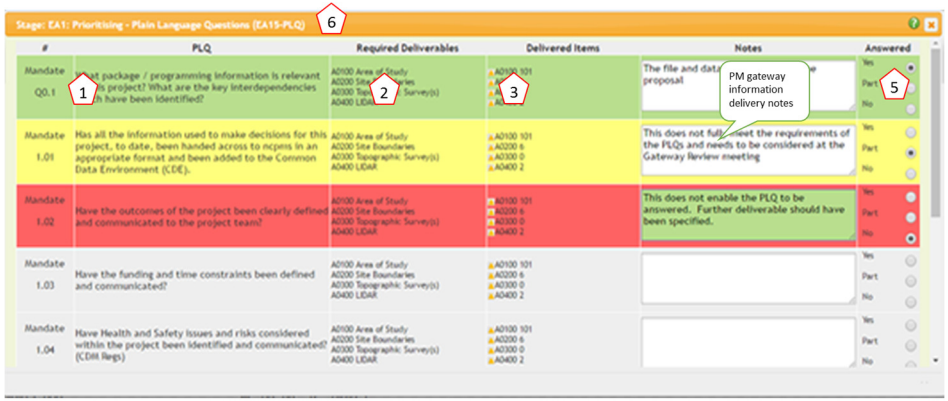

Figure 6 - Stage or event gateway plain language questions delivery review

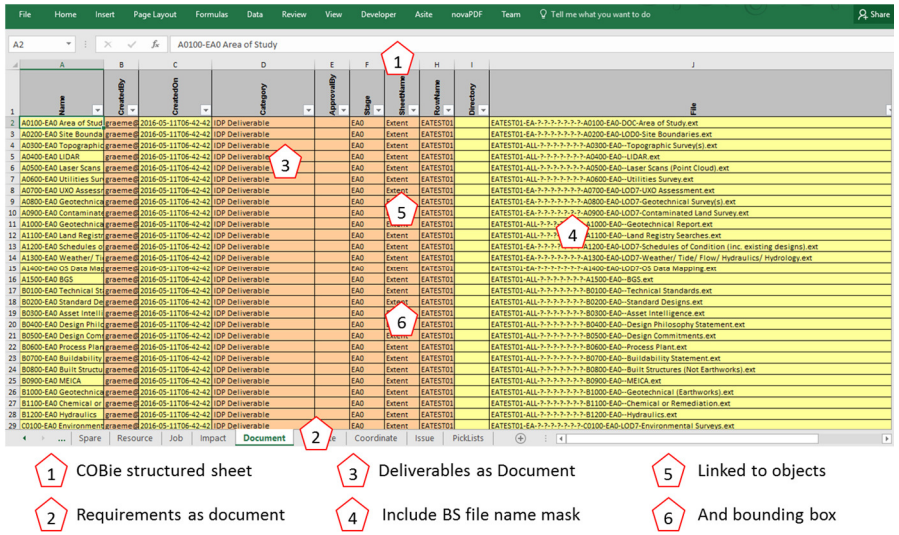

Figure 7 - Example BS1192-4 Data information requirements spreadsheet generated from the IDP confirming the contractual information requirements and deliverable file placeholders, file metadata requirements and links to object placeholders in the system. File metadata lookup pick lists can also be included and be used as a BS1192-4 data demand matrix for the required file and metadata deliverables.

Appendix 3 – Assurance

A major feature of the AIM CDE is to apply formal information delivery assurance to all procured information before it is available to be reliably used. This assurance should align to a standard delivery workflow such as the UK Government digital pathway (see below). Until published information has been verified as meeting the requirements: i.e. is all present and correct, and confirmed as answering the stage or event gateway plain language questions, published information cannot be relied upon or trusted.

An example assurance strategy mapping onto the digital pathway is shown below. This enables assurance to be progressively applied in setting up a project or contract, procuring the information, supplier mobilization, information delivery, and in validating the specified procured delivered information meets the plain language questions.

This section describes an exemplar contractual information management workflow and assurance points on the employer side of the contract line that can be managed by the employer within the AIM CDE.

Figure 8 shows the workflow stages to be mapped within the digital pathway.

Figure 9 shows the incremental steps A-I to implement a file and data verification and PLQ validation strategy all within the AIM CDE. Assurance applied to the supplier side of the contract line is not managed via the AIM CDE.

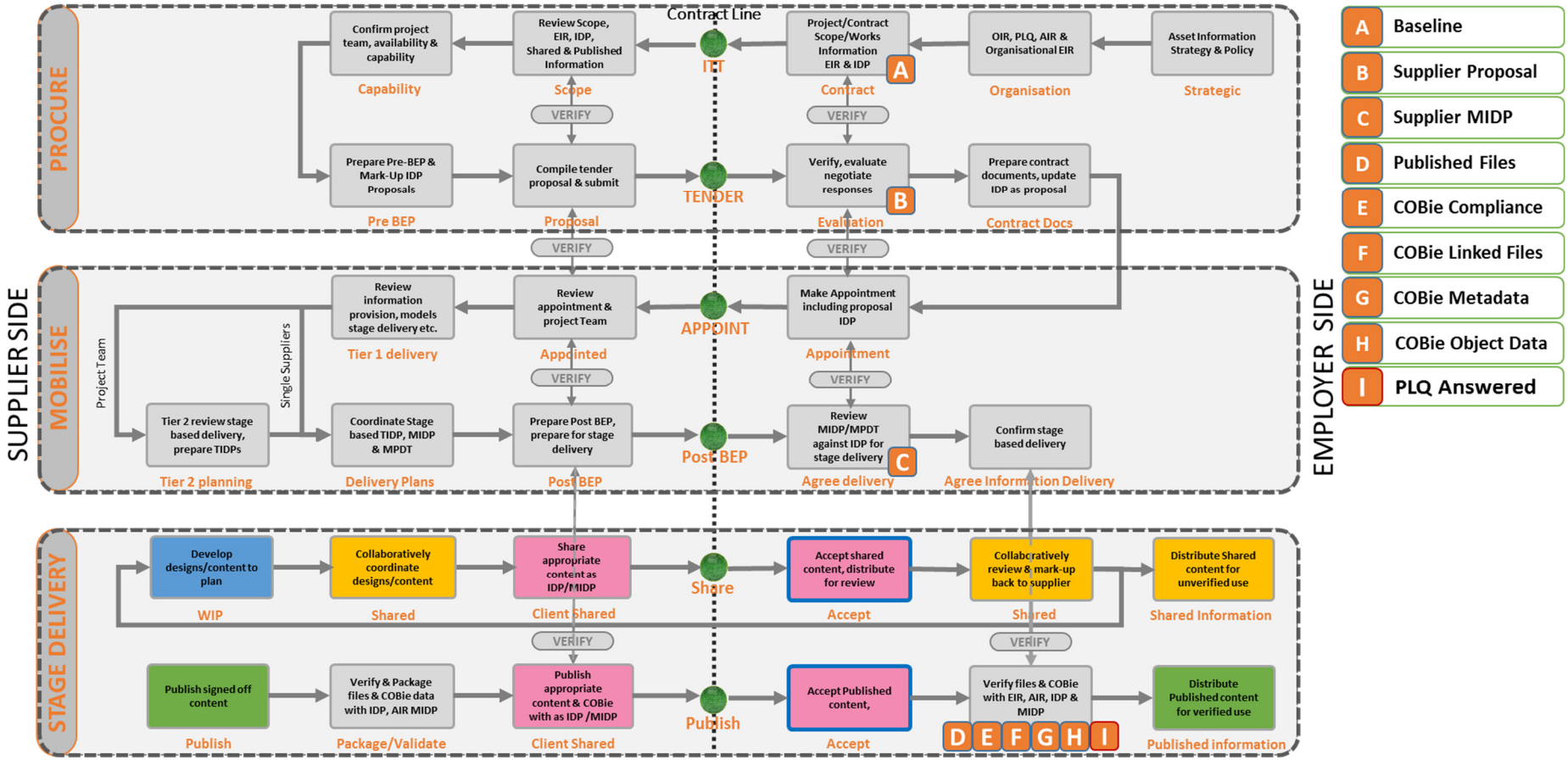

Figure 8 - Digital Pathway aligned assurance strategy

	Verification	Scope	Value	Possible Solution
A	IDP ITT vs Baseline [Internal Assurance]	Before issuing a project ITT (at any stage, any supplier) confirm the variance between the project information delivery plan (IDP) and a baseline standard to confirm completeness and variation	Assurance that the project variation from norm is justified and fully taken into account. Promotes the use of standard, repeatable and known deliverable components. Minimises EIR variations	Having created a project IDP, a method to compare the deliverable & stage items with a benchmark for the project type. This could be dynamically in the interface as deliverables are assigned or a RAG report run independently.
B	IDP Proposal vs ITT IDP [Procurement]	Each supplier will confirm its IDP proposal: ability, innovation & assurance on delivery, of information items and each needs to be compared with the invited plan to highlight variation	Enables assessment of tender proposals across the contending parties to assess capability, innovation and assurance, and value information delivery proposal. Minimises Pre BEP.	A method to compare each supplier IDP tender response with that issued with the tender, either dynamically in the interface or via a RAG report showing deliverable variations stage by stage.
C	MIDP vs IDP [Compliance]	The supplier MIDP as presented post appointment with the Post BEP and prior to each stage end. Confirm that all proposed IDP products have minimum MIDP items, highlight variance	Assurance of information delivery. Enables confirmation of MIDP delivery proposals against contractual IDP and prior to stage end. MIDP is a live controlled document subject to in stage development.	A method of comparing MIDP items against appointed IDP deliverables - at this stage, at least one MIDP item required per IDP deliverable. The MIDP is a live list subject to change control but not in itself triggering compensation events.
D	Presented Files vs MIDP [Completeness]	The presented 'published' files into the AIM CDE are confirmed against the MIDP (and IDP) and variance highlighted	Confirms file delivery against plan, stage/ LOD/ referencing to enable stage PLQ & gateway review, and assessment of ongoing project risk & reserve	The MIDP is a placeholder list of all files to be 'published' into the AIM CDE at each stage. A method of showing which MIDP items have been fulfilled with 'authorised' files present in the AIM CDE File Store.
E	Presented COBie vs IDP COBie etc. [Compliance]	The presented COBie is compliant and meets the EIR/IDP/BS1192-4/UNICLASS2015 requirements for entity naming & classification.	Ensures that the presented information is the correct format to be processes and act as the basis of presentation into the AIM CDE Published File & Data Stores	Verifying that the presented COBie file(s) is formatted to the COBie Information Requirements 'demand matrix' workbook generated from a client boilerplate workbook overlain with the project IDP/MIDP
F	Presented COBie vs Presented Files [Completeness]	Compare and highlight the variance between the COBie document tab files as a file manifest, and the presented files; confirm the url linkage capture into the AIM CDE data set.	Ensure that the required MIDP files are presented and linked into the data set in readiness for extraction into the AIM CDE Published Data Store and business use	Verifying that the presented COBie file documents tab Directory and File columns map to files present in the AIM CDE File Store and can be linked when the COBie is extracted into the AIM CDE Data Store
G	Presented COBie Metadata vs IDP Metadata [Completeness]	Confirm appropriate COBie (document tab) file (attribute tab) attribution values for the stage and LOD information completeness to the IDP COBie Information Requirements	Ensuring delivered file provenance and appropriate meta data definition before extraction into the AIM CDE Published data Store and business use	Verify that each presented Document Tab MIDP Item has the required provenance attribution completed for the stage of presentation in the IDP Information Requirements as a demand matrix
H	Presented COBie Object Data vs AIR COBie Library [Completeness & Continuity]	Confirm the presence of appropriate COBie attribution values for each defined object in the AIR Object Type Library for the stage	Ensure delivered data meets the brief and client requirements for each presented object before extraction into the AIM CDE Published Data Store and business use	Use of a client, sector or open AIR COBie Library as the Object Type Library 'demand matrix' to verify that presented COBie objects, relationships and data are complete and sufficient (continuity).
I	Presented Information Answers PLQ [Validation]	Confirm that the presented information has been specified sufficiently to fully answer each and every stage PLQ and present to Gateway Review	Ensure delivered specified information answers the stage Plain Language Questions to enable fully informed business and stakeholder decisions based on appropriate reliable information	Client (client agent) Assessment that the presented files and data is sufficient to individually answer the stage Plain Language Questions and present for stage Gateway Review.

Figure 9 - Delivery Assurance: File and data verification and PLQ validation

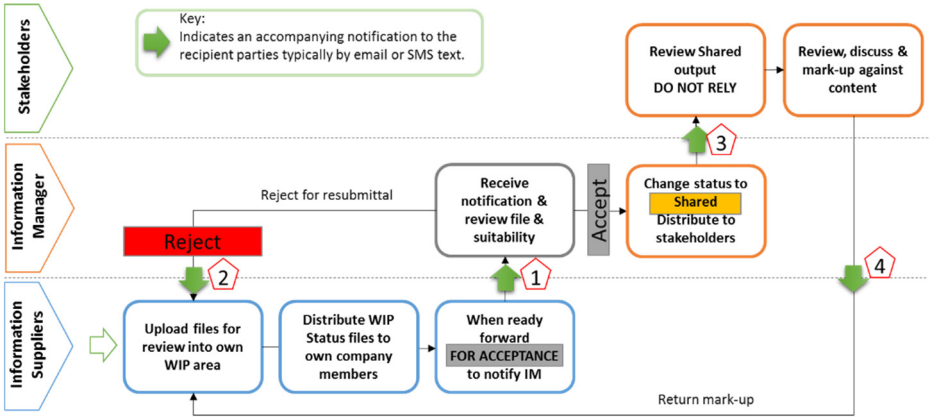

Figure 10 - Example Employers AIM CDE Shared suitability file acceptance workflow

Shared files presented 'for acceptance' (1) Files rejected (2) or Accepted to appropriate stakeholders for review (3). Stakeholders review mark-up and notify (4).

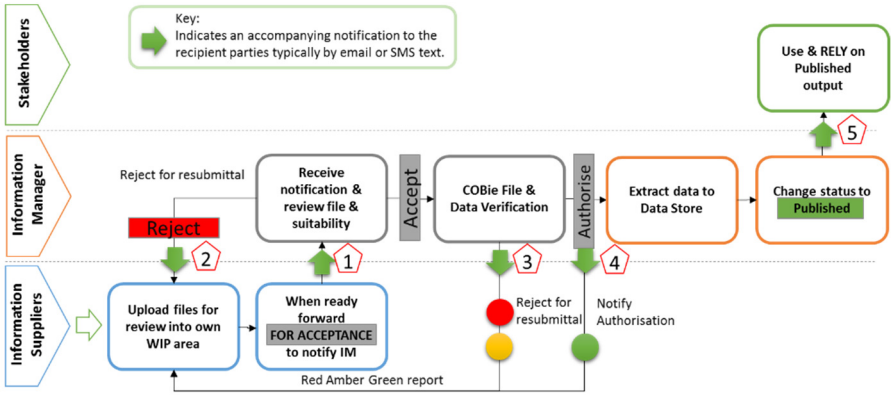

Figure 11 - Example Employers AIM CDE Published suitability workflow

Published files presented for acceptance (1). Rejected files (2) or accepted via verification process and a RAG report with amber or red failure (3) or green authorisation (4). Authorised *BS1192-4 data* is extracted to the Data Store and files pass to the File Store, all published AIM CDE (5). Both files and data can then be used and relied upon to the suitability, level of development and stage.

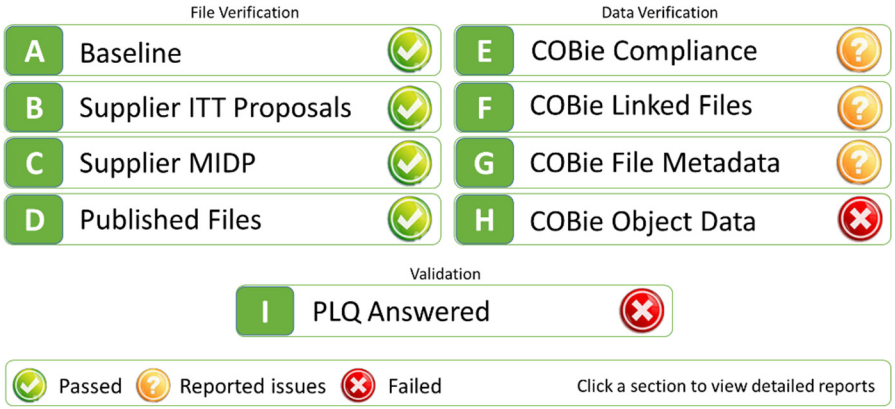

Figure 12 - Example AIM CDE Assurance Summary Report

Appendix 4 - Extended File Naming

File naming to a strict dash delaminated format is required to be to BS1192:2007 and PAS1192-2:2013 – BS file name structure. File uploads to the employer AIM CDE shall be named to an extended file name structure consisting of the BS file name plus additional metadata fields, the extended file name. Fully named and dash delimitated extended file names shall drag and drop upload without the requirement for manual profiling. Partially named dash delimitated files, including BS file names, shall require manual completion of the extended file name for each file.

It shall not be possible to upload an incorrectly named file: all fields may have pre-assigned values in the EIR/IDP/MIDP. To aide with the efficiency of metadata provision when uploading any files to the employer's AIM CDE the following metadata can be optionally added to the end of the BS file name which, if included, will be automatically profiled as metadata by the employer AIM CDE maintaining the file name portion in the file store. An example of extended BS1192 file names is shown in the diagram below.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Ref	- Originator	- Volume	- Location	- Type	- Role	- Number	- Status	- Rev	- DefRef	- Stage	- LOD	- Title	. EXT

BS1192 File Name

1	Ref	Employer assigned unique reference for the Project or Contract workspace	Master lookup
2	Originator	Employer defined unique reference for the contracted information supplier organisation	Master lookup
3	Volume	Employer defined unique Volume/Zone code confirmed by the information supplier(s)	Master lookup
4	Location	Employer defined unique Level/Region/Location code confirmed by the information supplier(s)	Master lookup
5	Type	Employer defined unique document/model/information type code	Master lookup
6	Role	Employer defined unique role/discipline code	Master lookup
7	Number	Unique document/drawing/file number assigned by the information supplier	Free text

Extended File Name

8	Status	Employer defined BS1192 Status/Purpose code assigned by information supplier	Master lookup
9	Revision	Information supplier assigned BS1192 instance revision code	Free text
10	DefRef	Employer defined unique Information Delivery Plan deliverable requirement code	Master lookup
11	Stage	Employer defined project or contract Plan of Work stage or event identifier	Master lookup
12	LOD	Employer defined Level of Detail / Level of Information definition aligned to Plan of Work	Master lookup
13	Title	Free text human readable title	Free text
14	EXT	Employer defined file format extension	Free text

Figure 13 - Example BS1192 extended file name attribution

Appendix 5 – AIM CDE British Standards Alignment

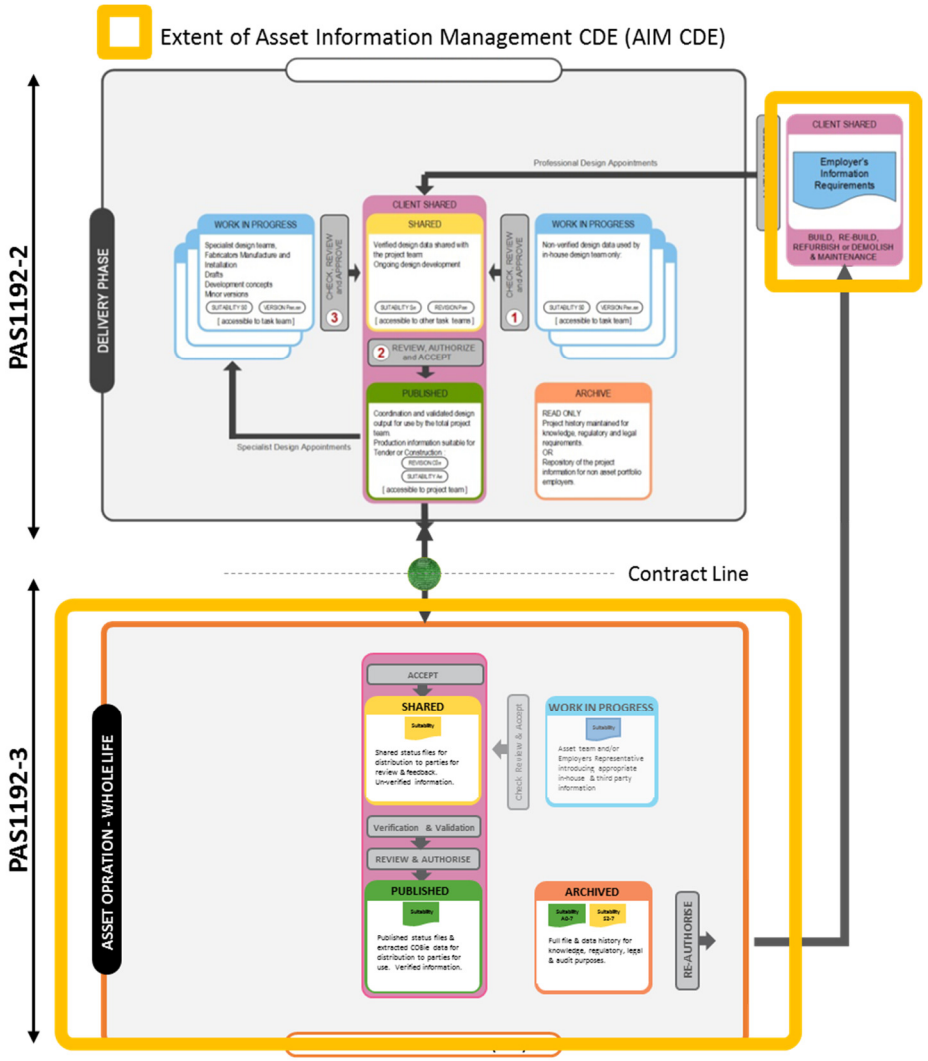

Figure 14 - AIM CDE PAS1192-2 & PAS1192-3 Alignment

Appendix 6 – Bibliography

BS 1192:2007 A2:2016	Collaborative production of architectural, engineering and construction information – Code of practice
PAS 1192-2:2013 A13	Specification for information management for the capital/delivery phase of construction projects using building information modelling
PAS 1192-3:2014	Specification for information management for the operational phase of assets using building information modelling
BS 1192-4:2014	Collaborative production of information Part 4: Fulfilling employer's information exchange requirements using COBie – Code of practice
PAS 1192-5:2015	Specification for security-minded building information modelling, digital built environments and smart asset management
BS 8536-1:2015	Briefing for design and construction – Part 1: Code of practice for facilities management (Buildings infrastructure)
BS 8536-2:2016	Briefing for design and construction – Part 2: Code of practice for asset management (Linear and geographical infrastructure)
CPNI	Guidance for BIM Level 2 Common Data Environments

Appendix 7 - Contributors

Contributor	Role	Organisation
Adrian Burgess	**Author**	**PCSG**
Graeme Tappenden	**Author**	**Lingwell Consulting**
Fiona Moore	**Editor**	**Cirrus Consultant Services**

Members of the UK Government BIM Working Group