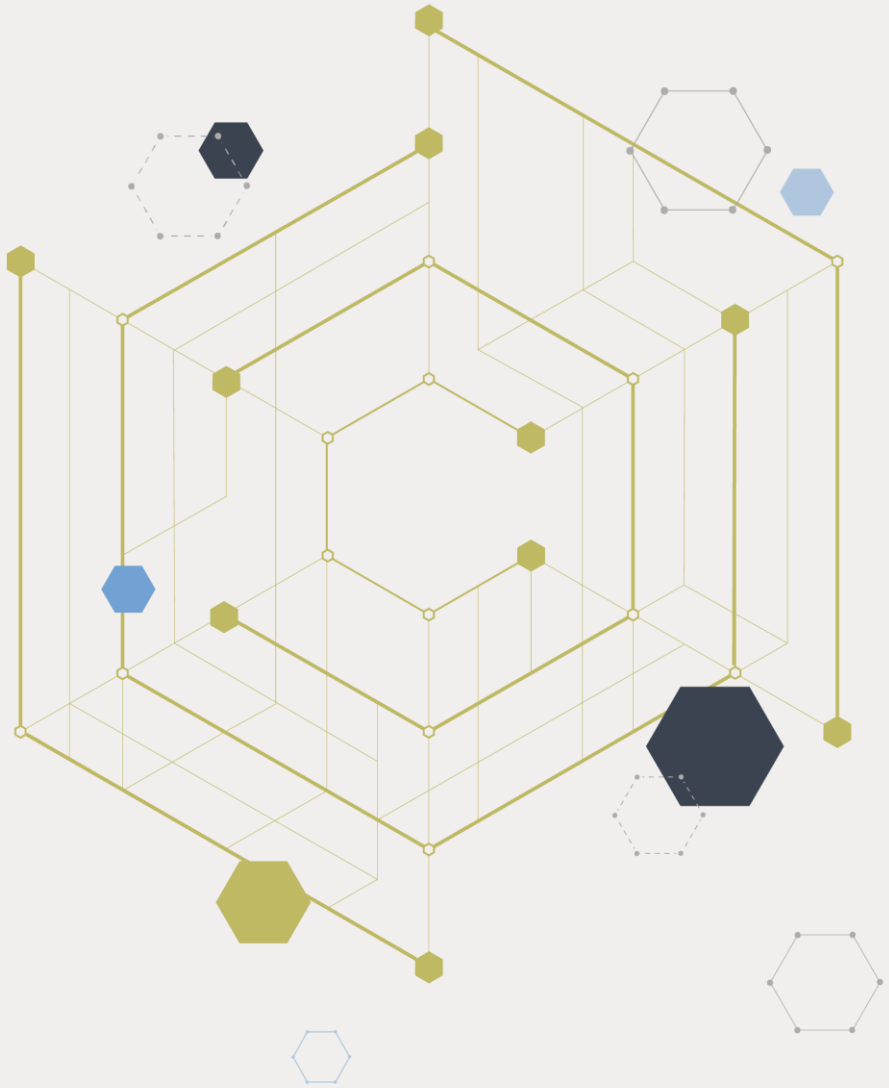


Welcome to…
Delivering Valuable Data

Launch of an Interoperability Code of Practice in the Built and Managed Environment

Agenda and Housekeeping

1. Interoperable information – why it matters to government – Fergus Harradence
2. A client perspective on interoperability – Fiona Moore
3. The Interoperability Code of Practice for Technologies – Paul Wilkinson
4. A supply-chain / technology user perspective – Terry Stocks

Q&A

Networking Lunch 12-12.30

Why interoperable information matters to Government

Fergus Harradence

Department for Business & Trade

Interoperable Information: why it matters to Government

Launch of the Interoperability Code of Practice

17 April 2023

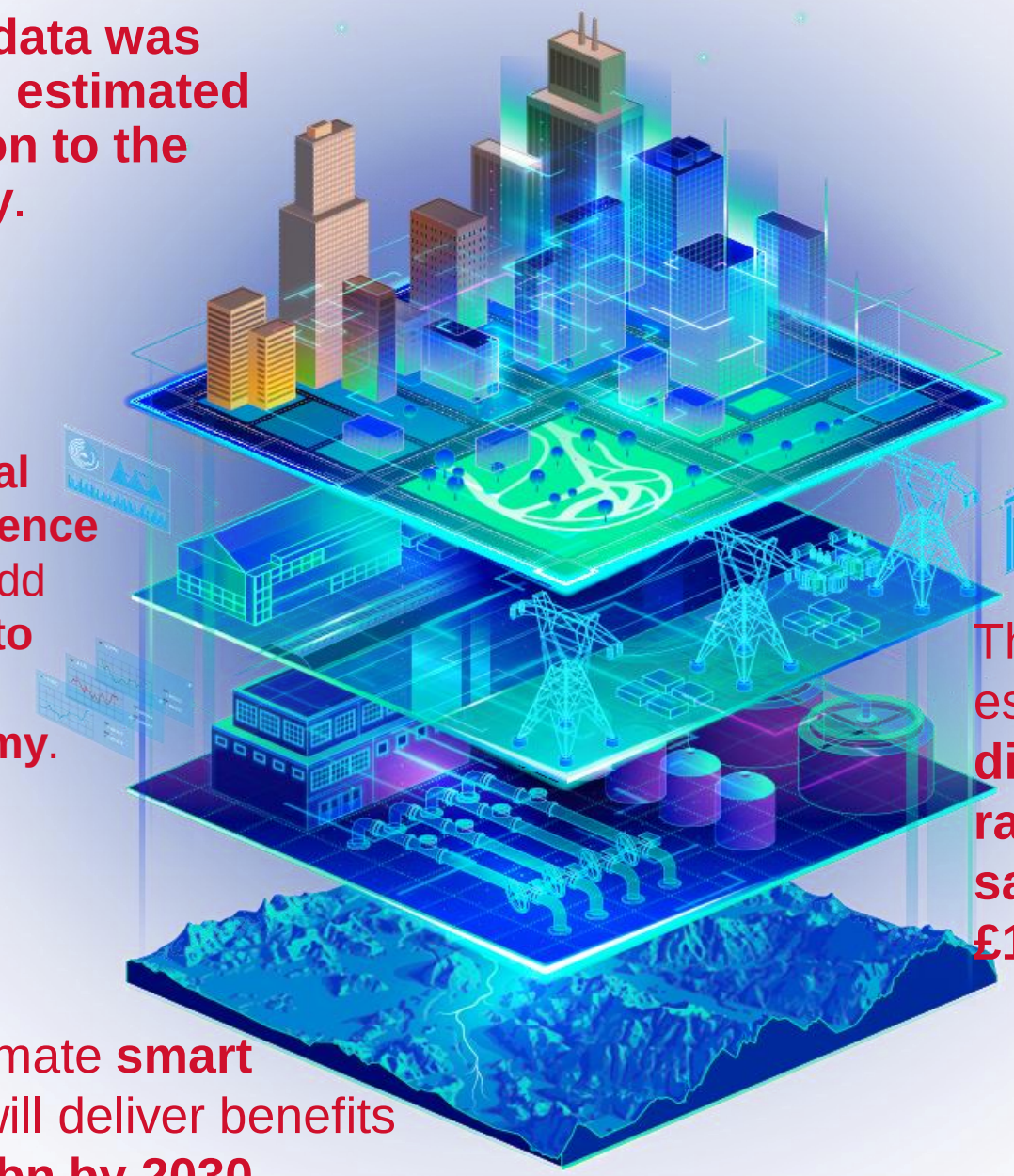
Data is critical to improving the built environment

"Data informs how our infrastructure is built, managed and eventually decommissioned, and real-time data can inform how our infrastructure is operated on a second by second basis. Data is now as critical a component of our infrastructure as bricks and mortar. **Data is part of infrastructure and needs maintenance in the same way that physical infrastructure needs maintenance. It must be updated, housed and made secure**."

Data for the Public Good, National Infrastructure Commission (Dec 2017)

- In 2017, **data was worth an estimated £50 billion to the economy**.

KPMG estimated **every £1 invested in data delivers a return of £6**.



Artificial Intelligence could add **10.3% to the UK economy**.

The NIC estimated that **the digitisation of rail assets** would **save nearly £100m pa**.

Ofgem estimate **smart metering** will deliver benefits **of £1.3-5.7bn by 2030**.

Government Construction policy is now driven by outcomes and the need to address the challenges of productivity, climate change, building safety and financial pressures

The Transforming Infrastructure Performance Roadmap to 2030 sets out the Government's strategic objectives in relation to data on the built environment

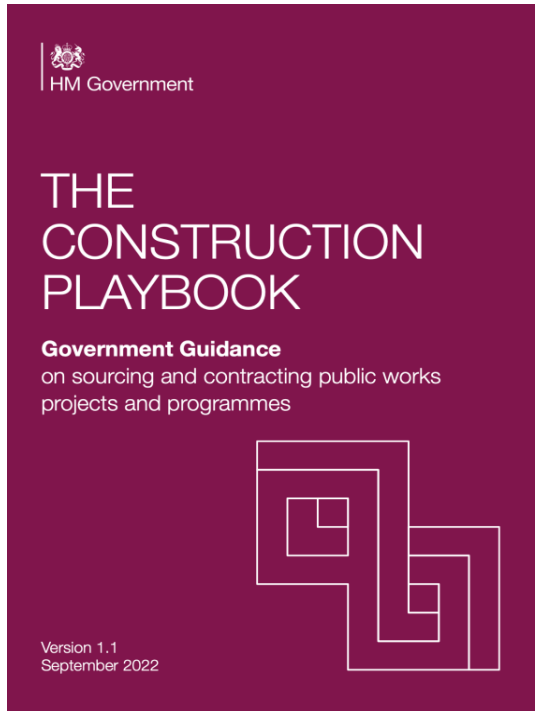
- **value** – mentioned 66 times
- "Government will also need to leverage **data** more effectively, as an enabler to more effective delivery, and also as the means of determining whether the desired outcomes have been achieved." (p.14)
- " …data will increasingly need to be made **interoperable**. … an enabler for the provision of the right information, at the right time, to the right people and to ensure the quality of the information is understood." (p.20)

Information management mandate Annex B

g. apply the same level of governance and rigour to the maintenance of its information, to ensure that it provides ongoing value and benefits to the client organisation. This will include the ability to share and exploit information, and also make information available for regulatory purposes.

The Construction Playbook emphasises the link between data and outcomes, and the importance of interoperability as an enabler

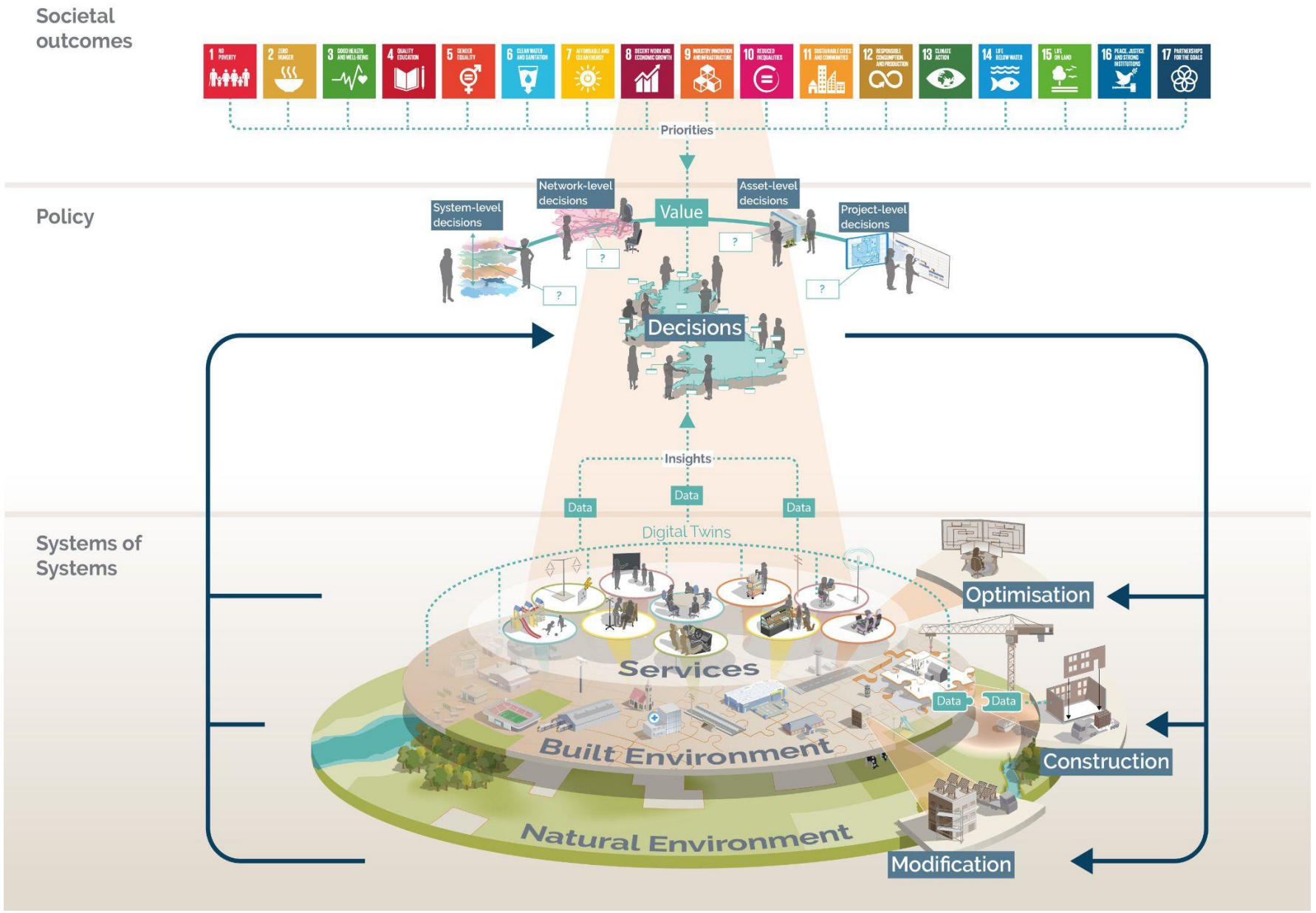
- ‘comply or explain’ guidance to UK government departments and arms-length bodies on procuring public works projects and programmes.
- Strongly **outcomes** focused (82 mentions)
- “**whole life**” mentioned 23 times
- **value** – mentioned 120 times
- “greater sharing of better **data**” (p.4)



Interoperability

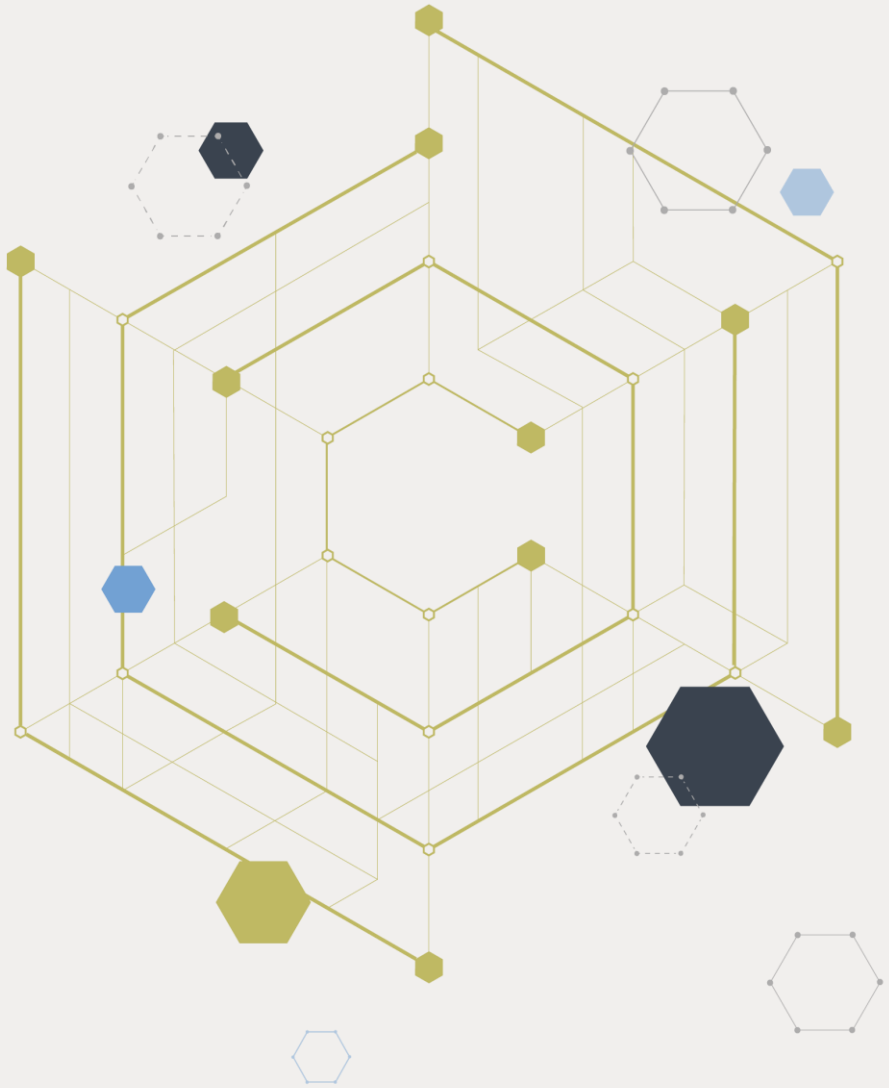
- The UK BIM Framework: “…standards, guidance and other resources that will deliver BIM **interoperability** and government soft landings” (p.23)
- Information Management Platform approach: “… guidance on information **interoperability** to promote the secure exchange and use of data and information between parties. (p.23)

The Roadmap to 2030 presents a vision for the future where we **collectively prioritise the societal outcomes we need,** and use **data**, technology and improved delivery models to achieve them through our interventions in the built environment." (p.6)



A client perspective on interoperability

Fiona Moore



Delivering Valuable Data

The Importance of the Interoperability Code of Practice for Technologies to Client Organisations

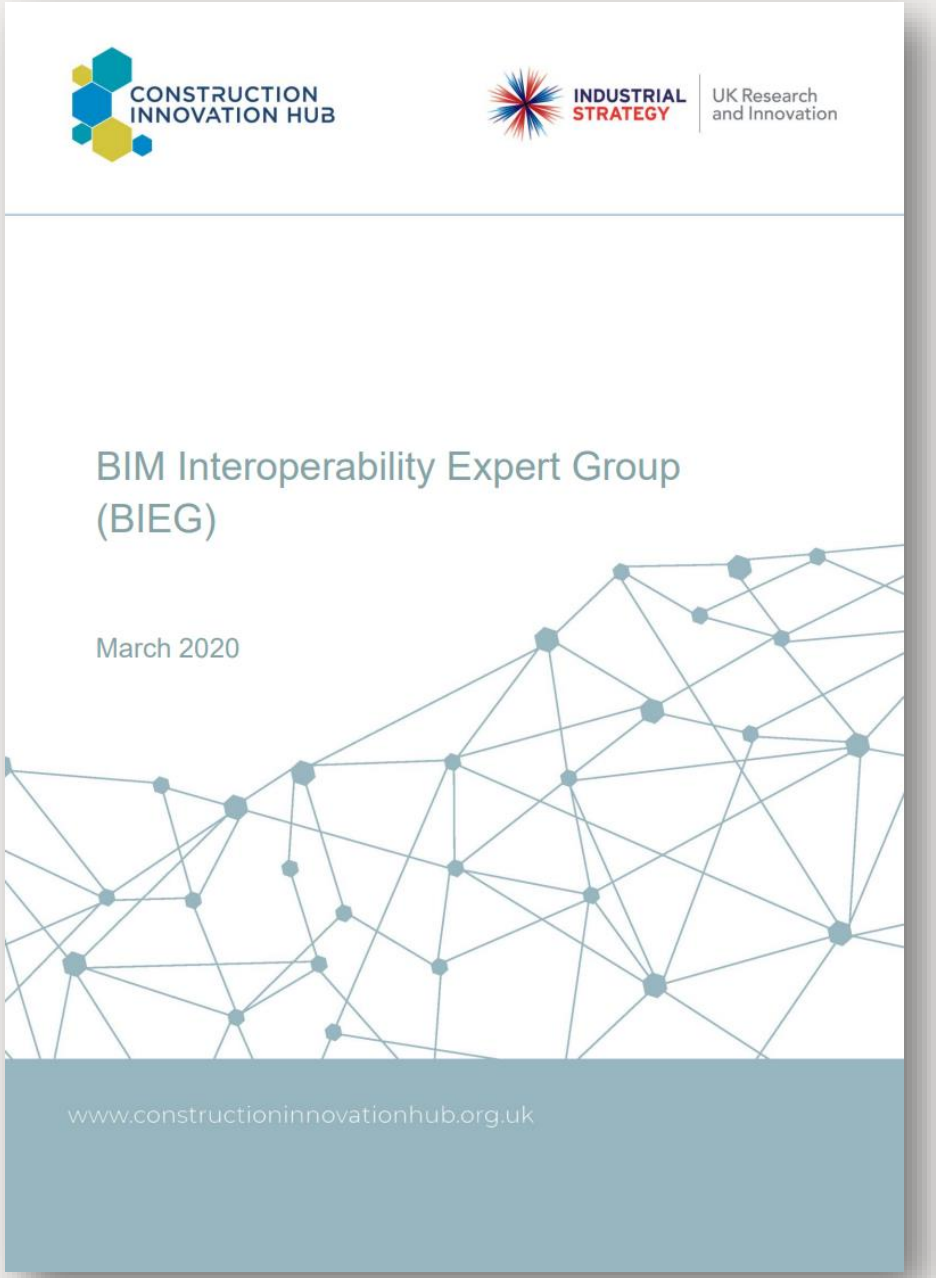
Fiona Moore, GIIG Technical Lead

Delivering Valuable Data an Interoperability Code of Practice for Technologies in the Built and Managed Environment:

‘ability to exchange and use information securely, ensuring that the information is independent of the technologies used to deliver it.’

“Interoperability supports the provision of a ‘Golden Thread of Asset Information’

Polling Industry



Interoperability Report

March 2020

Evidence from industry practitioners, technology providers and support organisations.

Key themes:

- practice not theory
- practice based on standards – UK BIM Framework (ISO19650)
- coordination
- key enablers

5. Primary recommendations / enablers

i. Classification Schema Alignment

Firstly, it is proposed that the Steering Group work with NBS to examine how Uniclass 2015 can be improved, supported and maintained going forward.

Once this initial engagement has been undertaken, other matters can be considered, including:

- How Uniclass 2015 aligns / maps to other conventions, such as CoClass.
- Alignment or mapping of appropriate aspects of Uniclass 2015 with other breakdown structures, such as NRM and SFG20.
- Support to help NBS to improve and then maintain Uniclass 2015 – including helping NBS to liaise with key construction industry sector stakeholders.

It should be noted that the BIEG also considered other schemas such as CoClass and OmniClass. It concluded that the most efficient way forward was to continue to support Uniclass 2015, whilst at the same time supporting its mapping to other schemas.

ii. COBie - Practical Application and Development

Liaise with the UK BIM Alliance and buildingSMART UKI, with support from buildingSMART International as appropriate, to explore the development of multiple Model View Definitions (MVDs). This work will start with COBie, for the reason that it continues to be a very important part of UK Government information procurement.

More specific work is likely to be identified once the initial liaison has taken place.

iii. Education and Skills

There is clear direction from those providing evidence that there is a lack of digital skills within the sector which needs to be urgently addressed.

This is an area which will involve wider engagement, and may need to be addressed by, and coordinated across, a number of different organisations.

iv. Industry Foundation Classes (IFC)

Liaise with buildingSMART International, and its UK/Ireland Chapter, to support the further development of IFC, with the aim of helping to voice the concerns of key construction industry stakeholders, as expressed by a number of the evidence providers (see Appendix B).

More specific work is likely to be identified once the initial liaison has taken place.

v. Standards

It is clear that work is required to clarify and communicate the Standards landscape and then to make sure appropriate training is available to help improve its application. Further discovery work will be required to correctly scope this work.

6. Secondary recommendations / enablers

During the course of the work a number of other facets of the interoperability agenda were raised. However, the BIEG agreed that these enablers required further evaluation, prior to issuing specific recommendations for a variety of reasons, including:

- lack of consensus on direction;
- requirement for further development and/or unlikely to enter the mainstream within the timeframe of this report;
- insufficient evidence to produce an acceptable level of recommendation; and
- some form of proprietary content

These secondary enablers are listed below in alphabetical order and NOT in order of priority. Each is explained Appendix B.

i. **Asset Information Model (AIM) Common Data Environments (CDE)**

ii. **Drivers and Enablers**

iii. **Global Unique Identifiers (GUID)**

iv. **Operational Focus**

v. **Product Data Templates (PDT)**

vi. **Proprietary software and the use of Application Program Interfaces (API)**

vii. **Standard Data Approach**

viii. **Procurement and Contracts**

In assessing each of the enablers and potential activities, it will be important for the Steering Group to take account of the work of others in the field, who may be working on other related projects within the CIH, the UK BIM Alliance and wider industry. The Steering Group should actively seek to share knowledge, avoid duplication and improve outcomes.

Interoperability Report

Recommendations from the sharp end - those specifying and delivering information

Technologies The Information Management Platform

IMP

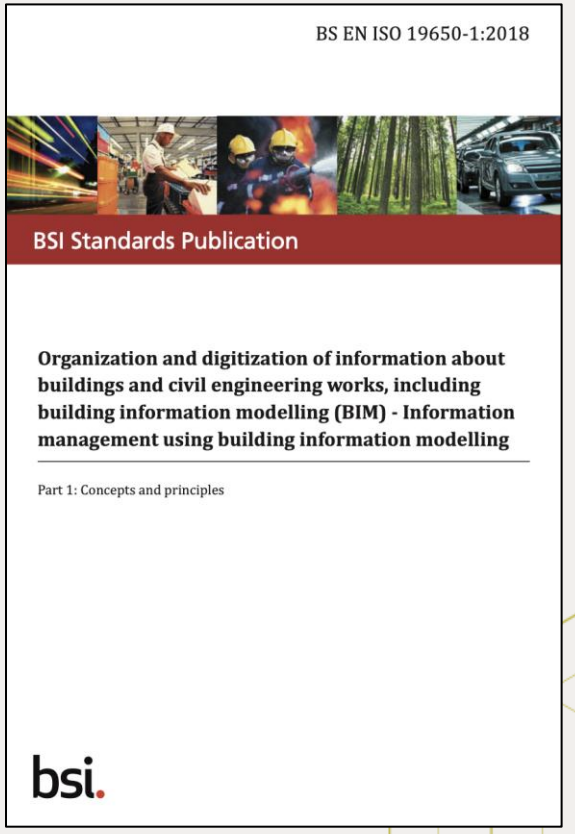
Requirements of the UK BIM Framework

ISO 19650-1 Principles

9 d. Provision of a CDE to manage and store shared information, with appropriate and secure availability to all individuals or parties who are required to produce, use and maintain that information.

11.1 Managing the collaborative production of information: a CDE solution and workflow should be implemented….

12. A Common Data Environment (CDE) solution and workflow... should be used for managing information during asset management and project delivery.



Information Management Platform:
Informing clients' operational decisions

Controlled Data Delivery

Control infrastructure data, automate assurance and integration, to inform their very best operational decisions.

Golden Thread System of Record

An auditable 'golden thread' system-of-record, immutably capturing, assuring and storing information and data, its provenance and purpose.

Data Quality Data Reliability

Providing the technology and tools to significantly improve data quality, completeness and reliability.

Data Visualisation System Integration

Providing an open-format, structured portfolio data model and referenced documents, to enable visualisation, analytics, insight and informed decisions

System of Systems Foundation Digital Twin

Building a reliable and exploitable information management resource, transferring insight and value, informing policy, for better social outcomes.

The processes an Information Management Platform supports

Specify

Standardised, scalable, content-managed

Procure

Framework-level minimum technical standards, reducing risk and cost

Deliver

Delivery certainty, against information requirements

Assure

Automated rule-based and subject matter expert assurance within short contract response times

Store

Immutable storage of contracted file content; structured data extraction into portfolio repository

Present

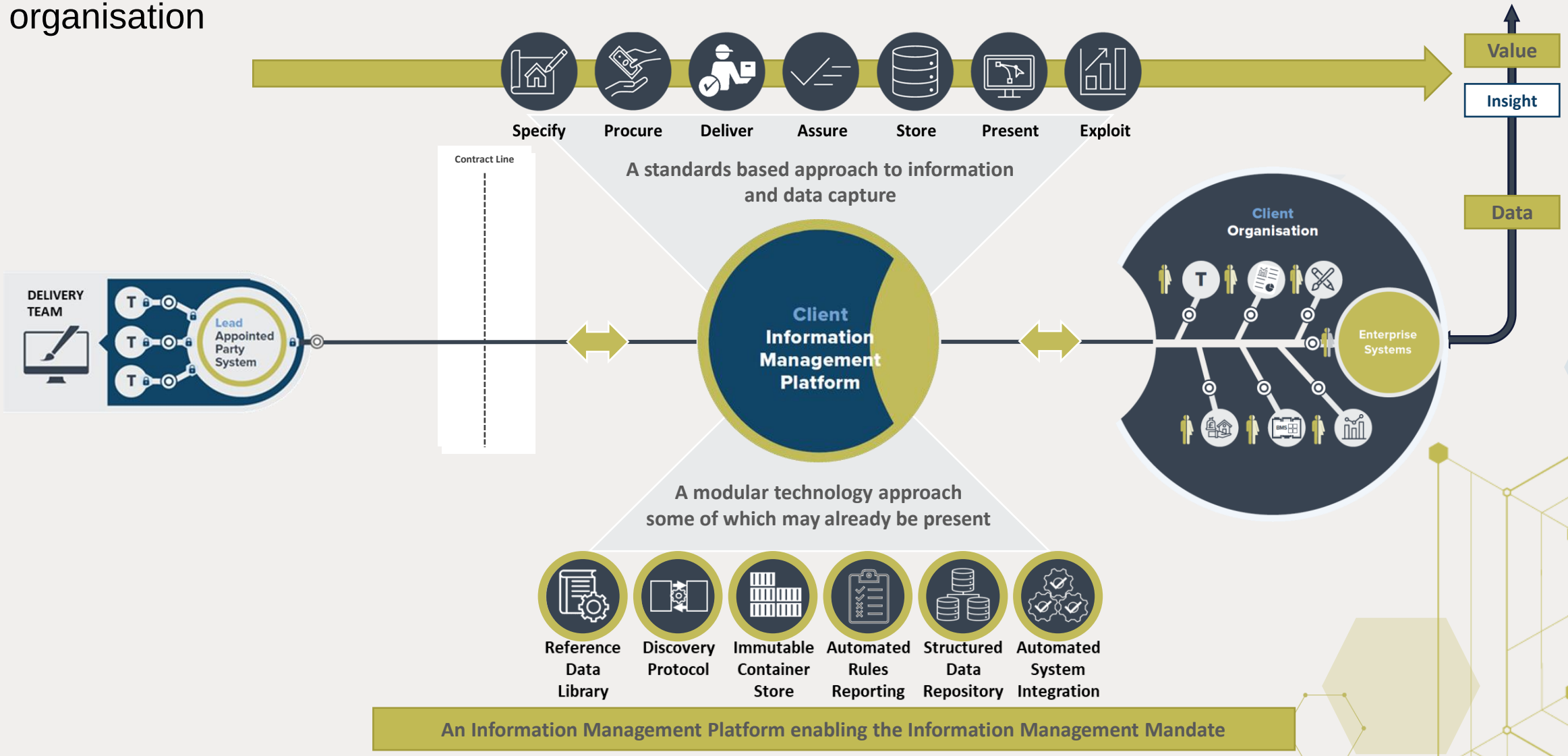
Visualisation, analytics and insight, performance dashboards and reporting

Exploit

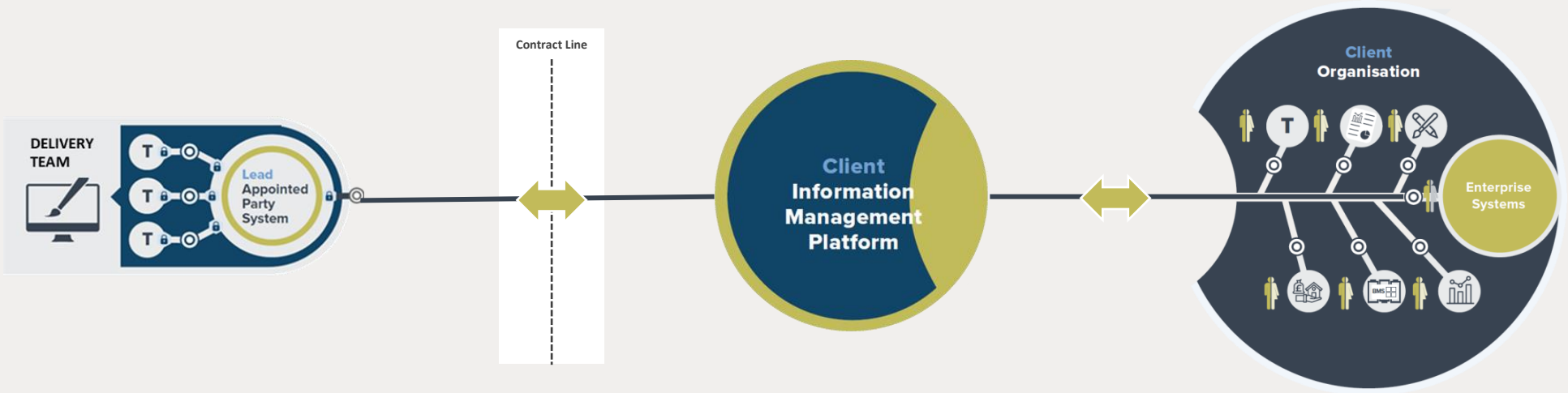
Automated enterprise and 3rd party system integration, enabling federated digital twins

Information Management Platform – a modular technology platform

A scalable modular technology pipeline - some of which may already exist in a client organisation



Information Management Platform – Technology Modules



Information Delivery Pipeline

Reference Data Library:
A curated and securely accessible collection of reference data standards and data sets required to be used for information management throughout the organisation, whether externally or internally authored.

Discovery Protocol:
An automated means to achieve interoperable system-to-system digital information exchange.

Immutable Container Store:
Access controlled store of project-based information which allows assurance activities to be undertaken through rules-based processes and inspections by subject matter experts, prior to the information being accepted into the Client's organisation

Automated Rules Reporting:
System for automating the generation of rules-based reports on data and information in the Immutable Container Store, with reports accessible only to authenticated internal and external users.

Structured Data Repository:
A repository of assured structured data, populated with records from the Immutable Container Store, which allows authorised users to explore, query and cross-reference information they are authorised to access using information visualisation and analytics tools.

Automated System Integration:
A system that transfers published, accepted and assured content from the Structured Data Repository to update each target enterprise system.

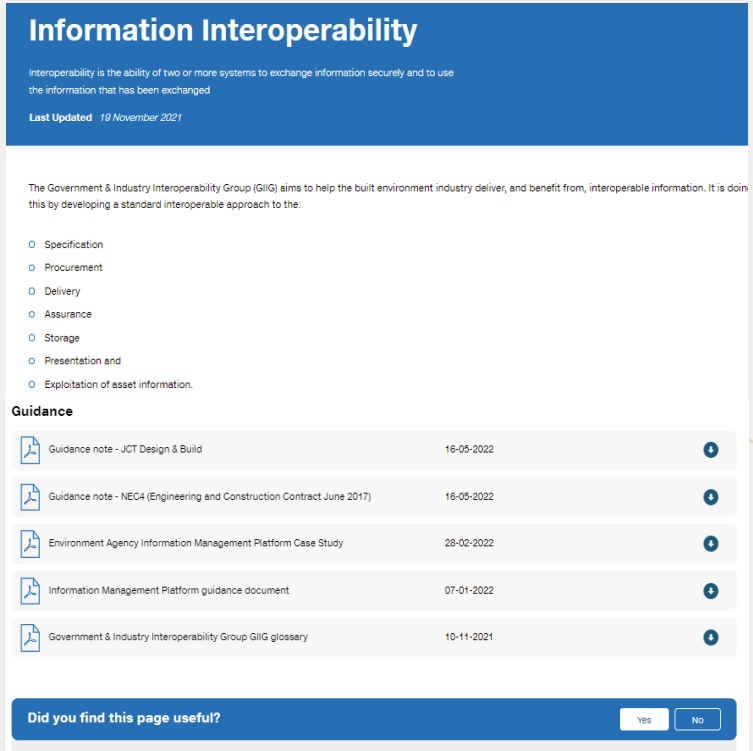
Published Resources

IMPACT Information Management Platform Assessment and Checklist Tool

https://www.ukbimframework.org/giig/

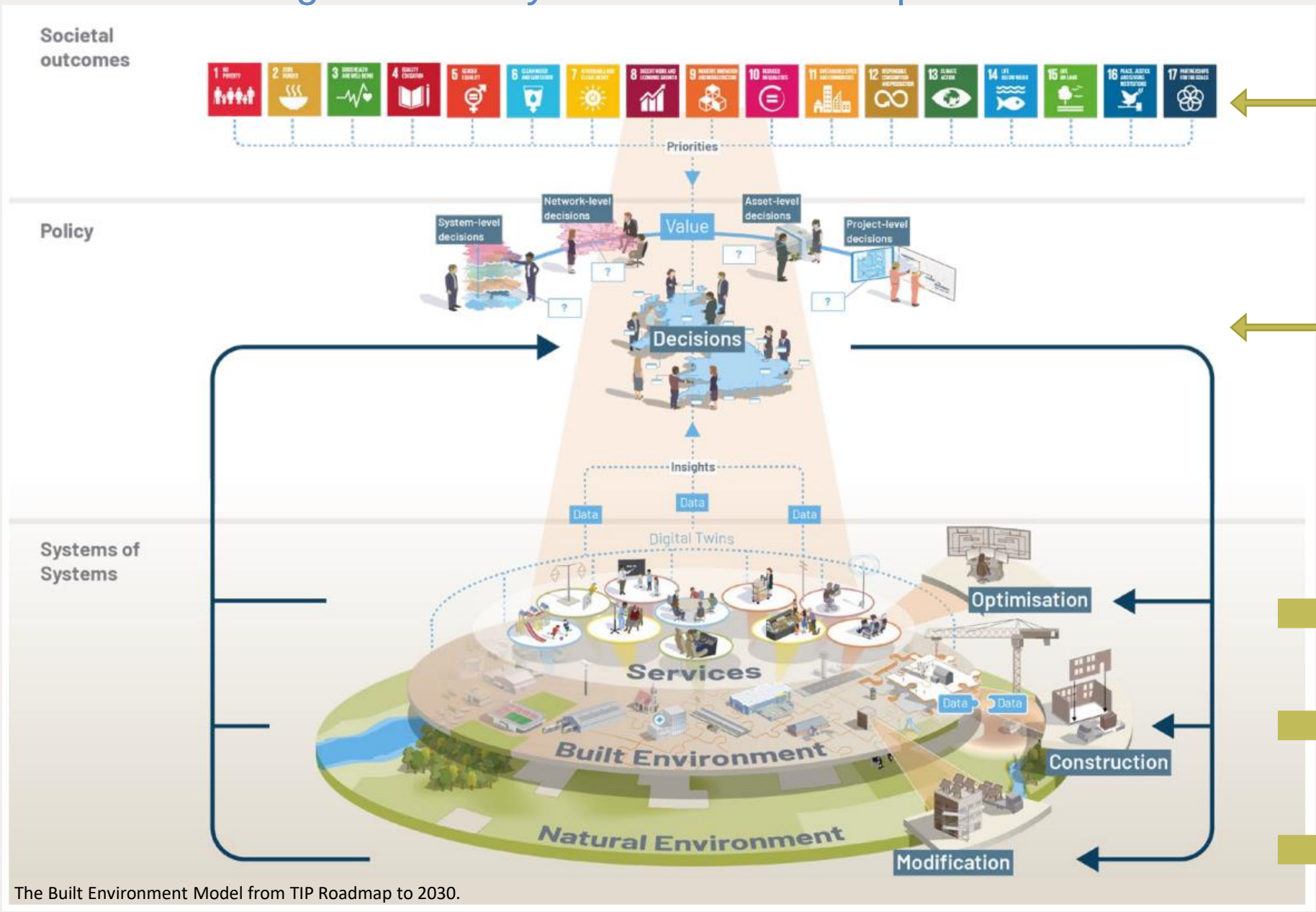
In addition to IMPACT:

- Step-by-step guidance on implementing an information management platform.
- A case study of the Environment Agency's modular technology approach.
- Contract clauses to support the procurement of interoperable information.
- Glossary – to increase understanding and drive consistency.



Information Management Platform:

enabling the delivery of the TIP roadmap to 2030



The Built Environment Model from TIP Roadmap to 2030.

Social outcomes

Value

Decisions

Insight

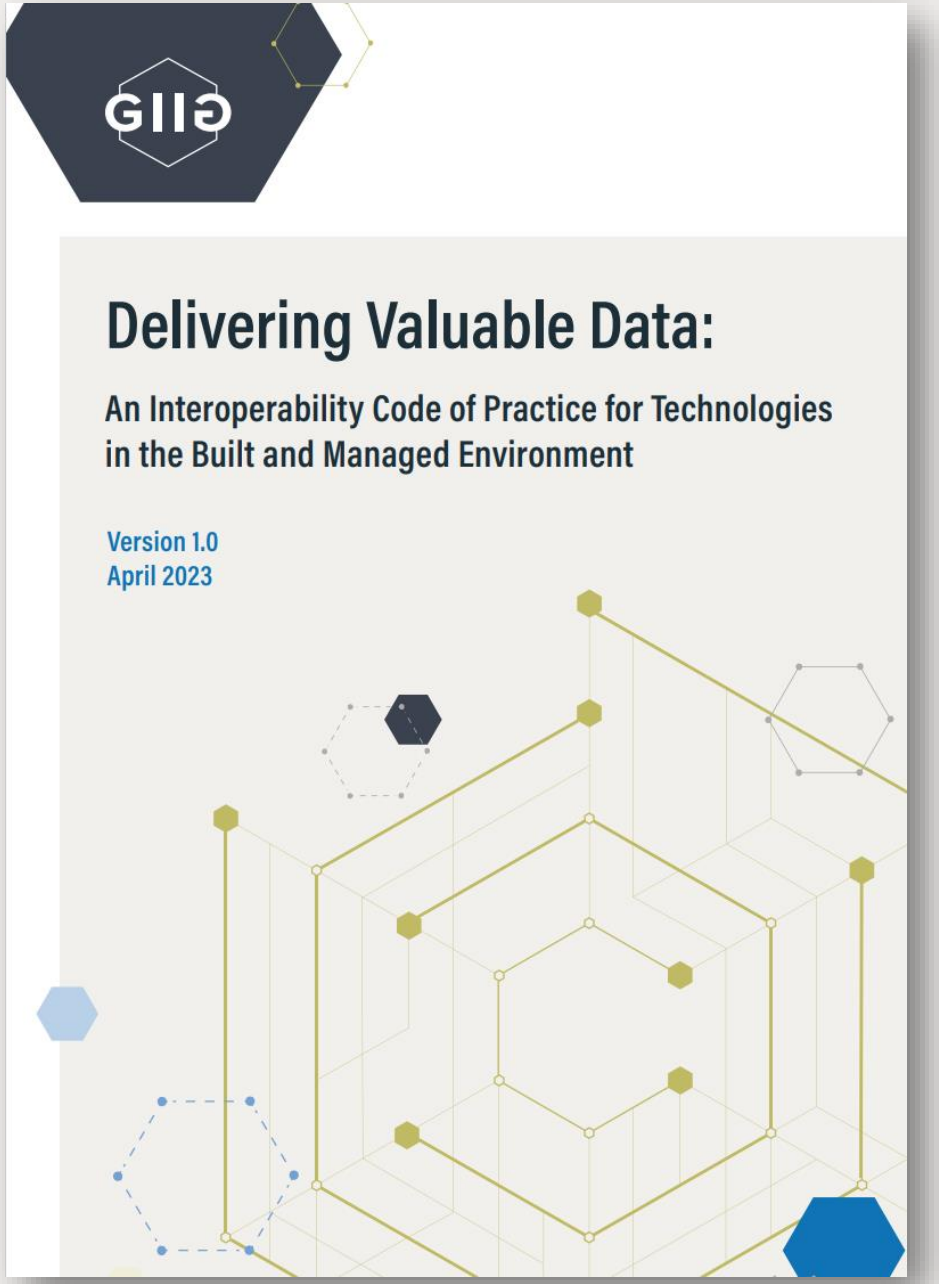
Data

Client Information Management Platform

Delivering Valuable Data

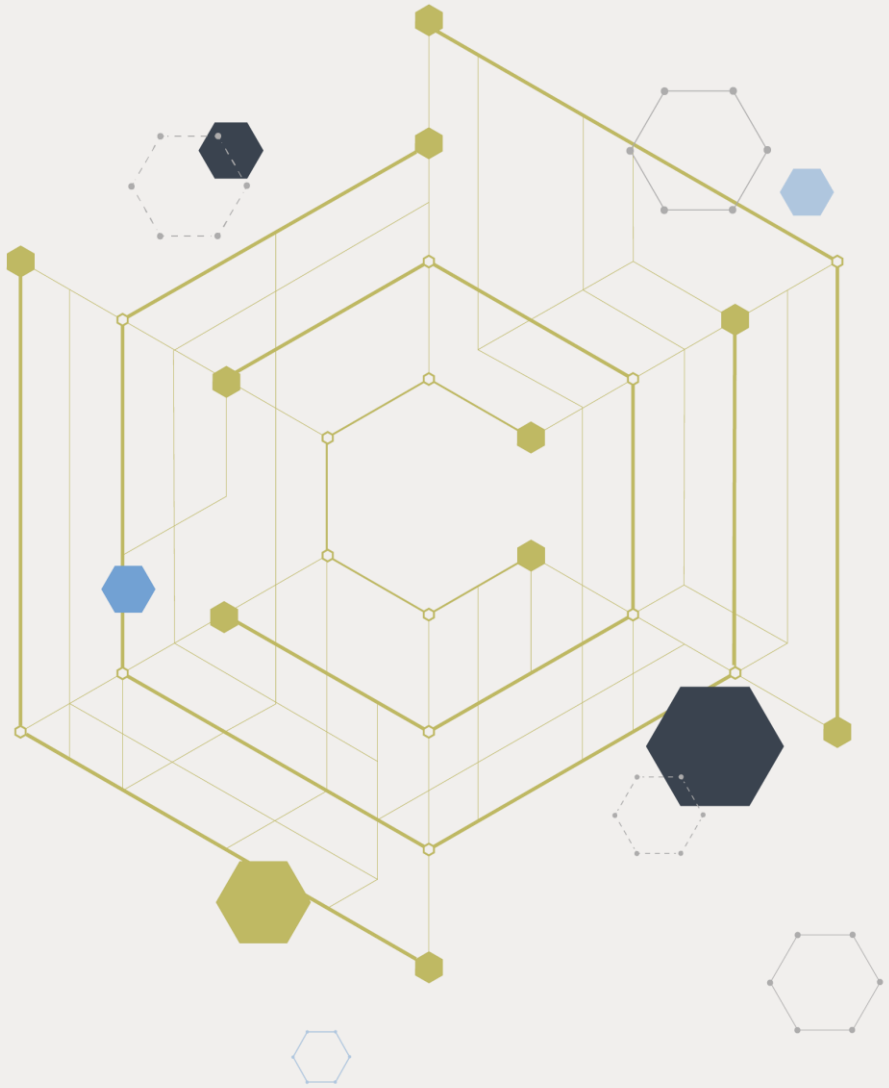
An Interoperability Code of Practice for Technologies in the Built and Managed Environment

April 2023


GIIG
Delivering Valuable Data:
An Interoperability Code of Practice for Technologies in the Built and Managed Environment
Version 1.0
April 2023

The Interoperability Code of Practice for Technologies

Paul Wilkinson



Delivering Valuable Data

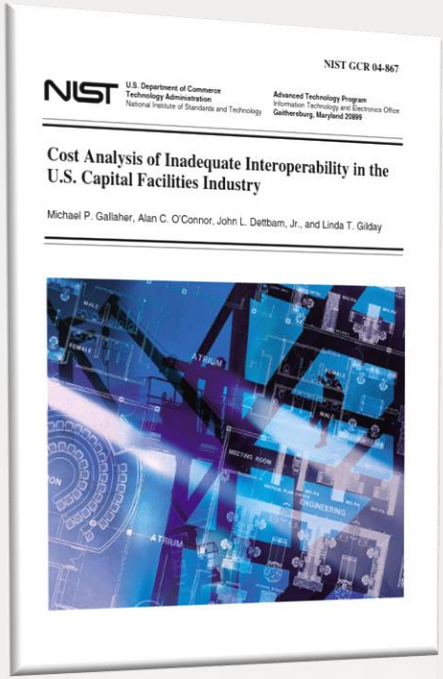
An Interoperability Code of Practice for Technologies in the Built and Managed Environment

Paul Wilkinson, chair of CoP working group

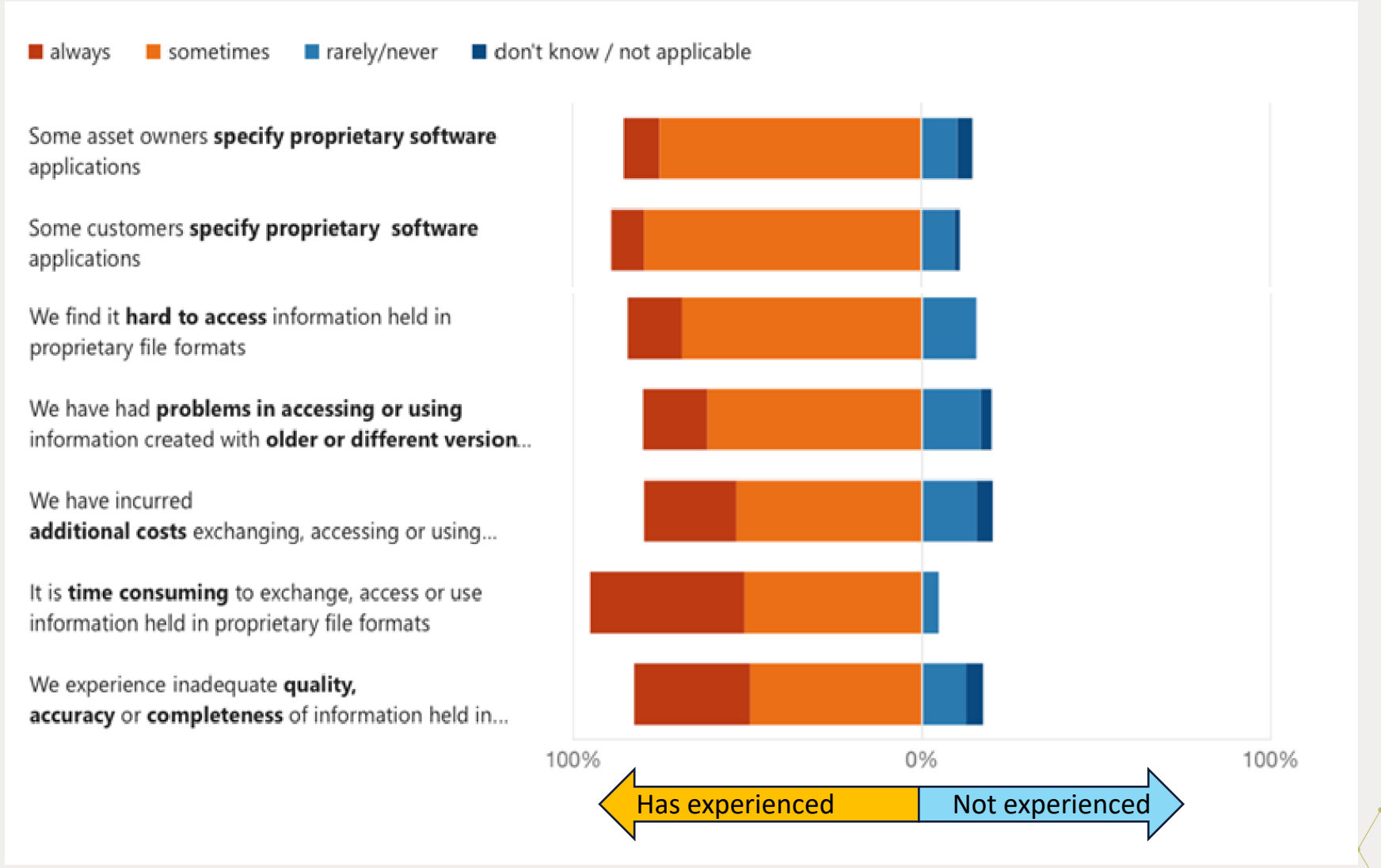
Why poor interoperability is a problem

Inadequate interoperability recognised as inhibiting industry performance since 1990s

- 2002 NIST analysis conservatively estimated annual cost of inadequate interoperability at **$15 billion *per annum*** *(2002 UK estimate £1bn/yr)*
- 2007 US survey: poor interoperability added:
  - over 3% to project costs
  - 3% to project schedules
- In UK, NAO: “managing inconsistent and poor-quality data … can take 60% to 80% of some civil servants’ time.”



2022 survey: interoperability issues



Objective

"To achieve '**greater sharing of better data**' and **deliver better whole life outcomes** in line with UK construction strategy, by developing a voluntary industry code of practice (and supporting mechanisms) for technologies to improve interoperability …"

British Standards definition: "A code of practice contains **recommendations and supporting guidance**, where the recommendations relevant to a given user have to be met in order to support a claim of **compliance**. …. Depending on the context and field of application, **a code of practice usually reflects current good practice as employed by competent and conscientious practitioners**." *(emphasis added)*

Primary audiences for CoP

- **technology providers** – developers of information management technologies and services used to create and provide information for industry users (and thus for asset owner/operators)
- **Asset owner/operators** – procurers of information, often also technology buyers and users
- **design, construction, facilities/asset management professionals** – technology buyers and users, with obligations to create and provide information to asset owner/operators

16 working group members

Andy Ward,
CEO, XBIM

Ben Wallbank,
BIM Strategy,
Viewpoint

Bruno Postle,
Diales Technical

John Egan, CEO,
BIMLauncher

Marek Suchoki,
Autodesk

Jack Seakins,
JLL Technologies

Paul Surin,
IBM

Simon McArthur,
Docuping

50% technology providers

David Bailey,
Group Property
Systems,
Manchester NHS

Fran Parkins,
Ministry of Justice

Patrick Owen,
Tideway

Bill Davis,
Ministry of Justice

25% owner/operators

Phil Thompson,
NG Bailey

Tom Oulton, Rider
Levett Bucknall

Andrew Krebs,
Digital Manager,
SWECO

Jo Harris,
Sodexo

25% supply chain

Context

Value Toolkit (v2.0, 2022)

TIP Roadmap to 2030 (2021)

Construction Playbook (2020, 2022)

UK BIM Framework (2019)

Construction Sector Deal (2018)

Building a Safer Future (2018)

Data for the Public Good (2017)

Transport Infrastructure Efficiency Strategy (2017)

Transforming Infrastructure Performance (2017)

Digital, Data and Technology Playbook (2022)

Guidance on knowledge asset management (2021)

UK Gov national data strategy (2020)

National geospatial strategy (2020)

CDDO Technology Code of Practice

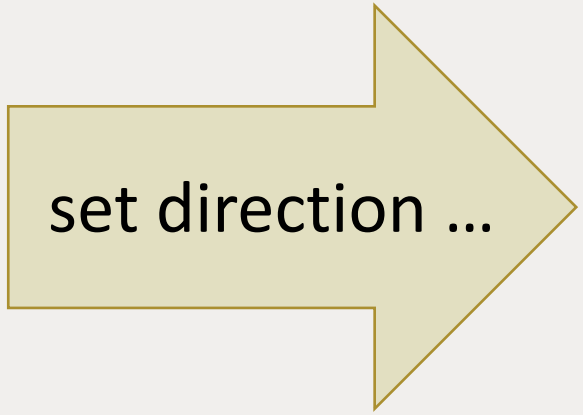
Open standards principles (2018)

UK Gov digital strategy (2017, 2022)

UK Gov industrial strategy (2017)

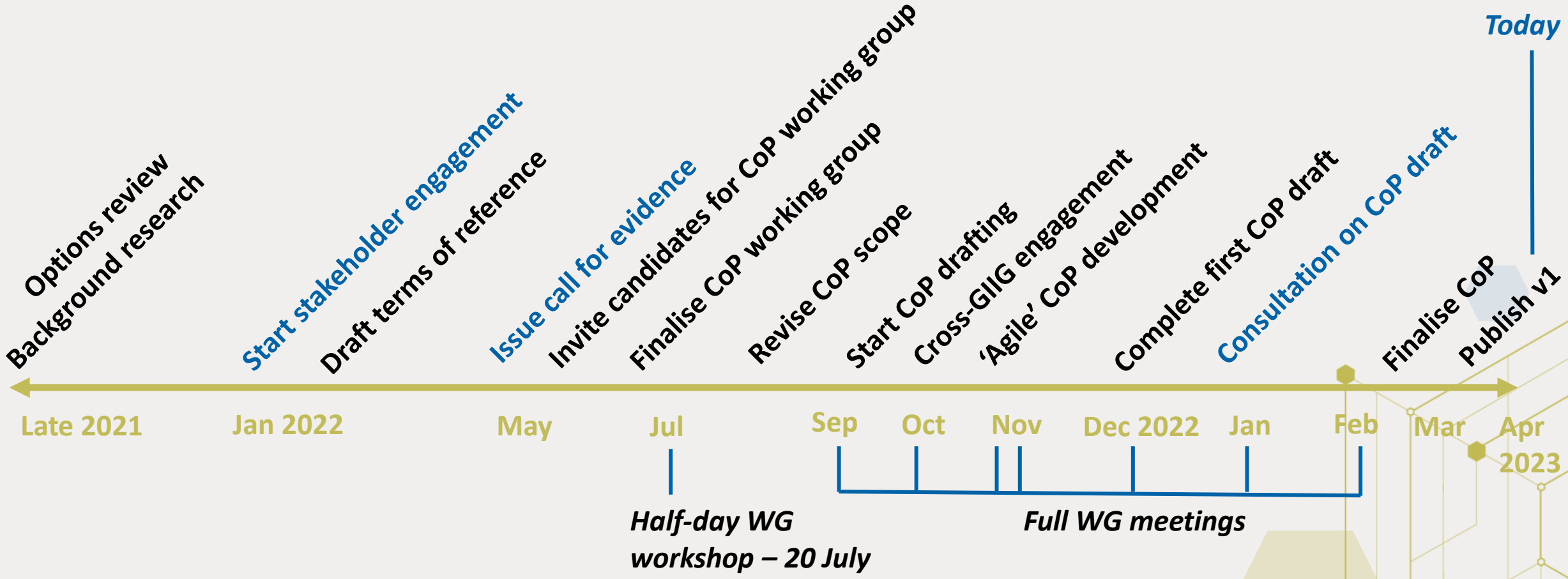
Context set Code of Practice direction

- Playbooks, TIP Roadmap
- UK BIM Framework
- CDDO Technology Code of Practice
- Data for the public good
- Open standards, APIs
- Client data control
- Avoiding vendor lock-in

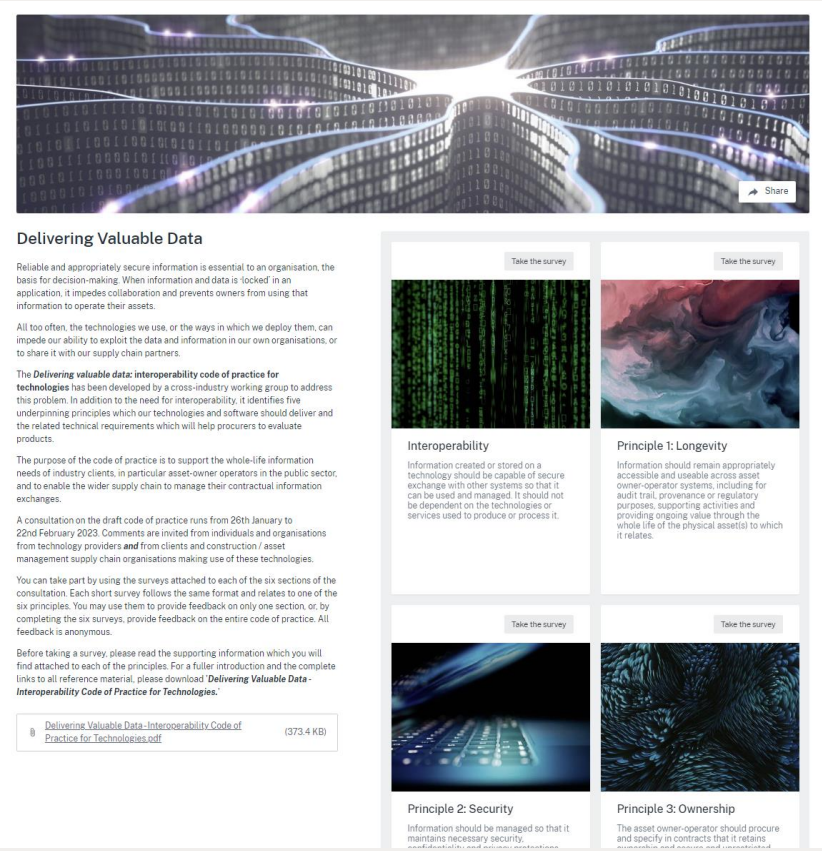


- **Interoperability**
- 5 underpinning principles:
  - **Longevity**
  - **Security**
  - **Data ownership**
  - **Value**
  - **Competition**

A consultative process



Draft Code of Practice: consultation



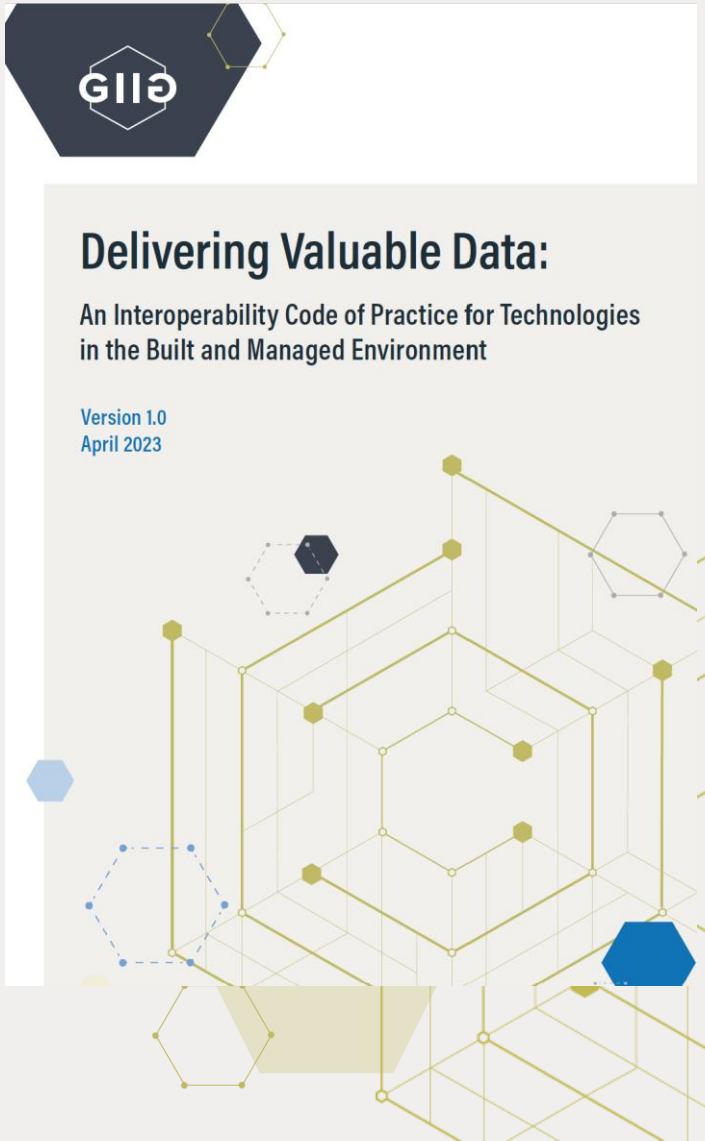
- four-week consultation period: 26 January – 22 February 2023
- draft Code of Practice available to download
- six online surveys
  (one per main section of the Code)
- **300+** participants, **117** comments, **94%** agreement with key need and principles, and strong support for technical requirements

Comments captured and reviewed

Of **117** written comments received and reviewed, a third resulted in changes incorporated in v1.0 of the Code

Example amendments raised by multiple respondents:

- Clarifications about long-term access to data (eg: for warranty, regulatory, PII purposes)
- Underline whole life use of data for ISO 19650-3 ‘trigger events’
- Emphasise security and ISO 19650-5 guidance, adding technical requirement for user access/permissions management
- Improve/clarify language on ‘open standards’



Interoperability

Information created or stored on a technology should be capable of secure exchange with other systems so that it can be used and managed.

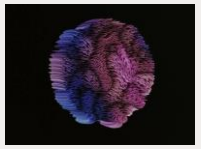
It should not be dependent on the technologies or services used to produce or process it.

Five underpinning principles

longevity – enabling long-term findability, access, reuse and exploitation, and continued value, of information

security – maintaining security, confidentiality and privacy protections, while allowing sharing of non-sensitive information for the public good

information value – enhancing the value of information created, managed and shared by technology-using professionals



information ownership – ensuring enduring ownership and control by asset owner-operators of valuable data about the assets they own

competition – promoting fair competition between technology providers (and indirectly among supply chain users of technologies)

Structure of core six sections of Code

1. Definition of principle
2. Brief explanation and context

3. What the principle means for technology providers

4. Related technical requirements

3 Interoperability

Information should be capable of secure exchange between two or more systems so that it can be used and managed. It should not be dependent on the technologies or services used to produce or process it.

This is the most important principle of the CoP, core to maintaining and maximising the value of information. Improving interoperability in the built and managed environment sector has been an objective of the UK Government since 2011.[7] It is a current requirement of UK construction strategy, particularly highlighted in the *TIP Roadmap* to 2030 and in the *Construction Playbook*. Both refer to the UK BIM Framework which, citing ISO 19650,[12] distinguishes between proprietary and open data (data available/visible to others and that can be freely used, re-used, re-published and redistributed by anyone). In this Code of Practice, the focus is on making data available in non-proprietary formats, or formats that are published as open standards.

Today, where a government department or agency is buying technology, the principle of interoperability is also covered in the *Government Functional Standard GovS 005: Digital, Data and Technology*,[14] the *Digital, Data and Technology Playbook* and the CDDO Technology Code of Practice. The *DDaT Playbook*'s key policies include adoption of non-proprietary data formats and use of interoperable data. It says: "The ability to exchange and share information and data between contracting authorities and suppliers and across government is key for long-term success. ...Operating in this consistent way will allow the interoperability between systems which fuels innovation."[15] Focusing on procurement of technologies, the *DDaT Playbook* stresses the need for interoperability:

> "Government's information assets, including data, should be able to be easily exchanged across platforms to make efficient use of the data we own. Contracting authorities should ensure that all contracts, including for commercial off-the-shelf (COTS) software, enable data extraction in a common format and IP and licencing requirements should be considered to ensure accessibility and transparency."[16]

The CDDO Technology Code of Practice Point 4, 'Make use of open standards,' urges use of open standards[17] technology so that it is easier to expand and upgrade, and to ensure it communicates with other technology.[18] The CDDO also advises Government buyers of technologies: "You should manage your data as an asset that is indopendont of any technology or service. This will involve using data standards to help you store your data so other government organisations can find and reuse it."[19] This will help Government to maximise the value of its collective information and reduce information value depreciation over time.

12

3.1 What the interoperability principle means for technology providers

Technology providers should ensure that their products or services support the exchange of non-proprietary information without loss, amendment, mis-interpretation or additional work for users, so that the integrity and value of information is not compromised.

While information will often be initially created and developed using proprietary software or services, when a supplier needs to exchange information with a contracting authority or other supplier, that information should be deliverable in an agreed non-proprietary form based on open FAIR principles,[20] so that it is also easily and immediately findable, accessible and reusable by the recipient. Recipients should not have to use a proprietary software to find, access or reuse information provided to them (this does not preclude the maintenance of records in both native and open forms where there is any uncertainty).

11 Government Construction Client Group, BIM Working Party Strategy Paper, *BIM: Management for value, cost and carbon improvement*, March 2011. "Government as a client can derive significant improvements in cost, value and carbon performance through the use of open shareable asset information."

12 ISO 19650-1, clause 5.1 states that information exchanges should be done using open standards wherever possible. This is also reiterated within ISO 19650-3, clause 5.1.5.

13 UK BIM Framework, ISO 19650 Guidance 9: Open data, building SMART and CoBie, v.1.0

14 *Government Functional Standard GovS 005: Digital, Data and Technology*, v.2 Principles: "When creating or providing and using digital services, government organisations and individuals shall ensure... [point 7] Digital and technology components are designed using mandatory government open standards where needed, and are adaptable, interoperable and shareable."

15 Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.4.

16 Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.6.

17 The *GOV.UK Open Standards Principles* (2018) defines an open standard as "A standard for which the specification or schema is publicly available, where the drafting and maintenance of the specification is open to all interested parties and is consensus-based, and where use of the resulting standard is royalty-free." This draws on a Cabinet Office Policy paper, *Open Standards principles* (updated 6 April 2018)

18 CDDO Technology Code of Practice, *Point 4: Make use of open standards*.

19 CDDO, *Manage your data for access and reuse*, (November 2020; see also CDDO advice in *Make better use of data*, updated March 2021.

20 As the UK's Geospatial Commission is developing a geospatial code of practice incorporating the FAIR principles (see *How FAIR are the UK's National geospatial data assets? Assessment of the UK's national geospatial data assets*), this Code of Practice has incorporated the FAIR approach. See also www.go-fair.org

13

3.2 Related technical requirements:

a. **Open standard formats and schemas** – Software should apply British or internationally recognised open standards for the rendering of common information in machine-readable formats – for example:

- ISO 8601:2004 for the presentation of dates and times
- World Geodetic System 1984 (WGS84), European Terrestrial Reference System 1989 (ETRS89) and OSGB36 (Ordnance Survey of Great Britain 1936 Datum – used in many UK data sets) standards for consistent exchange of location point information
- GeoJSON format for encoding and exchanging location information
- UK GEMINI 2.3 for geographic metadata
- ISO 3166 for country codes
- BS 7666-2 for property and street identification in Great Britain through unique property reference numbers (UPRNs) and unique street reference numbers (USRNs)[21]
- ISO 16739-1:2018 - Open relational data schemas (inherently more persistent than proprietary files) such as IFC (Industry Foundation Classes) and specific use cases such as Construction Operation Building information exchange (COBie)
- ISO 12006-2 for classification (Uniclass)

b. **APIs (application programming interfaces)** – Machine-level access to asset-related information management systems should, for example, be via extendable scripted RESTful or GraphQL APIs. The *Digital, Data and Technology Playbook* says: "APIs [should] conform to Central Digital and Data Office API technical and data standards, satisfy the requirements of the Technology Code of Practice..., and [be] well documented."[22] It stipulates APIs "should be used to enable effective data sharing... in interoperable, reusable and open formats. ...This is also enabled by the use of open data standards rather than bespoke ones."[23] The CDDO guidance also:

- advocates the OpenAPI Specification as a standardised way of describing RESTful web APIs. OpenAPI – specifically, OpenAPI version 3 – is recommended by the government Open Standards Board[24] to help government organisations be consistent in describing RESTful APIs, to generate accurate up-to-date API reference documentation, and to validate, version, maintain and update generated documentation
- provides guidance on good practice to follow in designing, building, hosting and operating secure APIs, including provision of i) data level security (ensuring users only have access to data they are authorised to see) and ii) application level security (ensuring only authorised users can access the API)

Also in relation to APIs, see ISO/IEC 20802-1:2016 - the Open Data Protocol (OData, an open protocol that allows the creation and consumption of queryable and interoperable REST APIs in a simple, standard way) and ISO/IEC 20802-2:2016 - the OData JSON format.[25]

Note: This section on the CoP's principle of interoperability should be read in conjunction with the following section.

14

Technical requirement | principles	Interoperability	Longevity	Security	Information ownership	Information value	Competition
Open standard formats and schemas	☑	☑			☑	☑
Open APIs	☑		☑		☑	☑
Immutability		☑				
Metadata		☑				
Workflow		☑				
Identity		☑				
Timestamps		☑				
Versioning		☑				
Provenance		☑				
Backward compatibility		☑				☑
Information segregation/ federation		☑	☑		☑	☑
Security certification			☑		☑	
Authorisation			☑		☑	
Authentication			☑		☑	
Access user interface			☑		☑	
Data residency/ sovereignty			☑	☑	☑	
Ownership & licensing				☑		
Data exploitation				☑		
Information transfer (returnability)				☑		
Non-retention				☑		

s.3: Interoperability

… the focus is on making data available in non-proprietary formats, or formats that are published as open standards …

Technology providers should…

… ensure that their products or services support the exchange of non-proprietary information without loss, amendment, mis-interpretation or additional work for users, so that the integrity and value of information is not compromised.

Related technical requirements (2):

- **Open standard formats and schemas** - eg: standard date/time, location information, open relational data schemas (eg: IFC) and use cases (eg: COBie)
- **APIs** “should be used to enable effective data sharing... in interoperable, reusable and open formats” (DD&T Playbook); recommends OpenAPI Specification (v3) as a standardised way of describing RESTful web APIs

3 Interoperability

Information should be capable of secure exchange between two or more systems so that it can be used and managed. It should not be dependent on the technologies or services used to produce or process it.

This is the most important principle of the CoP, core to maintaining and maximising the value of information. Improving interoperability in the built and managed environment sector has been an objective of the UK Government since 2011.[11] It is a current requirement of UK construction strategy, particularly highlighted in the *TIP Roadmap to 2030* and in the *Construction Playbook*. Both refer to the UK BIM Framework which, citing ISO 19650,[12] distinguishes between proprietary and open data (data available/visible to others and that can be freely used, re-used, re-published and redistributed by anyone). In this Code of Practice, the focus is on making data available in non-proprietary formats, or formats that are published as open standards.

Today, where a government department or agency is buying technology, the principle of interoperability is also covered in the *Government Functional Standard GovS 005: Digital, Data and Technology*,[14] the *Digital, Data and Technology Playbook* and the CDDO Technology Code of Practice. The *DDaT Playbook*'s key policies include adoption of non-proprietary data formats and use of interoperable data. It says “The ability to exchange and share information and data between contracting authorities and suppliers and across government is key for long-term success. ...Operating in this consistent way will allow the interoperability between systems which fuels innovation.”[15] Focusing on procurement of technologies, the *DDaT Playbook* stresses the need for interoperability:

“Government's information assets, including data, should be able to be easily exchanged across platforms to make efficient use of the data we own. Contracting authorities should ensure that all contracts, including for commercial off-the-shelf (COTS) software, enable data extraction in a common format and IP and licencing requirements should be considered to ensure accessibility and transparency.”[16]

The CDDO Technology Code of Practice Point 4, 'Make use of open standards', urges use of open standards[17] technology so that it is easier to expand and upgrade, and to ensure it communicates with other technology.[18] The CDDO also advises Government buyers of technologies: “You should manage your data as an asset that is independent of any technology or service. This will involve using data standards to help you store your data so other government organisations can find and reuse it.”[19] This will help Government to maximise the value of its collective information and reduce information value depreciation over time.

12

s.4.1: Longevity

Interoperability is not a short-lived or temporary requirement, nor is it solely related to asset delivery or operational activities….

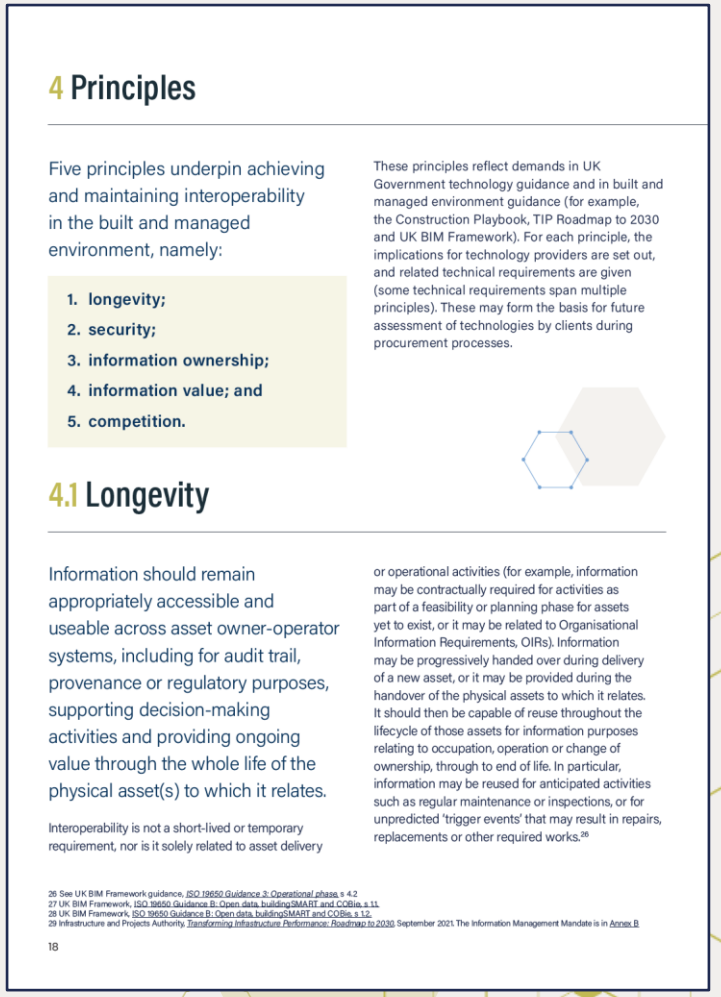
Informed by IMP requirements: assured, trusted, reliable information

Technology providers should …

… ensure that their products or services support the continued findability, accessibility, interoperability and reusability of information – including for audit trail, provenance or regulatory purposes – throughout the lifecycle(s) of the asset(s) to which it relates.

Related technical requirements (10):

- Open standard formats and schemas
- Immutability
- Metadata
- Workflow
- Identity
- Timestamps
- Versioning
- Provenance
- Backward compatibility
- Information segregation/ federation



4 Principles

Five principles underpin achieving and maintaining interoperability in the built and managed environment, namely:

1. **longevity;**
2. **security;**
3. **information ownership;**
4. **information value; and**
5. **competition.**

These principles reflect demands in UK Government technology guidance and in built and managed environment guidance (for example, the Construction Playbook, TIP Roadmap to 2030 and UK BIM Framework). For each principle, the implications for technology providers are set out, and related technical requirements are given (some technical requirements span multiple principles). These may form the basis for future assessment of technologies by clients during procurement processes.

4.1 Longevity

Information should remain appropriately accessible and useable across asset owner-operator systems, including for audit trail, provenance or regulatory purposes, supporting decision-making activities and providing ongoing value through the whole life of the physical asset(s) to which it relates.

Interoperability is not a short-lived or temporary requirement, nor is it solely related to asset delivery or operational activities (for example, information may be contractually required for activities as part of a feasibility or planning phase for assets yet to exist, or it may be related to Organisational Information Requirements, OIRs). Information may be progressively handed over during delivery of a new asset, or it may be provided during the handover of the physical assets to which it relates. It should then be capable of reuse throughout the lifecycle of those assets for information purposes relating to occupation, operation or change of ownership, through to end of life. In particular, information may be reused for anticipated activities such as regular maintenance or inspections, or for unpredicted 'trigger events' that may result in repairs, replacements or other required works.[26]

26 See UK BIM Framework guidance, *ISO 19650 Guidance 3: Operational phase*, s 4.2
27 UK BIM Framework, ISO 19650 Guidance B: Open data, buildingSMART and COBie, s 11.
28 UK BIM Framework, ISO 19650 Guidance B: Open data, buildingSMART and COBie, s 1.2.
29 Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. The Information Management Mandate is in Annex B

18

s.4.2: Security

Information should be managed so that it maintains necessary security, confidentiality and privacy protections while maximising opportunities for appropriate sharing of non-sensitive information for the public good.

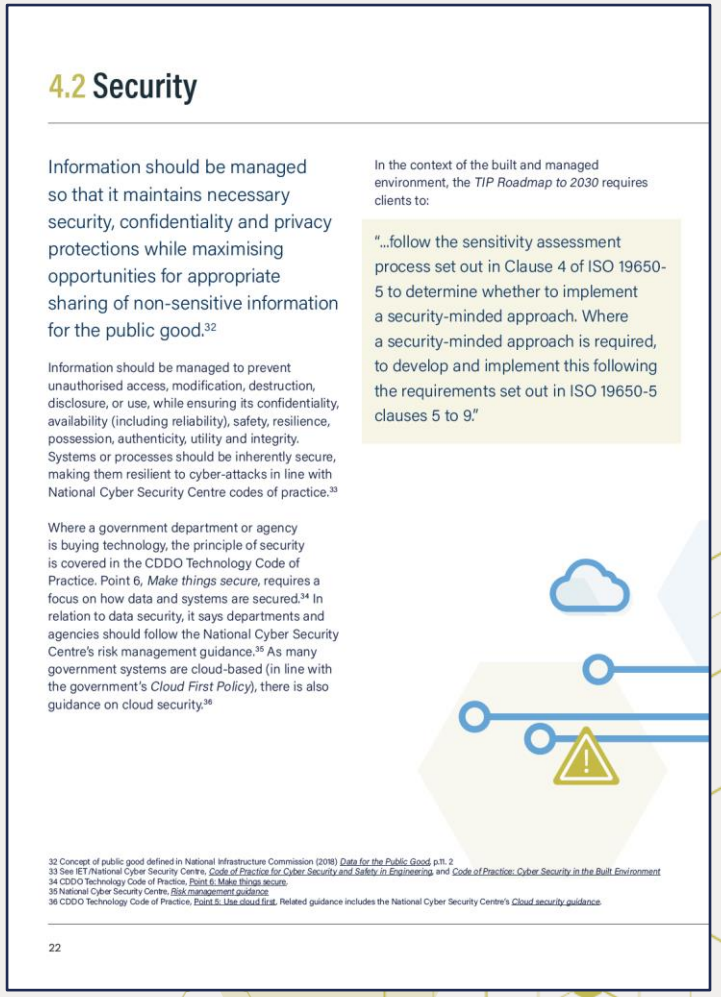
Technology providers should ...

… support a risk-based holistic approach addressing people, process, physical and technical security aspects in response to a documented risk assessment.

… adhere to advice from National Cyber Security Centre and National Protective Security Authority (formerly CPNI)

Related technical requirements (7)

- Security certification
- Authorisation
- Authentication
- User rights / permission management
- Access: UI
- APIs (security)
- Information segregation / federation



4.2 Security

Information should be managed so that it maintains necessary security, confidentiality and privacy protections while maximising opportunities for appropriate sharing of non-sensitive information for the public good.[32]

Information should be managed to prevent unauthorised access, modification, destruction, disclosure, or use, while ensuring its confidentiality, availability (including reliability), safety, resilience, possession, authenticity, utility and integrity. Systems or processes should be inherently secure, making them resilient to cyber-attacks in line with National Cyber Security Centre codes of practice.[33]

Where a government department or agency is buying technology, the principle of security is covered in the CDDO Technology Code of Practice. Point 6, *Make things secure*, requires a focus on how data and systems are secured.[34] In relation to data security, it says departments and agencies should follow the National Cyber Security Centre's risk management guidance.[35] As many government systems are cloud-based (in line with the government's *Cloud First Policy*), there is also guidance on cloud security.[36]

In the context of the built and managed environment, the *TIP Roadmap to 2030* requires clients to:

"...follow the sensitivity assessment process set out in Clause 4 of ISO 19650-5 to determine whether to implement a security-minded approach. Where a security-minded approach is required, to develop and implement this following the requirements set out in ISO 19650-5 clauses 5 to 9."

32 Concept of public good defined in National Infrastructure Commission (2018) *Data for the Public Good*, p.11. 2
33 See IET/National Cyber Security Centre, *Code of Practice for Cyber Security and Safety in Engineering*, and *Code of Practice: Cyber Security in the Built Environment*
34 CDDO Technology Code of Practice, Point 6: Make things secure.
35 National Cyber Security Centre, *Risk management guidance*
36 CDDO Technology Code of Practice, Point 5: Use cloud first. Related guidance includes the National Cyber Security Centre's *Cloud security guidance*

22

s.4.3: Information ownership

The asset owner-operator should procure and specify in contracts that it retains ownership and secures unrestricted direct control over its asset data for as long as required to satisfy asset lifecycle, portfolio or organisational information requirements.

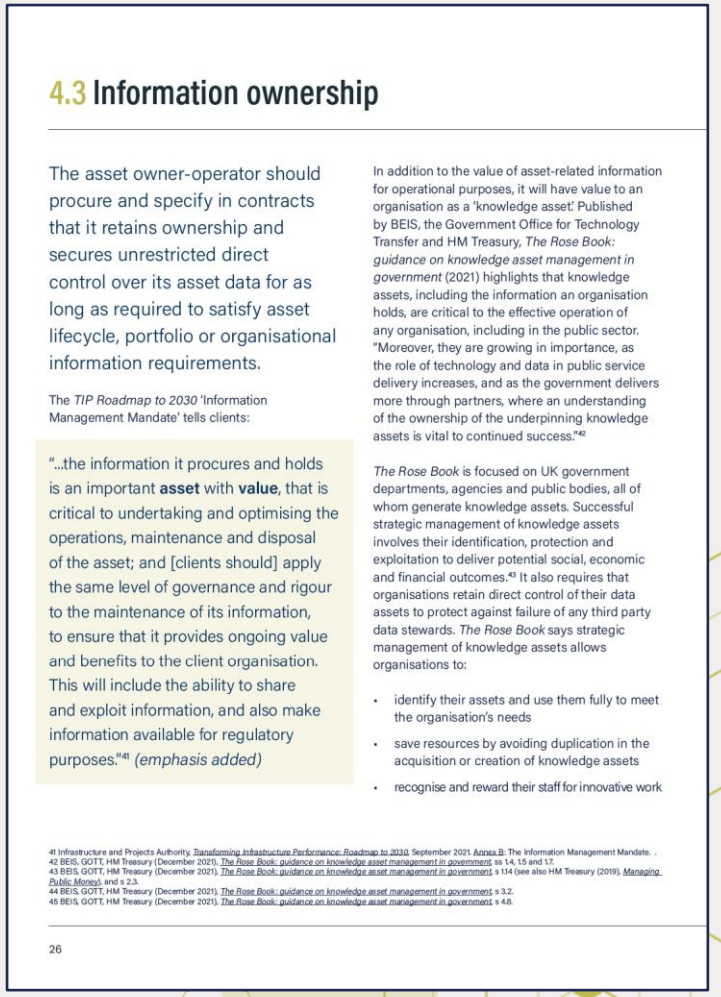
In addition to the value of asset-related information for operational purposes, it will have value to an organisation as a ‘knowledge asset’. *The Rose Book* also requires that organisations retain direct control of their data assets to protect against failure of any third party data steward.

Technology providers should …

… ensure that their products or services help asset owner-operators to assert and secure unrestricted ownership and control of their asset-related information.

Related technical requirements (5):

- Ownership and licensing
- Data residency / sovereignty
- Data exploitation
- Information transfer (returnability)
- Non-retention



4.3 Information ownership

The asset owner-operator should procure and specify in contracts that it retains ownership and secures unrestricted direct control over its asset data for as long as required to satisfy asset lifecycle, portfolio or organisational information requirements.

The *TIP Roadmap to 2030* ‘Information Management Mandate’ tells clients:

“…the information it procures and holds is an important **asset** with **value**, that is critical to undertaking and optimising the operations, maintenance and disposal of the asset; and [clients should] apply the same level of governance and rigour to the maintenance of its information, to ensure that it provides ongoing value and benefits to the client organisation. This will include the ability to share and exploit information, and also make information available for regulatory purposes.”[41] *(emphasis added)*

In addition to the value of asset-related information for operational purposes, it will have value to an organisation as a ‘knowledge asset.’ Published by BEIS, the Government Office for Technology Transfer and HM Treasury, *The Rose Book: guidance on knowledge asset management in government* (2021) highlights that knowledge assets, including the information an organisation holds, are critical to the effective operation of any organisation, including in the public sector. “Moreover, they are growing in importance, as the role of technology and data in public service delivery increases, and as the government delivers more through partners, where an understanding of the ownership of the underpinning knowledge assets is vital to continued success.”[42]

The Rose Book is focused on UK government departments, agencies and public bodies, all of whom generate knowledge assets. Successful strategic management of knowledge assets involves their identification, protection and exploitation to deliver potential social, economic and financial outcomes.[43] It also requires that organisations retain direct control of their data assets to protect against failure of any third party data stewards. *The Rose Book* says strategic management of knowledge assets allows organisations to:

- identify their assets and use them fully to meet the organisation’s needs
- save resources by avoiding duplication in the acquisition or creation of knowledge assets
- recognise and reward their staff for innovative work

41 Infrastructure and Projects Authority, Transforming Infrastructure Performance: Roadmap to 2030, September 2021. Annex B: The Information Management Mandate. .
42 BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, ss 1.4, 1.5 and 1.7.
43 BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, s 1.14 (see also HM Treasury (2019), *Managing Public Money*), and s 2.3.
44 BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, s 3.2.
45 BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, s 4.8.

26

s.4.4: Information value

Information an asset owner-operator procures and holds should be regarded as an important asset with intrinsic long-term value. Information should be created, exchanged, (re)used and updated so that it can maximise value (and minimise depreciation) for the owner-operator. The value of information should be enhanced through appropriate sharing, collaboration and exploitation.

Technology providers should …

… (1) ensure they are able to help contracting authorities and their suppliers to maximise the value of the information deliverables that users create and exchange, and …

… (2) particularly when providing long-term information management ‘stewardship’ services to an asset owner-operator, support users in maintaining the value of that information

Related technical requirements (8):

- Open standard formats and schemas
- Security certification
- Authorisation
- Authentication
- User rights / permission management
- Access: UI
- APIs (security)
- Information segregation / federation

4.4 Information value

Information an asset owner-operator procures and holds should itself be regarded as an important asset with intrinsic long-term value. Information should be created, exchanged, (re)used and updated so that it can maximise value (and minimise depreciation) for the owner-operator. The value of information should be enhanced through appropriate sharing, collaboration and exploitation.

Ownership of asset-related information is closely related to how an organisation might recognise and exploit the value of the information it holds. As previously mentioned, the *TIP Roadmap to 2030* tells clients: "…the information it procures and holds is an important asset with value"[48] and *The Rose Book guidance* (see 4.3 above) underlines how that information might be identified, protected and exploited by an organisation to deliver potential social, economic and financial outcomes. There is also an additional opportunity to maximise value during the delivery phase of built or managed assets, in the creation of asset information.

The Rose Book specifically mentions the need to minimise the cost of capturing and processing information, talking of opportunities to "save resources by avoiding duplication in the acquisition or creation of knowledge assets".

Any system or service should, as far as possible, reduce friction in the processes of acquiring, managing and delivering required information and maintaining its value and provenance.

Efficient development of knowledge assets is not possible if planning, design and construction information deliverables cannot be easily exchanged and reused between the software applications used by different organisations or disciplines. For example, imperfect or unreliable export/import processes, or the re-creation of the same information in different proprietary formats, is inefficient. 'Lean construction' processes, by contrast, streamline value-adding activities; they look to enable access to the right information in the right format by the right person at the right time and on their chosen device. This eliminates wasteful processes – for example, initial creation and/or correction of defective information, delivering too much information (too early), waiting for delayed information, additional processing/translation of information, needless dissemination and/or duplication of information, etc. Appropriate agreed lean construction processes should be recorded in the contractual agreement between the parties to facilitate this approach.

48 Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. Annex B: The Information Management Mandate.

30

s.4.5: Competition

Information practices should enable fair competition – between the technology providers whose tools enable the creation, exchange and management of information, and amongst users of the tools (eg: supply chain businesses involved in planning, design, delivery, operation, repair and maintenance, and management of assets).

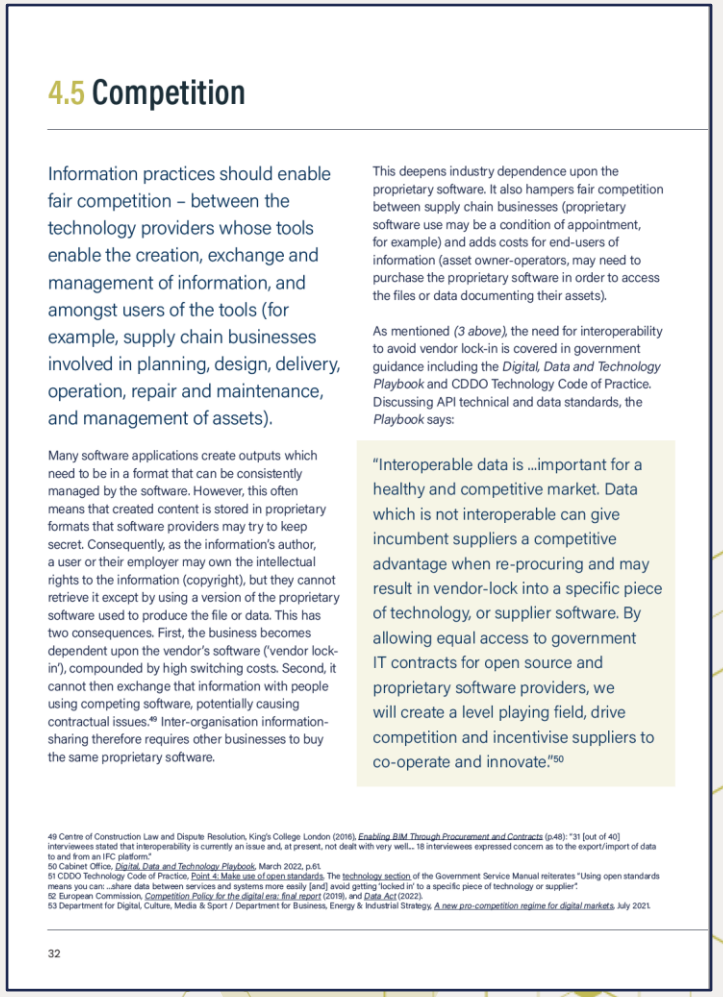
Interoperable data is ... important for a healthy and competitive market.

Technology providers should …

… ensure that their products or services support non-proprietary exchanges of information between contracting authorities and their suppliers, and between suppliers.

Related technical requirements (4):

- Open standard formats and schemas
- APIs
- Backwards compatibility
- Information segregation / federation



4.5 Competition

Information practices should enable fair competition – between the technology providers whose tools enable the creation, exchange and management of information, and amongst users of the tools (for example, supply chain businesses involved in planning, design, delivery, operation, repair and maintenance, and management of assets).

Many software applications create outputs which need to be in a format that can be consistently managed by the software. However, this often means that created content is stored in proprietary formats that software providers may try to keep secret. Consequently, as the information's author, a user or their employer may own the intellectual rights to the information (copyright), but they cannot retrieve it except by using a version of the proprietary software used to produce the file or data. This has two consequences. First, the business becomes dependent upon the vendor's software ('vendor lock-in'), compounded by high switching costs. Second, it cannot then exchange that information with people using competing software, potentially causing contractual issues.[49] Inter-organisation information-sharing therefore requires other businesses to buy the same proprietary software.

This deepens industry dependence upon the proprietary software. It also hampers fair competition between supply chain businesses (proprietary software use may be a condition of appointment, for example) and adds costs for end-users of information (asset owner-operators, may need to purchase the proprietary software in order to access the files or data documenting their assets).

As mentioned *(3 above)*, the need for interoperability to avoid vendor lock-in is covered in government guidance including the *Digital, Data and Technology Playbook* and CDDO Technology Code of Practice. Discussing API technical and data standards, the *Playbook* says:

"Interoperable data is ...important for a healthy and competitive market. Data which is not interoperable can give incumbent suppliers a competitive advantage when re-procuring and may result in vendor-lock into a specific piece of technology, or supplier software. By allowing equal access to government IT contracts for open source and proprietary software providers, we will create a level playing field, drive competition and incentivise suppliers to co-operate and innovate."[50]

49 Centre of Construction Law and Dispute Resolution, King's College London (2016), *Enabling BIM Through Procurement and Contracts* (p.48): "31 [out of 40] interviewees stated that interoperability is currently an issue and, at present, not dealt with very well... 18 interviewees expressed concern as to the export/import of data to and from an IFC platform."
50 Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.61.
51 CDDO Technology Code of Practice, Point 4: Make use of open standards. The technology section of the Government Service Manual reiterates "Using open standards means you can: ...share data between services and systems more easily [and] avoid getting 'locked in' to a specific piece of technology or supplier".
52 European Commission, *Competition Policy for the digital era: final report* (2019), and *Data Act* (2022).
53 Department for Digital, Culture, Media & Sport / Department for Business, Energy & Industrial Strategy, *A new pro-competition regime for digital markets*, July 2021.

32

Reaction / impact to date

- Very positive sentiment in comments received via public consultation platform
- Launch of Code public consultation covered in *BIM Plus* (27 January), and supported in opinion piece from technology provider (21 February)
- Question about the Code to be included in s.10 of BuildUK Common Assessment Standard
- Potential international application of Code approach (BuildingSMART Int'l)

Bridging the interoperability gap – a ***BIM Plus*** opinion piece by a contributor to the CoP consultation

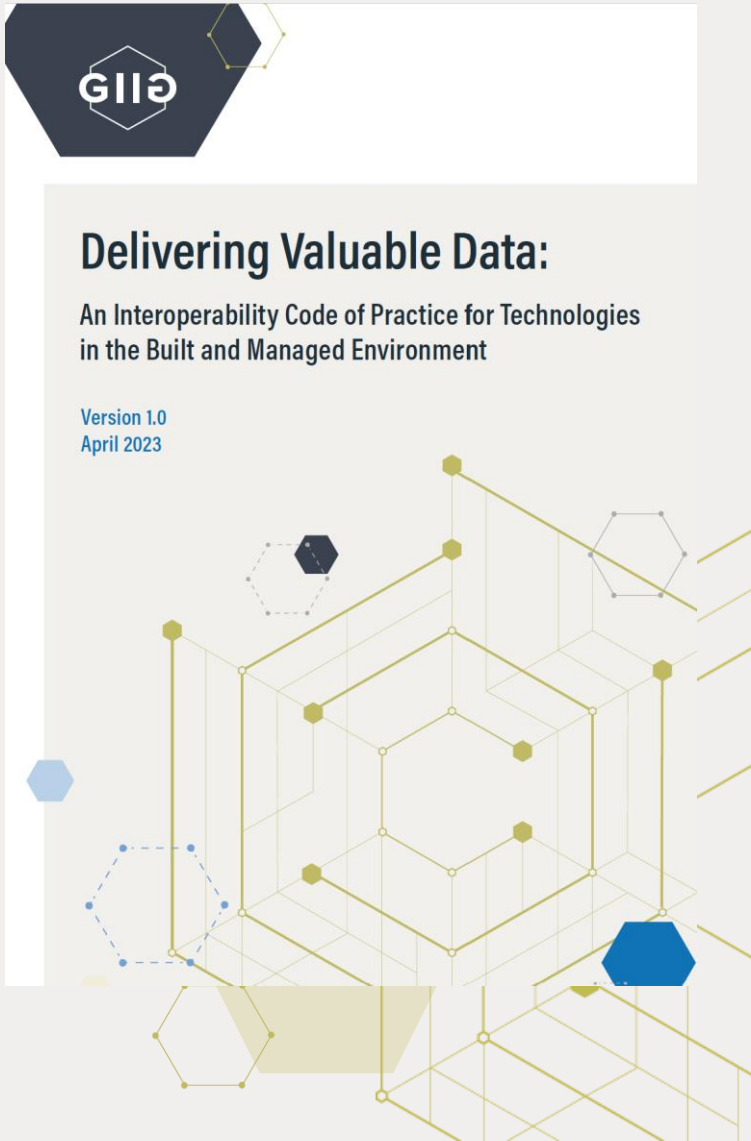
An affirmative step

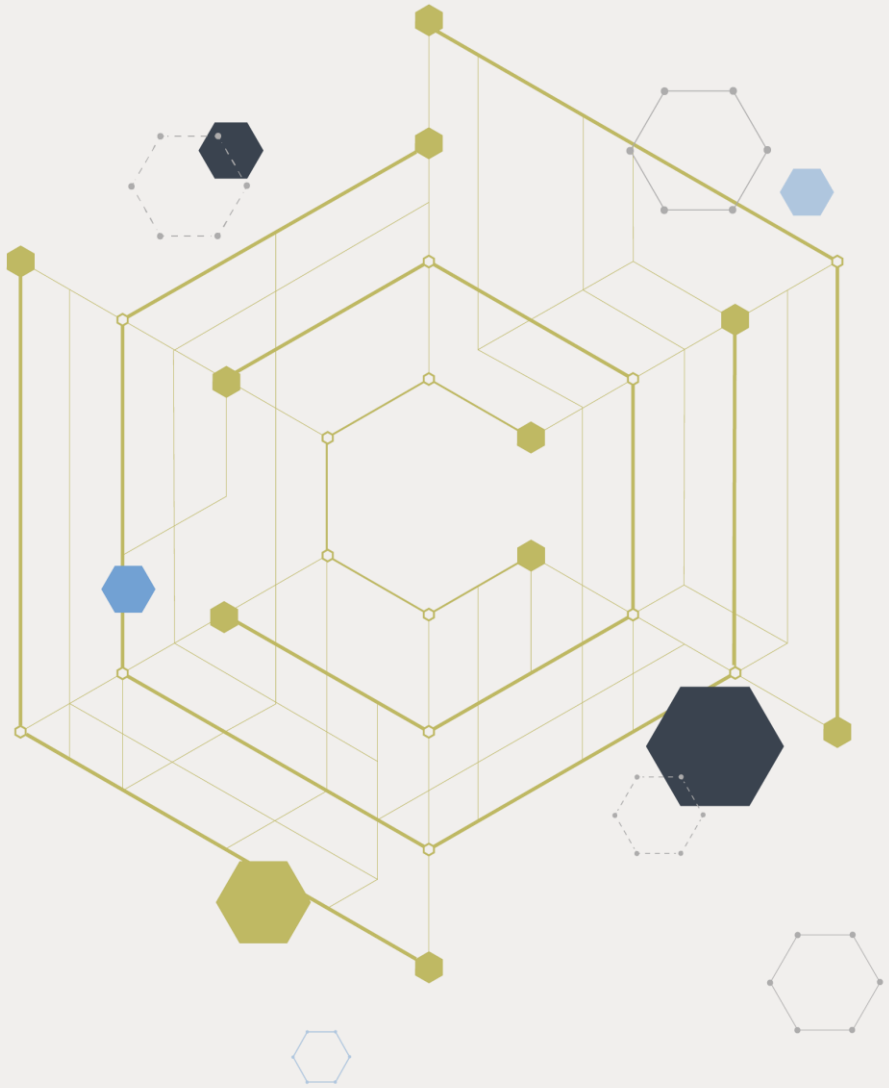
A code of practice is an affirmative step for industry resilience, and an important missing piece of the puzzle on the government's Transforming Industry Performance roadmap 2030.

John Ryan
CEO and co-founder, SymTerra
21.02.23

The end of the beginning… next steps

- Expand awareness of Code (v 1.0) beyond industry launch
- Provide mechanisms for sign-up to, and support for, the Code, including by procurers
- Establish self-sustaining industry ‘stewardship’ of the Code to …
  - … capture experience and industry feedback on Code adoption, including for procurement
  - … develop ‘bronze, silver, gold’ assessment
  - … develop Code version 1.1, and
  - … explore international dimension
- Further communications to follow ….





Delivering Valuable Data

An interoperability code of practice for technologies in the built and managed environment

Download from:
https://www.ukbimframework.org/giig/

A supply-chain / technology-user perspective

Terry Stocks

FAITHFUL + GOULD

Member of the SNC-Lavalin Group

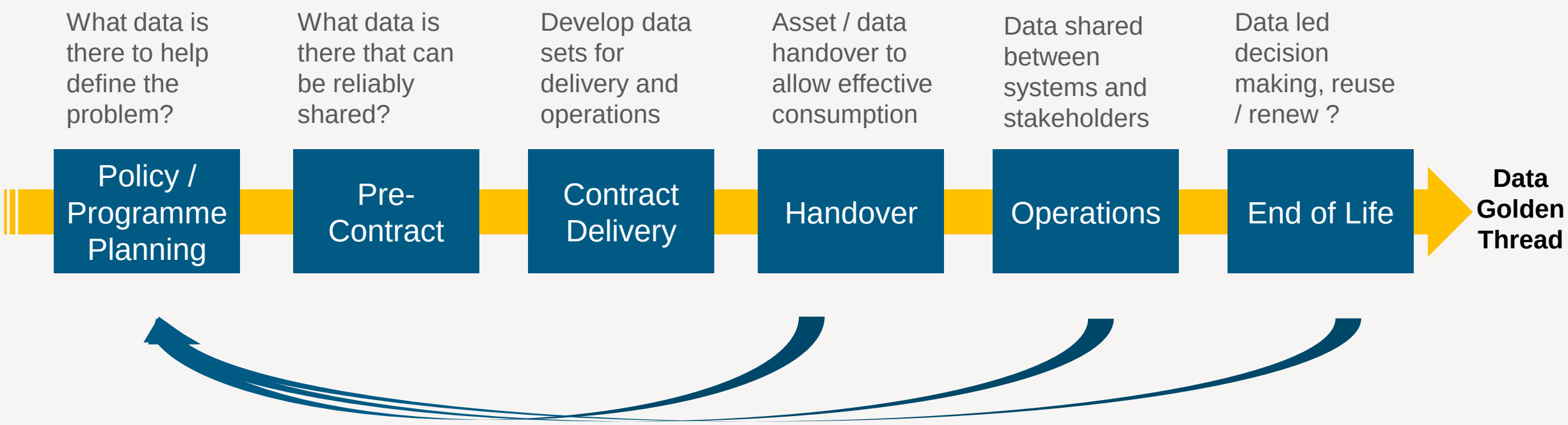
GIIG – Interoperability Code of Practice Launch

Terry Stocks MBE

Faithful + Gould

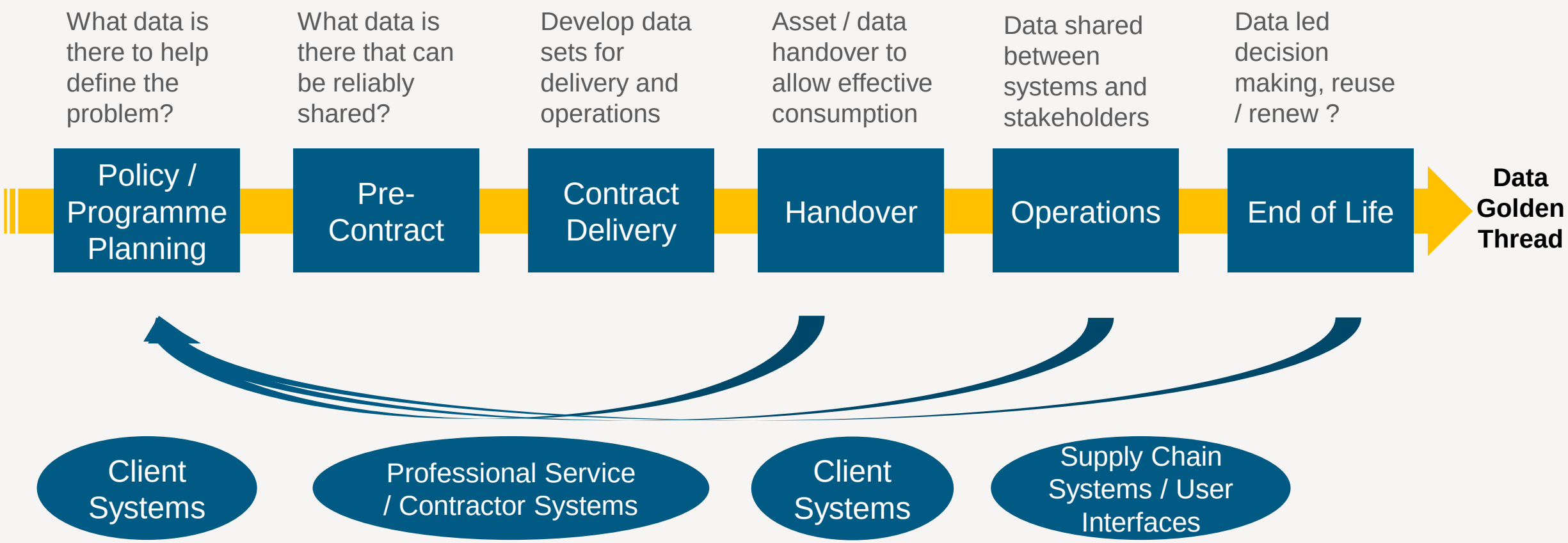
UK and Europe Director of Property

Who Needs Data ?



There is a potential for waste at every interface!

We All Need Data !



There is a potential for waste at every interface!

FAITHFUL+GOULD
Member of the SNC-Lavalin Group

So Why Interoperability ?

- Buying data once and using it lots of times has been an Information Management ‘mantra’ for some time!

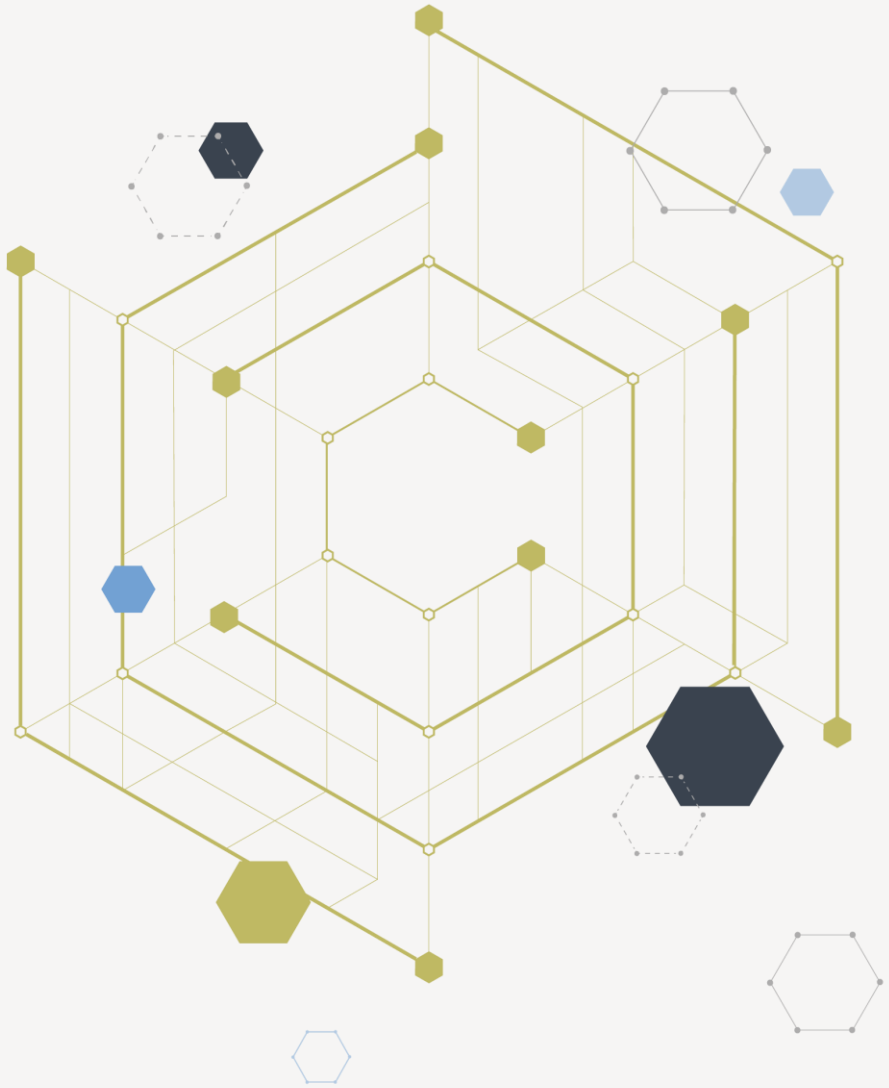
  Perhaps it should be -

- Buying ‘Data Once’ and using it lots of times ***on the systems we choose!***

The current landscape forces major investment and can be a barrier to effective Information Management adoption and practice

Software providers working together to enable real ‘interoperability’ would help unlock effective data sharing, improved end to end asset data management and planning

The Code of Practice for Interoperable Data is therefore a key document in delivering improved UK asset management delivery, performance and policy alignment.



Delivering Valuable Data

An interoperability code of practice for technologies in the built and managed environment

Download from:
https://www.ukbimframework.org/giig/

FAITHFUL+GOULD
Member of the SNC-Lavalin Group