PAS 186:2020

Smart cities – Supplying data products and services for smart communities – Code of practice

中國建築

HBSQI

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2020.

ISBN 978 0 539 00421 2

ICS 13.020.20

Publication history

First published December 2020

Contents

Foreword ii

Introduction iv

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Product and service recommendations (A) 4

5 People and process recommendations (B) 20

6 Compliance 28

Annexes

Annex A (informative) Illustrative compliance scorecards 29

Annex B (normative) Compliance levels for 4.5 (A5) 31

Bibliography 37

List of figures

Figure 1 – Overview of recommendations for smart communities suppliers vi

Figure 2 – Maturity model for smart community suppliers vi

List of tables

Table 1 – Key features of BS ISO 37106 smart community operating model v

Table 2 – Alignment with community vision – Compliance levels 4

Table 3 – Customer segmentation and insight – Compliance levels 6

Table 4 – Inclusivity – Compliance levels 8

Table 5 – Citizen-centric approach to privacy and identity management – Compliance levels 11

Table 6 – Integration between digital and physical assets – Compliance levels 15

Table 7 – Security and resilience – Compliance levels 18

Table 8 – Smart contracting – Compliance levels 21

Table 9 – Collaborative governance – Compliance levels 22

Table 10 – Skilled, empowered and integrated teams – Compliance levels 24

Table 11 – Agile delivery – Compliance levels 26

Table A1 – Illustrative scorecard for a compliant supplier 29

Table A2 – Illustrative scorecard for a non-compliant supplier 30

Table B1 – Clause 4.5 – Compliance levels 32

Table B2 – Clause 4.5 – Compliance levels – scoring 36

Foreword

This PAS was sponsored by CCTEB Intelligent Technology Co., Ltd., with funding from the Hubei Standardization and Quality Institute. Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 December 2020.

Acknowledgement is given to Chris Parker, CS Transform Limited, as the technical author, and the following organizations that were involved in the development of this PAS as members of the steering group:

- Atkins Global
- BSI Consumer & Public Interest Network
- Building Research Establishment
- CCTEB Intelligent Technology Co., Ltd.
- Central South Architectural Design Institute Co., Ltd.
- Connected Places Catapult
- CS Transform
- Electrical Contractors Association
- HIKVISION
- Huazhong University of Science and Technology
- Hubei Standardization and Quality Institute
- IBM UK Ltd.
- IOT/1, Internet of Things
- KnowNow Information Ltd.
- Local Government Association
- Thoughtworks
- Turner & Townsend
- University of Cambridge
- WSDRI Engineering and Research Incorporation Limited
- Wuhan Municipal Engineering Design & Research Institute. Co., Ltd

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a code of practice to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a code of practice, this PAS takes the form of guidance and recommendations. Particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

Relationship with other publications

This PAS is issued as part of a suite of BSI publications related to smart cities:

- PAS 180, *Smart cities – Vocabulary*, defines terms for smart cities, including smart cities concepts, across different infrastructure and systems elements and used across all service delivery channels (this PAS is in the process of being superseded by a new ISO standard based on its content);
- PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*, gives guidance for decision-makers from the public, private and third sectors on establishing a framework which can support the sharing of city data and the creation of interoperable information services (this PAS is in the process of being superseded by a new ISO standard based on its content);

- PAS 184, *Smart cities – Developing project proposals for delivering smart city solutions – Guide*, gives guidance on how good practice described in other BSI smart city publications can be applied when developing an individual project proposal within the broader smart city programme;
- PAS 185, *Smart cities – Specification for establishing and implementing a security-minded approach*, specifies requirements for establishing a framework for the security-minded management of smart cities and their associated infrastructure, as well as of data, information and services used to deliver city services;
- PD 8100, *Smart cities overview – Guide*, gives guidance on how to adopt and implement smart city products and services in order to facilitate the rapid development of an effective smart city;
- BS ISO 37106, *Sustainable cities and communities – Guidance on establishing smart city operating models for sustainable communities*, gives guidance on a good practice framework for decision-makers in smart cities and communities (from the public, private and voluntary sectors) to develop, agree and deliver smart city strategies that can transition their city's ability to meet future challenges and deliver future aspirations; and
- BS ISO/IEC 30182, *Smart city concept model – Guidance for establishing a model for data interoperability*, provides a framework that can normalize and classify information from many sources so that data sets can be discovered and combined to gain a better picture of the needs and behaviours of a city's citizens (residents and businesses).

The above documents are aimed primarily at leaders of local authorities. This PAS complements these publications by showing how suppliers of smart services and smart products can help support the delivery of smart cities, through the creation of data products and data services that are aligned with the good practice management approaches described in the existing BSI smart city publications.

Presentational conventions

The provisions of this code of practice are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

The word "should" is used to express recommendations of this PAS. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Where URLs for websites and webpages have been cited, they aim to provide ease of reference for the PAS user and are correct at the time of publication. The location of a webpage or website, or its contents cannot be guaranteed.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

Introduction

0.1 General

Smart communities require much more than just technology. Truly smart communities require citizen-centric and data-driven innovation – a new community operating model that cuts across organizational silos and sectoral barriers. The guiding principles for such a smart community operating model are set out in BS ISO 37106 (which supersedes PAS 181), with other documents in the BSI smart city publications giving more detail on specific elements – such as cross-silo data sharing (BS ISO/IEC 30182 and PAS 183), developing smart city projects and solutions (PAS 184), the implications for urban planning (PD 8100) and city security (PAS 185).

The above existing publications are aimed primarily at community authority leaders, making recommendations and requirements for actions to take to implement smarter ways of working across the community.

Implicitly, however, the BSI smart city publications also have significant consequences for the suppliers of smart services and smart products. This PAS makes these explicit, establishing recommendations for smart community suppliers at two levels:

- **Product:** recommendations for common specifications for data products and data services aimed at ensuring they have optimum impact on future development of the community; and
- **People and process:** good practice recommendations on how a smart community supplier engages with the community authority, covering the key roles, skills and business processes it deploys when developing, delivering and maintaining data products and data services.

This PAS is therefore a supplier-focused counterpart to the existing smart city publications. It aims to guide smart community suppliers of smart products and smart services during the implementation of smart city strategy by:

- helping to remove barriers for suppliers of data products and data services by defining a set of clear recommendations that help the design of products and services that meet city requirements;
- addressing market failures experienced by cities by ensuring data products and data services are not developed in isolation from solving real city problems and are based on a clear set of outcomes;
- addressing market concerns around ethics and security of smart city products and services, through embedding best practice in their design; and
- ensuring data products and services are developed in a citizen-centric and inclusive way.

0.2 Context

BS ISO 37106 brings together global good practice on how communities (and in particular cities) are moving towards a new “smart community operating model”, the key features of which are summarized in Table 1 below.

Table 1 – Key features of BS ISO 37106 smart community operating model

- **Investing in smart data**, i.e. ensuring that data on the performance and use of the community's physical, spatial and digital assets is available in real time and on an open and interoperable basis, in order to enable real-time integration and optimization of community resources
- **Managing community data as an asset in its own right**, both within the local authority and in collaboration with other significant data owners across the community
- **Empowering the community through community data**:
  - both at a technical level, through development of open data platforms; and
  - at a business level, through steps to enable a thriving market in reuse of public data together with release of data from commercial entities in a commercially-appropriate and privacy-protective way
- **Delivering integrated and citizen-centric services**, by:
  - providing citizens and businesses with public services that: are accessible in one stop, over multiple channels; engage citizens, businesses and communities directly in the creation of services; and are built around user needs, not the community's organizational structures; and
  - establishing an integrated business and information architecture which enables a whole-of-community view of specific customer groups for community services (e.g. commuters, elderly people, troubled families, disabled people, ethnic minorities)
- **Setting holistic and flexible budgets**, with a focus on value for money beyond standard departmental boundaries
- **Establishing community-wide governance and stakeholder management processes** to support and evaluate these changes

NOTE *Table 1 is adopted from BS ISO 37106.*

Moving towards such a smart community operating model is a lengthy process, requiring leadership over a sustained period of time and extensive collaboration between a wide range of stakeholders. To help manage this process, BS ISO 37106 outlines a set of guiding principles for community leaders to use as they drive change within the community over time. A high-level summary of the BS ISO 37106 guiding principles, as shown in Figure 1, is that a smart community is visionary, citizen-centric, digital, open and collaborative.

Suppliers can support communities in this drive to become smarter by embedding smart community recommendations in their own products and services. The box below illustrates the wide range of organizations that can valuably make use of this PAS.

ILLUSTRATIVE USE CASES

- **An application developer** (for example of citizen engagement tools) can use PAS 186 to demonstrate to city clients that its services are developed in highly user-centric and privacy-protective ways, support the city in delivering UN Sustainability Goals, and are easily interoperable with other digital services and infrastructure deployed in the city.
- **A smart city solutions provider** (for example, a supplier of "smart traffic lights") can use PAS 186 to demonstrate to city clients that their solution is secure and interoperable with other city systems – and is not just technically viable, but also delivered through a scalable business model and agile operating model.
- **A developer offering a complete service to design, build and operate a new city neighbourhood** can use PAS 186 to demonstrate to city clients that the new development will be citizen-centric, digitally-enabled and supportive of the management and improvement of city services.
- **A community authority** can embed PAS 186 in its procurement requirements from suppliers, to help ensure that products and services are aligned with city priorities and that the city is better able to implement innovation at scale.

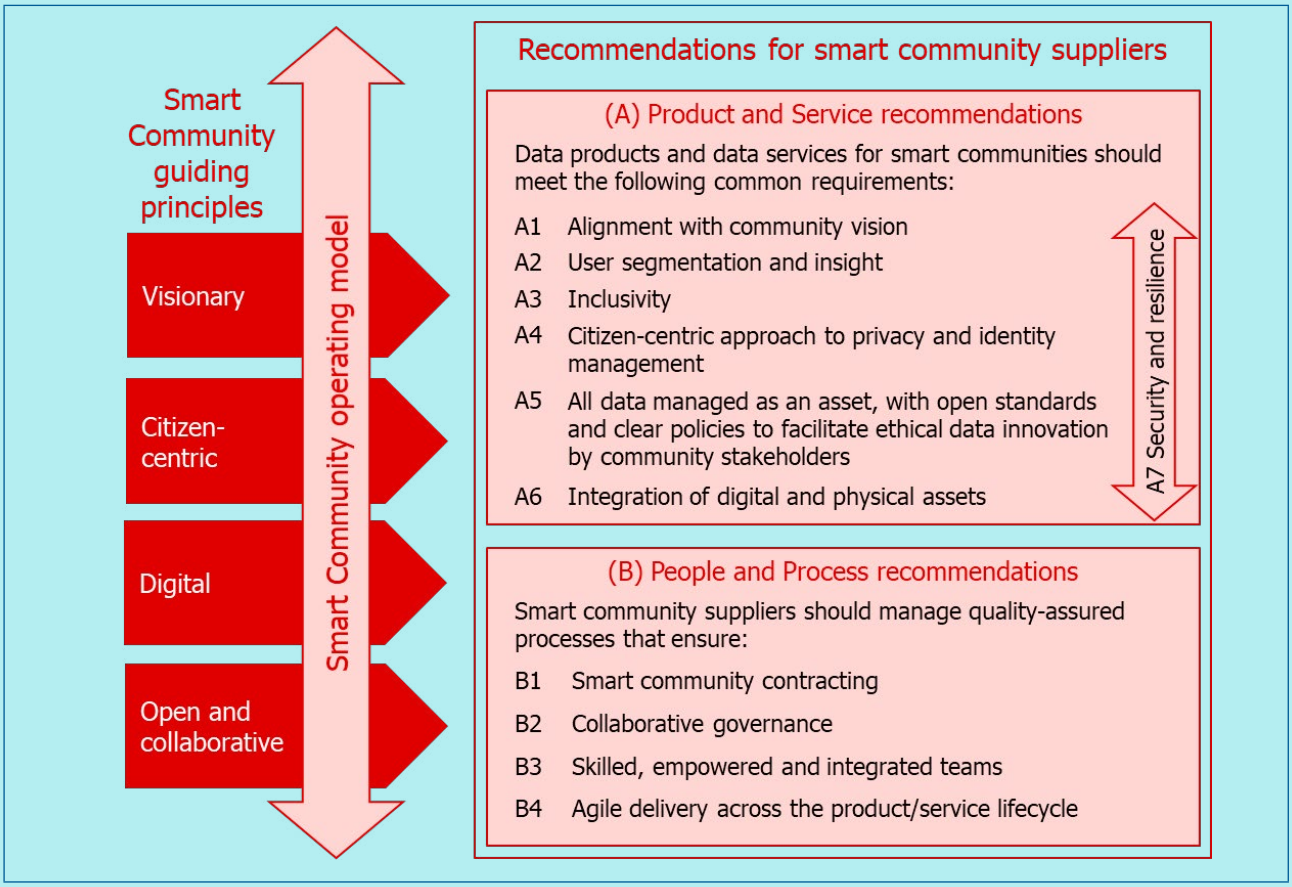
0.3 Overview of recommendations for smart community suppliers

Figure 1 gives an overview of the recommendations for smart community suppliers that are described in this PAS. These recommendations are common for all data products and data services being supplied to smart communities, and are at two levels:

a) product and service recommendations; and

b) people and process recommendations.

Figure 1 – Overview of recommendations for smart community suppliers



The recommendations summarized in Figure 1 are described in more detail in Clause **4** and Clause **5**.

For each individual recommendation, this PAS describes five levels of supplier maturity, in a structured way, allowing quantitative comparison, each mapped against the generic maturity levels defined in Figure 2. This five-level maturity model follows the methodology recommended in BS ISO 37153. Performance at Level 3 or more on this scale represents compliance by a supplier with that recommendation. Clause **6** gives further details on how different levels of performance across the different recommendations can be combined to give an assessment of whether or not the supplier conforms to the standard as a whole. Annex A presents an illustrative scorecard of how an individual supplier might be scored against this framework.

Figure 2 – Maturity model for smart community suppliers

1. Initial	Processes to manage this recommendation do not exist.
2. Partially fulfilled	Processes to manage this recommendation are managed on an ad hoc basis by the supplier.
3. Fulfilled	The supplier has established quality-assured processes to manage the delivery of this recommendation.
4. Improving	The supplier can demonstrate that it is measuring the impact of these processes, that positive impacts are being achieved, and that (where appropriate) the processes follow relevant international standards.
5. Sustainably optimizing	As at Level 4. In addition, the supplier can demonstrate clear evidence of systemic continual improvement, where relevant in real time or near real time.

1 Scope

This PAS gives recommendations for suppliers of data products and data services to smart cities and smart communities. This PAS is technology neutral and supplier impartial. Its recommendations are independent of the underlying IT infrastructures which hold and deliver data products and data services.

This PAS is for use by organizations that supply data products or data services for smart cities and smart communities, regardless of sector.

Stakeholders who are responsible for procuring, contracting or commissioning services might also benefit from this PAS by referencing it when detailing requirements for data products and data services within smart cities and/or smart communities.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document.[1)] For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Standards publications

BS EN ISO 19650-1:2018, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 1: Concepts and principles*

BS EN ISO 19650-2, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 2: Delivery phase of the assets*

BS EN ISO 19650-5, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 5: Security-minded approach to information management*

BS ISO 37120, *Sustainable cities and communities – Indicators for city services and quality of life*

PAS 185, *Smart Cities – Specification for establishing and implementing a security-minded approach*

PAS 7040:2019, *Digital manufacturing – Trustworthiness and precision of networked sensors – Guide*

Other publications

[N1] Caldwell, B., Guarino Reid, L., Vanderheiden, G., Chisholm, W., Slatin, J. and White, J., WCAG 2.1 *Web Content Accessibility Guidelines WCAG 2.1*.[2)]

[1)] Documents that are referred to solely in an informative manner are listed in the Bibliography
[2)] Available at <https://www.w3.org/TR/2018/REC-WCAG21-20180605/>

3 Terms and definitions

For the purpose of this PAS, the terms and definitions given in BS ISO 37100:2016 and the following apply.

3.1 citizen-centric

design and delivery of city services driven by the needs of citizens rather than the functional structures of a city's silos

***NOTE** The term citizen in this context includes residents, visitors, businesses and non-business groups within the city.*

[SOURCE: BS ISO 37106:2018, **3.3** – Note modified]

3.2 common data environment (CDE)

agreed source of information for any given project for collecting, managing and disseminating all relevant approved project documents for multi-disciplinary teams through a managed process

***NOTE** A CDE might use a project server, an extranet, a file-based retrieval system or other suitable toolset.*

[SOURCE: BS EN ISO 19650-1:2018, **3.3.15**]

3.3 community

group of people with an arrangement of responsibilities, activities and relationships

***NOTE** In many, but not all, contexts, a community has a defined geographical boundary.*

[SOURCE: BS ISO 37100:2016, **3.2.2**]

3.4 community authority

public body that has been given the authority by legislation or directives of a higher level of government to set general policies, plans or requirements for the community

3.5 data custodian

organization processing the data for a specific purpose or task related to the provision of a service

***NOTE 1** The data custodian role is different to that of the data owner in that the custodian does not own the data.*

***NOTE 2** From a data protection perspective the custodian is a data processor as defined in the UK Data Protection Act 2018 [1] and GDPR [2].*

3.6 data product

dataset or dataset series that conforms to a data product specification

[SOURCE: BS EN ISO 19131:2008+A1:2011, **4.6**]

3.7 data product specification

detailed description of a dataset or dataset series together with additional information that enables it to be created, supplied to and used by another party

[SOURCE: BS EN ISO 19131:2008+A1:2011, **4.7**]

3.8 data service

means or a method that organizations use to deliver results that users value and wish to achieve through use of one or more data products

***NOTE** These results are usually intangible although they might also include tangible elements.*

3.9 data subject

identified or identifiable living individual to whom personal data relates

[SOURCE: Data Protection Act 2018, Section 1(3) [1]]

3.10 open data

data which anyone is free to access, use, modify and share, subject to requirements that preserve provenance and openness

[SOURCE: PAS 185:2017, **3.1.27**]

NOTE 1 *Open data is either:*

a) in the public domain, i.e. without copyright or similar restrictions, whether by default or waiver of all such conditions; or

b) provided under an open licence.

NOTE 2 *The open licence may require distributions of the data to include attribution of contributors, rights holders, sponsors, and creators as long as any such prescriptions are not onerous.*

NOTE 3 *Any additional terms accompanying the data (such as terms of use, or patents held by the licensor) should not contradict the work's public domain status or terms of the licence.*

NOTE 4 *The right to modify open data relates to the creation and modification of derivatives of the licenced data, not to modification of the original underlying dataset.*

3.11 personally-identifiable information

information relating to an identified or identifiable living individual

[SOURCE: Data Protection Act 2018, Section 1(3) [1]]

NOTE *An "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:*

a) an identifier such as a name, an identification number, location data or an online identifier; or

b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

3.12 processing

operation or set of operations performed on information, or on sets of information

NOTE *Such operations might include:*

a) collection, recording, organization, structuring or storage;

b) adaptation or alteration;

c) retrieval, consultation or use;

d) disclosure by transmission, dissemination or otherwise making available;

e) alignment or combination; or

f) restriction, erasure or destruction.

[SOURCE: Data Protection Act 2018, Section 1(4) [1]]

3.13 real-time data

data made available with the requisite timeliness for the application for which its use is intended

NOTE 1 *It is important to recognize that the timeliness of data delivery is appropriate and proportionate to the application(s) that process it. Near instantaneous delivery of data, e.g. real-time voice communication, imposes specific communication and networking requirements that might not be justifiable in many smart city applications.*

NOTE 2 *In certain applications, for example, display of arrival times in transport systems (rail, bus, etc.) might be near-real-time, i.e. to the nearest minute rather than to the nearest second or part thereof. This does not detract from the consumer experience and provides greater flexibility in the design and processing of the raw data.*

3.14 smart community supplier

organization or part of an organization that has contractually agreed to help the community authority to design, deploy, deliver, or improve a data product or data service

3.15 trustworthy

appropriately addresses safety, reliability, availability, resilience and security issues

NOTE *PAS 186 uses this word only in relation to digital assets, applying the definition above. It also uses the related terms "trust" and "trusted" in relation to people and processes. These words have their natural language senses, which include an ethical dimension.*

[SOURCE: PAS 7040:2019, **3.1.44** – Note added]

4 Product and service recommendations (A)

*COMMENTARY ON CLAUSE **4***

This clause sets out seven key recommendations that flow from smart community principles in respect to the data product or data service itself:

***4.1** (A1)*	*Alignment with community vision*
***4.2** (A2)*	*User segmentation and insight*
***4.3** (A3)*	*Inclusivity*
***4.4** (A4)*	*Citizen-centric approach to privacy and identity management*
***4.5** (A5)*	*All data managed as an asset, with open standards and clear policies to facilitate ethical data innovation by community stakeholders*
***4.6** (A6)*	*Integration of digital and physical assets*
***4.7** (A7)*	*Security and resilience*

4.1 Alignment with community vision (A1)

*COMMENTARY ON **4.1 (A1)***

The starting point of BS ISO 37106 smart community framework is development of a vision for the future of the community – a vision that:

- is aligned with UN sustainable development goals;
- is developed in an iterative and collaborative manner with all key stakeholders;
- embraces the opportunities opened up by smart technologies, smart data and smart collaboration;
- uses digital modelling, data visualisation and other technologies to "bring to life" what it will be like to live and work in the community's vision for the future; and
- is measurable.

When smart community suppliers are supplying, or seeking to supply, a data product or data service to smart communities they should:

a) identify the social, economic and environmental outcomes that community leaders and key stakeholders are targeting;

b) undertake discovery so that the challenge that their data product or data service is addressing for the community in helping to achieve those outcomes is clearly defined; and

c) monitor and measure the impact of their data product or data service on those outcomes.

Suppliers should claim their level of conformity with **4.1** of this PAS in line with the criteria in Table 2, and as illustrated in the illustrative scorecard in Annex A.

Table 2 – Alignment with community vision (A1) – Compliance levels

1. Initial	The supplier is not able to demonstrate and measure the outputs or outcomes from its data product/service.
2. Partially fulfilled	The supplier is able to demonstrate the outputs from its data product/service (that is, the changes that users implement with the product/service), but is not able to demonstrate how these outputs flow through to create impact against one or more of the social, economic and environmental outcomes being targeted by communities (such as the sustainable development goals).
3. Fulfilled	The supplier is able to demonstrate (with clear and convincing evidence supported by a compelling theory of change) the impact that its product/service makes against one or more of the social, economic and environmental outcomes typically being targeted by the community (such as the sustainable development goals).
4. Improving	As at Level 3. In addition, the supplier is able to quantify impact using standardized community indicators described in BS ISO 37120.
5. Sustainably optimizing	As at Level 4. In addition, the supplier has established impact management systems which demonstrate progress towards community outcomes in real time.

INFORMATIVE – Additional resources for A1

Local authorities in most cities publish their vision and strategy for the city, often with quantified key performance indicators. Standardized resources that suppliers can also draw on to help demonstrate the outcome-focused nature of their product or service include:

- *The UN Sustainable Development Goals set out seventeen goals (supported by 169 quantified targets). These represent the social, economic and environmental outcomes that the leaders of 193 countries have committed to deliver.*
- *BS ISO 37101 describes six purposes of a sustainable community, providing a useful framework for applying the UN Sustainable Development Goals at the level of an individual city or community.*
- *BS IS0 37120 sets out a core set of 100 city indicators which enable quantified comparison of city performance. BS IS0 37120 and PD ISO/TR 37121 supplement this core set with additional indicators for, respectively, smart cities and resilient cities.*
- *PAS 184 provides detailed guidance on how to:*
  - *develop a "benefit map" for a smart city product or service, showing how the outputs it produces flow through to create socio-economic impacts;*
  - *underpin this with a clear and evidence-based theory of change that gives confidence that there is a genuine cause and effect flow from activities to outputs to outcomes.*
- *PAS 185 provides guidance on adoption of a security-minded approach to handling smart city data relevant to the collection and processing of evidence supporting impacts which might be sensitive, e.g. information about outcomes for individuals.*

4.2 User segmentation and insight (A2)

*COMMENTARY ON **4.2 (A2)***

The BSI smart city publications state that smart cities take a citizen-centric approach to all aspects of service design and delivery. In particular, the BS ISO 37106 guiding principles highlight the importance of:

- ***Detailed and segmented understanding of citizens' and businesses' needs** – which require:*
  - *a shared community-wide understanding of key user segments, based on evidence not assumptions;*
  - *real-time, event-level understanding of citizen and business interactions with community systems.*
- ***A highly participatory approach to service development** – which require:*
  - *stakeholders to be engaged directly in design and delivery of community services;*
  - *the adoption of a common co-design/co-production ethos across services.*

To support the development of such a citizen-centric, community-wide approach to service delivery, smart community suppliers should:

a) segment the user base for their data products and data services, aligning with any community-wide segmentation adopted by the community authority;

b) address the wider context-of-use: that is, understand the other stakeholders who, while not directly using the data product or data service, might be impacted by that use and whose needs are important for the community;

c) invest in user insight to understand user needs, not as a one-off input of initial research but through a continuous process of iterative design and user testing that:

   1) takes a co-design/co-creation approach to service design and delivery;

   2) defines different user profiles/personas to consider their specific needs, how they currently do things, what their pain points are, and how the product or service will help them do what they do and achieve their outcomes more easily;

3) ensures any specific additional needs of users who might need assistance in using digital products or services have been identified;
4) checks regularly that the product or service is meeting targeted user needs in practice, identifying opportunities for improvement; and
5) is informed both by user research at key stages (with different user profiles, including those that might have difficulty with accessing or using data products and services) and by data analytics and event-level use of digital services; and

d) share user insights with the community administration and other community stakeholders, in order to facilitate cross-service collaboration.

Suppliers should claim their level of conformity to **4.2** in line with the criteria in Table 3 and as illustrated in the illustrative scorecard in Annex A.

Table 3 – User segmentation and insight (A2) – Compliance levels

1. Initial	The supplier has carried out little user research or user analysis. It cannot demonstrate, with evidence, the user needs that its product or service meets and how those needs vary between different user segments.
2. Partially fulfilled	The supplier has an evidence-based and segmented understanding of its user base, including how user needs vary across segments.
3. Fulfilled	The supplier has an evidence-based and segmented understanding of its user base, including how user needs vary across segments. In addition, the supplier can demonstrate that it: • designs products and services jointly with their users, using iterative and participative approaches; • ensures that its user insight and service design processes explicitly address the needs of users who might need assistance in accessing or using digital products or services; and • understands how non-users might be impacted by the digital product or service, and ensures their needs are taken into account.
4. Improving	As at Level 3. In addition, the supplier: • uses appropriate standardized models for segmenting and describing user needs [A]; and • publishes and shares all user insight and market research with the community administration and community stakeholders (in accordance with relevant privacy and security best practices).
5. Sustaining optimizing	As at Level 4. In addition, the supplier's systems provide event-level data about access to or use of the data product or service by different user segments, which it publishes in open formats and in a privacy-protective way.

[A] For example those published at https://standards.esd.org.uk

INFORMATIVE – Additional resources for A2

The Government Service Design Manual [3] provides extensive guidance on how to use user insight to develop good public services, including through use of user profiles/personas.

BS EN ISO 9241-210 provides guidance both on understanding user needs and also on understanding the wider context-of-use, including needs of non-user stakeholder groups.

The UK's Local Government Association publishes standardized taxonomies of people's needs and circumstances that can assist with user segmentation. These are available for re-use under the UK Open Government Licence and are available online at https://standards.esd.org.uk – with Europe-wide taxonomies and some from other EU countries available at https://standards.esd-toolkit.eu.

These taxonomies include:

- *personal circumstances: a listing of the key conditions connected with or affecting a person or groups of people that are of most significance in shaping their needs (such as age, income, occupation, level of digital skills etc.);*
- *user needs: the personal requirements of a citizen that, if met, can support a positive change in circumstances (covering needs in categories such as mobility, health, housing, social inclusion);*
- *life events: the challenges or significant events that citizens face in everyday life and that might trigger a significant change in circumstances and needs;*
- *services: a catalogue of all services performed by a community authority (based on analysis of local services in England, Scotland, Belgium, Netherlands, Norway, Sweden and Germany); and*
- *others: including taxonomies that describe links to performance metrics, statutory powers/duties and records retention schedules.*

4.3 Inclusivity (A3)

*COMMENTARY ON **4.3 (A3)***

The guiding principles for smart cities set out in BS ISO 37106 include a commitment to ensuring the "inclusive digitization of our community" – with no stakeholder group left behind or excluded from the benefits of digitization. BS ISO 37106 sets out a number of recommendations for smart communities that follow from this, including: taking a proactive approach to the digitally-excluded in terms of training access and education; enabling the views and voices of the digitally-excluded to be heard and incorporated into decision-making about community services; and investing in assisted digital provision. PD ISO/IEC Guide 71 stresses that impairments can be permanent, temporary or vary on a daily basis, and sometimes they are not fully recognized or acknowledged. In addition, although some limitations can be minor in nature, combinations of limitations can pose significant problems for people (and in particular children) attempting to interact with systems.

Smart community suppliers should meet the following inclusivity recommendations.

a) **Inclusivity insight**: The supplier should be able to demonstrate that it identifies and researches the barriers that might exclude some stakeholder groups from using its data products and data services, including:
   1) people with impairments to their vision, hearing, mobility or thinking and understanding; and
   2) people who face other barriers to use of digital services, including: lack of trust and confidence, lack of access to the internet, lack of digital skills, and lack of perceived benefit from use of such services.

b) **Inclusivity-by-design**: The supplier should be able to demonstrate that it designs products and services in ways that address these barriers effectively and – as a minimum:
   1) meet Level AA of the WCAG 2.1 standard [N1]; and
   2) work on assistive technologies (including screen magnifiers, screen readers and speech recognition tools).

c) **Assisted access for those who cannot access and use the digital product or service without help**: The supplier should be able to demonstrate that it makes effective provision for, and does not disadvantage, those not able to access and use the product or service without help, including, for example:
   - provision of assisted digital support in person, on the telephone and/or via webchat; and
   - enabling authorized intermediaries to securely access and use the service on behalf of a main user.

Suppliers should claim their level of conformity to **4.3** in line with the criteria in Table 4 and as illustrated in the illustrative scorecard in Annex A.

Table 4 – Inclusivity (A3) – Compliance levels

1. Initial	The supplier cannot demonstrate any real engagement with interested parties, particularly those that might otherwise be digitally excluded from using their products or services.
2. Partially fulfilled	The supplier has demonstrated understanding of some of the barriers to engagement with and take up of their products or services, and has started to establish appropriate channels of engagement with some interested parties to obtain their involvement.
3. Fulfilled	There is clear evidence that an inclusive approach is being taken to product and service design, informed by research and engagement with user groups at risk of exclusion. All web content satisfies the recommendations of the WCAG2.1 standard [N1] to level AA conformance, and works on the most commonly used assistive technologies (including screen magnifiers, screen readers and speech recognition tools). Effective assisted digital measures are in place to meet the needs of people who cannot access the digital product or service without help.
4. Improving	There is clear evidence that an inclusive approach is being taken to product and service design, informed by research and engagement with user groups at risk of exclusion, and this approach follows an explicit good practice standard (such as BS 8878). All web content satisfies the recommendations of the WCAG2.1 standard [N1] to level AAA conformance.
5. Sustainably optimizing	As at Level 4. In addition, there is clear evidence that feedback systems are in place with user groups with accessibility problems and/or other risks of digital exclusion, and that these are driving continuous improvement.

INFORMATIVE – Additional resources for A3

Resources that suppliers can draw on when ensuring the inclusivity of their products and services include:

- ***BS ISO 37106:2018, guidance note [B11]** provides guidance on digital inclusion and channel management at a community-wide level;*
- ***PD ISO/IEC Guide 71 – Guide for addressing accessibility in standards** contains information on the requirements for people with different types of disability and how to enable the end user to carry out the relevant activity;*
- ***The Web Content Accessibility Guidelines published by the W3C** are the internationally recognized set of recommendations for improving web accessibility for people with disabilities. The latest version, WCAG 2.1 [N1], available at https://www.w3.org/TR/WCAG21/. WCAG 2,1 sets out four principles for accessibility (perceivable, operable, understandable and robust), supported by 13 guidelines – each of which is measured by testable success criteria with three levels of conformance: A (lowest), AA, and AAA (highest);*
- ***BS EN 301549, the European standard for digital accessibility,** provides guidance on how to use web content accessibility guidelines and address the needs of people with cognitive and mental health impairments;*
- ***BS 8878** defines good practices for ensuring the accessibility of any web product – including web sites, web applications, software as a service, cloud based services and other services accessed via a web browser. It is complementary to the WCAG guidelines, focusing not on the technical-level standards of WCAG but on the processes needed for planning and deployment of accessible web products;*
- ***BS 18477** helps service providers to identify and respond appropriately to different consumer needs and to deliver services that do not discriminate;*
- ***BS 7000-6** provides a comprehensive framework to help all private enterprises, public sector and not-for-profit organizations ensure that disabled people's needs are considered throughout the lifecycle of a product or service. The goal is to meet the needs of consumers of diverse age and capability in a wide range of contexts because appropriate access to information, products, services and facilities is a fundamental human right;*
- ***The Government Service Design Manual [3]** provides extensive guidance on how to design inclusive public services (https://www.gov.uk/service-manual/service-standard/point-5-make-sure-everyone-can-use-the-service);*
- ***ETSI TR 103 455 v0.84 (2019-11) [4]** provides guidance on human factors (HF); smart cities and communities standardization for citizens and consumers; and*
- ***G3ict's Smart Cities for All Toolkit [5],** provides a set of tools focused on ICT accessibility, to assist with tackling barriers to the digital inclusion of persons with disabilities and older persons (https://smartcities4all.org/english-toolkit/).*

4.4 Citizen-centric approach to privacy and identity management (A4)

*COMMENTARY ON **4.4 (A4)***

A smart community requires trust.
BS ISO 37106's guiding principles therefore highlight the importance of ensuring that all personally-identifiable data is held securely, and under the ownership and control of the individual citizen.
BS ISO 37106 establishes an approach to privacy and identity management in smart communities based around three pillars.

a) ***Federated business architecture.** First, a business architecture for identity management that is based on federation between a wide range of trusted organizations (e.g. the community authority, government departments, banks, employers) and a clear model for establishing trust between these organizations.*

b) ***Interoperable technical architecture.** Second, a technology architecture to support the interoperability of data and IT services, which does not rely on legacy siloed technical implementation, but which, in line with the service-oriented architecture (SOA) paradigm, uses internet-based gateway services to act as a broker between the different data and IT services of the participants in the federated trust model.*

c) ***Citizen-centric trust model.** Third, and perhaps most importantly, a user service model for identity management that places individuals themselves directly in control of their own data, able to manage their own data relationship with the city (and with clearly visible controls to reassure them that this is the case).*

4.4.1 General

Although smart community suppliers of data products and data services cannot deliver this federated, service-oriented and citizen-centric trust model individually, as this requires community-wide coordination, they should support this change by meeting the recommendations in **4.4.1.1** and **4.4.1.2**.

4.4.1.1 Privacy principles

The supplier should apply the following principles to all aspects of its data collection, data analysis and data management.

a) **Consent:** personally-identifiable data should only be collected, processed, stored or shared with the prior explicitly informed consent of the data subject – consent that is freely given, that explicity includes consent to any sharing with third parties, and that is ongoing (with a clear right to opt out of consent both initially and in future)[3].

b) **Purpose:** personally-identifiable data should only be used for limited and explicitly-stated purposes that are made clear to the data subject at the time of data collection, and not for any other purposes without first gaining informed consent from the data subject.

c) **Proportionality:** when personally-identifiable data is requested and stored, the type of data collected should be the minimum required to carry out the stated purpose. Individual users of the data should only be given the minimum access to that data that they need, and the data should not be kept for longer than is necessary for that purpose. When personally-identifiable data is used in any data analysis process which does not require individuals to be identified, this "proportionality principle" requires that the dataset should be anonymized.

d) **Child protection**: data processing that relates to children should have their protection designed into it explicitly from the outset, aiming for protections appropriate to their age and changing needs.

e) **Personal access and control:** Data subjects should be enabled[4] to:

   1) access and take copies of data that is held about them;
   2) easily correct inaccuracies in data that is held about them;
   3) request removal of data that is held about them; and
   4) object to the use of data that is held about them in certain circumstances.

f) **Transparency:** Individuals should be informed how their data is being used and stored, and provided with contact information for those responsible for data protection within the supplier organization. Privacy notices should be short, clear and easily accessible inclusively to all. In case of a breach, the supplier should notify affected individuals (and where appropriate, the relevant regulatory authorities) and keep clear records of the incident and their response to it. The supplier should use a "plain language" policy for all public documents. Audit and traceability processes should be established for all data sharing/transfer so that individuals' data protection rights can be exercised and maintained across the data ecosystem.

g) **Public safety:** In collecting, processing and storing data that might impinge on public safety or is required to inform, manage and assure public safety, the supplier should adopt appropriate and proportionate measures to secure the data, in accordance with PAS 185.

   NOTE 1 *Unauthorized access to, modification of, or denial of access to public safety data could have significant impact on the safety and/or security of a smart city.*

h) **Accountability:** The supplier should establish and publicize effective complaints and redress mechanisms for data subjects who believe their data is not being managed properly.

NOTE 2 *Attention is drawn to local, sectoral or national data protection laws that apply to the supplier's business. The principles described in a) to h) are to facilitate compliance with the EU's General Data Protection Regulation [2] but are also more generally applicable for communities and suppliers seeking to adopt good practice.*

[3] Unless other clear legal bases for processing exist: such as contractual obligations; legal obligations; when it is carried out in the interest of the public (for example, police camera systems); and preserving the vital interests of the data subject. Further guidance on these legal bases is available in the UK from the Information Commissioner's Office at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/. Even in cases where an alternative legal basis exists, seeking consent is often a good practice.

[4] The ability of data subjects to modify records and request removal of data is subject to legal requirements in respect of record-keeping required for fraud and crime detection and/or prevention, and the need to retain appropriate and proportionate records for audit and similar purposes.

4.4.1.2 Privacy-by-design

The supplier should establish clear management processes that integrate privacy and data protection, in line with the privacy principles described in **4.4.1.1**, into all aspects of its work from the outset. These processes should ensure that:

a) privacy and data protection is factored into the design, core functionality and operation of all systems, services, products and business practices;

b) the supplier anticipates data protection risks and privacy-invasive events before they occur, and takes steps to mitigate them;

c) personal data is automatically protected by default in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;

d) IT and other systems support enable clear audit trails of who has accessed personal data; and

e) all sub-contractors and external data processors used by the supplier adopt similar processes which are routinely monitored and assured.

Suppliers should claim their level of conformity to **4.4** in line with the criteria in Table 5 and as illustrated in the illustrative scorecard in Annex A.

Table 5 – Citizen-centric approach to privacy and identity management (A4) – Compliance levels

1. Initial	The supplier has no documented policies and processes setting out how it will ensure privacy and data protection.
2. Partially fulfilled	The supplier has documented policies and processes setting out how it will ensure privacy and data protection.
3. Fulfilled	The supplier has established clear and documented management processes to ensure compliance with the privacy principles described in this PAS (compliance, consent, purpose, proportionality, child protection, personal access and control, transparency, accountability).
4. Improving	As at Level 3. In addition, the supplier has implemented a recognized international standard for privacy and data protection that is of direct relevance to its business.[A)]
5. Sustainably optimizing	As at Level 4. In addition, the supplier actively engages with the community authority and other community stakeholders to develop shared assets and common tools for use in privacy and identity management, within a federated and service-oriented business and technical architecture.

[A)] For example BS EN ISO/IEC 27018 for cloud services.

INFORMATIVE – Additional Resources for A4

- *BS ISO 37106:2018 guidance note [B11] sets out recommendations to community leaders on development of a community-wide framework based on an open and federated business model, a service-oriented IT architecture and a citizen-centric trust model;*
- *BS ISO/IEC 29184 specifies notice and consent-based privacy management in practice, including a sample Kantara Consent Receipt, https://kantarainitiative.org/confluence/display/archive/WG+-+Consent+and+Information+Sharing+-+CISWG (a best practice specification for creating machine and human readable consent receipts) in Annex B;*
- *BS ISO/IEC 27701:2019, Security techniques – Extension to ISO/IEC 27001;*
- *BS EN ISO/IEC 27002 for privacy information management – Requirements and guidelines;*
- *PAS 185:2017 gives additional guidance on taking a security-minded approach in respect of all personally-identifiable data in a smart city context;*
- *"The Anonymisation Decision-Making Framework" provides detailed guidance on the principles and practices to be applied when anonymising personally identifiable data (as recommended in subclause **4.4.1.1** c). https://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf;*
- *The UK's Information Commissioner publishes extensive guidance on how to follow a privacy-by-design approach to data protection at www.ico.org.uk. This includes specific guidance on "Age appropriate design: a Code of Practice for Online Services";*
- *BS EN ISO/IEC 27018 addresses privacy-by-design in the specific context of cloud services;*
- *PD ISO/IEC Guide 51 on consumer safety protection; and*
- *The ANEC Pocket Guide on Using Consumer Data gives guidance on privacy in the context of data transfer and trading: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-ICT-2015-G-040.pdf.*

4.5 All data managed as an asset, with open standards and clear policies to facilitate ethical data innovation by community stakeholders (A5)

*COMMENTARY ON **4.5 (A5)***

The BSI smart community specifications aim to ensure that community data is managed as an asset – with clear accountabilities for maintaining and getting social and economic impact from data sets, supported by clear, principle-based rules for promoting ethical re-use and innovation with data within a "community information marketplace".

In particular:

- *BS ISO 37106 sets out the overall strategic framework for this community information marketplace;*
- *BS ISO/IEC 30182 provides a top-level concept model against which all types of community data can be mapped, in order to promote interoperability;*
- *PAS 183 provides a more detailed decision-making framework for determining the appropriate model of open data or data sharing within the community information marketplace; and*
- *PAS 185 provides a systematic security-minded approach for the protection of personal and sensitive data that is shared as part of smart city operations and services.*

Individual smart community suppliers cannot by themselves deliver all of the recommendations from the BSI smart city publications because these involve decisions and actions by community leaders. But they can support community leaders in their development of a thriving community information marketplace by making sure that their individual data products and services are managed in accordance with smart community principles.

4.5.1 General

Smart community suppliers should work to ensure that all community data produced and/or managed is in accordance with **4.5.2** to **4.5.6** and claim with these criteria in line with Annex B.

4.5.2 Owned and authoritative

Each dataset should be managed by an accountable data custodian, who is responsible for the legal compliance, security, quality and re-usability of the data. The data custodian should ensure that the data and information security triage process set out in PAS 185:2017 (Clause **9**) has been undertaken and that, where required, any

data and information sharing agreements are in place prior to sharing the data. All data being published or exchanged by a smart community supplier with external stakeholders should be made accessible at source rather than as a copy. Where there are duplicate versions of a dataset in use within the community, the smart community supplier should work with the community authority and relevant stakeholders to designate a specific owner and authoritative source of that data, ensuring that all parties access that data directly (for example, via an API).

4.5.3 Discoverable and interoperable

Data products for smart communities should be easy to locate and combine with data from other sources. Data products should:

a) be published in appropriate open machine-readable formats (provided this is appropriate in the light of the security considerations of **4.7**). In particular:
   1) tabular data should be published as CSV;
   2) building information modelling data should be published in COBie or IFC format;
   3) other structured non-tabular data should be published in a relevant open standard, where available, for example using: geospatial data published as GeoJSON or KML, and JSON, XML, RDF, GTFS; and
   4) real-time data or data being used in services should be made available via a well-documented API.

b) have comprehensive metadata to aid discoverability and ideally a schema specifying the ranges and values of each field;

c) use common taxonomies to describe terms within key metadata fields in order to facilitate data linking; and

d) be made available for bulk download or via an API either on the web or through a platform with reliable permanent access that is supported over time.

4.5.4 Re-usable

Data products and data services should, in accordance with the security triage in **4.7**, be made available for re-use by other stakeholders under documented policies in accordance with a) to c).

a) Data products involving data that in isolation, or when combined and/or aggregated with other data, is neither personal nor commercially-confidential or otherwise sensitive should be published under an open data licence which:
   1) allows unrestricted access to the data;
   2) allows the data to be adapted, modified, combined with other data and re-published or shared: free of charge and subject at most to the recommendation for attribution;
   3) explicitly allows the commercial use of data; and
   4) is published online and included within the metadata for the data product.

b) Other data products – including data products being marketed for commercial gain – should be accompanied by documented policies (such as licences or data-sharing agreements) setting out the basis on which sharing and re-use of that data by community stakeholders may be undertaken in an ethical, privacy-protective, consent-based and legally-compliant manner. Users who wish to use such data should be required to make a legally-binding commitment to abide by these policies.

c) Data services that have been funded in whole or in part by the community administration should be made available either at no cost to all users or under any other business model provided that it uses FRAND terms (fair, reasonable and non-discriminatory). The data products that underpin such data services should be made available directly to community stakeholders as described in a) (that is, users should be able to access the raw data, not just data bundled within a value-adding data service).

4.5.5 Fit-for-purpose

The quality of the data (including its accuracy, timeliness and completeness) should be sufficient to meet its intended purpose. The smart community supplier should be able to demonstrate that it has a clear and evidence-based understanding of user requirements for data quality, and appropriate processes in place to ensure that those requirements are met. Demonstrating fitness for purpose should include a statement of known sources of potential error.

4.5.6 Used in an ethical manner

The way data is collected, analysed and used should be driven by a clear ethical framework, aimed at minimizing, mitigating and disclosing any potential biases that could lead to unfair or incorrect outcomes.

INFORMATIVE – Additional resources for A5

A wide range of British and International standards are available to support smart community suppliers in establishing quality-assured processes to meet these recommendations. Of particular relevance are:

- ***Owned and authoritative:***

  PAS 183 gives further details on the roles and responsibilities of a data custodian in a smart city context.

  BS ISO/IEC 38505-1 and PD ISO/IEC TR 38505-2 give a broader framework for embedding this within a holistic approach to data governance across the whole organization.

- ***Discoverable and interoperable:***

  PAS 212 provides a framework for ensuring effective machine-to-machine interoperability via standardized and easily discoverable APIs.

  BS ISO/IEC 30182 provides an over-arching framework against which different standardized vocabularies can be mapped in order to facilitate cross-sectoral interoperability in a smart city context.

  For many types of common dataset there exist open standards for representing that information as structured data which are to be used as much as is possible. Examples of such standards include schemas found on http://schema.org/.

- ***Re-usable:***

  The international definition and specification of an open licence is available at http://opendefinition.org/od/2.1/en/.

  A widely-used conformant example of such a licence is the UK Open Government Licence (which is the default licence for use by UK public sector organizations).

  *PAS 185 provides a systematic security-minded approach for the protection of personal and sensitive data that is shared as part of smart city operations and services – including (see **9.1.3**) advice on good practices in the development and management of Data and Information Sharing Agreements that support the sharing and exchange of data that cannot be published as open data.*

- ***Fit-for-purpose:***

  ISO/TS 8000-1 provides a systematic framework for ensuring that user recommendations for data quality are understood and delivered in a quality-assured way.

- ***Used in an ethical manner:***

  The UK Government's Data Ethics Framework provides a systematic process for identifying and managing potential biases in the collection and use of data. https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework

4.6 Integration between digital and physical assets (A6)

*COMMENTARY ON **4.6 (A6)***

The smart community operating model described in BS ISO 37106 requires communities progressively to integrate their digital and physical assets, "ensuring that data on the performance and use of the city's physical, spatial and digital assets is available in real time and on an open and interoperable basis, in order to enable integration and optimization of city resources".

This requires investment in sensors and communication networks, data analytics, and development over time of a virtual model of the community's assets to inform scenario planning and community decision-making. And it requires intensive collaboration between the community administration and its different suppliers in order to ensure that individual investments build towards a more integrated and interoperable whole.

Individual suppliers of physical assets to communities cannot by themselves deliver the whole of the vision described, but by meeting certain common requirements, they can ensure that the assets they develop and manage are future-proofed, functioning as effective building-blocks towards the wider vision.

4.6.1 General

Suppliers of physical assets for smart communities should conform to the recommendations in **4.6.2** and **4.6.3** and claim their level of conformity with these criteria in line with Table 6.

4.6.2 Smart enablement

Suppliers of physical assets for smart communities should ensure that physical assets are smart-enabled from the outset. This means that suppliers should work with the community and other physical and digital asset owners to define and implement:

- an appropriate lifecycle for the assets that meets the needs of community stakeholders;
- the data and information that is required to measure the performance of the physical asset in-use across its planned lifecycle and to make required decisions to adjust performance;
- how this is to be provided (format, method of utilisation and visualisation);
- the smart-enabled technology that is required (e.g. networked sensors);

- the standards that this technology should meet (including deployment of networked sensors in a manner consistent with the systematic approach set out in PAS 7040 so that the trustworthiness of the sensor data can be assured);
- methods to ensure their effective deployment, testing, commissioning and handover of the smart-enabled assets; and
- methods to establish suitable maintenance, renewal and end of life disposal of the assets.

NOTE *It is easier and cheaper to put in place the foundations for a smart community within a development or infrastructure project at the initial planning and implementation stages than to seek to retro-fit them later. For example:*

- *digging and retro-fitting communications networks can represent anything up to 80% of the cost of installation, so it is likely to be cost-effective to ensure that adequate provision is built into new developments at the construction stage; and*
- *sensor networks can be installed much more cheaply when the development or infrastructure is being built.*

4.6.3 Collaborative engagement

Suppliers of physical assets for smart communities should engage collaboratively with the community administration and other asset developers to develop and share digital models of the assets (except in cases where the classification of the model does not allow this, for example in relation to critical national infrastructure). Smart community suppliers of physical assets should develop virtual models of the asset, its usage patterns and its performance – deploying relevant open standards wherever possible – and make that model easily available for re-use by third parties either as open data or under fair and non-discriminatory terms. For suppliers of construction projects commissioned by the UK public sector, these models should conform to BIM Level 2 (as described in the BS EN ISO 19650-1, BS EN ISO 19650-2 and BS EN ISO 19650-5).

Suppliers should claim their level of conformity to **4.6** in line with the criteria in Table 6 and as illustrated in the illustrative scorecard in Annex A.

Table 6 – Integration between digital and physical assets (A6) – Compliance levels

1. Initial	Physical assets developed and/or managed by the supplier are not digitally-enabled. • There is insufficient investment in sensors and connectivity to deliver trustworthy and timely data on the status, usage and performance of the asset. • No digital model of the asset has been developed.
2. Partially fulfilled	The supplier has established clear management processes to ensure one of the following: • provision of trustworthy and timely data on the status, usage and performance of the asset; or • all parties in the supply chain can collaborate digitally within a Common Data Environment that provides security-minded access to a digital model of the asset, associated with all project information in digitized form.
3. Fulfilled	The supplier has established clear management processes to ensure both: • provision of trustworthy and timely data on the status, usage and performance of the asset; and • all parties in the supply chain can collaborate digitally within a Common Data Environment that provides security-minded access to a digital model of the asset, associated with all project information in digitized form.

Table 6 – Integration between digital and physical assets (A6) – Compliance levels *(continued)*

4. Improving	As at Level 3. In addition, the supplier enables third parties outside the supply chain to: • access trustworthy and timely data about the asset via API; and • make use of the digital model of the asset, including through use of common standards to support interoperability with other models of other community assets or systems.
5. Sustainably optimizing	As at Level 4. In addition, there is clear evidence that the supplier works collaboratively with the community administration to facilitate broad engagement by community stakeholders in: • analysis of data on the status and performance of community assets to improve neighbourhood management and service delivery; and • using digital modelling of the community's assets to test and compare different options, evaluating their likely impact on the community, and to engage stakeholders in more meaningful consultation and co-creation of community spaces.

INFORMATIVE – Additional resources for A6

A wide range of British and International standards are available to support smart community suppliers in establishing quality-assured processes to meet these recommendations for specific asset classes. Of particular relevance are:

a) Smart enablement of physical assets

PAS 184 provides guidance and checklists on how to integrate digital into all aspects of project design and delivery.

PD 8100 gives advice to both planners and developers on how to integrate digital within new developments within the built environment.

PAS 7040 provides a systematic approach for the creation, deployment and operation of trustworthy networked sensors. The approach is applicable outside of the manufacturing sector to sensors installed during the construction and maintenance of built assets.

b) Digital modelling of assets

BS EN ISO 19650-1 provides recommendations for effective building information modelling during the design and construction phase.

BS EN ISO 19650-2 specifies requirements for effective building information modelling during the operational phase.

BS EN ISO 19650-5 provides a systematic security-minded approach for the protection of data related to built assets during the design, construction and operational phases.

c) Trustworthiness of digital assets

PD ISO/IEC TR 24028, Information technology – Artificial intelligence, provides an overview of trustworthiness in artificial intelligence.

4.7 Security and resilience (A7)

*COMMENTARY ON **4.7 (A7)***

Smart communities can achieve significant benefits by making community data more open, more interconnected and available in real-time. But this shift also entails security risks that need to be managed.

Looking beyond information security to the broader resilience of community systems (and in particular, essential systems such as water and energy supply), increased use of smart technologies is both an opportunity and a potential threat. On the one hand, smart systems offer new ways of making communities more resilient to external shocks – because of increased ability to model the future, and increased agility to adapt in the face of change. On the other hand, increased inter-connectedness can lead to both increased levels of vulnerability and diminishing levels of resilience if not effectively managed. The increasing dependence on complex interactions between different organizational components, data and information sets, services and systems raises significant risks that need to be identified and mitigated.

Smart community suppliers should embed security and resilience in all stages of the design, development and operation of data products and services. A holistic approach to security should be implemented, according to the context in which the data product or data service operates and considering cyber, people, physical, information and processes. In particular, they should meet the common recommendations as listed in a) to f) and claim their level of compliance with these criteria in line with Table 7.

a) **IT infrastructure security:** Using the approach set out in PAS 185, smart community suppliers should identify the IT security risks they face, and implement plans and controls to mitigate those risks. As a minimum, they should ensure that they conform to the five controls against cyber-attack as listed in 1) – 5).
   1) **Securing networks and internet connectivity:** Suppliers should design, configure and operate networks so as to adopt a segmented architecture with appropriate controls in place to prevent network traversal by attackers and deliver a defence in depth approach.
   2) **Secure configuration of devices and software:** Only necessary software, accounts and apps are used, with appropriate security settings selected rather than default settings, and with unneeded functionality switched off.
   3) **Controlled access by users:** With the exception of open unrestricted access data (that is data openly published on the Internet with no registration requirements), suppliers should control access to data through user accounts that apply the following principles:
      i) for users who do not have administration privileges, the access control mechanism should be proportionate to the sensitivity of the data that is being accessed; and
      ii) for users who have administration privileges, the granting of such privileges should be carefully controlled and managed, and removed when no longer required. Enhanced access control mechanisms should be employed to reduce the risk of unauthorized access to or use of these accounts.
   4) **Protection from viruses and other malware**: Suppliers should implement appropriate anti-malware defences, such as those integrated into major operating systems, whitelisting and sandboxing.
   5) **Patch management:** Suppliers should ensure that all the devices, software and apps they use are kept up-to-date using a secure update method that does not require change to user settings or introduce unforeseen changes in functionality (any change should be properly publicized).

b) **Data and information security.** Smart community suppliers should identify the key risks to data and information security, at all stages of the data and information lifecycle, and implement plans and controls to mitigate those risks (taking into account the considerations set out in PAS 185:2017, **7.5**). As a minimum, they should address the four key potential breaches of data and information security within smart cities identified by PAS 185:
   1) loss or disclosure of intellectual property and/or commercially sensitive data or information;
   2) loss or disclosure of personal data;
   3) corruption of, or loss of access or unauthorized changes to, metadata; and
   4) corruption of, or loss of access or unauthorized changes to, referential master data.

Smart community suppliers should identify the key risks to data and information security, at all stages of the data and information lifecycle, and implement plans and controls. These should include processes to audit the status of information security and detect breaches, to store information for audit, and to enable reporting of security vulnerabilities by third parties.

c) **System reliability and availability:** Smart community suppliers should work with users to establish requirements relating to uptime and availability, including provisions for service availability during planned maintenance or unplanned downtime, and establish processes to ensure those requirements are delivered.

d) **System resilience:** Smart community suppliers should ensure that their own systems are resilient, with planned and tested redundancy. They should also collaborate with the community administration and community stakeholders, through open and accountable processes, to strengthen the resilience of community systems that use the supplier's data products and services (and in particular, essential systems such as water and energy supply).

e) **Physical security:** Smart community suppliers should establish controls to ensure the trustworthiness and security of digital built assets within the built environment (such as data centres), informed by the triage process and best practices in accordance with BS EN ISO 19650-5. This should include appropriate controls over physical access to relevant buildings.

f) **Incident response:** Suppliers should establish incident management policies and processes and ensure the processes are regularly rehearsed. When considering incident response measures, a supplier should have rehearsed, workable plans to enable business continuity, disaster recovery and restoration of services to citizens, based on fall-back service provision, which may be either predominantly manual or less IT and data intensive. These plans should include notification and support to users, and where appropriate, the relevant regulatory authorities, about incident response and recovery. Wherever practical the supplier should design systems and services so that they gracefully degrade in the face of adverse situations and can be restored in a phased manner.

NOTE 1 *The five controls listed at a) are the minimum requirements for the UK-backed Cyber Essentials scheme.*

NOTE 2 *PAS 185:2017, Clause* ***8*** *provides guidance on planning for the handling of security breaches and related incidents.*

Suppliers should claim their level of conformity to **4.7** in line with the criteria in Table 7 and as illustrated in the illustrative scorecard in Annex A.

Table 7 – Security and resilience (A7) – Compliance levels

1. Initial	The supplier has no documented assessment of the risks to its IT, data and information security, and no documented plan for managing those risks.
2. Partially fulfilled	The supplier has identified and assessed the risks to its IT, data and information security, and has established clear and documented processes to manage those risks that are recorded in a security strategy and security management plan as specified in PAS 185. The supplier engages with the community authority and other community stakeholders to align with local resilience planning and strengthen the broader security and resilience of community systems that use its data products and/or data services.
3. Fulfilled	As at Level 2. In addition, the supplier has embedded its key IT, data and information security measures within service level agreements.
4. Improving	As at Level 3. In addition, the supplier has implemented a recognised international standard for information security that is of direct relevance to its business, and has secured third-party certification of compliance. [A)]
5. Sustainably optimizing	As at Level 4. In addition, the supplier takes a leading role in security and resilience across multiple component providers to smart cities, including leading resilience training, exercising and testing of plans.

[A)] For example BS ISO/IEC 27001, or BS ISO/IEC 27017 for suppliers of cloud services.

INFORMATIVE – Additional resources for A7

- *PAS 185 establishes a framework for the security-minded management of smart cities and their associated infrastructure, as well as of data, information and services used to deliver city services.*
- *Cyber Essentials is a UK Government-backed scheme to help organizations protect themselves against cyber-attack. Tools and guidance to support conformity to the Cyber Essentials requirements are available at https://www.cyberessentials.ncsc.gov.uk/.*
- *Guidance on risk assessment and resilience in the UK context, including the role of Local Resilience Forums, is published by the Cabinet Office at https://www.gov.uk/guidance/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed.*
- *BS ISO/IEC 27001 provides a flexible system for identifying information security risks and choosing controls to address them.*
- *BS ISO/IEC 27017 adapts BS ISO/IEC 27001 to address security controls in the specific context of cloud services.*
- *BS 67000 provides practical guidance and tools for increasing city resilience.*
- *PAS 7040 provides a systematic approach for the creation, deployment and operation of trustworthy networked sensors. The approach is applicable outside of the manufacturing sector to sensors installed during the construction and maintenance of built assets.*

5 People and process recommendations (B)

*COMMENTARY ON CLAUSE **5 (B)***

This clause describes four key recommendations for smart community suppliers to meet in respect of the key business processes, roles and skills that they bring to bear in their engagement with the community authority:

(B1)	*Smart community contracting*
(B2)	*Collaborative governance*
(B3)	*Skilled, empowered and integrated teams*
(B4)	*Agile delivery across the product lifecycle*

*As in Clause **4**, each recommendation is described below using the same common table format.*

5.1 Smart community contracting (B1)

*COMMENTARY ON **5.1 (B1)***

BS ISO 37106 recommends that smart community leaders ensure that their procurement and contracting policies be aligned with the following smart contracting principles.

- ***Focus on procuring business outcomes:** specify what the supplier should achieve, not how it should achieve it (in general, this includes procuring services, not assets).*
- ***Build open data into all procurements:** be clear that all data are to be owned by the community, not the supplier, or establish clear requirements for the supplier to make data available via open standards and fair, reasonable and non-discriminatory terms.*
- ***Incentivize innovation and collaboration:** ensure that contractual arrangement encourages collaboration with others to create new social and economic impact, and the sharing of common community assets.*
- ***Avoid supplier lock-in**, by integrating interoperability requirements into all ICT procurement, using off-the-shelf products and open standards wherever possible, and factoring in the costs of exit from the outset.*

These principles aim to ensure that community contracts with external suppliers act as enablers rather than blockers for successful smart community initiatives, facilitating innovation and community-wide integration.

Smart community suppliers should embed smart contracting principles within: their model contracts; the individual contracts that they negotiate with specific community administrations; and their day-to-day business processes for delivering data products or services.

This means, in particular:

a) **outcome focus:** contracts should include Key Performance Indicators and payment milestones linked to ethical delivery of outputs for users of the product or service and, where appropriate, to social, economic and environmental outcomes for the community;

b) **shareable data**: contracts should include provisions ensuring that all data produced under the contract is:

1) owned by the community authority; and
2) discoverable, interoperable and re-usable as open data or securely-shareable data (using common data formats and standardization) as specified in recommendations **4.5.3** and **4.5.4;**

c) **openness and collaboration**: contracts should:

1) facilitate integrated team working between the supplier, the client and the broader supply chain, by establishing clear rules and standards for a common data environment within which all parts of the supply chain will securely share project-related data throughout the contract lifecycle;
2) clearly set out the basis on which any new digital or physical assets created through the contract will be made available for re-use by other community stakeholders; and
3) adopt open contracting principles, by publishing data through the life of the contract.

d) **no lock-in**: contracts should set out a clear basis for exit, including provisions for ensuring transfer (to the community authority or to an alternative supplier nominated by the authority) of all data and other assets needed to maintain supply of a data service and provisions for accountability, responsibility and redress.

Suppliers should claim their level of conformity to **5.1** in line with the criteria in Table 8 and as illustrated in the illustrative scorecard in Annex A.

Table 8 – Smart community contracting (B1) – Compliance levels

1. Initial	The supplier does not embed any of the smart contracting principles (outcome focus, open data, openness and collaboration, no lock-in) in its contracts with community authorities.
2. Partially fulfilled	The supplier embeds at least one of the four smart contracting principles (outcome focus, open data, openness and collaboration, no lock-in) in its contracts with community authorities.
3. Fulfilled	The supplier embeds all four smart contracting principles (outcome focus, open data, openness and collaboration, no lock-in) in its contracts with community authorities.
4. Improving	As at Level 3. In addition, the supplier arranges external audits of its contracts to give assurance to its community clients that they are compliant with all smart contracting principles.
5. Sustainably optimizing	As at Level 4. In addition, the supplier implements regular contract review mechanisms in conjunction with its community clients, aimed at reviewing performance against the strategic intent of the smart contracting principles and identifying opportunities for improvements to the commercial and contractual relationship.

INFORMATIVE – Additional resources for B1

- *BS ISO 37106:2018, guidance note [B4], sets out recommendations to city leaders on the overall procurement framework needed to support smart city development.*
- *BS 10754-1 specifies measures for improving the trustworthiness of systems, software and services. It is intended to be a widely applicable approach that can be customized for any organization and software.*
- *PAS 185 gives additional guidance on taking a security-minded approach in respect of all personally-identifiable or otherwise sensitive data in a smart city context.*
- *Guidance to local authorities on technological and digital procurement is published by the Local Government Association at https://www.local.gov.uk/National-technological-and-digital-procurement-category.*
- *Model contracts that embed smart recommendations have been published by the UK Government Crown Commercial Service (CCS):*
  - *Model Services Contract (2014) applicable for contract value of £10m or more https://www.gov.uk/government/publications/procurement-policy-note-0414-model-services-contract.*
  - *PPN 06/14 Short form terms and conditions for goods and services https://www.gov.uk/government/publications/procurement-policy-note-0614-short-form-terms-and-conditions.*
- *The Open Contracting Data Standard (OCDS) enables disclosure of data and documents at all stages of the contracting process by defining a common data model: https://standard.open-contracting.org/latest/en/.*
- *A number of standards help suppliers demonstrate to clients that they maintain high levels of quality across all their contracting and delivery processes, notably BS EN ISO 9001, Quality management systems – Requirements and BS 95009, Public sector procurement – Generic requirements for organizations providing products and services.*

5.2 Collaborative governance (B2)

*COMMENTARY ON **5.2 (B2)***

Collaborative governance is essential for smart communities. BS ISO 37106 recommends an overall framework for cross-sectoral leadership and governance on a community-wide basis that is designed to "ensure clear accountabilities for the delivery and ongoing monitoring of every intended outcome."

PAS 184 sets out a good practice framework for leadership and governance at the level of an individual smart community project.

Smart community suppliers should work with the community authority to establish clear, effective and collaborative governance mechanisms for the delivery of data products and/or services, and of the intended outcomes from those products and services. In particular, suppliers should meet the following recommendations and claim their level of conformity to these criteria in line with Table 9.

a) **Top-level project sponsorship:** a senior and empowered supplier representative is accountable for the security and success of the data product and/or service, and participates in a joint governance board throughout the duration of delivery.

b) **Team integration:** the supplier, the broader supply chain and the client-side team from the community authority, wherever appropriate, including user representatives, collaborate as an integrated team. This includes:

   1) establishment of a common data environment, in which all members of the supply chain securely share data, workflows and collaboration tools; and

   2) collaborative risk and issue management, whereby the supplier openly shares risk and issue registers with the community authority, working closely with the authority to identify and manage any risks to successful delivery of the data products or services and to achievement of their desired outcomes.

c) **Regular client contact and progress reviews against performance measures:** the supplier allows for and plans in regular progress reviews to ensure delivery remains on track against agreed key performance indicators and milestones, providing all necessary management information to enable effective review of progress.

Suppliers should claim their level of conformity to **5.2** in line with the criteria in Table 9 and as illustrated in the illustrative scorecard in Annex A.

Table 9 – Collaborative governance (B2) – Compliance levels

1. Initial	The supplier lacks the necessary governance processes and procedures to drive successful delivery. There is no clear locus of accountability at senior level within the supplier, and the work of the supplier's team is disconnected from related work by the client-side team in the community authority.
2. Partially fulfilled	The supplier implements clear and documented governance processes to drive successful delivery in collaboration with the community authority.
3. Fulfilled	As at Level 2. In addition, these governance processes include: • top-level project sponsorship by a senior and empowered supplier representative who is accountable for security and success of the project, and participates in a joint governance board throughout the duration of delivery; • team integration between the supplier, the community authority and the broader supply chain, including use of a common data environment and shared risk and issue management; and • regular client contact and progress reviews against agreed KPIs that are SMART (specific, measurable, achievable, relevant, time-bound).
4. Improving	As at Level 3. In addition, the supplier has adopted an appropriate good practice standard for project management (such as PRINCE2 Agile).
5. Sustainably optimizing	As at Level 4. In addition, the supplier provides management information on the status and performance of the project to the community authority in real-time through digital dashboards, accessible over multiple devices.

INFORMATIVE – Additional resources for B2

- *BS ISO 37106:2018 guidance note [B2] sets out recommendations to city leaders on an overall framework for smart city governance.*
- *PAS 184:2017 guidance note [B1] sets out recommendations on how to apply this approach to an individual project.*
- *More broadly, there is a wide range of project and programme management methodologies and good practice to draw on in designing appropriate governance arrangements, such as:*
  - *PRINCE2: Project In Controlled Environments (updated 2017);*
  - *PRINCE2 Agile;*
  - *PMBOK: The Project Management Body of Knowledge (v6 2017);*
  - *Managing Successful Programmes (MSP); and*
  - *Agile Project Management (APM).*

5.3 Skilled, empowered and integrated teams (B3)

*COMMENTARY ON **5.3 (B3)***

For smart communities to prosper it is essential for communities to create and deploy teams of people that have the capabilities and capacity to bring ambitious community visions and strategies to life, optimizing the use of both people power and supporting technologies. PAS 184 provides a checklist of critical success factors for smart city projects, and in relation to teams and skills these include:

- *mapping out the skills needed to deliver the smart community project, and establishing clear plans for acquiring and maintaining them;*
- *ensuring that the roles, responsibilities and lines of accountability for all people involved in delivering the project are clear; and*
- *establishing effective mechanisms to maximize social and economic impact from all the skills available across the partners involved in delivery of the smart community project.*

5.3.1 General

Smart community suppliers should meet the following recommendations and claim their level of conformity to these criteria in line with Table 10.

5.3.2 Skills mapping and management

The supplier should have clear and documented processes for:

a) establishing a team structure that:
   1) brings together the appropriate mix of skills and capabilities that is needed to deliver the community authority's objectives; and
   2) ensures all roles and work responsibilities are clearly defined and articulated, with the interfaces to and dependencies with the community authority clearly mapped from the beginning.

b) ensuring that team roles are filled with appropriately skilled, trained and empowered people;

c) personnel security, including the development of security management skills and maintenance of an appropriate and sustainable security culture;

d) managing the team as an integrated and cohesive whole, even where team members might be drawn from different organizations across the supply chain;

e) incentivising the team to meet community goals through appropriate objectives, community feedback, performance management and rewards;

f) evolving the team and its training, as necessary, through different phases of the agile delivery process (for example, early delivery phases might require more focus on analysis of user needs, whereas further down the line there will be greater focus on quality assurance and performance management); and

g) managing skills as individuals leave or join the team.

5.3.3 Establishing a set of core responsibilities

As part of their broader skills mapping and managing work (see **5.3.2**), the supplier should ensure that the following four core responsibilities, as a minimum, are delivered by appropriately skilled and empowered people throughout the lifecycle of the engagement with the community:

a) outcomes ownership (this responsibility should be taken by a senior representative from the supplier);

   NOTE 1** This senior representative has overall accountability within the supplier organization for helping the community authority client ensure that the data product or data service delivers its intended business benefits. The outcomes owner has ultimate responsibility for the quality, performance, security and impact of the product or service, and for ensuring that all necessary business processes are followed. The outcomes owner participates in contract governance with the community authority at the highest level, including acting as a point of escalation for the delivery teams. As such, the outcomes owner is responsible for delivering the recommendations of **5.2.

NOTE 2 *In projects or programmes following PRINCE2 methodologies, the outcomes owner will have the role of "Senior Supplier".*

b) product management;

NOTE 3 *This responsibility ensures that the product or service as a whole is developed in ways that respond effectively and securely to user needs and business recommendations. They lead development of the vision for the product or service, and marshal all the resources needed to bring that vision into reality.*

c) delivery ownerership; and

NOTE 4 *This responsibility manages all the processes required to give the client and the outcomes owner assurance that the project will be delivered securely, on time and in budget. This includes leading on delivery of* ***5.2*** *(which covers establishment and management of a common data environment, shared risk and issue management processes, and regular reporting against agreed KPIs).*

d) data custodianship.

NOTE 5 *This responsibility ensures that all data within the project is securely managed as a discoverable, re-usable asset. While many team members might have a role in data management, the data custodian takes overall accountability for ensuring data conforms to* ***4.4*** *and* ***4.5****.*

NOTE 6 *These four responsibilities are not intended to capture every role needed for successful development and delivery of data products and data services. (Depending on the nature of the product or service, other necessary roles might include user researchers, content designers, developers, accessibility experts, business analysts, web engineers, data scientists, quality assurance and testing experts and so on.) Rather, these four are a minimum core that are essential in all cases to ensure alignment with the smart community principles and critical success factors set out in BSI smart city publications.*

NOTE 7 *These responsibilities are not all necessarily full-time roles, and not all necessarily taken by different people (that is, for a smaller project one person with the right skill set might take multiple responsibilities). The key is that these responsibilities are effectively resourced to meet the needs of the project.*

Suppliers should claim their level of conformity to **5.3** in line with the criteria in Table 10 and as illustrated in the illustrative scorecard in Annex A.

Table 10 – Skilled, empowered and integrated teams (B3) – Compliance levels

1. Initial	The supplier has not clearly defined the roles and responsibilities within their delivery team and how these relate to relevant related roles within the community authority and broader supply chain.
2. Partially fulfilled	The supplier has clear and documented processes covering at least some of the following: • team structure; • ensuring team roles are filled with appropriately skilled, trained and empowered people; • personnel security, including the maintenance of an appropriate and sustainable security culture; • managing the team as an integrated and cohesive whole across organizational boundaries; • incentivising the team to meet community goals through appropriate objectives, community feedback, performance management and rewards; • evolving the team and its training, as necessary, through different phases of the agile delivery process; and • managing skills as individuals leave or join the team.

Table 10 – Skilled, empowered and integrated teams (B3) – Compliance levels *(continued)*

3. Fulfilled	The supplier has clear and documented processes covering all of the following: • team structure – including at least four core responsibilities: – outcomes ownership; – product management; – delivery management; and – data custodianship. • ensuring team roles are filled with appropriately skilled, trained and empowered people; • personnel security, including the maintenance of an appropriate and sustainable security culture; • managing the team as an integrated and cohesive whole across organizational boundaries; • incentivising the team to meet community goals through appropriate objectives, community feedback, performance management and rewards; • evolving the team and its training, as necessary, through different phases of the agile delivery process; and • managing skills as individuals leave or join the team.
4. Improving	As at Level 3. In addition, the supplier uses a recognised good practice standard of relevance to their business to support their work on skills management (such as SFIA or IIP, Investors in People), using appropriate digital tools to document and manage the processes involved.
5. Sustainably optimizing	As at Level 4. In addition, the supplier shares the outputs of its skills management tools with the community authority, enabling a joint process of review to drive continuous service improvement.

INFORMATIVE – Additional resources for B3

- *PAS 183 gives further details on roles for data management across a smart city, including how the data custodian role inter-relate with these.*
- *SFIA (Skills Framework for the Information Age) provides a model for describing and managing competencies for ICT professionals for the 21st century, and is intended to help match the skills of the workforce to the needs of the business: https://www.sfia-online.org/en.*
- *IIP (Investors in People) is a standard for people management, offering accreditation to organizations that adhere to the Investors in People Standard. In 2017 this organization transitioned from the UK government into a Community Interest Company. More details are available at https://www.investorsinpeople.com/.*

5.4 Agile delivery across the product/ service lifecycle (B4)

*COMMENTARY ON **5.4 (B4)***

PAS 184 recommends that smart community projects take an agile approach to delivery of digital products and services, in order to ensure that these are developed in ways that:

- *are tightly focused on meeting user needs;*
- *take an iterative, phased approach that starts small, takes stock of lessons learned and then scales up gradually; and*
- *minimizes risks of failure or under-delivery associated with "big bang" approaches to delivery.*

Smart community suppliers should meet the following recommendations.

a) **Use proven agile methodologies to develop data products and data services.** In particular, suppliers should follow the approach as per bullets 1) – 5):

1) **Discovery:** a short phase in which the supplier researches user needs (including both end users and internal users within the local authority), explores the wider context-of-use (including the needs of non-users impacted by the project), finds out what it should be measuring, and explores technological or policy-related constraints.

2) **Alpha:** a short phase in which the supplier prototypes solutions for users' needs – testing with a small group of users or stakeholders, and getting early feedback about the design of the service.
3) **Beta:** the supplier is now developing against the demands of a live environment, understanding how to build and scale while meeting user needs – and releasing a version to test in public.
4) **Live:** the supplier iteratively improves the product or service, reacting to new needs and demands, and meeting targets set during its development.
5) **De-commissioning:** even the best product or service might eventually need to be de-commissioned (either because it reaches a natural retirement point or because evaluation shows it is not delivering the expected impacts), and the supplier should manage this with the same care and user focus as went into building and maintaining it.

b) **Quality assurance and continuous improvement during live operations.** During the live phase of the product or service, the supplier should operate management processes designed to ensure high levels of quality and to drive continuous improvement.

Suppliers should claim their level of conformity to **5.4** in line with the criteria in Table 11 and as illustrated in the illustrative scorecard in Annex A.

Table 11 – Agile delivery across the product/service lifecycle (B4) – Compliance levels

1. Initial	The supplier has no clear and documented process for managing development, operation and eventual de-commissioning of its products and services.
2. Partially fulfilled	The supplier uses clear and documented processes for managing either: • the development of human-centric data products and data services using agile methodologies; or • quality assurance, trustworthiness, security and continuous improvement of the product or service during live operations.
3. Fulfilled	The supplier uses clear and documented processes for managing both: • the development of human-centric data products and data services using agile methodologies; and • quality assurance, trustworthiness, security and continuous improvement of the product or service during live operations.
4. Improving	As at Level 3. In addition, the supplier has adopted appropriate good practice standards to support these processes[A)] and has clear processes for establishing when and how the product or service might need to be retired.
5. Sustainably optimizing	As at Level 4. In addition, the supplier is able to demonstrate clear and quantified evidence of the benefits it is delivering to users through continuous improvement.

[A)] For example PRINCE2 Agile in the development phase, and BS EN ISO 9001 or BS ISO/IEC 20000-1 during business-as-usual operations.

INFORMATIVE – Additional resources for B4

- *The Government Service Design Manual [3] gives extensive advice on how to manage agile development of public services, drawing on agile methodologies such as those from:*
  - *PRINCE2 Agile; and*
  - *Agile Project Management (APM).*
- *BS EN ISO 9241-210, Human-centred design processes for interactive systems, provides guidance both on how to put user needs and experience at the centre of the design process, and also how to ensure that the design process addresses needs of non-user stakeholder groups.*
- *PAS 184 gives detailed guidance on how to develop smart city products and services in ways that apply iterative, agile methodologies not just to the product itself but to the broader business mode and operating model through which it can successfully be deployed at city-wide scale.*
- *PAS 185 gives additional guidance on taking a security-minded approach in respect of all personally-identifiable or otherwise sensitive data in a smart city context.*
- *BS EN ISO 9001 is the international standard that specifies requirements for a quality management system (QMS). Organizations use the standard to demonstrate the ability to consistently provide products and services that meet user and regulatory requirements.*
- *BS 10754-1 specifies measures for improving the trustworthiness of systems, software and services. It is intended to be a widely applicable approach that can be customized for any organization and software.*
- *BS ISO/IEC 20000-1 is the international standard that specifies an integrated process approach when the service provider plans, establishes, implements, operates, monitors, reviews, maintains and improves a service management system (SMS). This is closely linked to ITIL processes.*
- *ITIL (the IT Infrastructure Library) is a service management framework, providing guidance to service providers on the provision of services and on the processes, functions and other capabilities needed to support services. It is structured around four functions (service strategy, design, transition and operation) and contains 26 processes.*

6 Compliance

This PAS sets out a total of eleven recommendations:

- Seven product recommendations as described in Clause **4;**
- Four people and process recommendations as described in Clause **5.**

For each of these recommendations, Clauses **4** and **5** describe levels of compliance on a 1 – 5 maturity scale, on which Level 3 equates to "recommendation fulfilled" and Levels 4 and 5 then define successive levels of over-performance. These performance levels can be expressed as scores which can then be averaged to express compliance with this PAS overall. (Levels 1 – 5 correspond to score 1 – 5.)

Given the very wide range of products, services, suppliers and industry sectors covered by the scope of this PAS, not all of the recommendations will be equally important in every case. For a supplier to be conformant with this PAS as a whole, it is therefore not essential to achieve Level 3 on every one of the eleven recommendations. Rather, a conformant supplier should achieve:

- a minimum score of at least three on Clause **4.7** (Security and resilience);
- a minimum score of at least two on every other recommendation; and
- an average score of three or above on both the cluster of product recommendations and the cluster of people and process recommendations.

NOTE *To determine the average score for a cluster of recommendations, add up all the individual scores for the recommendations in that cluster, then divide by the number of recommendations in the cluster. For example, a supplier scoring Level 2 on* ***5.1****, Level 3 on* ***5.2*** *and* ***5.3****, and Level 4 on* ***5.4*** *would score an average of Level 3 for People and Process recommendations.*

Annex A presents an illustrative scorecard of how an individual supplier might be scored against this framework.

Annex A (informative)
Illustrative compliance scorecards

*The scorecard below shows an illustrative scorecard for an individual supplier assessed against this PAS. This supplier is compliant with PAS 186 because it meets the criteria described in Clause **6** Compliance:*

- *a minimum score of at least three on Clause **4.7** (Security and resilience);*
- *a minimum score of at least two on every other recommendation; and*
- *an average score of three or above on both the cluster of product recommendations and the cluster of people and process recommendations.*

Table A.1 – Illustrative scorecard for a compliant supplier

(A) Product and Service recommendations	Level 1	Level 2	Level 3	Level 4	Level 5	Score
A1 Alignment with community vision						4
A2 User segmentation and insight						3
A3 Inclusivity						3
A4 Citizen-centric approach to privacy and identity management						3
A5 All data managed as an asset, with open standards and clear policies to facilitate ethical data innovation by stakeholders:						4
a) Owned and authoritative						*5*
b) Discoverable and interoperable						*4*
c) Re-usable						*3*
d) Fit-for-purpose						*4*
e) Used in an ethical manner						*4*
A6 Integration of digital and physical assets						4
A7 Security and resilience						3
AVERAGE SCORE FOR PEOPLE AND SERVICE REQUIREMENTS:						3.43

See Annex B, Table B2 for details on how the individual scores for A5a) to A5e) combine into an overall score for Recommendation A5

(B) People and Process recommendations	Level 1	Level 2	Level 3	Level 4	Level 5	Score
B1 Smart community contracting						4
B2 Collaborative governance						3
B3 Skilled, empowered and integrated teams						3
B4 Agile delivery across the product/service lifecycle						3
AVERAGE SCORE FOR PEOPLE AND PROCESS REQUIREMENTS:						3.25

The scorecard below shows an illustrative scorecard for a second supplier. Although the average scores are the same as in Table A1 (3.43 for product and service, and 3.25 for people and process), this supplier may not claim conformity to this PAS. This is because the supplier is assessed at Level 1 for A7 Security and resilience – and a minimum score of two is required on every individual recommendation to claim compliance with PAS 186 as a whole. The supplier would still be able to claim compliance on the other individual recommendations.

Table A.2 – Illustrative scorecard for a non-compliant supplier

(A) Product and Service recommendations	Level 1	Level 2	Level 3	Level 4	Level 5	Score
A1 Alignment with community vision						4
A2 User segmentation and insight						5
A3 Inclusivity						3
A4 Citizen-centric approach to privacy and identity management						3
A5 All data managed as an asset, with open standards and clear policies to facilitate ethical data innovation by stakeholders:						4
a) Owned and authoritative						*5*
b) Discoverable and interoperable						*4*
c) Re-usable						*3*
d) Fit-for-purpose						*4*
e) Used in an ethical manner						*4*
A6 Integration of digital and physical assets						4
A7 Security and resilience						1
AVERAGE SCORE FOR PRODUCT AND SERVICE REQUIREMENTS:						3.43

See Annex B, Table B2 for details on how the individual scores for A5a) to A5e) combine into an overall score for Recommendation A5

(B) People and Process recommendations	Level 1	Level 2	Level 3	Level 4	Level 5	Score
B1 Smart community contracting						4
B2 Collaborative governance						3
B3 Skilled, empowered and integrated teams						3
B4 Agile delivery across the product/service lifecycle						3
AVERAGE SCORE FOR PEOPLE AND PROCESS REQUIREMENTS:						3.25

Annex B (normative)
Compliance levels for 4.5 (A5)

*COMMENTARY ON **ANNEX B***

*Clause **4.5** recommends that all data be managed as an asset, with open standards and clear policies to facilitate ethical data innovation by community stakeholders. As set out in Clause **4**, this over-arching recommendation consists of five main sub-recommendations: smart community suppliers ensure that all community data they produce and/or manage is:*

a) owned and authoritative;

b) discoverable and interoperable;

c) re-usable;

d) fit-for-purpose; and

e) used in an ethical manner.

Compliance levels for each of these sub-recommendations are described in Table B.1.

Table B.2 shows how a supplier's scores on these five individual components combine to give an overall assessment of the supplier's level of maturity against this A5 set of recommendations.

Table B.1 – Clause 4.5 – Compliance levels

	Level 1	Level 2	Level 3	Level 4	Level 5
Owned and authoritative data	The data product or service has no clear accountable owner within the supplier. Multiple data users keep and manage duplicate versions of the data.	A named data custodian takes personal responsibility for the compliance, quality and re-usability of the data. The data custodian has undertaken a baseline assessment of current data quality, documenting known quality issues.	As at Level 2. In addition: • The data custodian engages with users of the data to understand and document their recommendations for the data, and manages a plan to close any gapsbetween current and required quality levels. • Where the data product is duplicated within other community stakeholders, the data custodian works with these stakeholders and the community administration to agree a specific owner and authoritative source which all stakeholders can access directly.	As at Level 3. In addition: • feedback mechanisms have been established to allow data users to request quality improvements; and • where the data product has been agreed as single authoritativesource of data for community stakeholders, it can now be accessed directly by all relevant users and is accompanied by clear service level agreements.	As at Level 4. In addition, there is clear evidence that effective processes are in place to enable user-driven continuous improvement of the data product or data service.

Table B.1 – Clause 4.5 – Compliance levels *(continued)*

	Level 1	Level 2	Level 3	Level 4	Level 5
Discoverable and interoperable data[5)]	The data is: • inaccessible by third parties because it is not published on the web or currently shared with other organizations.	The data is: • published on the web or shared with external organizations via an API; and • Accompanied by some metadata describing the data.	The data is: • published on the web in an open, machine-readable format or via an API; • accompanied by a rich set of metadata; and • described using relevant standardized vocabularies to populate terms in key metadata fields.	As at Level 3. In addition, • published data: ✓ is available for bulk download; ✓ has a schema; ✓ uses URIs / URLs to enable others easily to link their data to it; • schema and metadata are signposted in relevant national and international data hubs to facilitate discoverability; and • APIs conform to the Hypercat standard (PAS 212); • all standardized vocabularies used have been mapped against the PAS 185 Smart City Concept Model in order to facilitate cross-sectoral interoperability.	As Level 4. In addition: • the data is linked to other relevant data to provide context; and • automated validation systems are in place to check data compliance with the schema and to preserve integrity of links.

[5)] The maturity levels for 'Discoverable and Interoperable Data' draw on the Five Star deployment scheme for open data developed by Sir Tim Berners-Lee, but expanded to cover shared data as well as open data.

Table B.1 – Clause 4.5 – Compliance levels *(continued)*

	Level 1	Level 2	Level 3	Level 4	Level 5
Re-usable data	The data is not accompanied by any policy describing the basis on which it might be re-used.	The existence of the data is published on the web, along with details of the terms and conditions on which third parties may access and re-use the data.	The data is made available for re-use by third parties under clear, fair, ethical and documented policies. These policies are based on one of the following: • an open data licence; or • fair, reasonable and non-discriminatory licence terms.	As at Level 3. In addition, the licence terms follow widely-used standard models such as: • the UK Open Government Licence; and • the Creative Commons licences.	As at Level 4. In addition, there is clear evidence that effective processes are in place to enable user-driven continuous improvement of the terms and conditions surrounding re-use of the data product or data service.
Fit-for-purpose data	There are significant quality problems with the data and this is not documented.	There are significant quality problems with the data and this is documented and explained to data users.	Data quality is fit for current purposes, and the supplier can evidence this against documented user recommendations for data quality. Any remaining quality issues are documented and explained.	As at Level 3. In addition, the supplier actively engages with potential data users to understand how improvements to data quality could support new use cases for the data.	Data quality is fit for purpose for both existing and potential uses of the data, based on clear, documented user-research and feedback.

Table B.1 – Clause 4.5 – Compliance levels *(continued)*

	Level 1	Level 2	Level 3	Level 4	Level 5
Data is used in an ethical manner	The supplier has not established and documented processes aimed at ensuring that collection, analysis and use of its data is managed in accordance with a clear ethical framework.	The supplier has established and documented processes aimed at ensuring that collection, analysis and use of its data is managed in accordance with a clear ethical framework.	As at Level 2. These processes cover, as a minimum: • **Fair data collection:** datasets are representative of the relevant population, with processes in place to minimize, mitigate and disclose any potential biases within the dataset; • **Fair use of data:** systems to analyse and make use of data are routinely tested to avoid both algorithmic and human bias; and • **Transparency and accountability:** the basis on which algorithms process data to make decisions is made public (subject to any necessary restrictions to protect privacy and intellectual property rights); and affected individuals are offered simple ways to request human intervention or challenge an automated decision.	As at Level 3. In addition, these processes are supported by systematic deployment of a widely-adopted data ethics diagnostic tool, such as the UK Government's "Data Ethics Workbook" or the Open Data Institute's "Data Ethics Canvas"	As at Level 4. In addition, there is clear evidence that effective processes are in place to enable stakeholder feedback and continuous improvement to the supplier's data ethics practices.

Table B.2 – Clause 4.5 – Compliance levels – scoring

1. Initial	The supplier's average score across all five components is 1.5 or lower.
2. Partially fulfilled	The supplier's average score across all five components is higher than 1.5 but Level 3 has not been reached.
3. Fulfilled	The supplier scores at least Level 3 on each of the five components.
4. Improving	The supplier scores at least Level 3 on each of the five components. In addition, the average score across all components is 3.5 or more.
5. Sustainably optimizing	The supplier scores at least Level 3 on each of the five components. In addition, the average score across all components is 4.5 or more.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7000-6, *Design management systems – Part 6: Managing inclusive design – Guide*

BS 8878, *Web accessibility – Code of practice*

BS 10754-1, *Information technology – Systems trustworthiness – Part 1: Governance and management specification*

BS 18477, *Inclusive service provision – Requirements for identifying and responding to consumer vulnerability*

BS 67000, *City resilience – Guide*

BS 95009:2019, *Public sector procurement – Generic requirements for organizations providing products and services*

BS EN 301549, *Accessibility requirements for ICT products and services*

BS EN ISO 9001, *Quality management systems – Requirements*

BS EN ISO 9241-210, *Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems*

BS EN ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

BS EN ISO/IEC 27018, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

BSI ISO 37100:2016, *Sustainable cities and communities – Vocabulary*

BS ISO 37101, *Sustainable development in communities – Management system for sustainable development – Requirements with guidance for use*

BS ISO 37106:2018, *Sustainable cities and communities – Guidance on establishing smart city operating models for sustainable communities*

BS ISO 37153, *Smart community infrastructures – Maturity model for assessment and improvement*

BS ISO/IEC 20000-1, *Information technology – Service management – Part 1: Service management system requirements*

BS ISO/IEC 27001:2017, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO/IEC 27017, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

BS ISO/IEC 27701:2019, *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines*

BS ISO/IEC 29184, *Information technology – Online privacy notices and consent*

BS ISO/IEC 30182, *Smart city concept model – Guidance for establishing a model for data interoperability*

BS ISO/IEC 38505-1, *Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data*

ISO/TS 8000-1, *Data quality – Overview*

PAS 180, *Smart cities – Vocabulary*

PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*

PAS 184, *Smart cities – Developing project proposals for delivering smart city solutions – Guide*

PAS 212, *Automatic resource discovery for the Internet of Things – Specification*

PD 8100, *Smart cities overview – Guide*

PD ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

PD ISO/IEC Guide 71, *Guide for addressing accessibility in standards*

PD ISO/IEC TR 24028, *Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence*

PD ISO/IEC TR 38505-2, *Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management*

PD ISO/TR 37121, *Sustainable development in communities – Inventory of existing guidelines and approaches on sustainable development and resilience in cities*

Other publications

[1] GREAT BRITAIN. Data Protection Act 2018. London: The Stationery Office.

[2] General Data Protection Regulation EUROPEAN COMUNITIES. 95/46/EC. Council Directive 95/46/EC of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).[6)]

[3] *Government Service Design Manual.* Available from: https://www.gov.uk/service-manual

[4] ETSI TR 103 455 v0.84 (2019-11), *Human Factors (HF); Smart cities and communities standardization for citizens and consumers.* Available from: http://www.etsi.org/standards-search

[5] G3ict's Smart Cities for All Toolkit. Available from: https://smartcities4all.org/#toolkits

Further reading

IoT SECURITY FOUNDATION. *IoT Security Compliance Framework*, Creative Commons, 2016. Available from: https://www.iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

IoT SECURITY FOUNDATION. *Secure Design Best Practice Guides*, Creative Commons, 2018. Available from: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf

IoT SECURITY FOUNDATION. *Vulnerability Disclosure Best Practice Guide*, Creative Commons, 2016. Available from: https://www.iotsecurityfoundation.org/wp-content/uploads/2017/01/Vulnerability-Disclosure.pdf

IoT SECURITY FOUNDATION. *HOME IoT Security Architecture and Policy*, Creative Commons, 2016. Available from: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf

IoT SECURITY FOUNDATION. *ENTERPRISE IoT Security Architecture and Policy*, Creative Commons, 2018. Available from: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf

[6)] Available at <https://gdpr-info.eu/>

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Relations
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscription Support
Tel: +44 345 086 9001
Email: subscription.support@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com