PAS 2017:2014

Guide for digital infrastructure to enable access to digital content for small-scale commercial enterprises

Department for Culture Media & Sport

bsi.

Publishing and copyright information

ISBN 978 0 580 80584 4

ICS 35.240.60

Publication history

First published January 2014

Contents

Foreword

This PAS was sponsored by the Department for Culture, Media & Sport (DCMS). Its development was facilitated by the British Standards Institution (BSI) and it was published under licence from The British Standards Institution. It came into effect on 31 January 2014.

Acknowledgement is given to Mike Perry of the Building Research Establishment (BRE) as the Technical Author for this PAS.

BSI also wishes to acknowledge the following organizations that were involved in the development of this PAS as members of the steering group:

- British Telecom (BT);
- Building Research Establishment (BRE);
- Core Cities
- Department for Culture, Media & Sport (DCMS);
- Digital Birmingham;
- Global Smart Transformation Limited (GST Ltd.);
- Health over Internet Protocol (HoIP);
- Intellect Technology Association;
- Nexans;
- OpenHub Smart Homes Limited;
- Qmara Limited.

Wider comments from other interested parties were invited by BSI. The expert contributions made by the organizations and individuals consulted in the development of this PAS are gratefully acknowledged.

The PAS process enables a specification 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.

Relationship with other publications

PAS 2017 aligns with the structure given in PAS 700:2009 and references it where relevant.

PAS 2016:2010 was sponsored by the Department for Business, Innovation & Skills (BIS) in order to provide guidance regarding digital communications infrastructures to, and within, new build domestic dwellings. The concept of PAS 2017 was to address a similar issue, to follow on from PAS 2016 and provide guidance for the provision of digital infrastructure and data access within commercial premises designed to be used by small-scale commercial enterprises. The different approaches taken by PAS 2016 and PAS 2017 and the slight differences in terminology is an indication of the rapid changes occurring within the digital communications industry and the development of work around smart city systems.

Use of this document

As a guide, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any 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.

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 this PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific Acts:

- The Health and Safety at Work etc. Act 1974 [1];
- The Private Security Industry Act 2001 [2].

Introduction

We live in challenging times. Across the globe the economic climate is uncertain. A direct consequence of this economic uncertainty is a dramatic increase on resource constraints, particularly on public service resources of all types.

These challenges are particularly acute in dense urban communities (cities) because of the intensity and complexity of demands.

Overcoming these challenges requires new ways of thinking and new ways of delivering resources, such as public services. Traditional delivery methods are becoming outdated and unsustainable. Other physical and social resources, e.g. energy, transport, social care, are also using outdated delivery methods.

The daily operations of a modern city are founded on data and information flows. This is particularly important where supply is required to meet demand. For historical reasons, each resource delivery stream has developed, and is presently operated, as an independent resource channel, having little or no interaction with related resource channels. The data and information about, for example, energy, is locked into an energy silo.

Digital infrastructure provides an opportunity to make radical changes in the way that contemporary and future communities monitor, manage and control resource consumption. By providing small-scale commercial enterprises with adequate digital infrastructure and access to digital content, there is the potential to make data openly accessible. Subsequently, it would be possible to freely transmit the data and information flows that are currently locked into different delivery silos across a variety of services and businesses. This city (or community-wide) concept of digital infrastructure is discussed in Clause **4** and Clause **5** in PAS 2017.

Opening access to different data and information flows could result in:

- the integration of service delivery (this is increasingly important in complex physical and social city environments);
- the engagement of the public sector with the private sector in the delivery and maintenance of public services (thereby divesting the public purse of the cost liability of delivering public services while potentially improving private sector efficiency); and
- the development of new service and content offerings, driven by the commercial sector. Such new service and content offerings could be innovative delivery vehicles for public services and enable commercial activity. In particular, this could be beneficial for small-scale commercial enterprises (see **5.1**, Note 1), which form part of the small to medium-sized enterprise (SME) sector.

Such outcomes align with the aim of city authorities to drive economic recovery and reduce the cost of public service delivery in the socio-economic and geographic areas for which they are responsible. The concept of access to open data is referred to as an integrated data platform.

Clause **6** of PAS 2017 provides recommendations about the type of digital infrastructure small-scale commercial enterprises need to have in place in their working environment (wherever this might be) to provide effective communications with the integrated data platform and their market delivery processes.

This page deliberately left blank.

1 Scope

PAS 2017 provides guidance on:

- the digital infrastructure and enabling access to digital content required to support commercial activities for small-scale commercial enterprises;
- how to assess the requirements of the digital infrastructure and access to digital content to support small-scale commercial enterprise operations and smart city digital systems;
- the need for open-access systems and interoperability between such systems;
- standards and supporting documentation for digital infrastructure and digital service systems.

This PAS is not intended to:

- provide guidance on digital infrastructure within the premises of commercial organizations having more than 20 people;
- provide guidance on digital infrastructure and accessing digital content within residential premises;
- provide guidance on entire smart city digital systems.

The primary audience groups for this PAS are:

- local authorities and other public service specifiers who have a major role in defining policy and in developing smart city systems;
- private sector owners and investors in business parks and industrial centres;
- specifiers of digital systems, developers, builders and installing and commissioning contractors, who are responsible for delivering, installing and commissioning digital infrastructure and enabling access to digital content.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensible for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7671, *Requirements for electrical installations*

PAS 700:2009, *Provision of ICT facilities and services in workplaces – Specification*

IEEE 802.11b, *Wireless network specification*

3 Terms and definitions

For the purpose of this PAS the following terms and definitions apply.

3.1 cabling

infrastructure constructed from cables (made of copper, silica or plastic) used for the transmission of digital data and digital content

NOTE 1 *At the time of publication, copper is the dominant medium for cabling, although silica and plastic optical fibre are increasingly used, and are preferred where high bandwidth is required, e.g. video-on-demand services.*

NOTE 2 *"Cabling" might also be referred to as "cabled media".*

3.2 data catalogue

collection of data and information collated in near real time, in response to end user enquiries on specific issues

NOTE 1 *Data catalogues are not static repositories, but are formed in response to user enquiries and exist for the life time of the enquiry. This eliminates the need to maintain large, expensive and static databases. Data catalogues are an output of digital platforms. They are distributed intelligence, which is a core component of smart city (or community) systems.*

NOTE 2 *Real time collation of data and information is unlikely to be achieved, due to the scale of operations, although digital operations might be able to achieve a close time-frame.*

3.3 data warehouse

central repository of open access data and information, created by hosting or integrating information from different sources

NOTE *A data warehouse is an essential component of an integrated data platform, and is the source of digital content.*

3.4 digital infrastructure

framework required for digital communications allowing reception of data and information services delivered externally, and for the transmission of digital data and information

3.5 integrated data platform

virtual platform serving a community area, such as a city, through which digital infrastructure and digital data used and provided by public services, industries and private businesses can be shared and exchanged

NOTE *The integrated data platform forms the basis of a smart city system. See also Clause* ***5****.*

3.6 internet service provider (ISP)

commercial supplier of digital infrastructure, digital content and access to digital content

3.7 interoperability

ability of different application functions to use shared information in a consistent way

NOTE 1 *This requires interworking as a building block as well as coexistence, and adds business rules, processes, and security provisions that enable applications to be joined together.*

NOTE 2 *Interoperability is a methodology that can give end users the confidence to buy and specify products from different companies both in the present and in the future, knowing that they operate together. Achieving this requires several phases of standardization to ensure that there is integration from the physical connectors to the way systems function. There are three phases of integration, which are: co-existence, interworking and interoperability.*

NOTE 3 *CWA 50560 is an interoperability framework specification for services to the home.*

3.8 open data

data that is freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control

3.9 smart city system

integrated system of digital infrastructure and access to digital content to monitor, manage and control physical and social resource

NOTE 1 *These systems are capable of a diverse range of functions, including providing a context to encourage and enable economic activity – particularly for small-scale commercial enterprises.*

NOTE 2 *A "smart city" system is often also referred to as a "future city" or "next generation" system.*

4 City (and community) resources for the support and development of data information flows

Cities and communities, on a national and international level, are considered to be primary drivers of economic activity, in terms of both growth and recovery. In the current economic climate, cities – UK cities in particular – are not performing economically as well as expected.

While cities can be used as a primary driver of economic growth, they cannot achieve this result in vacuo. Without an effective suite of delivery mechanisms to channel physical and social resources to a city's population, the effectiveness of the city as an economic unit is likely to be impaired. The economic performance of a city is inextricably linked to its physical and communications infrastructures, and the delivery of physical and social resources through these infrastructures. Therefore, a holistic (or whole systems) approach, in the form of an integrated data platform (see Clause **5**), needs to be adopted within a city to help it achieve increased operational efficiency, optimize the use of resources and deliver maximum benefits both in the present and in the future.

A holistic approach can help to address challenges regarding economic performance, environmental sustainability, health and well-being, and mobility and transport in the following ways.

- *Economic performance*. In the UK, and internationally, creating a context to support economic recovery and growth is seen as the primary challenge, particularly in response to the need to create employment growth. Achieving economic turnaround is not an isolated issue for any one city, but has to be delivered in the face of a global economic crisis. Routes to economic recovery are being sought, including finding new ways to leverage cities' financial strength and developing new ways to encourage business growth.
- *Environmental sustainability*. This is a fundamental and international challenge. At the current levels of consumption, taking into account the forecast growth in population (and therefore the rate of consumption of resources), many resources are predicted to become unsustainable in the next few decades.[1)] One example of this is energy. The future viability of any city requires a resilient and affordable energy supply, while also meeting obligations to reduce carbon emissions and provide clean (low carbon) energy. Simultaneously satisfying all these requirements is an exacting challenge.
- *Health and well-being*. Almost every city by definition is cosmopolitan; each city has a mixed socio-economic demographic. Many cities in the UK, and internationally, face the problem of how to improve general conditions including, for example, social and economic deprivation in parts of the city and the impact of this on the health and well-being of the city's population. The demand on financial, social and community resource that is needed to address this challenge is, in many cities, unsustainable.
- *Mobility and transport*. This challenge includes how to utilize digital infrastructure to support distributed working (i.e. remote and home working); the core of the theme is connectivity. Many cities have inadequate transport networks and traffic congestion. Achieving affordable connectivity within the city is challenging for a significant proportion of many cities' populations, thereby impacting on work, leisure and recreation, which are central to any city's economic performance and environmental sustainability.

One possible way of responding to these challenges and enabling resource and information-sharing is through the creation of an integrated data platform.

[1)] Further information regarding environmental sustainability can be found from the United Nations Economic and social council commission for sustainable development [3].

5 Integrated data platform

5.1 General

The central concept behind an integrated data platform is to deliver substantial additional benefits to all community areas, such as a city, by extending the application of existing digital infrastructure and digital data. This enables resources to be shared and costs to be reduced. The digital infrastructure and digital data used by public services (e.g. transport and healthcare), a variety of industries and private businesses, have the potential to be incorporated into an integrated data platform, enabling them to exchange data and to provide each other with access to open data. By forming part of an integrated data platform, small-scale commercial enterprises could also reap its benefits (see **5.2** for further information).

NOTE 1 *A small-scale commercial enterprise comprises 20 people or fewer.*

Traditionally within cities, services such as health and transport have operated in silo, without factoring in the impact of related resource issues. An important principle of the operation of an integrated data platform, and interoperability, is to provide open access to both public and private data which is currently locked away within such services. Much of this data is within the domain of public service providers (particularly the local authorities) and other major service providers within the city. This integrated data platform forms the basis of a smart city system, which is discussed further in **5.3**.

NOTE 2 *While extensive discussion of smart cities systems is outside the scope of this PAS, a series of smart cities standards are currently in development, including PAS 181 regarding a smart city framework, and PAS 180, which provides a common vocabulary and shared understanding of smart cities definitions.*

In summary, the integrated data platform is a radical approach affecting the implementation of digital infrastructure and access to digital content, and involving the individual with the collective. When delivering, installing and commissioning digital infrastructure and access to digital content, the potential to integrate them with an integrated data platform should be taken into account, wherever practicable. A new philosophy is also needed for the management, monitoring and control of resources. The foundations of this new approach are the integration of different delivery mechanisms and access to open data.

5.2 Data integration and small-scale commercial enterprises

Digital infrastructure and access to digital content, when combined with best practice business processes and tools, can enable a small-scale commercial enterprise to function more effectively than if the enterprise relies solely on its own limited digital infrastructure and access to digital content. Incorporating a small-scale commercial enterprise into an integrated data platform can also aid the development of the integrated data platform. Consequently, this can create a mutually beneficial environment for public and private sectors and potentially aid the creation of new forms of public value, new service models, and new business growth.

The open data accessible to a small-scale commercial enterprise through an integrated data platform could provide the small-scale commercial enterprise with the possibility of realizing sustainable and cost effective resource and service delivery in both public and private sectors.

A small-scale commercial enterprise could derive a number of benefits from the implementation of an integrated data platform.

An integrated data platform has the potential to:

a) create an environment to aid market growth and enable the development of a smart city system, its services, technologies and applications;

b) be:
   1) a vehicle for commercial engagement with public sector service delivery, driving new business models and services, and offsetting public sector cost liabilities; and
   2) a mechanism through which to carry out predictive analysis to inform timely decisions to drive improvements in service outcomes, thus improving the quality of life for citizens;

c) drive innovation and increase value by application of commercial and public data assets;

d) tailor response services to meet individual requirements and deliver services 24 hours a day, seven days a week;

e) enable:
   1) improved service delivery transparency, effective integration within and between service delivery channels, avoiding duplication of information and improving the cost effectiveness of service delivery; and
   2) greater efficiency of resources using multiple delivery channels, reducing waste and redundant activity, and driving improvements in public sector productivity.

5.3 Model for public and private service integration and delivery

The concept of a smart city system, as shown in the Figure 1 delivery model, illustrates the underlying principles for integrated service delivery through the integrated data platform. Realizing these principles in practice requires the identification of a specific model for service and content delivery.

The integrated data platform shown in Figure 2 illustrates a model that is designed to integrate selected data on demand from multiple sources in order to drive new forms of service delivery, engage with, and support, entrepreneurial activity.

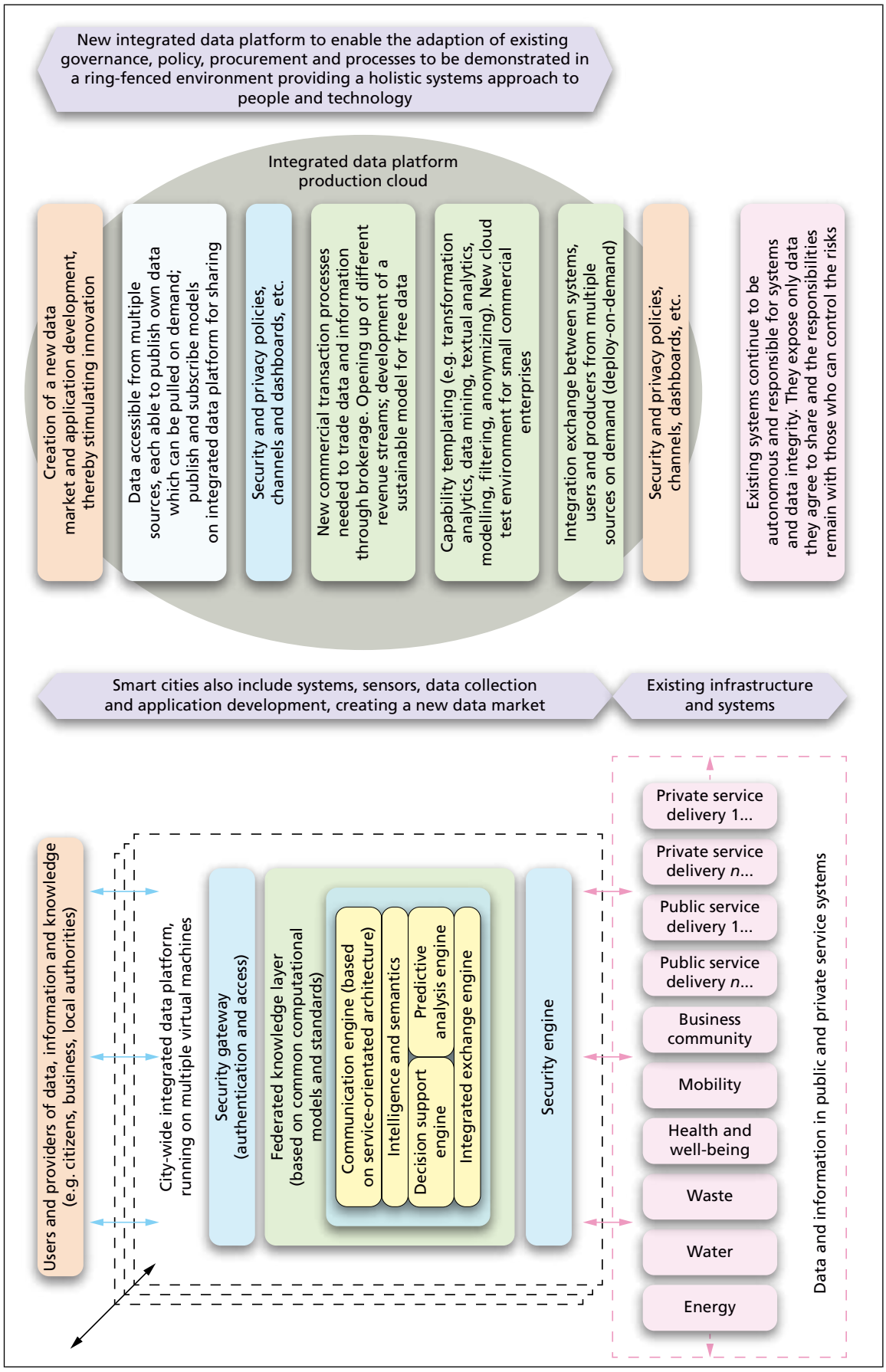
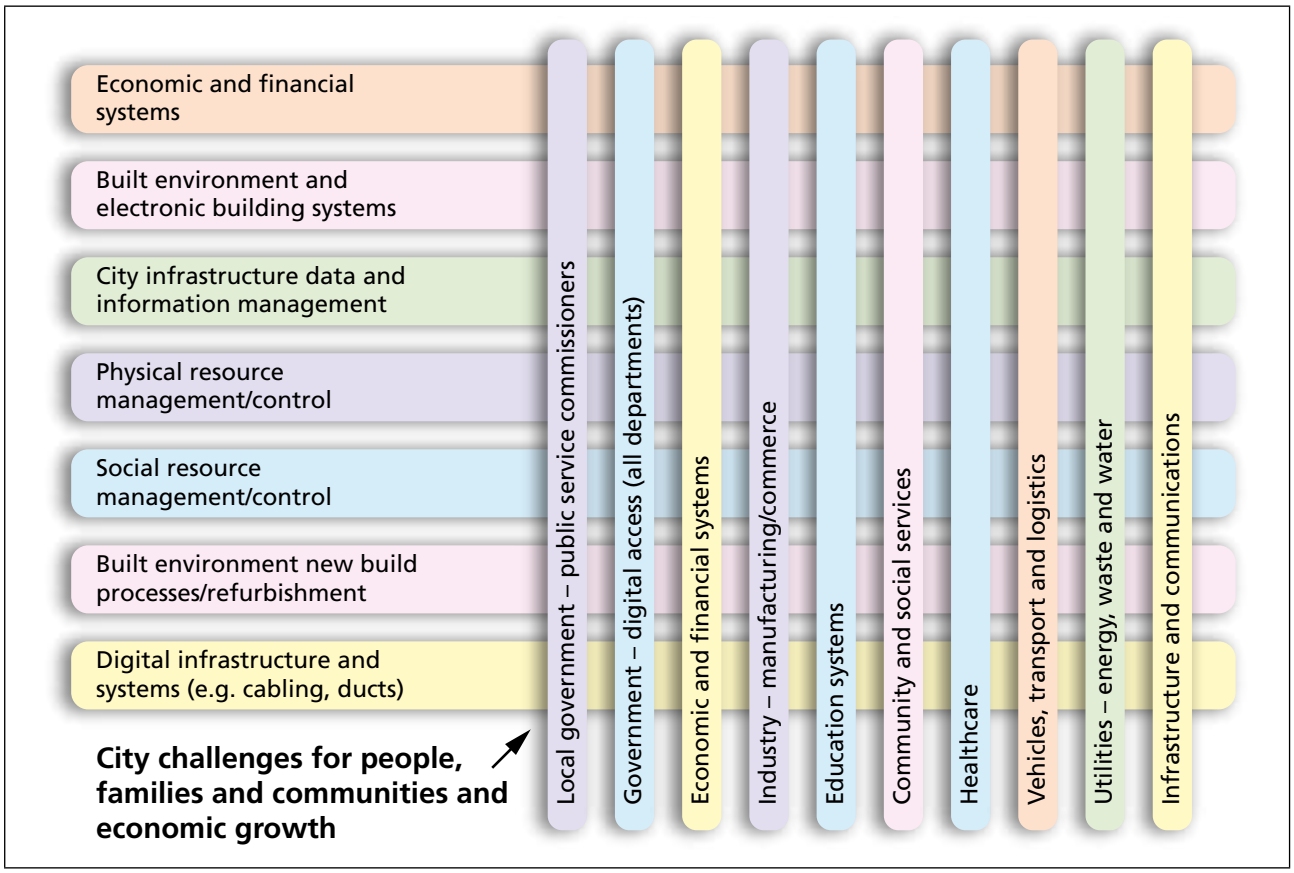


Figure 1 – A model for public and private service delivery

Figure 2 – A simplified view of the central elements of public and private service delivery in smart city and community systems



NOTE *The vertical elements of the diagram are examples of different, existing service delivery channels that operate in a city. It is important to note that this list is not complete, and is likely to change and expand in the future. The horizontal elements of the diagram are the diverse parts of the physical digital infrastructure that enable integration between the different service channels. It is through these communication channels that content and services can be delivered. The need for alternative delivery mechanisms within and between the different service delivery channels creates a major opportunity for the small-scale commercial enterprises, both directly in supporting service delivery through the infrastructure, and through service innovation; for example, small-scale commercial enterprises developing applications to support market delivery of content and services.*

The integrated data platform can provide a gateway for information from sources both internal to, and external to, smart city systems. The information can be accessed in real-time and transactions can be carried out in which data can be pulled on demand and not stored but forwarded directly to the requested destination. This innovative approach has several major advantages over the traditional data warehouse and data catalogue approaches.

Some of these advantages are as follows.

- Data has a large overhead of maintenance to keep updated and its integrity maintained. As part of the integrated data platform, data is maintained by those that are best placed to do so and have a direct interest in the quality of the data. By passing the data in near real-time, the data life is the responsibility of the receiver, not the intermediary.
- Large data storage facilities are not required and the development of a commercial revenue stream can be implemented easily via the connection of the data provider and the data receiver in exactly the same way as a commercial internet transaction is carried out.
- The uncertainty of what data to collect, store and maintain can be avoided as submissions and requests are self-defining and data maintenance is left to those who have personal interest in the integrity and maintenance of the data. Published information availability and subscribed requests can require the system to be scaled as the market develops.
- The platform can deliver security and anonymized data by use of aggregation and compilation techniques. This can provide re-assurance to those parties involved in opening their data to wider audiences.
- A controlled open application development environment can allow innovation to flourish, while light touch checks and measures can be implemented for end users.
- The architectural concept provides a distributed, scalable and flexible integrated data platform approach to the issues of hardware, software, application, communication and database provision.

The concept of the integrated data platform aims to provide an engine to drive managed transformation across all city systems over time. Implementation is most likely to occur in a phased and incremental fashion, beginning with a city's highest priority areas, including, for example, energy, public transport, assistive living.

When implementing an integrated data platform, historical data should be accessed. This can provide some contextual background and reasons for its application. Ideally, such information can also increase the effectiveness of the integrated data platform through providing information for correlation, analysis and pattern detection. Where this results in more reliable predictions or deductions being made, it can provide a base on which to build optimal city models and affect continual process improvement. Access to structured data storage architecture and strategy is essential for this process.

5.4 Conceptual model of city information flows

The key element in progressing integrated data platforms is developing an understanding of the new modes of business operation to support sustainable delivery of the wide range of societal and built environment services that can be delivered through the infrastructure.

New forms of commercial operation are likely to be required for the new mode of operation. These include businesses operating on commercially sustainable principles, that have due consideration for the social and environmental cost, and return benefit to the small or large, local or distributed communities that they serve.

The principles of this type of model are likely to be a central pillar of the new delivery mechanisms for societal services.

6 Digital infrastructure for small-scale commercial enterprises

6.1 General

Effective communications have always played a pivotal role in underpinning the development of business concepts. Digital infrastructure provides a widely available and cost effective backdrop, enabling efficient communications. In this way it has the potential to help small-scale commercial enterprises (especially start-ups) to establish and develop themselves. There are a number of essential activities where access to digital infrastructure can support the development, maintenance and growth of a business concept.

Some examples of essential activities for a small-scale commercial enterprise are given in the following list.

a) Developing a business concept:
   1) carrying out research and development to establish a business concept, either as a product or solution;
   2) where required, carrying out patent searches, and registering a patent for the product or solution;
   3) enabling validation of the proposed business concept prior to launch;
   4) building collaborative partnerships, where applicable.

b) Accessing services and information to prepare the business concept for launch, for example:
   1) financial services;
   2) identifying and resolving legal issues;
   3) supporting services;
   4) matching recruitment needs against locally available skills and capabilities.

c) Setting-up and launching the business:
   1) establishing an online presence (including a web site) as a base of operations;
   2) supporting back-office processes (e.g. procurement essential to the business);
   3) putting in place processes to collect payments from clients.

d) Marketing the business by using the digital infrastructure to:
   1) broadcast publicity and raise awareness about the services or products of the small-scale commercial enterprise;
   2) carry out market research;
   3) connect with potential clients.

e) Implementing innovative approaches for developing the business concept (e.g. crowd sourcing).

f) Implementing customer relations systems.

g) Maintaining and expanding business operations.

h) Supporting mobile and flexible working.

One of the key challenges for a small-scale commercial enterprise is raising awareness of the company and its business offering. Without this visibility the business concept is not viable: there can be no interaction with the market place and potential clients if these clients are not aware of the company. Digital infrastructure can provide a medium through which a small-scale commercial enterprise can raise its market profile.

It is important to note that the digital infrastructure, while being vitally important as a medium for broadcasting and collating information and data, carries no content. The content has to be created and acted on by the small-scale commercial enterprise. The success of the small-scale commercial enterprise remains vested in factors such as the validity of its business concept and its ability to successfully interact with the market place.

6.2 Scale of communications facilities

Subclause **6.3** uses a four layer model to give guidance on the implementation of digital (information and communications technology, ICT) facilities and for accessing digital content in commercial premises.

The four layers of facilities and requirements for accessing digital content are as follows:

- Layer 1: Building;
- Layer 2: Infrastructure;
- Layer 3: Basic services;
- Layer 4: Extended services.

This four layer model provides a framework for assessing and implementing the different requirements of small-scale commercial enterprises.

NOTE *PAS 700 is a specification for the provision of information and communications technology (ICT) facilities and services in workplaces. The four-layer model for implementing ICT facilities given in PAS 2017 aligns with the four-layer approach given in PAS 700.*

Table 1 provides a summary of the minimum digital infrastructure and digital facilities recommendations for small-scale commercial enterprises.

Table 1 – Summary of digital infrastructure and facilities recommendations

Digital infrastructure element/facility	Recommended?
Layer 1: Building	
Provision for generic telecommunications cabling	No
Lighting	Yes
Raised access flooring	No
Electricity supply	Yes
Building security	Yes
Availability of workspace	Yes
Radio frequency transmittance	Yes
Layer 2: Infrastructure	
Provision for generic telecommunications cabling	No
Network security	Yes
Wireless networking	No
Availability of an internet connection	Yes
Working environment	Yes
Layer 3: Basic services	
Service and functionality level agreements (e.g. SLAs)	Yes
Provision of ICT-ready work areas	Yes
Telephone services	Yes
Internet services	Yes
Technical support	Yes [A)]
Layer 4: Extended services	
Extended telephone services	No
Extended internet services	Yes
Video conferencing	No
Data backup service	Yes
Print services	No
Public wireless networking	No
Co-location facilities	No
Email services	Yes
Back-up power supply	No
Disaster recovery facilities	Yes

[A)] This might be provided by a third party.

NOTE *This table was adapted from PAS 700:2009, Table 1.*

6.3 Internal digital infrastructure for small-scale commercial enterprises

6.3.1 Layer 1: Building

6.3.1.1 General

There are assumed to be two broad categories of small-scale commercial enterprise premises:

a) single room premises, generally for start-up companies (e.g. a single office over a shop); or

b) small rented commercial space greater than a single workspace, capable of supporting up to approximately five-person workspaces (e.g. space in an incubator unit).

Most of the discussion regarding resource delivery and the integration of data is concerned with businesses operating from single workspaces. For small-scale commercial enterprises operating in larger workspaces for up to approximately five people, then the discussion regarding the conceptual model of information flows (see **5.4**) is likely to be more applicable.

6.3.1.2 The workspace

The physical workspace should be adequately spacious for the relevant business to be conducted. The office furniture, the distribution of ICT equipment and the installation of digital infrastructure should include provision for the following:

- lighting;
- heating;
- cooling;
- air quality; and
- air conditioning (where installed).

NOTE *Attention is drawn to the Health and Safety at Work etc. Act [1]. See also PAS 700.*

6.3.1.3 Power

An assessment of the electricity required by the small-scale commercial enterprise using the workspace should be undertaken. The supply of electricity to the workspace should be able to meet these power requirements. Electrical wiring should conform to BS 7671.

Where required, distribution boards and cables should be labelled for ease of identification.

6.3.1.4 Building security and safety

Security measures should be implemented in the working space to protect the physical security of the ICT facilities and digital communications infrastructure. These should include measures against fire, vandalism and criminal attack. The type of security measures to be implemented should be determined after carrying out an assessment of the risks and threats.

Examples of security measures that should be included are as follows:

- physical protection, e.g. secure locks, secure storage units (see BS EN 1047-1 and BS EN 1300);
- use of an intruder alarm system (see BS EN 50131-1 and PD 6662);
- CCTV surveillance (see BS EN 50131-1 and BS 8418); and
- access control system (see BS EN 50133-1) or manned security (see BS 7499).

NOTE *Requirements for security staff can be found in BS 7858. Attention is also drawn to the requirements for SIA licensing under the Private Security Industry Act 2001 [2].*

However, it should be recognized that prevention of loss of hardware is not always possible and that therefore the security of critical data should be considered (see **6.3.2.1** and **6.3.4.1**).

6.3.1.5 Availability of workspace

The following issues might need to be addressed when assessing a business case for a workspace.

a) Allowing adequate space for incoming utilities, including digital infrastructure, if this has not already been installed.

b) Obtaining the landlord's permission for installation work.

c) Constraints associated with the workspace where it forms part of a listed building.

d) The duration for which the workspace is available (the investment case for ICT and digital infrastructure could be negated if the tenancy period is too short).

e) Local risks (e.g. flooding, neighbouring heavy industry or construction work requiring access to off-site back-up facilities for the small-scale enterprise's business systems, information and data).

6.3.1.6 Radio frequency transmittance

Small-scale commercial enterprises are likely to make extensive use of wireless-borne digital transmissions. Therefore, those responsible for delivering, installing and commissioning digital infrastructure and enabling access to digital content should check the reliability of wireless signal reception in the workspace they are proposing to use and confirm it to be adequate for the purposes of the small-scale commercial enterprise before entering into any contractual agreements concerning leasing or renting of the workspace.

Where the transmission and reception of wireless digital transmissions is deliberately inhibited by the building owner or the internet service provider, written notification should be given to prospective lessees before any contractual agreements are signed.

6.3.2 Layer 2: Infrastructure

6.3.2.1 Network security

If the building is multi-tenanted, the building owner is often responsible for the network security within the building. Responsibility for the network security within the building should be confirmed in writing with the small-scale commercial enterprise.

The party responsible for network security within the building should continually review the network security at intervals prescribed and agreed with the small-scale commercial enterprise. Where network vulnerabilities (and wireless network vulnerabilities, see **6.3.2.2**) are identified, either as the result of a review or as the result of new information that becomes known by the responsible party, necessary measures should be undertaken by the responsible party to mitigate against, or eliminate, the vulnerability. The party responsible for the network security within the building should communicate with the tenants to ascertain, and meet, the security network requirements of the small-scale commercial enterprises. Reviews should also include consideration of any improvements that can be made. Wherever practicable, such improvements should be implemented.

In the case of single workspaces for use by small-scale commercial enterprises, the security provided by the company's internet service provider (ISP), combined with security systems installed in the business's ICT might be sufficient for most business communications. However, some organizations might also require confirmation that the end user's equipment meets the organization's security criteria.

It is the responsibility of the small-scale commercial enterprise to put adequate firewall and ICT security systems in place, and to check that these satisfy the requirements of the other users (commercial and non-commercial) with whom they communicate.

NOTE *Further information on information security and network security can be found in BS ISO 27001, BS ISO 27032, BS ISO/IEC 29192 (all parts), BS ISO/IEC 27033-2 and BS ISO/IEC 18028 (all parts).*

6.3.2.2 Wireless networks

Where the building owner or landlord provides a wireless network, it should conform to IEEE 802.11b as a minimum. As new vulnerabilities and risks are constantly emerging, the most up-to-date advice available at the time of implementation should be sought regarding appropriate security measures.

The party responsible for wireless network security within the building should continually review the network security at intervals prescribed and agreed with the small-scale commercial enterprise. Where wireless network vulnerabilities are identified, either as the result of a review or as the result of new information that becomes known by the responsible party, necessary measures should be undertaken by the responsible party to mitigate against, or eliminate, the vulnerability. The party responsible for the wireless network security within the building should communicate with the tenants to ascertain, and meet, the security network requirements of the small-scale commercial enterprises.

NOTE 1 *At the time of publication, the current advice is to secure the wireless network by a minimum of WPA2 encryption using a strong password with Wireless Protected Setup (WPS) capability turned off in the wireless access point configuration menus. (A strong password is one that cannot easily be guessed by an attacker. The length of a password, its complexity and unpredictability in terms of alphabetical, numerical and symbolic combinations determine its overall strength. However, it is important to note that other effective security controls against, for example, wiretapping, phishing and keystroke logging might also be necessary.)*

NOTE 2 *Information regarding cyber security, including wireless and network security and communications and electronic data security, can be found from the IASME Consortium website, http://www.iasme.co.uk, and the CESG website, http://www.cesg.gov.uk. PAS 555 is a specification for the governance and management of cyber security risk and might also be of interest.*

Where a small-scale commercial enterprise uses only mobile devices and ICT equipment connected wirelessly, this displaces the need for cabling.

NOTE 3 *Wireless networking is not functionally equivalent to cabled digital infrastructure. Wireless networks provide lower reliability of transmission, security and transmission rates. If the security network is intended for applications such as video transmission, the installation of cabled digital infrastructure might be preferred.*

6.3.2.3 Internet connectivity

The building owner or landlord should provide external network connectivity that is capable of delivering an internet connection and that conforms to PAS 700:2009, **7.4.2**, **7.4.3** and **7.4.4**.

NOTE 1 *The availability of an internet connection depends on a number factors, which can impact on the practicality of installing an internet link (see PAS 700).*

NOTE 2 *The lead time for installation of an internet connection can be significant.*

NOTE 3 *The cost of installing an internet connection might negate the value of the business case for the small-scale commercial enterprise proposing to use, rent or lease the single workspace.*

6.3.3 Layer 3: Basic services

6.3.3.1 Level of service

Where the single workspace is rented or leased to include internet connectivity, digital infrastructure facilities or ICT equipment, the level of service and level of functionality being provided should be stipulated in a written agreement(s) between the building owner, landlord or operator and the small-scale commercial enterprise.

NOTE *This might be in the form of a service level agreement (SLA).*

The full terms and conditions of the written agreement should be made available to the small-scale commercial enterprise before any contractual agreements are in place.

It is advisable that the written agreement includes:

- the specified functionality of the internet connectivity, digital infrastructure facilities or ICT equipment;
- the fees incurred for the use of the internet connectivity, digital infrastructure facilities or ICT equipment;
- the maximum lead times and time to attendance for the provision of all internet connectivity, digital infrastructure facilities or ICT equipment facilities and services;
- that in the case of a workplace that is ready to be occupied, the maximum lead time for the provision of the basic services given in **6.3.3** is one week from the date that the internet service provider accepts the order;
- the times during which the internet connectivity, digital infrastructure facilities and ICT facilities and services are available for use; and
- the minimum notification period for planned downtime.

6.3.3.2 Readiness of the single workspace area

If the single workspace is rented or leased as an ICT-ready workspace, then the services and facilities should be ready for use from the first day of occupation by the small-scale commercial enterprise, or a written agreement produced giving the lead time to achieve full operation.

6.3.3.3 Telephone services

The single workspace should be provided with at least one operational telephone point connected to the public telephone network, and a handset compatible for use with the telephone service.

The requirement for connection to the public telephone applies to both analogue and digital telephone points.

The telephone service should offer, as a minimum, direct dial to the single workspace, including from the public telephone network.

6.3.3.4 Internet services

If an internet connection is provided as part of a single work place agreement this may be provided through a telecommunications outlet, or by wireless network.

For the single workspace, the internet connection speed should be a minimum of:

- Download speed: 4 Mbps
- Upload speed: 1 Mbps

NOTE *It is important to select the external internet connection to meet the performance criteria specified in any SLA between the internet service provider and the small-scale commercial enterprise.*

6.3.3.5 Technical support

The small-scale commercial enterprise should be provided with access to technical support for the ICT equipment, digital infrastructure and the means for accessing the digital content they are using to operate their business. Such technical support is most likely to be remote technical support, and should, as a minimum, be available during the company's normal hours of operation.

6.3.4 Layer 4: Extended services

6.3.4.1 Data backup

It is recommended that small-scale commercial enterprises are provided with data backup facilities. These should include:

- local external hard drive backup of all business information and data; and
- off-site storage of all business information and data.

Off-site storage should be one or more of the following:

- online (i.e. cloud based);
- able to provide instant, always on access to stored data; or
- traditional data backup (i.e. tape or DVD may be used though this might require more thought and planning, to include, for example, sufficient backup storage and to provide backup storage in a different geographical location from the central data).

6.3.4.2 Disaster recovery

The small-scale commercial enterprise is recommended to have in place ICT and work place disaster recovery arrangements. The data backup facilities (see **6.3.4.1**), are a major component of these facilities; additionally, an alternative work place from which restored data backup can be accessed should be identified. These alternative facilities should enable full recovery within one working day.

NOTE *Requirements for ICT disaster recovery facilities can be found in PAS 700:2009,* ***8.11****.*

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 7499, *Static site guarding and mobile patrol services – Code of practice*

BS 7858, *Security screening of individuals employed in a security environment – Code of practice*

BS 8418, *Installation and remote monitoring of detector-activated CCTV systems – Code of practice*

BS EN 1047-1, *Secure storage units – Classification and methods of test for resistance to fire – Part 1: Data cabinets and diskette inserts*

BS EN 1300, *Secure storage units – Classification for high security locks according to their resistance to unauthorized opening*

BS EN 50131-1, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

BS EN 50133-1, *Alarm systems – Access and control systems for use in security applications – Part 1: System requirements*

BS ISO/IEC 18028 (all parts), *Information technology – Security techniques – IT network security*

BS ISO 27001, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO/IEC 27032, *Information technology – Security techniques – Guidelines for cybersecurity*

BS ISO/IEC 27033-2, *Information technology – Security techniques – Part 2: Guidelines for the design and implementation of network security*

BS ISO/IEC 29192 (all parts), *Information technology – Security techniques – Lightweight cryptography*

CWA 50560, *Interoperability framework requirements specification for service to the home (IFRS)*

PAS 180, *Smart cities – Vocabulary*

PAS 181, *Smart city framework – Guide to establishing strategies for smart cities and communities*

PAS 555, *Cyber security risk – Governance and management – Specification*

PAS 2016:2010, *Next generation access for new build homes – Guide*

PD 6662, *Scheme for the application of European standards for intrusion and hold-up alarm systems*

Other publications

[1] UNITED KINGDOM. Health and Safety at Work etc. Act 1974. London: The Stationery Office.

[2] GREAT BRITAIN. Private Security Industry Act 2001. London: The Stationery Office.

[3] UNITED NATIONS ECONOMIC AND SOCIAL COUNCIL. ENV/DEV/1206. Commission on sustainable development. Nineteenth session, second meeting. May 2011.[2)]

[2)] Available on: http://www.un.org/News/Press/docs/2011/envdev1206.doc.htm

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

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

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similarly for PASs, please notify BSI Customer Services.

Tel: +44 (0)845 086 9001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)845 086 9001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop**. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)845 086 9001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)845 086 9001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **http://shop.bsigroup.com/bsol**

Further information about British Standards is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

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

ISBN 978-0-580-80584-4