PAS 1192-5:2015

Specification for security-minded building information modelling, digital built environments and smart asset management

CPNI
Centre for the Protection of National Infrastructure

bsi.

Publishing and copyright information

ISBN 978 0 580 88257 9

ICS 91.010.01

Publication history

First published May 2015

Contents

List of figures

Foreword

This PAS was sponsored by the Centre for the Protection of National Infrastructure (CPNI). 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 May 2015.

Acknowledgement is given to the technical authors Alexandra Luck and Hugh Boyes, and to the following organizations that were involved in the development of this PAS as members of the steering group:

- Atomic Weapons Establishment
- BIM Technologies Alliance
- CESG
- Construction Industry Council
- Centre for the Protection of National Infrastructure
- Crossrail Ltd
- EC Harris LLP
- Engineering Construction Strategies Ltd
- FCO Services - part of the Foreign & Commonwealth Office
- Houses of Parliament (Parliamentary Estates Directorate)
- HS2
- The Institute of Asset Management
- Laing O'Rourke
- Metropolitan Police Service
- Ministry of Justice
- Mott MacDonald
- Network Rail
- NG Bailey
- Ove Arup and Partners Ltd
- University College London
- Co-opted

Acknowledgement is given to BSI technical committee IST/33 , IT – Security techniques for their participation in the PAS Steering Group.

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

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

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Information about this document

Copyright is claimed on the wedge element of Figure 1. Copyright holders are Mark Bew and Mervyn Richards.

Copyright is claimed on Figure 3. The copyright holder is Hugh Boyes.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is "shall".

Commentary, explanation and general informative material is presented in 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").

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.

Particular attention is drawn to the following specific regulations:

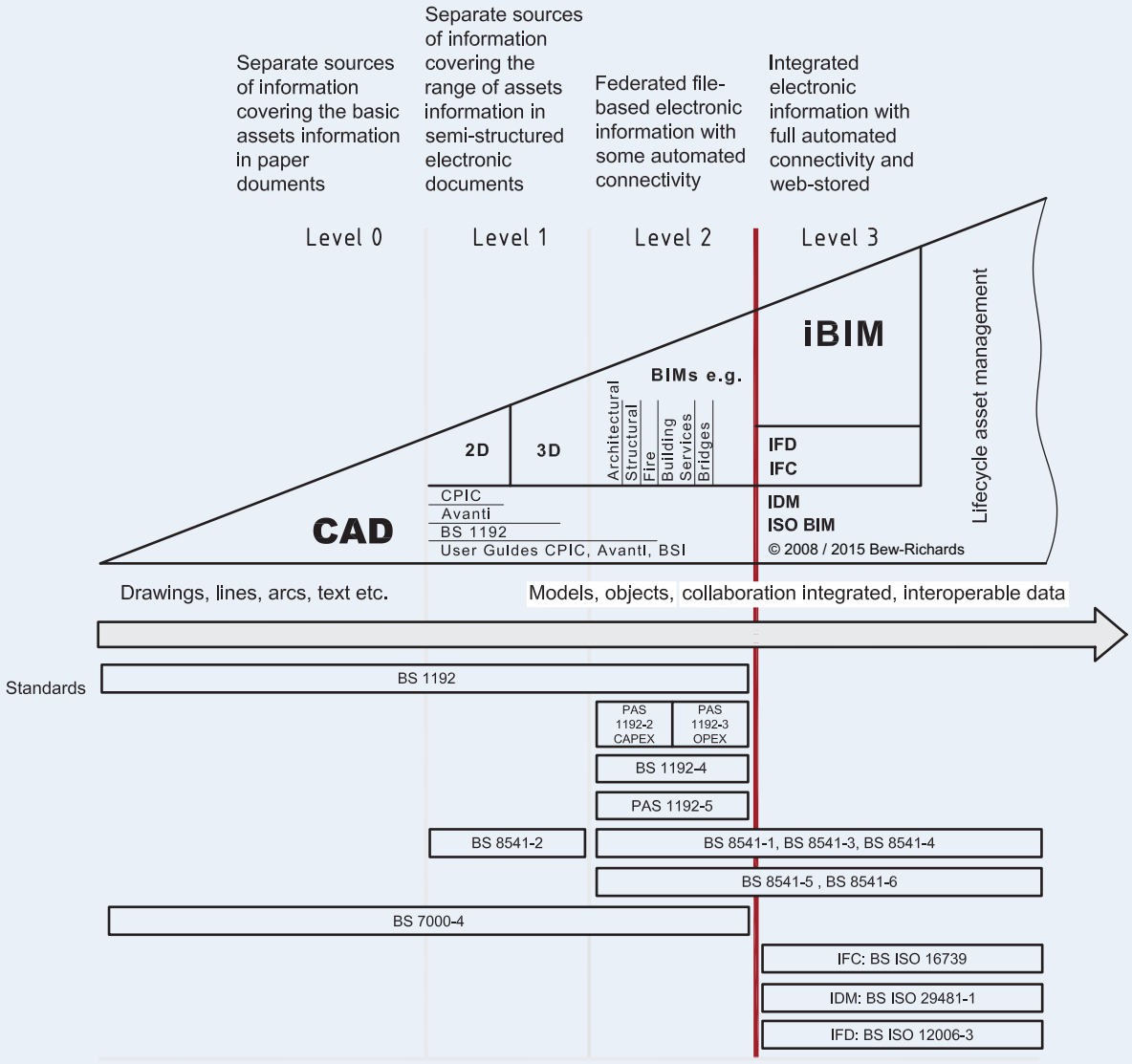
- Data Protection Act 1998 [1];
- Environmental information Regulations 2004 [2];
- Freedom of Information Act 2000 [3];
- Serious Organised Crime and Police Act 2005 [4];
- Official Secrets Act 1989 [5];
- Computer Misuse Act 1990 [6];
- Freedom of Information (Scotland) Act 2002 [7];
- Planning and Compulsory Purchase Act 2004 [8];
- Privacy and Electronic Communications Regulations 2003 [9];
- Public Records Acts 1958 and 1967 [10];
- Re-use of Public Sector Information Regulations 2005 [11].

Introduction

In May 2011, the UK Government published the Construction Strategy[1)] aimed at reducing the cost of public sector assets by up to 20% by 2016.

The strategy calls "for a profound change in the relationship between public authorities and the construction industry to ensure the Government consistently gets a good deal and the country gets the social and economic infrastructure it needs for the long-term". This is reinforced by the Industrial Strategy Construction 2025[2)], published in July 2013.

Figure 1 – BIM maturity levels



***NOTE** Copyright is claimed on the wedge element of Figure 1. Reproduction of this element and making products from it might infringe that copyright. Details of the copyright owners can be found in the Foreword.*

[1)] Available from https://www.gov.uk/government/publications/government-construction-strategy

[2)] Available from https://www.gov.uk/government/publications/construction-2025-strategy

PAS 1192-5 is a companion document to PAS 1192-2, PAS 1192-3 and BS 1192-4, and makes extensive reference to the definitions and concepts contained within them. Users are therefore encouraged to obtain copies of these documents which are summarized on http://shop.bsigroup.com/Navigate-by/PAS and are available as downloads. In common with these documents, PAS 1192-5 applies to both building and infrastructure assets and assumes a certain knowledge regarding building information modelling (BIM) and BS 1192:2007. However, the scope of PAS 1192-5 is wider than the concepts contained within the rest of the series, encompassing security-minded approaches to both digital environments and the management of new and existing built assets.

The built environment is experiencing a period of rapid evolution. The adoption of BIM and the increasing use of digital technologies in the management of assets throughout their life will have a transformative effect on the parties involved in their design, construction and management. Projects that are either developing new assets or solutions, or modifying or managing existing ones, will become much more collaborative in nature. This will be achieved by promoting more transparent, open ways of working, and through the sharing and use of both detailed models and large amounts of digital information.

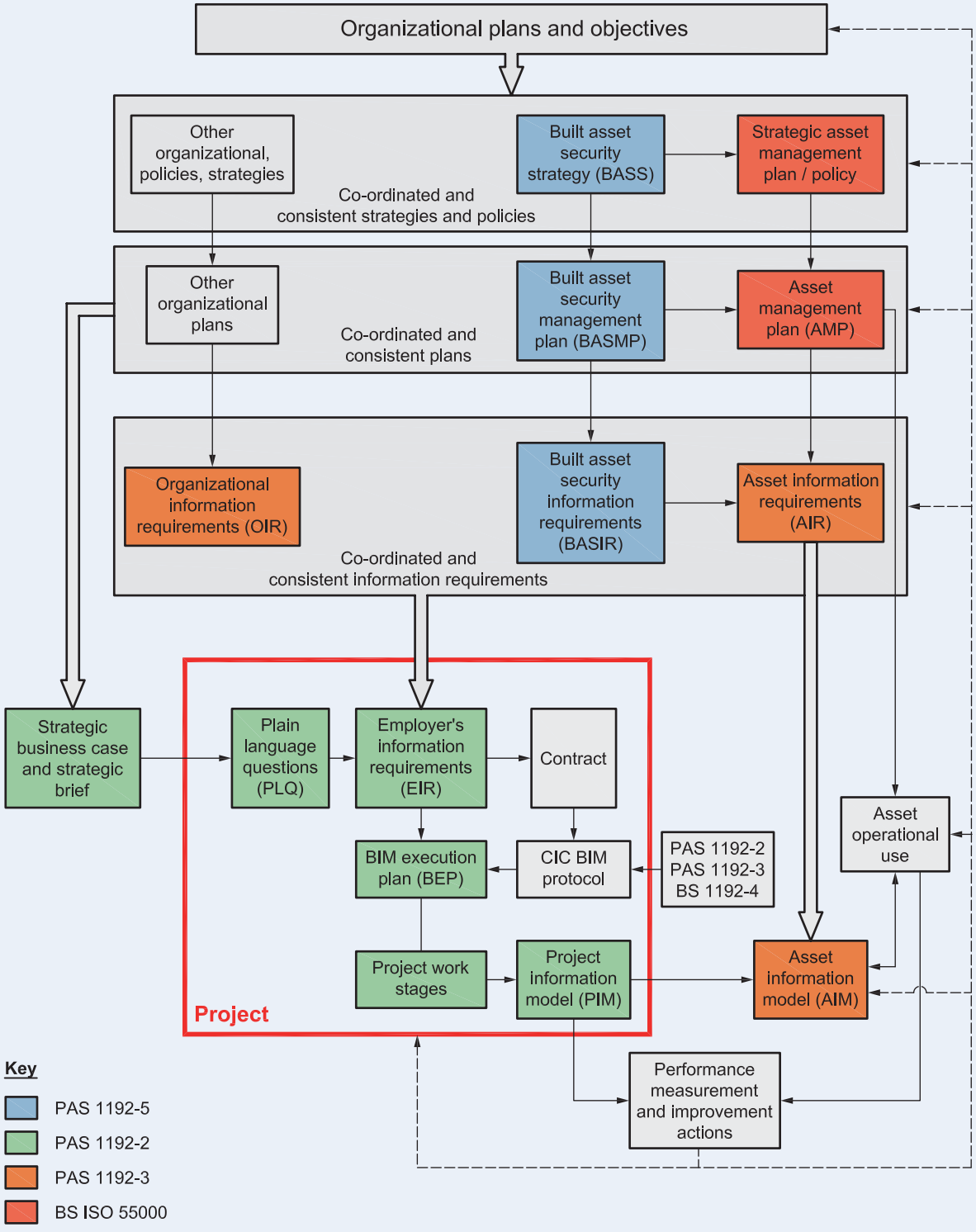
Digital built environments will need to deliver future fiscal, functional, sustainability and growth objectives, and will therefore impact on procurement, delivery and operational processes including far greater cross-sector collaboration. The increasing use of computer-based technologies will support new ways of working, such as the development of off-site, factory-based fabrication and on-site automation. Sophisticated cyber-physical systems will, using a combination of sensors and actuators, work in real-time to influence outcomes in the real world. They will be used to achieve benefits such as increases in energy efficiency and better asset lifecycle management by capturing real-time data about asset use and condition. These systems can already, and will increasingly, be found in transportation, utilities, infrastructure, buildings, manufacturing, health care and defence, and will interact as integrated cyber-physical environments, for example in the development of Smart Cities and Grids.

As a consequence of this increasing use of, and dependence on, information and communications technologies in the built environment, there is a need to address the inherent vulnerability issues, in particular to take appropriate and proportionate measures to:

- protect information about the location and properties of sensitive assets or systems not otherwise generally visible directly or through other sources;
- protect certain information pertaining to sensitive assets or systems, the location of which can be readily identified; and
- recognize and address where the aggregation or association of data, or an increase in the accuracy of the location of assets or systems could compromise the security or operation of a built asset.

This PAS provides a framework to assist asset owners and stakeholders in understanding the key vulnerability issues and the nature of the controls required to deliver the trustworthiness and security of digital built assets within the built environment. Its purpose is not in any way to undermine the collaboration upon which both projects utilizing digital technologies and asset management systems are centred, but to ensure that information is shared in a security-minded fashion. It encourages the adoption of an appropriate, proportionate, need-to-know approach to the sharing and publication of information about built assets that could be exploited by those with hostile or malicious intent. Figure 2 shows the integration of this security-minded approach with other strategic policies and plans, and with the information requirements for the digitally-enabled delivery, maintenance and operation of built assets.

Figure 2 – The integration of the security-minded approach



***NOTE** Developed by CPNI, Alexandra Luck and Hugh Boyes as part of the PAS 1192-5 development process.*

Implementation of the measures outlined in this PAS will assist in not only reducing the risk of the loss or disclosure of sensitive information which could impact on safety and security, but also on the loss, theft or disclosure of commercial information and intellectual property. Any such incidents can lead to significant reputational damage, impacting through lost opportunities and the diversion of resources to handle investigation, resolution and media activities, in addition to the disruption of, and delay to, day-to-day operational activities.

1 Scope

This PAS specifies requirements for the security-minded management of projects utilizing digital technologies, associated control systems, for example building management systems, digital built environments and smart asset management. It outlines security threats to information during asset:

- conception, strategy and briefing;
- procurement;
- design;
- construction;
- commissioning and handover;
- operation and maintenance;
- performance management;
- change of use/modification; and
- disposal/demolition.

It explains the need for, and application of, trustworthiness and security controls throughout a built asset's lifecycle (including the full project lifecycle) to deliver a holistic approach encompassing:

- safety;
- authenticity;
- availability (including reliability);
- confidentiality;
- integrity;
- possession;
- resilience; and
- utility.

This PAS addresses the steps required to create and cultivate an appropriate safety and security mindset and culture across many partners, including the need to monitor and audit compliance.

It provides a foundation to support the evolution of future digital built environments, for example intelligent buildings, infrastructure and smart cities, but does not detail technical architectures for their implementation. While the processes contained within it may be applicable to other data management systems, this PAS does not specifically address issues relating to these systems.

This PAS is intended for use by asset owners or, within a project utilizing digital technologies, the employer. It will also be of interest and relevance to those organizations and individuals employed by an asset owner and involved in the design, construction, maintenance and management of built assets, especially those who wish to protect their commercial or security-related information and intellectual property.

The approach outlined in this PAS is applicable to any built asset or portfolio of assets where asset information is created, stored, processed and viewed in digital form. It is also applicable to the capture of digital survey data as part of day-to-day asset management processes or in anticipation of a future project.