Introduction to **PAS 1192-5**:2015

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

National Protective Security Authority

bsi.

Introduction

PAS 1192-5:2015 is a specification for security-minded building information modelling (BIM), digital built environments and smart asset management. It details the approach to applying appropriate and proportionate measures to manage the security risks that affect a built asset, in whole or in part, asset data and information.

The adoption of BIM and the increasing use of digital technologies in the management of assets, whether buildings or infrastructure, will have a transformative effect on those involved in their design, building and management. It will do this by promoting:

- more transparent, open ways of working;
- cross-sector collaborative working and the sharing of information; and
- better asset lifecycle management by capture of data about its real-time use and condition.

PAS 1192-5 specifies the processes which will assist organisations in identifying and implementing appropriate and proportionate measures to reduce the risk of loss or disclosure of information which could impact on the safety and security of:

- personnel and other occupants or users of the built asset and its services;
- the built asset itself;
- asset information; and/or
- the benefits the built asset exists to deliver.

Such processes can also be applied to protect against the loss, theft or disclosure of valuable commercial information and intellectual property.

Embedding good security can give competitive advantage to commercial enterprises by protecting their key assets and building trust with their stakeholders and customers in the services and products they provide. For those involved in the design and delivery of new or modified assets, it can also enhance global positioning in the international construction market, particularly for high profile and sensitive projects.

PAS 1192-5:2015 was commissioned by the National Protective Security Authority (NPSA), who provided the technical authors for its development. The British Standards Institution (BSI) facilitated its production with input from a panel of industry experts.

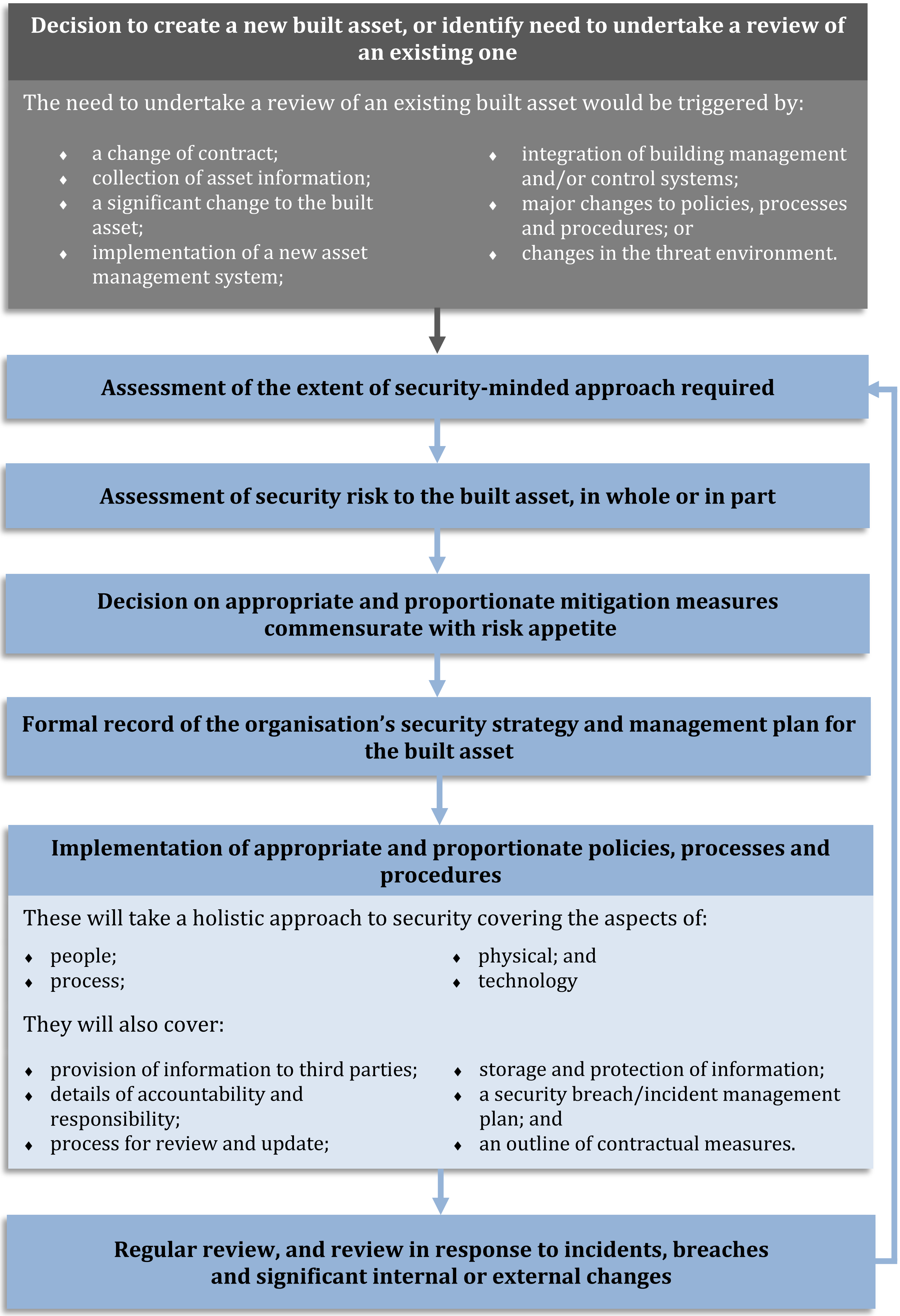
Purpose of this booklet

This booklet provides a high level overview of the key components of PAS 1192-5. The full version of the PAS is available to download at **http://shop.bsigroup.com/pas1192-5**

Who is it for?

PAS 1192-5 is applicable to any built asset or portfolio of assets which is deemed sensitive. It is for use by asset owners or, within a project, the employer. It will also be of interest and relevance to other organizations and individuals involved in the design, construction, maintenance and management of built assets, especially those who wish to protect their commercial information and/or intellectual property.

Summary of the PAS 1192-5 process



Decision to create a new built asset, or identify need to undertake a review of an existing one

The need to undertake a review of an existing built asset would be triggered by:

- a change of contract;
- collection of asset information;
- a significant change to the built asset;
- implementation of a new asset management system;
- integration of building management and/or control systems;
- major changes to policies, processes and procedures; or
- changes in the threat environment.

Assessment of the extent of security-minded approach required

Assessment of security risk to the built asset, in whole or in part

Decision on appropriate and proportionate mitigation measures commensurate with risk appetite

Formal record of the organisation's security strategy and management plan for the built asset

Implementation of appropriate and proportionate policies, processes and procedures

These will take a holistic approach to security covering the aspects of:

- people;
- process;
- physical; and
- technology

They will also cover:

- provision of information to third parties;
- details of accountability and responsibility;
- process for review and update;
- storage and protection of information;
- a security breach/incident management plan; and
- an outline of contractual measures.

Regular review, and review in response to incidents, breaches and significant internal or external changes

What is a sensitive built asset?

A sensitive built asset is defined as one which, as a whole or in part, may be of interest to a threat agent for hostile, malicious , fraudulent and criminal behaviours or activities.

What makes a built asset sensitive?

A built asset, in whole or in part, is sensitive if it:

a) is a designated site under sections 128 or 129 of the Serious Organised Crime and Police Act 2005;

b) forms part of the critical national infrastructure (only the asset, the lead government department and NPSA will be aware of its status);

c) fulfils a defence, law enforcement, national security or diplomatic function;

d) is a commercial site involving the creation, trading or storage of significant volumes of valuable materials, currency, pharmaceuticals, chemicals, petrochemicals, or gases;

e) constitutes a landmark, nationally significant site or crowded place (as determined by The National Counter Terrorism Security Office [NaCTSO]);

f) is used or is planned to be used to host events of security significance; and/or

g) has been judged could be used to significantly compromise the integrity of the built asset as a whole, or its ability to function. The specific assets or asset attributes which shall be considered include, as a minimum:

   i) location, routes, cabling, configuration, identification and use of control systems;

   ii) location and identification of permanent plant and machinery;

   iii) structural design details;

   iv) location and identification of security or other control rooms;

   v) location and identification of regulated spaces or areas housing regulated substances (e.g. nuclear isotopes and bio-hazards) or information; and

   vi) technical specification of security products and features.

Even if a built asset does not fall into the categories which would make it sensitive, there may be business benefits from applying a security-minded approach to its management.

The need for a security-minded approach, and the breadth of the protection measures required, is determined by the Security Triage Process, shown in Figure 5 of PAS 1192-5.

Assessment of risk

Where a security-minded approach is adopted, a key component of the process set out in PAS 1192-5 relates to the management of risk.

The employer or asset owner needs to assess potential vulnerabilites and threats, in combination with an assessment of the nature of harm which could be caused.

The assessment needs to identify the high level security risks associated with:

- people;
- process;
- physical; and
- technology.

It should also identify and record risks associated with intellectual property, commercial data, and information collected or held about neighbouring built assets.

Included in PAS 1192-5

The concept of security

Security issues

The holistic approach to security

Understanding the overall security threat to a built asset

Sources of security advice

Risk mitigation

For each identified risk it will be necessary to assess possible mitigation measures. The process should consider and record:

- ✓ The cost of the measure and its implementation;
- ✓ The achievable risk reduction;
- ✓ The potential cost saving;
- ✓ The measure's impact on asset usability, efficiency and appearance;
- ✓ The potential for the measure to create further vulnerabilities;
- ✓ Delivery of business benefits.

Residual risks

It is important for any residual risks to be re-assessed and put through the risk mitigation process until they fit within the organization's risk appetite.

Built Asset Security Strategy

The Built Asset Security Strategy will comprise a record of :

- ✓ The extent of the security-minded approach required;
- ✓ The built asset security risk management strategy;
- ✓ A list of those to be informed of residual risks;
- ✓ The mechanisms for reviewing and updating the strategy.

Security policies, processes and procedures

The specific security risks identified in the Built Asset Security Strategy should be addressed through the policies, processes and procedures contained in the Built Asset Security Management Plan. This plan should take a holistic approach, encompassing people and process, as well as physical and technological security. The measures should be appropriate and proportionate to both the sensitivity of the built asset and the related security risks.

Coverage of the polices, processes and procedures

People:

- identification of high risk positions;
- security screening and vetting;
- security competency requirements;
- security awareness and training;
- induction of personnel and organizations;
- access to asset models and information;
- demobilisation of personnel.

Physical:

- physical security measures at locations used to design, deliver, operate and support the built asset;
- physical security measures required at the location of the built asset;
- protective measures for equipment storing asset models and information;
- protective measures for computing and electronic devices.

Process:

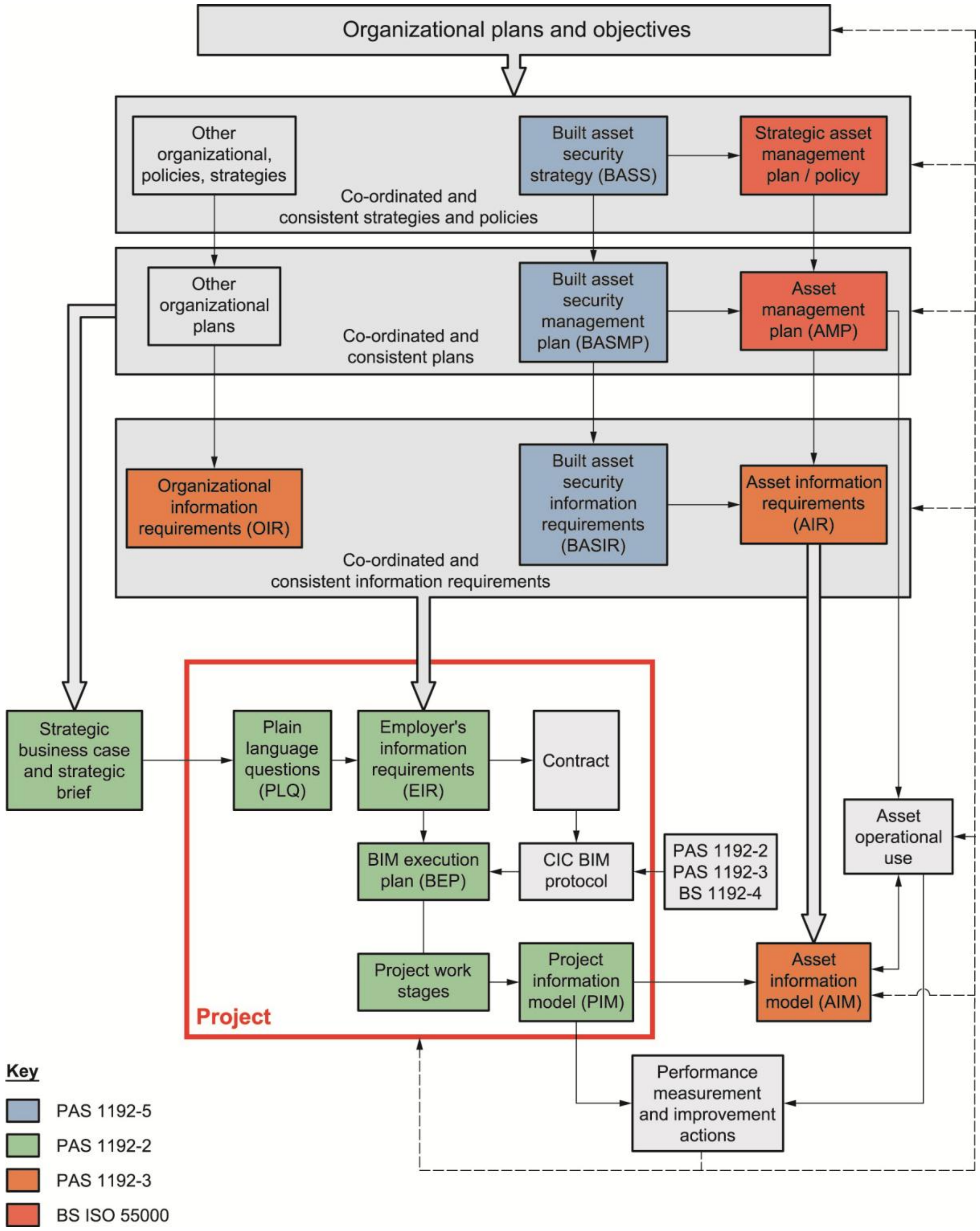
- granting individuals access to data and information;
- handling asset information relating to neighbouring assets;
- handling sensitive and/or classified information and documents;
- disclosure of information to third parties;
- control over change of asset information.

Technology:

- cyber security of systems;
- security of interconnections between different systems;
- configuration and management of systems processing and storing asset information;
- level of software trustworthiness;
- demobilisation of organizations;
- secure deletion, destruction and/or removal of access to asset information.

Embedding security

The security-minded approach must be integrated with other strategic policies, plans, and requirements for the delivery, maintenance and operation of built assets.


Organizational plans and objectives
Other organizational, policies, strategies
Built asset security strategy (BASS)
Strategic asset management plan / policy
Co-ordinated and consistent strategies and policies
Other organizational plans
Built asset security management plan (BASMP)
Asset management plan (AMP)
Co-ordinated and consistent plans
Organizational information requirements (OIR)
Built asset security information requirements (BASIR)
Asset information requirements (AIR)
Co-ordinated and consistent information requirements
Strategic business case and strategic brief
Plain language questions (PLQ)
Employer's information requirements (EIR)
Contract
BIM execution plan (BEP)
CIC BIM protocol
PAS 1192-2
PAS 1192-3
BS 1192-4
Asset operational use
Project work stages
Project information model (PIM)
Asset information model (AIM)
Project
Performance measurement and improvement actions
Key
PAS 1192-5
PAS 1192-2
PAS 1192-3
BS ISO 55000

NOTE Developed by NPSA, Alexandra Luck and Hugh Boyes as part of PAS 1192-5 development process

PAS 1192-5 provides a comprehensive framework to help organisations adopt a security-minded approach to the use of information and data in the built environment.

Acknowledgement

PAS 1192-5 was commissioned by the National Protective Security Authority (NPSA). Acknowledgment for its development is given to the external technical authors (Alexandra Luck and Hugh Boyes). Production was facilitated by the British Standards Institution (BSI). In addition we would like to thank the following contributing organisations:

- Atomic Weapons Establishment
- BIM Technologies Alliance
- CESG
- Construction Industry Council
- Co-opted members
- Centre for the Protection of National Infrastructure
- Crossrail Ltd
- EC Harris LLP
- 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

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

How to order a copy

Copies of PAS 1192-5 may be downloaded from: http://shop.bsigroup.com/pas1192-5