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.

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 It will be withdrawn upon publication of its content in, or as, a British Standard.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

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:

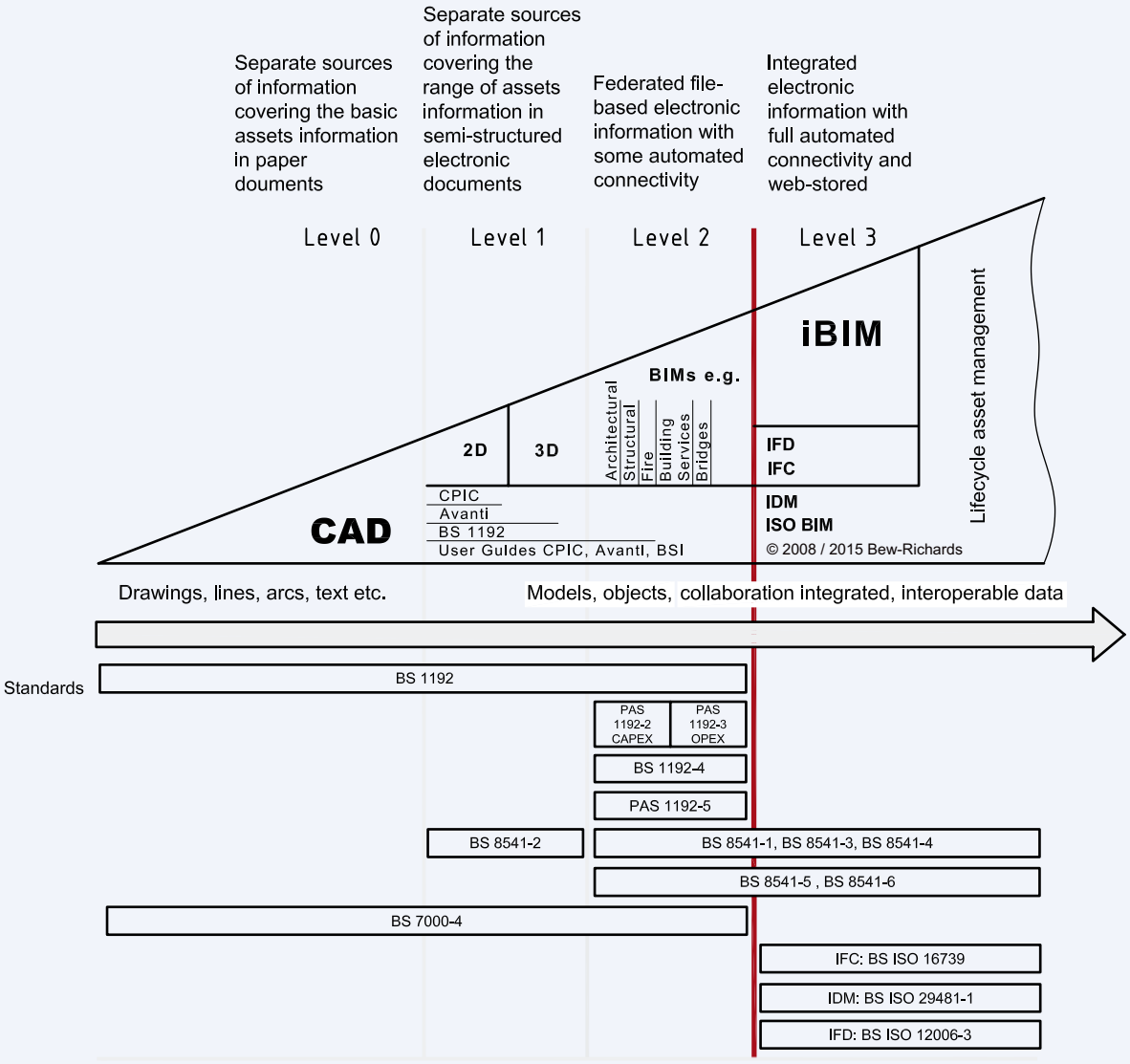
- Data Protection Act 1998 [1];
- Environmental information Regulations 2004 [2];
- Freedom of Information Act 2000 [3];
- Serious Organised Crime and Police Act 2005 [4];
- Official Secrets Act 1989 [5];
- Computer Misuse Act 1990 [6];
- Freedom of Information (Scotland) Act 2002 [7];
- Planning and 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.

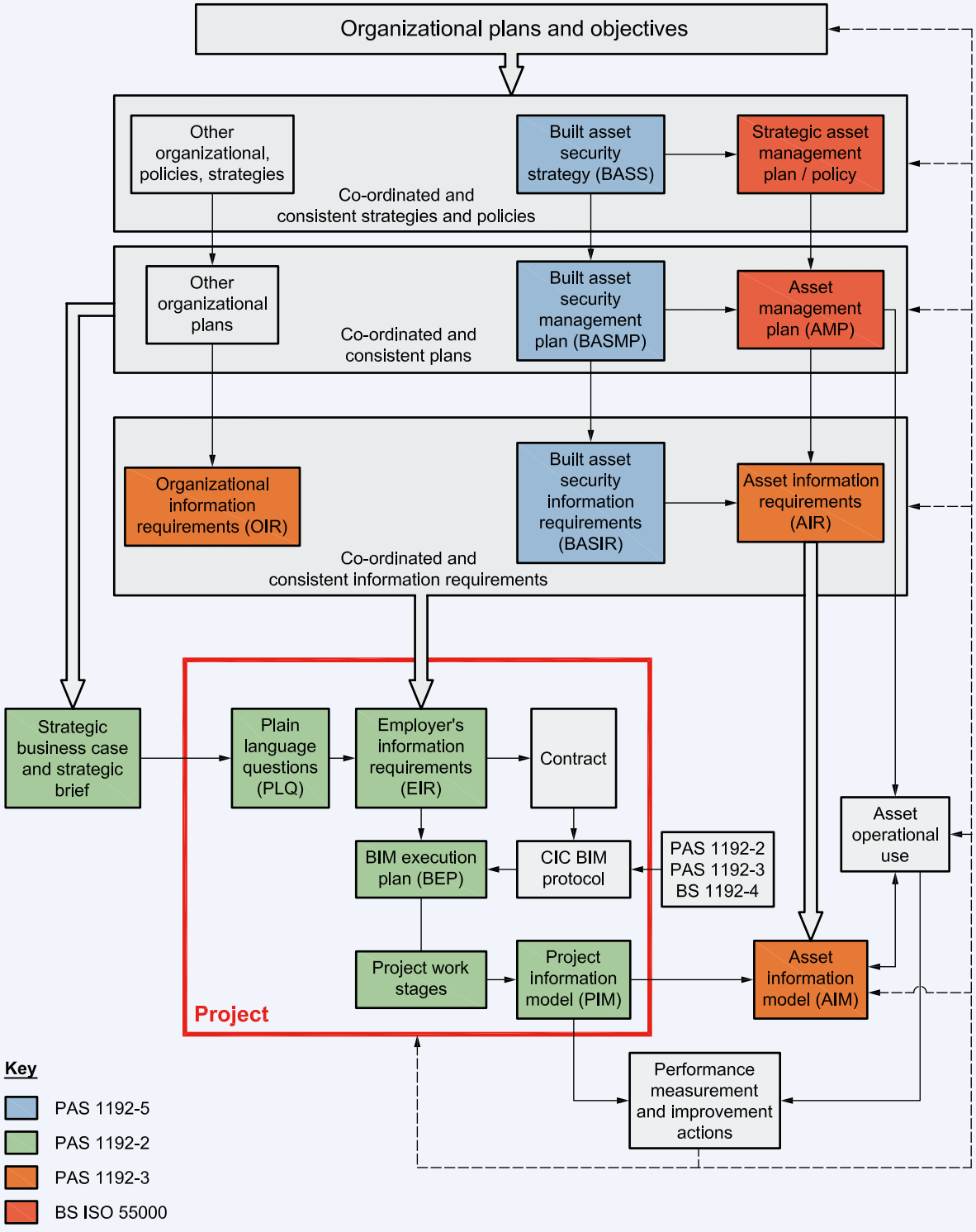
Digital built environments will need to deliver future fiscal, functional, sustainability and growth objectives, and will therefore impact on procurement, delivery and operational processes including far greater cross-sector collaboration. The increasing use of computer-based technologies will support 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.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable 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 ISO 55000, *Asset management – Overview, principles and terminology*

PAS 1192-2:2013, *Specification for information management for the capital/delivery phase of construction projects using building information modelling*

PAS 1192-3:2014, *Specification for information management for the operational phase of assets using building information modelling*

BS 1192-4:2014, *Collaborative production of information – Part 4: Fulfilling employer's information exchange requirements using COBie – Code of practice*

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

3.1.1 asset

item, thing or entity that has potential or actual value to an organization

[BS ISO 55000:2014, **3.2.1**]

NOTE 1 *An asset may be fixed, mobile or movable. It may be an individual item of plant, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets.*

NOTE 2 *An asset may also comprise information in digital or in printed form.*

NOTE 3 *The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial or non-financial.*

3.1.2 asset information

data or information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization

NOTE *Asset information can include design information and models, documents, images, software, spatial information and task or activity-related information.*

3.1.3 asset management

coordinated activity of an organization to realize value from assets

[BS ISO 55000:2014, **3.3.1**]

NOTE 1 *The term "activity" has a broad meaning and can include, for example, the approach, the planning, the plans and their implementation.*

NOTE 2 *In this PAS this includes realizing value from networks and systems of assets.*

3.1.4 asset owner

individual or organization that owns the built asset and any associated asset information, is the asset operator or licensee, or is the operator of the system of which the built asset is a component

3.1.5 baseline security measures

contractually required measures relating to personal and commercial information

3.1.6 building information modelling (BIM)

discrete set of electronic object-oriented information used for design, construction and operation of a built asset

NOTE 1 *Models are a component part of the project information model (PIM) which comprises all information developed during the design and construction phases of a project, and the asset information model (AIM) which comprises the maintained information used to manage, maintain and operate the asset.*

NOTE 2 *BIM practice in accordance with the UK Government BIM mandate is for discrete models to be produced for specific purposes by separate organisations. Models can be brought together through a process of model federation.*

3.1.7 built asset

building, multiple buildings (e.g. a site or campus) or built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.) that is the subject of a construction project or where the asset information is held in a digital format

NOTE 1 *The built asset may include associated land or water, for example, the catchment area for a water company or the navigation channels for a dock.*

NOTE 2 *The built asset may comprise a portfolio or network of assets.*

3.1.8 built asset security manager

individual reporting directly to, or employed by, the employer or asset owner and undertaking the role of security management

3.1.9 common data environment (CDE)

single source of information for any given project or built asset, used to collect, manage and disseminate all relevant approved files, documents and data for multi-disciplinary teams in a managed process

NOTE 1 *For further description of its use during a project see explanatory to PAS 1192-2.* ***A.30****.*

NOTE 2 *Sensitive information would not normally be contained within a CDE unless that CDE is held within a secure environment.*

3.1.10 cyber hygiene

conditions and practices that serve to promote or preserve cyber safety and security by individual system users

NOTE *Good cyber safety and security practices are not dissimilar to good health practices related to infection and disease control, i.e. taking appropriate steps to prevent infection (e.g. malware), seeking advice in the case of a suspected infection, and when infection occurs, isolating it or taking steps to prevent further spread.*

3.1.11 cyber-physical system (CPS)

system designed as an entity, or set of entities, with a specific purpose, or to meet a capability objective

NOTE *A CPS should include a computational aspect (cyber) and a physical aspect working together to accomplish a task or function. The cyber aspect has a controlling or influencing role over the physical parts of the system, for example, a complex environmental conditioning system for a building or pressure and flow control systems in a utility network.*

3.1.12 design team

sub-set of the project delivery team and/or task team that is involved in the delivery of the brief, concept, definition and design stages of the project

3.1.13 employer

individual or organization named in an appointment or building contract as the employer

[PAS 1192-2:2013, **3.20**]

3.1.14 enterprise

entity constituting multiple organizations within the supply chain

3.1.15 hostile reconnaissance

activity of acquiring information about a target with the view to planning to attack, compromise, disrupt or destroy that target

NOTE 1 *The target may be an individual, organization, enterprise or built asset, in whole or in part.*

NOTE 2 *The planned hostile action might be physical or cyber in nature.*

3.1.16 information manager

organizational representative appointed by the employer or asset owner, who is responsible for establishing governance and assuring data and information flow to and from the common data environment (CDE) during the design, construction, operation and maintenance, and disposal or decommissioning of a built asset

3.1.17 information management

policies, processes, procedures and tasks applied to inputting, processing and generation activities to ensure accuracy, authenticity, confidentiality and integrity of information

3.1.18 need-to-know

grant of access to data or information relating to sensitive assets and systems for an individual or organization where such access must be necessary in order for them to perform their role satisfactorily and safely

3.1.19 neighbouring built assets

built assets that share a boundary (including beneath it or overhead) with the built asset under consideration, or that are in the neighbourhood of that built asset but physically separated by a public or private street, public or privately-owned open space or similar features

3.1.20 organization

person or group of people that has its own function with responsibilities, authorities and relationships to achieve its objectives

[BS ISO 55000:2014, **3.1.13**]

3.1.21 personally identifiable information

personal data as defined in the Data Protection Act 1998 [1]

3.1.22 personnel

individuals employed by an organization, including contractors or temporary staff used to fulfil roles that may be undertaken by that organization

3.1.23 project delivery team

group of organizations or individuals contracted either directly or indirectly to deliver services or products to the project, and personnel from the employer or asset owner who are directly involved in the management, planning and delivery of the project

3.1.24 risk appetite

function of an organization's capacity to bear risk

3.1.25 security management

role in connection with the project or the management of the asset which is responsible for security of the built asset and associated asset information during the design, construction, operation and maintenance, and disposal or decommissioning of a built asset

3.1.26 security-minded

understanding and routine application of appropriate and proportionate security measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities

3.1.27 sensitive built asset

built asset, as a whole or in part, that may be of interest to a threat agent for hostile, malicious, fraudulent and/or criminal behaviours or activities

3.1.28 sensitive information

information, the loss, misuse or modification of which, or unauthorized access to, could: adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the information

3.1.29 smart

application of autonomous or semi-autonomous technology systems to achieve greater utilization of resources, limiting or reducing per capita resource consumption to maintain or improve quality of life

[PAS 180:2014, **3.1.61**]

3.1.30 smart city

effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens

[PAS 180:2014, **3.1.62**]

3.1.31 smart grid

electricity network that uses information and communications technology (ICT) to integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies

[PAS 180:2014, **3.1.65**]

3.1.32 threat

potential cause of an incident which may result in harm to a system or organization

3.1.33 vulnerability

weakness of an asset or group of assets that can be exploited by one or more threats

3.2 Acronyms

AIM – asset information model

AIR – asset information requirements

ALO – architectural liaison officer

BASIR – built asset security information requirements

BASMP – built asset security management plan

BASS – built asset security strategy

BEP – BIM execution plan

BIM – building information modelling

BS – British Standard

BYOD – bring your own device

CDE – common data environment

CESG – the national technical authority for information assurance

CIO – chief information officer

CISO – chief information security officer

COBie – construction operation building information exchange

CPDA – crime prevention design advisor

CPNI – Centre for the Protection of National Infrastructure

EIR – employer's information requirements

FM – facilities management

IAAS – infrastructure as a service

ISO – International Standards Organization

MIDP - master information delivery plan

NaCTSO – National Counter Terrorism Security Office

OIR – organizational information requirements

PAAS – platform as a service

PAS – publicly available specification

PIM – project information model

RSES – Register of Security Engineers and Specialists

SAAS – software as a service

SB/IMP – security breach/incident management plan

SPF – security policy framework

TIDP – task information delivery plan

4 Understanding the security context

4.1 The concept of security

The employer or asset owner shall be aware of the range of potential security issues which are applicable to its business, assets, personnel and other occupants or users of the asset.

NOTE 1 *Security operates on a number of levels ranging from national security issues (e.g. protection against terrorism and detecting hostile acts by nation states), to tackling organized crime, and to preserving the value, longevity and ongoing use of an enterprise's assets, whether tangible (e.g. a building or physical stock), or intangible (e.g. preventing the loss or disclosure of intellectual property and nationally or commercially sensitive information). It also includes the handling of privacy issues (e.g. the protection of personally identifiable information).*

Good security can offer competitive advantage to commercial enterprises by protecting their key assets and engendering trust by their stakeholders and customers in the services or products that are provided. For those involved in the design and delivery of new or modified assets, it can also provide competitive global positioning in the international construction market, particularly for high profile and sensitive projects.

Good security requires holistic risk assessment and applying the principles of proportionality to achieve an appropriate balance of the costs and constraints associated with protecting an asset versus the impact that its loss, compromise or failure can have on the organization and the organization's stakeholders.

NOTE 2 *It is important to recognise that once information has been published on the internet, or otherwise made publicly available, it is virtually impossible to delete, destroy, remove or secure all copies of the released information. In addition, the release of aggregated, apparently innocuous information can result in exposing sensitive or security information. Therefore appropriate checks should be made before any information is made widely available.*

4.2 Security issues

4.2.1 Hostile reconnaissance

For sensitive or potentially sensitive built assets, the employer or asset owner shall seek advice to gain an understanding of the range of traditional and evolving techniques of hostile reconnaissance to which the business, asset, asset-related digital information or personnel could be vulnerable.

NOTE 1 *Information on sources of advice can be found in* ***5.1.2****, Notes 1, 2 and 3.*

NOTE 2 *During hostile reconnaissance, the hostile party will be looking for information:*

- *it can exploit about security (e.g. physical vulnerabilities or system configuration);*
- *to identify the modus operandi and chance of success;*
- *about the state of security (i.e. the chances of being detected);*
- *about the pattern of life of an individual or group of individuals.*

From the perspective of the hostile party, achieving successful attack planning depends on the reliability of this information and the ability to acquire it without being detected.

NOTE 3 *While there are tools for detecting and reporting physical reconnaissance, the increasing use of digital data and information to support project modelling, digital built environments and smart asset management provides an avenue for hostile reconnaissance that might reduce or eliminate the need for physical reconnaissance prior to launching an attack.*

4.2.2 Malicious acts

The employer or asset owner shall be aware of the increased business risks associated with the failure or impaired performance of systems which depend on information technology arising from malicious acts caused by a range of external and insider threats, such as damage caused by malware, hackers or disaffected personnel.

NOTE *Widespread use of digital and information technologies creates increased business risks which could manifest themselves as loss of availability, functionality or performance, or the loss or corruption of digital artefacts.*

4.2.3 Loss or disclosure of intellectual property

The employer or asset owner shall be aware of the need to protect its own and others' intellectual property which it holds or which may be developed, and shall understand the potential consequences of the loss of, unauthorized access to, or improper use or re-use of that information.

NOTE 1 *Intellectual property encompasses a range of material, including trade secrets, proprietary processes, technical specifications and detailed calculations or methodologies. Organizations often invest heavily in the development of intellectual property and through its use, licensing and sale can deliver significant commercial and economic benefits. The piracy, theft or unauthorized use of intellectual property can be damaging to the organization and a country's economy as a whole.*

NOTE 2 *Consideration should be given by other parties to protecting their intellectual property from loss, unauthorized access, or improper use or re-use.*

4.2.4 Loss or disclosure of commercially sensitive information

The employer or asset owner shall be aware of the need to protect pricing, price sensitive or market sensitive data, especially during a tender or procurement process, and shall understand the potential consequences of the loss of, or unauthorized access to, that information.

NOTE *In competitive markets there is a need to address the risks of commercial espionage, including measures to prevent the loss of, or unauthorized access to, pricing or price sensitive data. Failure to provide adequate protection of data or information during tendering processes can damage both purchasers and suppliers.*

4.2.5 Release of personally identifiable information

The employer or asset owner shall be aware of the need to safeguard personally identifiable information, in particular when responding to requests for information under Environmental Information Regulations [2] or Freedom of Information Act [3].

NOTE *Unauthorized access to personally identifiable information can enable more targeted social engineering and phishing attacks.*

4.2.6 Aggregation of data

For sensitive or potentially sensitive assets, the employer or asset owner shall seek advice to gain an understanding of the increased risks and sensitivity that occur through aggregation of data.

NOTE 1 *Information on sources of advice can be found in* ***5.1.2****, Notes 1, 2 and 3.*

NOTE 2 *Data aggregation can occur through manual or automated processes and refers to where data is collected and collated, and possibly analysed to allow meaningful and useful interpretation of initially isolated or independent facts or data. It has the potential to increase the business impact of any compromise, whether accidental or intentional. The data aggregation risks can arise from:*

a) data aggregation by accumulation, where the volume of asset information stored together increases the level of impact that would occur if the data was compromised;

b) data aggregation by association, where the association of different types of asset information, which in themselves have little or no impact when compromised, when associated together, have a higher level of impact;

c) a combination of accumulation and association; or

d) disclosure of too much data or information, e.g. in response to a public access request, allowing a third party to draw inferences from the disclosed material or create unplanned associations.

NOTE 3 *Individual facts or data items might not create a harmful situation, but the aggregation of data or information could allow a hostile party to develop a better understanding and more comprehensive picture regarding the project or built asset, and the association of particular assets with each other. For example, when designing a security system, there will be a need for sensors (e.g. motion detectors and CCTV cameras). Physical information about the size and installation requirements of individual components is unlikely to be sensitive, but the aggregated data comprising the detailed system design, including the location of sensors, their capability and field of view, is more sensitive as it would enable an assessment of system capabilities and physical security vulnerabilities.*

4.3 Holistic approach to security

The employer or asset owner shall appreciate that in respect of a built asset, a holistic approach needs to address security around the aspects of people and process, as well as physical and technological security.

NOTE 1 *People – Individuals need to be aware of, and understand, the security measures in place if the organization is to gain buy-in and develop security-minded behaviour in its personnel, including taking responsibility for security issues.*

NOTE 2 *Process – Ineffective or inefficient security processes are often ignored by employees, contractors and suppliers, which can lead to significant security risks, while implementation of good quality security-minded processes can contribute to the effectiveness of the overall security regime.*

NOTE 3 *Physical security – the security of the built environment and individual built assets depends on:*

a) the physical protection of the built asset;

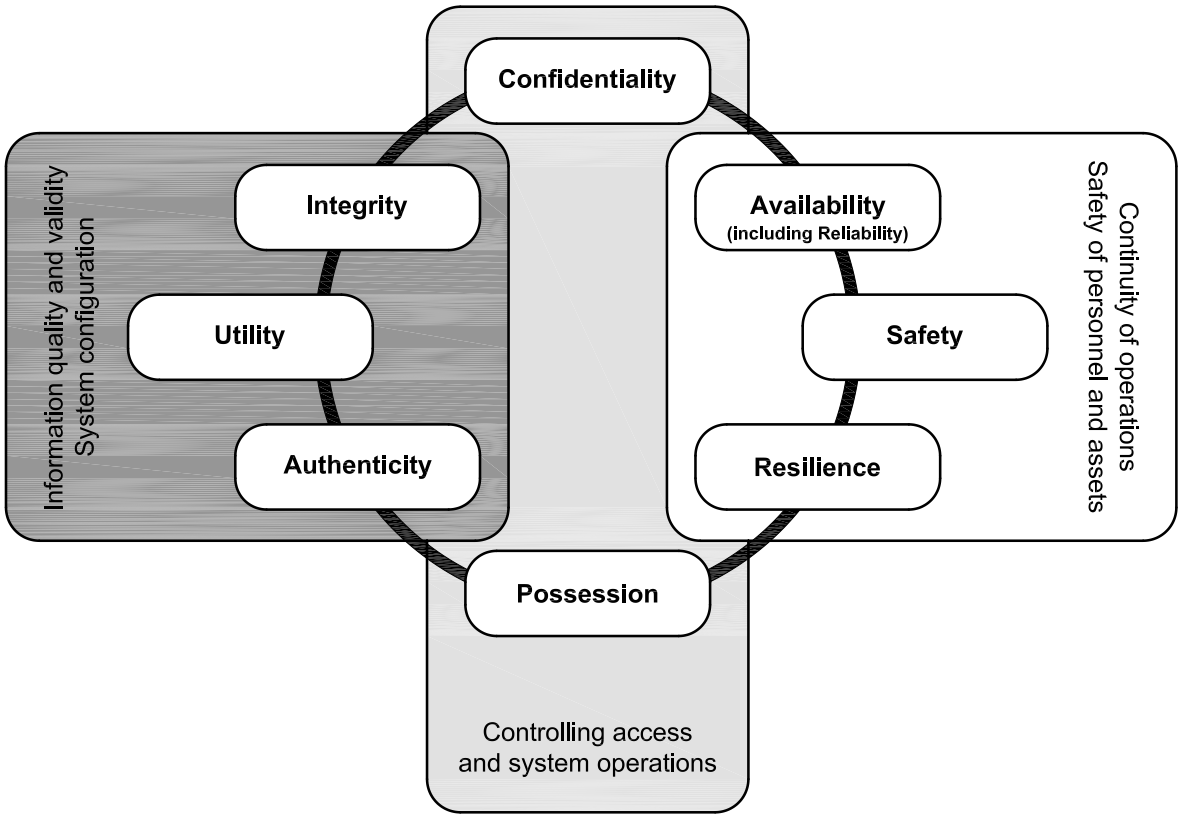
b) the physical security of information assets related to the built asset and its neighbouring built assets; and

c) the physical protection of buildings, systems and data used to design, deliver, operate and support the built asset.

***NOTE 4** Technological security – technical security considerations for the cyber-physical systems that are employed in the digital built environment are shown in Figure 3 and based on the following facets:*

- *confidentiality – the control of access and prevention of unauthorized access to information or data, which might be sensitive in isolation or in aggregate;*
- *integrity – maintaining the consistency, coherence and configuration of information and systems, and preventing unauthorized changes to them;*
- *authenticity – ensuring that inputs to, and outputs from, built asset systems, the state of the system and any associated processes, information or data, are genuine and have not been tampered with or modified;*
- *utility – that asset information and systems remain usable and useful across the lifecycle of the built asset;*
- *availability (including reliability) – ensuring that the asset information, systems, and associated processes are consistently accessible and usable in an appropriate and timely fashion. To achieve the required availability may require each of these to have an appropriate and proportionate level of resilience;*
- *possession – the design, implementation, operation and maintenance of built asset systems and associated processes so as to prevent unauthorized control, manipulation or interference;*
- *resilience – the ability of the asset information and systems to transform, renew and recover in a timely way in response to adverse events; and*
- *safety – the design, implementation, operation and maintenance of built asset systems and related processes so as to prevent the creation of harmful states which may lead to injury or loss of life, or unintentional environmental damage.*

Figure 3 – Technical security considerations for the cyber-physical systems that are employed in the digital built environment



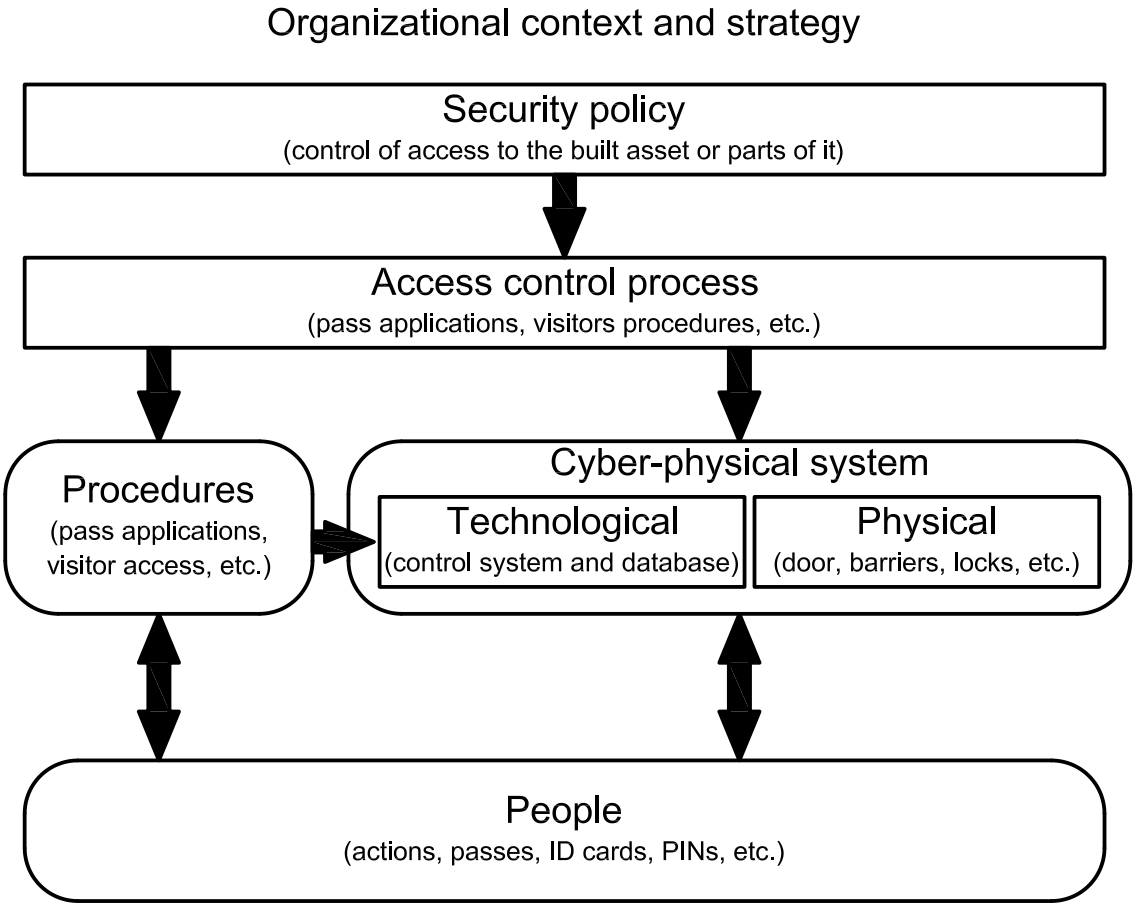
***NOTE** Copyright is claimed on Figure 3. Reproduction of this figure and making products from it might infringe that copyright. Details of the copyright owner can be found in the Foreword.*

NOTE 5 *The control of access by individuals to a building or sensitive area can be used to illustrate the interaction between the four aspects of a security policy:*

- *people – those individuals who are authorized to access the building or area should be issued with, and then carry and display, an appropriate pass and/or access control card;*
- *process – there should be an established process, supported by relevant procedures to determine which individuals may access the building or area and the nature of their access;*
- *physical – there should be appropriate physical controls to manage the granting or refusal of access to individuals. The controls may be manual (e.g. a guard operating a barrier) or automated through the use of passes/access control tokens, etc. There should also be no uncontrolled access or egress routes for the building or area; and*
- *technological – these may include measures to verify the identity of the pass or card holder (e.g. using two factor authentication such as the use of badge/card readers and the holder entering a PIN number via a keypad), anti-forgery measures for access passes, and the use of databases or automated systems to verify access privileges.*

As illustrated in Figure 4, only through the implementation and operation of appropriate measures addressing all four aspects can physical access to the building or area be assured.

Figure 4 – Example of interaction of security aspects to provide access control to a building



NOTE *Developed from source material provided by CPNI, Alexandra Luck and Hugh Boyes*

5 Understanding the overall security threat to a built asset

5.1 Applying the security triage process

5.1.1 The employer or asset owner shall apply the security triage process outlined in Figure 5 to identify the need for a security-minded approach to be applied to the built asset and associated asset information, as a whole or in part, and whether planned or existing.

NOTE 1 *Triggers for assessing the security requirements for an existing asset include:*

a) *a change of contract for facilities or asset management/maintenance;*

b) *collection of asset information including laser scanning and high-resolution imagery;*

c) *a significant change to the built asset, e.g. change of use, change of occupier, remodelling, extension or major structural alterations, or change of sensitivity;*

d) *implementation of a new asset management system, including change or replacement of an existing system;*

e) *integration of building management and/or control systems, in particular access control and intrusion detection systems, with the asset management system for the built asset;*

f) *changes to the operating environment of the built asset (e.g. political, economic, social, technological, legal or environmental) requiring implementation of major changes to existing asset management policies, processes and procedures; or*

g) *marked changes in the threat environment for the built asset which require improvements in the management of asset information.*

NOTE 2 *To reduce the likelihood that sensitive information or data is inappropriately stored, disseminated or used, the triage process should be conducted before or as soon as possible after any of the trigger points listed in* ***5.1.1****, occur.*

5.1.2 If there is any uncertainty as to whether:

- a built asset, in whole or in part, is sensitive;
- there is a need to protect particular asset information or information about a neighbouring built asset;
- there is a need for retrospective actions; or
- particular retrospective actions are appropriate

the employer or asset owner shall seek advice from appropriate security advisors.

NOTE 1 *Depending on the nature, use or function of the built asset, there might be a number of sources of specialist security advice available to the employer or asset owner. This advice typically covers personnel, physical and cyber security. For sensitive built assets, advice will be available from a combination of CPNI, CESG, NaCTSO and lead Government departments.*

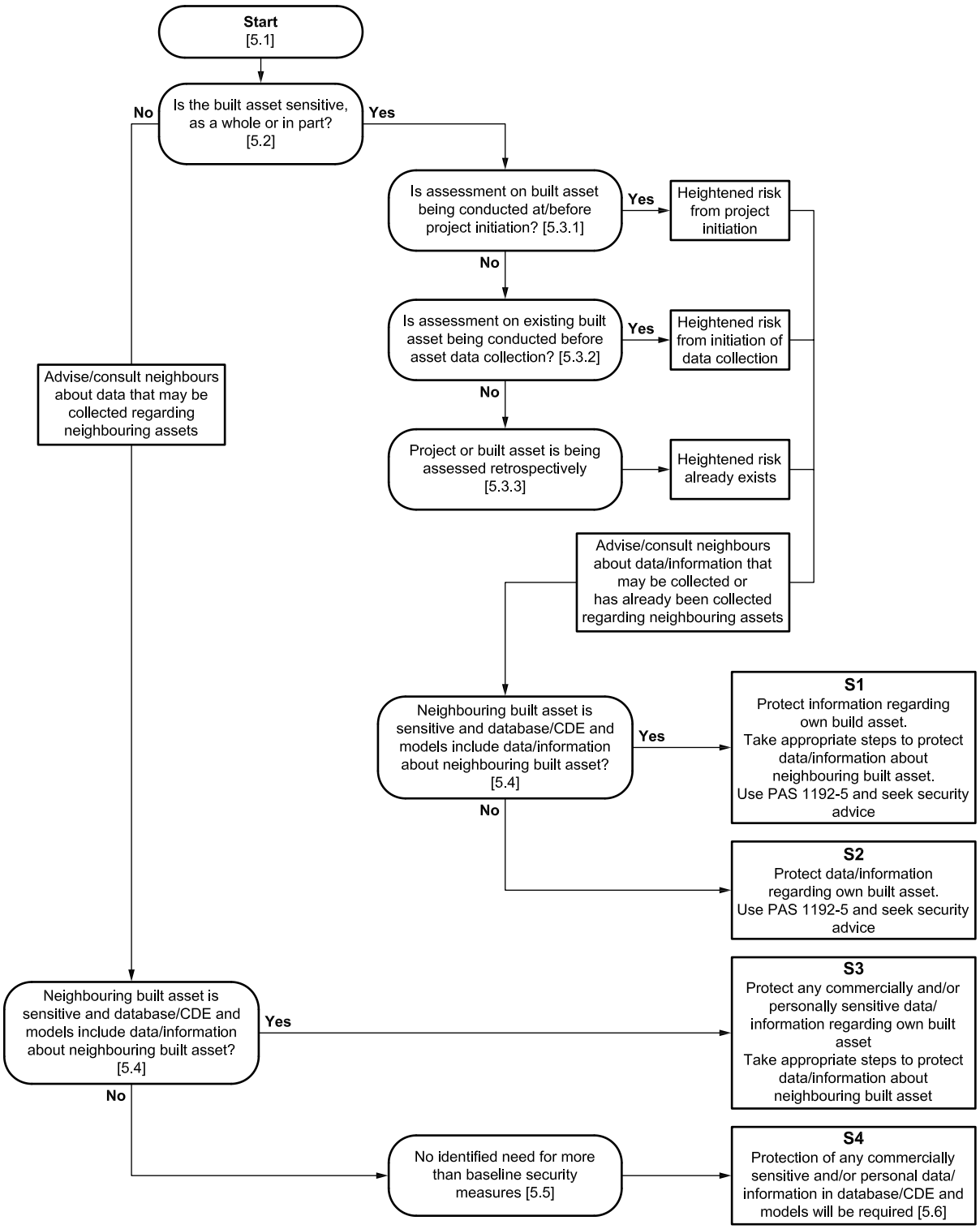
For other built assets, e.g. a high profile commercial building, the employer or asset owner's built asset security manager, along with the police architectural liaison officer (ALO) (or in London, the crime prevention design advisor [CPDA]), who will be embedded in the Local Authority Planning Office, and where necessary, specialist security advisors (e.g. a member of the Register of Security Engineers and Specialists [RSES][3]) should be able to assess the security threats and vulnerabilities to provide appropriate professional advice on security requirements and countermeasures.

NOTE 2 *RSES is sponsored by CPNI. The register was established to promote excellence in security engineering by providing a benchmark of professional quality against which its members have been independently assessed. Its members are engineers, applied scientists and specialists who apply their knowledge to securing the built environment and infrastructure.*

NOTE 3 *Where the built asset is being constructed outside the United Kingdom, specialist security advice and threat assessment may be required. For projects involving UK Government aid and development funds, advice should be sought from the sponsoring department. For all other projects, the employer may consult local experts, or specialist international risk and security management organizations.*

[3] See http://www.rses.org.uk

Figure 5 – Security triage process to identify the need for a security-minded approach to the built asset and associated asset information



NOTE *Developed from source material provided by CPNI, Alexandra Luck and Hugh Boyes.*

5.1.3 The employer or asset owner shall record the outcome of the application of the security triage process for each built asset to which it is applied, including where there is no identified need for more than baseline security measures.

5.1.4 Where the recorded outcome details the security protection level or classification level of a built asset, the information shall be managed on a strict need-to-know basis and shall be subject to security measures, appropriate to the level of risk, with regard to its creation, storage, distribution and use.

5.2 Definition of a sensitive built asset

The term sensitive built asset shall apply to any built asset, as a whole or in part, that:

a) is a designated site under sections 128 or 129 of the Serious Organised Crime and Police Act 2005 [4];
b) forms part of the critical national infrastructure (only the asset owner, the lead government department and CPNI 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 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.

***NOTE** The fact that a built asset does not fall within the criteria described in **5.2** does not preclude the application of a higher level of security if the employer or asset owner wishes to adopt this.*

5.3 Sensitive built assets

5.3.1 Built asset assessed at or before project initiation

If a planned built asset has been determined to be sensitive, the employer or asset owner shall, following the requirements of this PAS, implement a security-minded approach to the creation and exchange of asset information pertaining to that asset before procurement or use of any external consultancy services.

***NOTE** Any publicity surrounding development of sensitive built assets might be of interest for hostile reconnaissance from the earliest stages in the design process.*

5.3.2 Built asset assessed before asset data collection initiation

If work is being planned to collect detailed asset information in digital format, either as a precursor to a project or as part of the ongoing asset management of an existing built asset, the asset owner shall, following the requirements of this PAS, implement a security-minded approach to the capture, creation, processing, storage and exchange of asset information pertaining to that asset prior to commencing the data collection.

***NOTE 1** Any publicity surrounding surveying or asset management data pertaining to sensitive built assets might be of interest for hostile reconnaissance from the earliest stages in the data collection and management processes.*

***NOTE 2** Where the data collection is to support the tendering or re-letting of contracts related to the operation and maintenance of the built asset, the asset owner should consider how the collected data is structured and stored to enable suitable controls to be applied to more sensitive data.*

5.3.3 Built asset assessed retrospectively

On a pre-existing built asset the asset owner shall, following the requirements of this PAS, implement a security-minded approach to managing the asset, taking into consideration an assessment of the extent to which information is already in the public domain.

***NOTE 1** Release of information into the public domain may have occurred in a number of ways including information:*

a) published by the employer or asset owner, for example on websites, in press releases, in planning applications or in tender documents;

b) presented in public forums, for example conferences, professional journals and the trade press;

c) disclosed by public bodies in response to specific requests, for example freedom of information requests; environmental information requests etc.; and/or

d) leaked or accidentally disclosed.

***NOTE 2** In instances where security risks are identified retrospectively, the extent to which the employer can identify how information has been used and disseminated is important.*

5.4 Managing asset information relating to neighbouring built assets

5.4.1 Prior to collecting any information about a neighbouring built asset, or where information is already held, the employer or asset owner shall, unless prohibitive for commercially or locally sensitive reasons, consult with that asset's owner/occupier/operator to establish what measures need to be applied to the capture, handling, dissemination, storage and use of the non-publicly available information.

***NOTE 1** When undertaking construction or maintenance activities on a built asset it is often necessary to hold information about adjacent or neighbouring built assets. This information can range from detailed physical survey information about above ground and underground structures, infrastructure networks and systems, utilities etc., to information about its operations or access arrangements, e.g. where hazardous materials are being stored.*

***NOTE 2** It is generally only necessary to avoid showing built assets, in part or in whole, that are not otherwise generally visible directly or through other sources. However, it may also be necessary to protect certain information pertaining to assets the location of which can be readily identified, for example the field of view of CCTV cameras, or where aggregation or association of data may compromise the security or operation of the neighbouring built asset, or where an increase in accuracy may aid hostile reconnaissance of the neighbouring built asset.*

5.4.2 Where it is necessary and appropriate to hold information about a neighbouring built asset or the owner/occupier/operator of a neighbouring or adjacent built asset has indicated that they are sharing sensitive information, the employer or asset owner shall, following the requirements of this PAS, adopt an appropriate security-minded approach to the capture, handling, dissemination, storage and use of this information.

***NOTE** The employer or asset owner should consider the following scenarios in respect of information about adjacent and/or neighbouring built assets:*

a) No information is held or will be included in a CDE, models and/or information exchanges – in this scenario it is unlikely that additional security measures will be required;

b) The CDE, models and information exchanges do, or will only, include limited publicly available information about the neighbouring built asset, with no further augmentation or interpretation – in this scenario there is unlikely to be a need for any enhanced protection of the information;

c) The CDE, models and information exchanges do, or will, include information about the neighbouring built assets which is not publicly available, e.g. detailed survey information that involved access to the neighbouring built assets, where there is aggregation of significant amounts of publicly available information (with or without further augmentation or analysis), or information about utility routes and underground structures – in this scenario there is likely to be a need for enhanced protection of the information.

In scenario c), the additional measures required to protect the information about the neighbouring built asset will depend on that asset's nature and/or sensitivity.

5.5 No identified need for more than baseline security measures

Where the triage process does not indicate a need for the implementation of more than baseline security measures (i.e. those measures relating to personal and commercial information which are contractually required), the employer or asset owner shall consider whether there are business benefits to be derived from applying a security-minded approach to the management of the built asset and asset information.

***NOTE** Whilst none of the measures outlined in this PAS are essential for projects or built assets that fall within this category, it is prudent that employers and asset owners take appropriate steps to minimize threats arising from fraud and other criminal activity and from cyber security incidents.*

5.6 Cyber security good practice

5.6.1 Where the project or built asset operations involve the electronic exchange of information, the employer or asset owner shall require all organizations and their personnel with access to asset information and/

or systems to take appropriate cyber security measures to protect that information, the built asset and any associated cyber-physical systems.

***NOTE** In the UK the Government recommends that all its suppliers should as a minimum meet the requirements of the Cyber Essentials scheme[4] and Security Policy Framework (SPF)[5]*

5.6.2 Where a CDE, model(s), or information exchange does, or will, include any personally identifiable or sensitive information, or any commercial information, the employer or asset owner shall require parties having access to the information to adopt appropriate processes and procedures to protect the information.

***NOTE 1** It is recommended that employers review existing routine information management provisions within their agreements so that the employer's rights to manage the flow of information in a project are understood by all parties.*

***NOTE 2** Routine use of confidentiality and non-disclosure agreements provides employers with control over the dissemination of potentially sensitive information.*

***NOTE 3** Unless the employer or asset owner wishes to adopt any higher level of security, there is no necessity for requirements of the remainder of this PAS to be applied to the project or built asset as currently assessed.*

[4] See https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[5] See https://www.gov.uk/government/publications/security-policy-framework

6 Appointment of a built asset security manager

6.1 Where the security triage process identifies a need for a security-minded approach, the employer or asset owner shall nominate a suitably qualified and experienced individual to fulfil the role of built asset security manager.

NOTE *On smaller projects the built asset security manager role is likely to be a part-time function and fulfilled by an individual who may undertake or be responsible for security and other duties. However that individual will still need to be suitably qualified and experienced to undertake the role. On larger or more complex projects it is likely that it will be a full-time post.*

6.2 The built asset security manager role shall be employed by, or report directly to, the employer's or asset owner's organization and shall:

a) provide a holistic view of the security issues and threats to be addressed;

b) offer guidance and direction on the handling of risks;

c) take ownership, manage, and assist in the development of the built asset security strategy (BASS) (see Clause **7**);

d) be accountable for security decisions that are taken;

e) take ownership, manage, and assist in the development of the built asset security management plan (BASMP) (see Clause **8**);

f) take ownership, manage, and assist in the development of security breach/incident management plan (SB/IMP) (see Clause **9**);

g) take ownership, manage, and assist in the development of the built asset security information requirements (BASIR) (see Clause **10**);

h) assist in the development of plain language questions and employer's information requirements (EIR) in projects;

i) assist in the development and reviewing of any tendering and project planning documentation;

j) be responsible for promoting a security-minded culture;

k) brief advisors, specialists and supply chain on relevant aspects of the BASS, BASMP and BASIR;

l) advise on the need for, and undertake, the review and auditing of documentation, policies, processes and procedures relating to the security of the built asset; and

m) where appropriate and necessary, seek appropriate professional security advice to provide additional guidance throughout the lifecycle of the project and/or asset.

NOTE 1 *Information on sources of security advice can be found in* ***5.1.2****, Notes 1, 2 and 3.*

NOTE 2 *The built asset security manager does not perform any design role within a project.*

6.3 It shall be acceptable for the built asset security manager to delegate specific security tasks or duties to functional roles to manage on a day-to-day basis (e.g. personnel security to HR, cyber security to the chief information security officer (CISO), chief information officer (CIO), or chief digital officer, and asset management functions to the asset manager or facilities manager). However, the built asset security manager shall remain responsible for the operational effectiveness of each of these aspects of security.

7 Developing the built asset security strategy (BASS)

7.1 General

7.1.1 The employer or asset owner shall develop and maintain a BASS which shall include:

a) the security requirements determined by the security triage process;

b) the built asset risk management strategy (see **7.2**) comprising:

   i) the record of the risk assessment;

   ii) the record of the risk mitigation process;

   iii) the measures to be implemented;

   iv) a summary of the residual risks;

c) a list of those to be informed about the residual risks; and

d) the mechanisms for reviewing and updating the BASS (see **7.3**).

7.1.2 The BASS shall take into consideration relevant legislation and standards which are relevant to the built asset under consideration (see Clause **13**).

7.1.3 Access to any part of the BASS which specifies the security protection level or classification level of a project, details security risks or potential mitigation measures, for example sensitive requirements or systems, shall be managed on a strict need-to-know basis, with all such information subject to security measures, appropriate to the level of risk, with regard to its creation, storage, distribution and use.

NOTE 1 *For UK public sector construction projects, the employer's representatives and project delivery team should consult the separate guidance material issued regarding security and resilience of public buildings by contacting CPNI.*

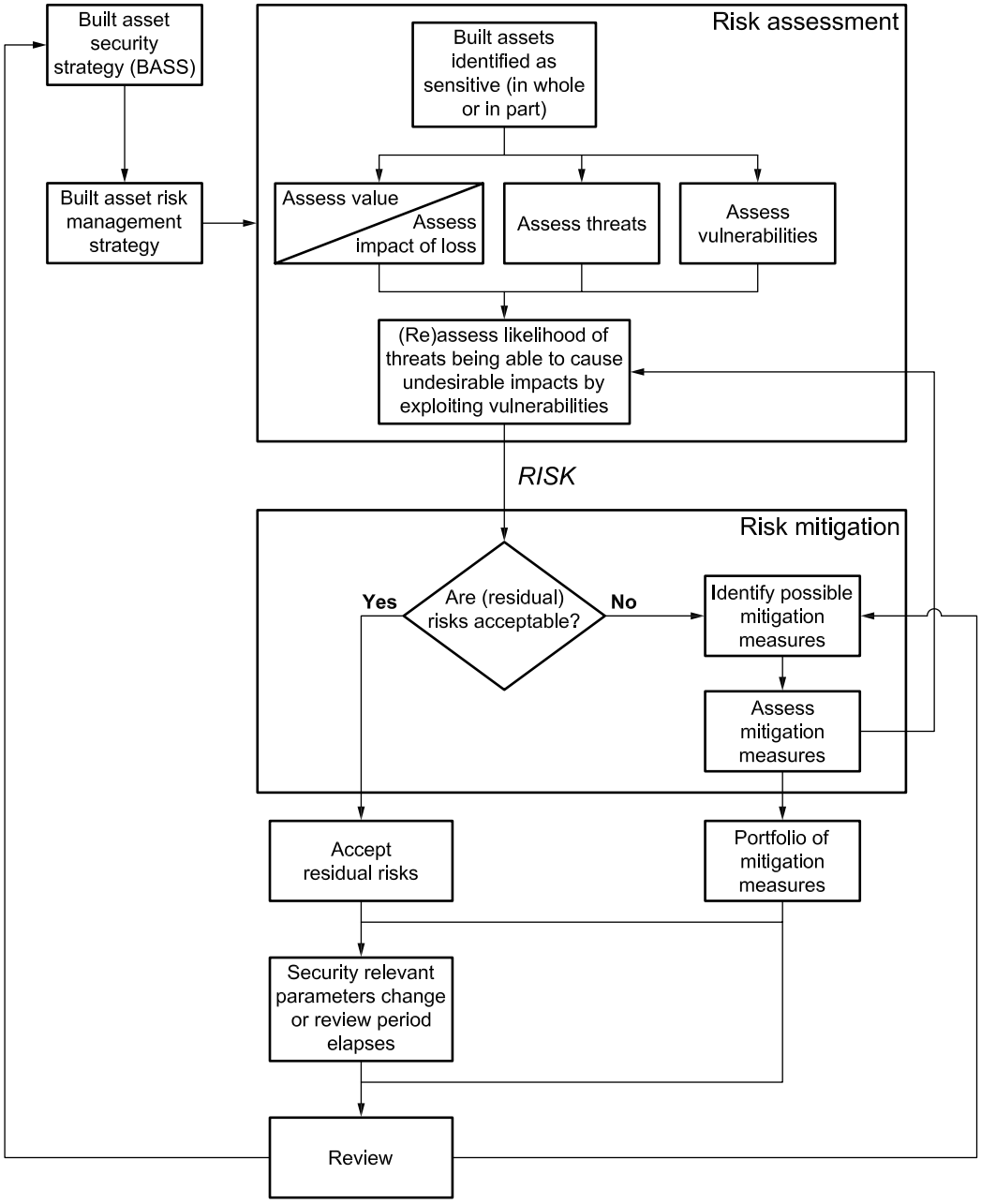
NOTE 2 *Significant volumes of information may be generated during a project's strategy stage when the employer is considering business need. This information may be particularly sensitive when political, economic, social, technology, legal and environmental issues are being examined, and when stakeholders are being identified and assessed.*

7.1.4 Where the project or asset management of the built asset will involve access to information covered by the Official Secrets Act [5] (see **13.1.6**) or to sensitive built assets, the employer shall notify the supply chain at the bid stage of any specific security requirements that will affect: its individual contracts; technology systems that may form part of the supply chain; premises; and personnel.

7.2 The built asset risk management strategy

7.2.1 The employer or asset owner shall develop a risk management strategy for the built asset (see Figure 6).

Figure 6 – The built asset risk management strategy



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

7.2.2 Undertaking a risk assessment for the built asset

7.2.2.1 The employer or asset owner shall, in addition to considering opportunities, undertake a strategic risk assessment for the built asset by assessing the potential threats and potential vulnerabilities in combination with an assessment of the nature of the harm which could be caused to: 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, be they societal, environmental and/or commercial.

***NOTE** Where information about an existing asset has already been published, the employer or asset owner should consider appropriate measures to manage any risks arising, recognising that once information has been published on the internet or otherwise made publicly available, it is virtually impossible to delete, destroy, remove or secure all copies of it.*

7.2.2.2 The risk assessment shall identify and record the high level security risks associated with four areas: people, process, physical and technological security.

***NOTE** Further advice on the risk assessment process is available on the CPNI website and/or by contacting CPNI.*

7.2.2.3 The risk assessment shall also identify and record risks associated with:

a) the employer's intellectual property and commercially sensitive data or information;

   ***NOTE 1** The employer or asset owner should protect any sensitive data or information regarding its business plans, operations, and intentions which it makes available to the supply chain. This is particularly important where it is stored and processed on IT systems and personal IT equipment that do not belong to the employer and which may become the target for third parties seeking to obtain commercially sensitive data or information about the employer or asset owner, its plans and current operations.*

   ***NOTE 2** In addition to any process or technical security measures it may be prudent for the employer or asset owner to put in place appropriate non-disclosure or confidentiality agreements.*

b) any intellectual property owned by the supply chain and its commercially sensitive data or information to which the employer or asset owner will have access; and

   ***NOTE** The CIC BIM Protocol[6] envisages that a significant volume of intellectual property created and owned by advisors, consultants and suppliers might be stored in the CDE. This creates security concerns where the intellectual property is particularly valuable or attractive, or where access to the data or information might increase security risks to the built asset or the asset's users. The BASS for the asset or project should address the security of intellectual property and the control of access to it.*

c) information collected or held about other built assets in the vicinity of the work being undertaken by the project and the finished built asset (see **5.4**).

7.2.3 Determining the risk mitigation approach

7.2.3.1 The employer or asset owner shall identify and record possible mitigation measures for each identified risk from the perspective of preserving or protecting the built asset in order that it delivers optimum commercial, economic and social value to the asset's owner, users and stakeholders.

7.2.3.2 The assessment of each measure shall identify and record:

a) the cost of the mitigation measure and its implementation;

b) the risk reduction which could be achieved;

c) the predicted cost saving;

d) other impacts which the mitigation measure might have on the asset (which could include usability, efficiency and appearance);

e) the potential for the measure to create further vulnerabilities; and

f) whether the measure delivers any business benefits.

***NOTE 1** Business benefits which might be delivered by introducing appropriate security controls as countermeasures might include:*

- *reducing overall business risk;*
- *aiding development of robust and repeatable business processes; and*
- *ensuring the value of assets and information is understood and measures are taken to protect both.*

***NOTE 2** Where the built asset is a portfolio or network of assets, the risk mitigation should take into account the impact on the portfolio or network of any security threat to particular assets.*

7.2.3.3 The employer or asset owner shall use this information to determine what mitigation measures, if any, are put in place for each of the risks identified in the risk assessment.

***NOTE** Achieving effective security requires the use of proportionate countermeasures to the potential*

[6] Available from: http://cic.org.uk/download.php?f=the-bim-protocol.pdf

people, process, physical and technological risks related to the built asset. A proportionate countermeasure should be pragmatic, appropriate and cost effective.

7.2.3.4 The employer or asset owner shall establish a suitable mechanism throughout the lifecycle of the asset for reviewing the effectiveness of the current mitigation measures, including re-examining potential mitigation measures when those in place are not delivering the desired outcome.

7.2.4 Residual risks

7.2.4.1 Following the risk mitigation process, the employer or asset owner shall identify and record any residual risks.

7.2.4.2 The employer or asset owner shall continue to undertake the risk assessment and risk mitigation processes on these residual risks until a point is reached where the organization's risk appetite is not exceeded.

7.2.4.3 The employer or asset owner shall record the whole of this process and document the accepted residual risks.

7.3 Review of the BASS

7.3.1 The employer or asset owner shall establish a suitable mechanism for performing periodic reviews of the BASS throughout the lifecycle of the built asset to identify and assess any risks which have changed for political, economic, social, technological, legal or environmental reasons, and which impact on the built asset, asset information and/or digital systems.

***NOTE** For portfolios of assets, the BASS may need to be reviewed at a higher frequency in relation to any assets or systems which are deemed to be more sensitive.*

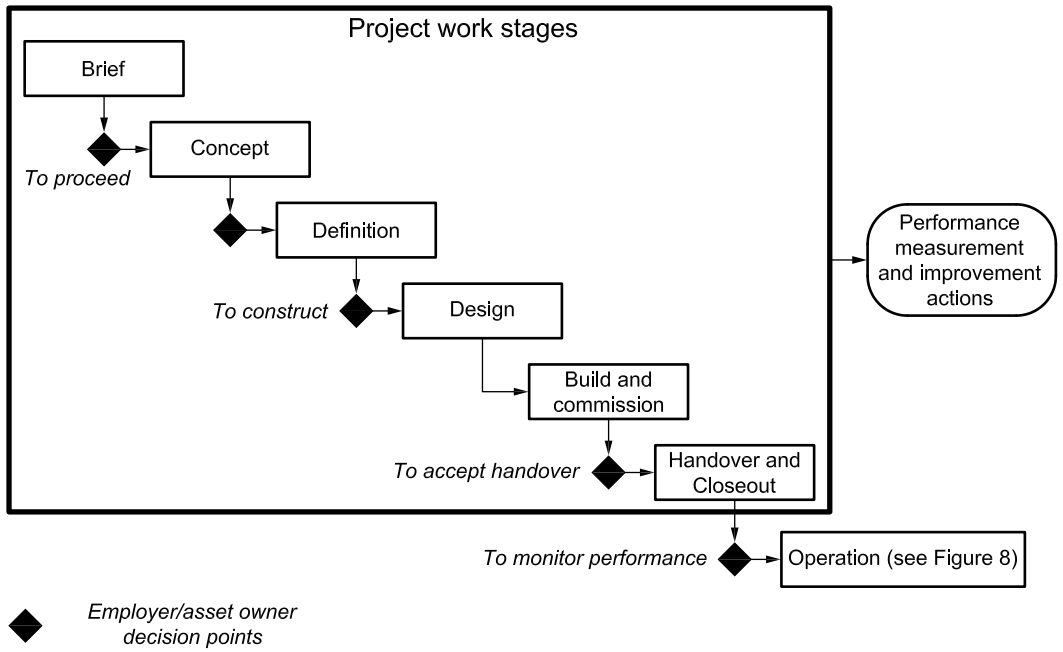
7.3.2 Reviews shall also be undertaken at major milestones in the built asset's lifecycle, e.g. when moving from design into build, and from build into operation.

***NOTE** The work stages and decision points within a project are shown in Figure 7.*

7.3.3 The employer or asset owner shall establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on the built asset, asset information and/or digital systems. The triggers for initiating such a review and the timetable for its completion shall be set out within the BASS documentation.

***NOTE** Events that might require event-triggered reviews are listed in **5.1.1**, Note 1.*

Figure 7 – The project work stages and decision points



***NOTE** Developed from source material provided by CPNI, Alexandra Luck and Hugh Boyes.*

8 Developing a built asset security management plan (BASMP)

8.1 General

8.1.1 The employer or asset owner shall develop, maintain and implement a BASMP for the lifecycle of the built asset which addresses the specific security risks or combinations of risks identified in the BASS in a consistent and holistic manner (see Figure 2).

8.1.2 The BASMP shall comprise the following elements:

a) covering the people, process, physical and technological aspects of the built asset, the related asset information, and building-related systems (see **8.2** to **8.5**):

   i) policies which set out the security-related business rules derived from the BASS;

   ii) processes which are derived from the security policies and provide guidance on their consistent implementation throughout the lifecycle of the asset; and

   iii) procedures that comprise the detailed work instructions relating to repeatable and consistent mechanisms for the implementation and operational delivery of the processes;

   NOTE 1 *As an example:*

   i) a policy may be required relating to the management of access to a CDE which contains data or information about a sensitive asset;

   ii) the process accompanying the policy will identify the key steps for identifying an entitlement to access specific asset information, and the mechanisms for granting and revoking access in order to fulfil the requirements of the policy;

   iii) the procedure for applying for an individual to have access to the CDE might include a requirement to obtain information relating to:

   - *the individual's personal and contact details;*
   - *their role;*
   - *the areas of the CDE which they are entitled to access;*
   - *the privileges required (create, read, update, delete, archive);*
   - *the duration of access; and*
   - *the person required to approve the grant of access.*

   NOTE 2 *A failure to maintain processes can result in them being ignored or lead to the adoption of informal local practices. In either case the result might be to undermine the relevant security policies.*

   NOTE 3 *The failure to develop and maintain effective security procedures can result in breakdown of processes and lead to personnel ignoring or bypassing security controls.*

b) where applicable, project logistical security requirements (see **8.6);**

c) the process and procedures for the provision of information to third parties (see **8.7);**

d) accountability and responsibility for security (see **8.8**);

e) monitoring and auditing requirements (see **8.9**);

f) the mechanisms for reviewing and updating the BASMP (see **8.10**);

g) a plan for the storage and protection of asset information that is retained during the period required to comply with legal or other regulatory requirements and with any specific requirements of the employer, whichever is longer, as well as that retained for asset management purposes. The plan shall also detail the arrangements for the secure disposal of the asset information when it is no longer required for these purposes;

h) a security breach/incident management plan (SB/IMP) (see Clause **9**); and

i) an outline of the contractual measures required for the adoption of an appropriate and proportionate security-minded approach throughout the supply chain (see **11.4**).

NOTE *Any gaps or omissions in the BASMP will reduce both the effectiveness of the BASS and the chance that an effective, holistic, security-minded culture will be created.*

8.1.3 When undertaking a project, the employer shall use the BASMP to inform its strategic business case and strategic brief, and through those, its plain language questions and subsequent EIR (see Figure 2).

NOTE 1 *The plain language questions should be written so as to allow the employer to ascertain how security is being addressed throughout the project lifecycle.*

NOTE 2 *The BASMP should, where appropriate, be cross-referenced to the other security management policies and plans which the employer or asset owner has in place.*

8.1.4 Access to any part of the BASMP which details the security level or classification of a project, sensitive requirements or systems, or security-related policies, processes and procedures shall be managed on a strict need-to-know basis, with all such information subject to appropriate security measures with regard to its creation, storage, distribution and use.

NOTE 1 *The BASMP should be structured so that individual sections, chapters or annexes can easily be distributed to the supply chain without needing to circulate the whole document. For example, the SBI/IMP should be widely available and therefore should be written to enable distribution to all parties having access to the CDE.*

NOTE 2 *The information available should be sufficient to allow health and safety requirements to be met.*

8.2 Personnel aspects

The employer or asset owner shall develop, manage and implement policies, processes and procedures relating to personnel security which shall include, where appropriate and proportionate to the identified security risks:

a) identification of high-risk positions within the employer's or asset owner's organization and any organizations employed on the contract or providing services to the employer or asset owner;

   NOTE *A high-risk position is defined as one which has access to the details of the BASS, BASMP and/or information relating to sensitive assets, or one that fulfils an IT system administration or information management role.*

b) security screening and vetting requirements for individuals employed on the contract, both in general and specific roles;

c) the security competence requirements of individuals in specific roles;

d) the general security awareness and training requirements to develop and promote a security-minded culture;

e) the role-based security training requirements in its supply chain to facilitate the adoption and maintenance of a security-minded culture;

   NOTE *Role-based security training may be required by a wide range of individuals involved with a project or built asset, including:*

   i) security personnel within suppliers or contractors;

   ii) the information manager and those responsible for managing information within their own organization;

   iii) purchasing personnel (regarding the security aspects of contracts); and

   iv) personnel managers (regarding the handling of the insider threat and disciplinary matters relating to security breaches).

f) the induction of personnel and organizations joining the project delivery team or providing services to the employer or asset owner so that they are appropriately briefed on their responsibilities and the required security-minded culture, including:

   i) the need to provide and record general security awareness training as part of a project, or ongoing operations, alongside health and safety, project or site familiarisation and other similar training;

   ii) mandatory topics to be covered by these awareness sessions (e.g. good cyber hygiene practices, the arrangements for accessing information and gaining access to the site of the built asset, etc.) and the required learning outcomes from each;

   NOTE *Provided this awareness training is delivered in accordance with a set of defined learning outcomes consistent with the BASMP, it may be delivered on behalf of the employer or asset owner by the training organization that delivers other health and safety and project or site familiarisation training.*

g) access requirements to models and associated asset information; and

   NOTE 1 *The access requirements should address the information lifecycle (i.e. the ability to create, read, update and delete information) as well as privileges such as the ability to approve or reject a transaction.*

   NOTE 2 *Access to data and information relating to sensitive assets and systems should be limited to those who have a genuine need-to-know in order to fulfill their job role or function. For example, during the construction phase, a groundworks contractor does not need to know the detail of the design and specification of the IT and security systems installation that will be installed within a building. However, they will need to be aware of underground cable and building service routes.*

h) demobilisation of personnel who are leaving the project or asset management team, including the secure deletion, destruction and/or removal of access to project or asset information, from their personal devices.

   NOTE *With the trend of some organizations towards bring your own device (BYOD) and the*

use of individual contractors or consultants, there is a need to ensure that sensitive information is not retained on their personal IT devices once they are demobilised. Where the individual requires continuing access to the information for the period required to comply with legal or other regulatory requirements and with any specific requirements of the employer, whichever is longer, appropriate measures should be put in place to protect the information.

8.3 Process aspects

The employer or asset owner shall develop, manage and implement policies, processes and procedures relating to process aspects which shall include as a minimum:

a) granting individuals access to the CDE;

b) handling asset information relating to neighbouring, separately-owned assets including utilities;

c) handling sensitive and/or classified information and documents;

***NOTE** If data is to be exported for activities such as rendering, appropriate security measures should be applied to protect sensitive information.*

d) version and change control processes and procedures for asset information.

8.4 Physical aspects

The employer or asset owner shall develop, manage and implement policies, processes and procedures relating to physical aspects which shall include as a minimum:

a) physical security measures required at the locations used to design, deliver, operate and support the built asset, including the provider of the CDE if applicable;

b) physical security measures required at the location of the new or existing built asset;

c) where appropriate, protection of neighbouring built assets not otherwise generally visible and/or accessible;

d) protective measures required for equipment comprising the CDE;

e) protective measures associated with the use of computing and electronic devices on the construction site; and

f) protective measures associated with the use of computing and electronic devices on, or in, the completed built asset.

8.5 Technical aspects

The employer or asset owner shall develop, manage and implement policies, processes and procedures relating to technical aspects which shall include as a minimum:

a) measures related to the cyber security of systems processing and storing project information;

b) measures related to the cyber security of systems acquiring, processing and storing asset information;

***NOTE** A risk-based approach to the management of all systems storing, processing and forwarding information should be taken.*

c) the security of interconnections between such systems;

d) configuration management and change control processes and procedures for the systems processing and storing project and asset information;

e) the required level of software trustworthiness;

***NOTE** Software trustworthiness is based on the principles of safety, reliability, availability, resilience and security which, along with software trustworthiness levels and implementation framework, are described in PAS 754:2014.*

f) demobilisation of organizations who are leaving the project or asset management team, including the secure deletion and/or destruction of project or asset information held by those organizations, and/or removal of access to that information; and

g) where asset information is retained for the period required to comply with legal or other regulatory requirements, and with any specific requirements of the employer, whichever is longer, the measures to be applied by design consultants, contractors and the supply chain regarding the security of that retained information, and the measures to be applied following that period to ensure secure deletion, destruction and/or removal of access to project or asset information.

***NOTE 1** An increasing number of cloud solutions are available for project collaboration and asset management purposes. The term 'cloud' covers a diverse range of solutions, including software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). There are also a variety of delivery models including vendor (external) cloud, private (internal) cloud, hybrid cloud and community cloud[7),8)].*

[7)] For further information see http://www.cpni.gov.uk/documents/publications/2010/2010005-vp_cloud_computing.pdf?epslanguage=en-gb

[8)] For further information see http://www.theiet.org/factfiles/it/cloud-computing-page.cfm and any associated documents.

NOTE 2 *There are a number of risks associated with cloud computing, which could include:*

a) lack of standards;

b) confused security and privacy model(s);

c) extended enterprise risk;

d) data leakage;

e) application and platform security risks;

f) legal disclosure and interception in a foreign territory;

g) discontinuity of service;

h) vendor lock-in; and

i) lack of third party assurance.

NOTE 3 *Risk mitigation measures that should be considered include:*

a) contractual agreements covering data location and cross-border data transfers, quality assurance principles, continuity assurance and recovery guarantees, compensation and service termination issues, and UK legal jurisdiction;

b) clarification of security model(s), including restrictions on access to data hosted on common platforms;

c) data encryption to ensure secure data at rest and in transit;

d) separation of data, i.e. demonstrable separation of the asset information from other customer or asset data; and

e) assurance of quality of service levels, and compliance with privacy and security requirements.

8.6 Project logistical security requirements

Where applicable, the BASMP shall set out:

a) the requirement for advice to be sought from specialist sub-contractors on sensitive assets or systems in order that the developing design is consistent with the needs of those assets or systems;

b) the requirement for the construction methodology to be such that the construction or installation of sensitive assets, and the fitting-out of sensitive areas, to be programmed for a time where access to those assets or areas can be limited to a number of specialist contractors;

c) the requirement for lead designers to establish the logistics required for the installation of any sensitive assets with specific handling requirements to determine the latest stage in the construction process at which they can be installed;

d) appropriate and proportionate security measures around any sensitive assets which, for logistical reasons, have to be installed earlier than would generally be desirable; and

e) appropriate and proportionate measures to limit, or disrupt the success of, physical hostile reconnaissance.

8.7 Provision of data or information to third parties

8.7.1 Planning applications

The BASMP shall detail the approach to be taken in the submission of models and construction information as part of the statutory planning process and shall require that sensitive information be suitably separated and protected. This may include redaction or removal of space or room labels, the removal of information regarding sensitive features, uses of protective measures and providing unstructured information in formats such as hard copy, images or non-interactive PDF formats, rather than giving access to interactive models.

NOTE *The submission of digital data and models to planning, statutory and regulatory authorities when seeking planning consent for a new asset or changes to an existing asset can reveal security sensitive information about the asset and its operational use. Where a project involves such information, the employer or its representative, should enter into a dialogue with the local planning authority prior to submission of information to the authority, so that suitable measures can be put in place*[9]*.*

8.7.2 Other regulatory and statutory processes

The BASMP shall detail the approach to the supply and exchange of data and information with third parties when complying with regulatory and statutory process relating to the design, construction or operation of a built asset, for example building control regulation and fire regulations.

NOTE *Where the third party is subject to the provisions of the Freedom of Information Act [3] and other such public access or transparency legislation, the employer or asset owner should liaise with the third party to ensure that any sensitive information is afforded appropriate protection.*

[9] Further information can be found at: http://planningguidance.planningportal.gov.uk/blog/guidance/crown-development/sensitive-information-in-planning-applications/

8.7.3 Public access to information

The BASMP shall detail the approach to protect sensitive data or information that shall be taken where a request for information is received by an organization that is covered by Environmental Information Regulations [2] or Freedom of Information [3] legislation. This shall consider the impact of releasing the asset-related information, including the potential issues arising from data aggregation.

NOTE 1 *For public organizations, where data or information may be requested under Environmental Information Regulations [2] or Freedom of Information [3] legislation, steps should be taken by such an organization to:*

- *prevent leakage of security-related information;*
- *protect commercially sensitive data and intellectual property; and*
- *safeguard personally identifiable information, taking into account the range of attributes that can be used to identify individuals.*

Based on an assessment of the risk of disclosing detailed information about a built asset, it might be necessary and appropriate to adopt measures to reduce the detail and granularity. Measures that might be necessary include, but are not limited to:

- *limiting access to particular types of asset information;*
- *redacting sensitive information (e.g. description of the functions of individual rooms); and*
- *providing unstructured information in formats such as hard copy, images or non-interactive PDF formats, rather than giving access to interactive models.*

NOTE 2 *Public sector organizations and the owners and operators of the critical national infrastructure should consult the separate guidance material prepared by CPNI.*

8.7.4 Public presentations

The BASMP shall detail aspects of the built asset and/or sensitive assets or systems in relation to specification, design, construction and operation that are not to be discussed or displayed at public events, or made publicly available on websites or in marketing and other material.

NOTE *As a general principle, details, illustrations and models of sensitive security features in any building should not be displayed at public events or made publicly available.*

8.8 Managing accountability and responsibility for security

The BASMP shall:

a) detail the maintenance of security accountability within the employer or asset owner;

b) detail the management of security responsibilities within the supply chain, including the requirement for security to be retained at senior levels within the supply chain, with responsibility delegated appropriately, in order that it can be effectively and efficiently managed;

NOTE 1 *In order that security policies, processes and procedures are effective, it is essential that there is a flow down of responsibility within both the organization and the contracts/supply chain.*

NOTE 2 *In large projects the formation of a security committee, consisting of the built asset security manager, the information manager and the key roles in the consultants and contractors with responsibility for security, is recommended. This provides a mechanism for: aiding communications regarding the flow of responsibility; sharing of security-related information; increasing overall accountability; and the embedding of security-minded behaviour into the project.*

NOTE 3 *Where there is extensive use of contract personnel, the CPNI Good Practice Guide[10] on the secure procurement of contracting personnel is relevant.*

c) for each individual policy in the BASMP:

i) identify the senior role within the relevant entity accountable for its implementation;

ii) identify the senior role within the relevant entity accountable for its maintenance; and

iii) identify the individual or organization that has day-to-day responsibility for managing its delivery

NOTE *In the built environment, projects and the ownership and use of the built asset can involve a complex set of stakeholders and relationships. Whilst adhering to the security policies is a responsibility of all individuals involved in the design and operation of the built asset, there is a need for clear accountability for security management.*

[10] Available from: http://www.cpni.gov.uk/Documents/Publications/2014/2014-07-29-contracting-guidance.pdf

8.9 Monitoring and auditing

8.9.1 The BASMP shall set out the appropriate and proportionate monitoring and auditing measures which shall take place across the lifecycle of the asset, which shall include assessing:

a) the implementation of all security policies, processes and procedures affecting the built asset, including;
   i) the exchange and delivery of asset information throughout the asset lifecycle; and
   ii) the handling or storage arrangements implemented for sensitive information;

   ***NOTE** It is important that for sensitive assets and systems, additional information should not be included in the information exchange beyond the set of information that has been specified.*

b) the compliance of its suppliers with the security policies, processes and procedures specified in the BASMP including, within a project, checking the model(s) and accompanying information contained at each information exchange to assess their consistency with the employer's security requirements, as a minimum on a risk-based sampling approach;

   ***NOTE** As a project progresses through the stages and the level of detail becomes more extensive, the application of risk-based sampling to security controls should be more selective/focussed.*

c) sensitive asset information contained in the model(s), accompanying information and databases, with the removal of any information which compromises the product; and

d) the management of security controls that operate throughout the operational lifecycle of the built asset.

***NOTE 1** The employer or asset owner may delegate some responsibility for compliance verification to a lead facilities management supplier, but will retain accountability for the overall effectiveness of security controls.*

***NOTE 2** This monitoring or auditing will be in addition to any actions that may result from an incident or breach.*

8.9.2 The BASMP shall require that only those suitably qualified and experienced shall undertake this monitoring and auditing work.

8.10 Review of the BASMP

8.10.1 The employer or asset owner shall establish a suitable mechanism for performing periodic reviews of the BASMP to check that it remains fit-for-purpose. Where necessary, it shall be updated to reflect any identified gaps, shortcomings or organizational changes, or changes which have arisen for political, economic, social, technological, legal or environmental reasons, and which impact on the built asset, asset information and/or digital systems.

***NOTE 1** For portfolios of assets, the BASMP may need to be reviewed at a higher frequency in relation to any assets or systems which are deemed to be more sensitive.*

***NOTE 2** The employer or asset owner should maintain awareness of legal and regulatory changes that could affect the security of the built asset and related asset information and where necessary, make adjustments in policies, processes and procedures to comply with those changes.*

***NOTE 3** Changes in the political, legislative or regulatory environment could have an impact on information held in the CDE or asset management repository. This might necessitate changes to the arrangements for sharing or use of asset information, or require the introduction of additional security or privacy measures to protect sensitive or personally identifiable information. Legal or regulatory changes could affect the structure and/or operation of a built asset, for example in relation to the security or resilience of critical infrastructure or compliance with building and environmental regulations. They may also require changes to the creation, storage and use of asset information, for example, public access to information on environmental and energy aspects of the built asset.*

***NOTE 4** If changes to the BASMP are introduced, the changes could potentially constitute a scope change under a contract and the potential impact of this change should be accounted for in the review process.*

8.10.2 Reviews shall be undertaken at major milestones in the built asset's lifecycle, e.g. when moving from design into build, and from build into operation (see Figure 7).

8.10.3 The employer or asset owner shall establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on the built asset, asset information and/or digital systems. The triggers for initiating such a review and the timetable for its completion shall be set out within the BASMP documentation.

***NOTE** Events that might require event-triggered reviews, are listed in **5.1.1**, Note 1.*

9 Developing a security breach/incident management plan (SB/IMP)

9.1 General

9.1.1 If the provisions in the BASS and BASMP fail, the employer or asset owner shall consider the business continuity and disaster recovery scenarios that may affect the operation and viability of projects utilizing digital technologies and digital built assets, and shall put in place appropriate risk assessment and risk mitigation plans, to reduce the impact of failure or disruption on its operations and those of its stakeholders.

9.1.2 The employer or asset owner shall create and maintain a SB/IMP tailored to the enterprise, its function, and the assets that may be affected, to be followed both by its own personnel and, where appropriate, by its supply chain.

9.1.3 The SB/IMP is intended to enable an effective and coordinated response to incidents and shall include:

a) a record of the risk assessment of potential risks to the organization, its function, its assets, personnel and third parties in the event of a security breach or incident (see **9.2**);
b) a record of the risk mitigation measures including:
   i) the forensic readiness measures required to enable, when required, the capture of forensic information about an incident for use by law enforcement, and/or detailed analysis of the root causes of the incidents;
   ii) the process to be followed on discovery of a breach/incident (including near misses, i.e. narrow avoidance of a security breach/incident) (see **9.3.1**);
   iii) business continuity measures required in the event of system failure, impairment or non-availability;
   iv) the disaster/incident recovery actions required in the event of serious failure scenarios;
   v) steps to be taken to contain and recover from the event (see **9.3.2**);
c) the review process to be followed following a security breach or incident, including:
   i) the process for assessing the ongoing risk (see **9.4.1**);
   ii) the process for evaluating the breach/incident and the response (see **9.4.2**);
d) a review of the CDE hosting provider's incident management plan where applicable;
e) the need for contractual provisions to handle breaches/incidents caused by a professional advisor, contractor or supplier (see **11.4.6**); and
f) the mechanisms for reviewing and updating the SB/IMP (see **9.5**).

NOTE *It is important to ensure that the disaster recovery systems afford the same level of security for the asset information as the systems in use on a day-to-day basis.*

9.1.4 Access to any part of the SB/IMP which details sensitive information (for example, risks to the enterprise, its function, its assets, personnel and third parties) shall be managed on a strict need-to-know basis, with the information contained within it subject to appropriate security measures with regard to its creation, storage, distribution and use. Key parts of the SB/IMP shall be widely available and shall therefore be written to enable, in the main, distribution to all parties having access to the CDE.

9.2 Risk assessment of the potential risks in the event of a security breach or incident

9.2.1 General

The employer or asset owner shall follow the risk assessment process shown in Figure 6 to assess the potential risks arising in the event of a security breach or incident.

9.2.2 Types of security breaches/incident

The employer or asset owner shall be aware of the range of potential security breaches or incidents which are applicable to its business, assets and personnel.

NOTE 1 *Security breaches can take a number of forms including:*

a) loss or theft of documents, storage media, IT equipment, attractive or valuable items;
b) loss, theft or unauthorized access to information or data;

c) loss, compromise, unauthorized manipulation or change of project or asset information;

d) unauthorized access to the built asset, or a restricted access area within the built asset;

e) loss of keys, access control tokens, passes, etc.;

f) planting of bugs or other surveillance devices; and

g) unauthorized access to, misuse of, or fraudulent use of IT systems.

***NOTE 2** A security breach is an incident in which any of the above types of circumstance (or other pertinent to the employer or asset owner) occurs, either accidently or deliberately.*

***NOTE 3** A near-miss is an incident in which a security breach is narrowly avoided either accidentally or through deliberate action.*

9.2.3 Understanding the type and potential impact of security breaches on a built asset

Taking into account the nature of the built asset, the employer or asset owner shall identify the types of security breaches that might occur, their potential impact and how a breach could involve and impact on stakeholders and other parties.

***NOTE 1** The severity of a breach or incident depends on the extent to which it harms an organization and its stakeholders. The harm may be physical, financial, economic or reputational. From a cyber-security perspective, there is a risk that a breach could result in data or information being compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorized individuals.*

***NOTE 2** Being prepared to handle security breaches can reduce the impact or damage by containing the situation.*

9.2.4 Understanding the potential impact of failure or impaired performance of systems

The employer or asset owner shall determine the nature and extent of business risks associated with the failure or impaired performance of extensive systems that depend on information technology, both internally and within the supporting supply chain.

***NOTE** Business risks might be manifest as a loss of availability, functionality or performance, or the loss or corruption of digital artefacts. Risks can arise from failure of system components, whether hardware or software related, loss of power or communications (connectivity), or malicious acts such as damage caused by malware, hackers or disaffected personnel.*

9.3 Risk mitigation

9.3.1 Discovery of a breach or incident

9.3.1.1 The employer or asset owner shall set out the steps to be taken in the event of a discovery of a breach or incident which shall include:

a) the persons to be contacted immediately and their contact details;

b) the procedures used to identify the concerned parties;

c) the mechanisms for notifying concerned parties and information to be provided;

d) handling any third party, regulator, media or public interest in the event of a breach or incident.

9.3.1.2 In the event of an incident where there has been loss or theft of data, unauthorized access to data, information or systems, or interference with computer systems, the relevant parties shall be notified.

***NOTE 1** Where discovery procedures are not established by project-specific security provisions in appointment documents and contracts, it is recommended that employers incorporate discovery requirements in non-disclosure agreements.*

***NOTE 2** The parties to be notified can be determined by whether the breach occurs as part of a project or during ongoing operations, and by legal and contractual obligations. These parties might include the employer, asset owner and operator, the data owner, and in the event of compromise of personally identifiable information, the affected individuals. Other parties might include customers, clients, personnel, regulatory bodies, the Information Commissioner, and law enforcement agencies.*

9.3.2 Containment and recovery

9.3.2.1 The employer or asset owner shall set out the steps to be taken in the event of a security breach/ incident to contain and recover from the event that include:

a) measures for reducing further damage or loss;

b) assessment of what has been lost, compromised, damaged or corrupted; and

c) the circumstances under which a collection of evidence for law enforcement purposes is required.

9.3.2.2 Under circumstances where it is necessary to collect evidence for law enforcement purposes, all evidence (i.e. both physical and digital) that may aid an investigation to identify the cause of the event and the perpetrators, shall be preserved and collected before any recovery actions are taken, unless the immediate need for such actions is critical to life.

***NOTE** It is important that forensic evidence is collected before recovery actions are taken, as these actions might destroy or contaminate the digital forensic evidence. The recovery actions for digital systems might involve restoring data and systems, remedial action to prevent further incidents and, following the initial recovery steps, security awareness training to reduce the risk or re-occurrence. For UK-based projects, any evidence collection for law enforcement purposes should be in accordance with ACPO Good Practice Guide for Digital Evidence (2012)[11].*

9.4 The review process

9.4.1 Assessment of ongoing risk

9.4.1.1 Following the initial containment and recovery actions, the employer or asset owner shall undertake an assessment of the ongoing risk. This assessment shall examine the causes of the event, identify potential countermeasures, and assess the residual risk as well as any potential new or exacerbated risk arising from the event.

9.4.1.2 Relevant policies, process and procedures shall be updated to reflect the findings of the assessment and to reduce the opportunity for, or where possible prevent, a re-occurrence.

9.4.2 Evaluation and response

9.4.2.1 Following the handling of a security breach/incident the employer or asset owner shall require the relevant organization to collaborate with it to undertake a post-incident evaluation of the event and the organization's response.

***NOTE 1** An important post-incident activity is the formal evaluation of the way that the event was handled. This checks the understanding of the cause of the breach or incident and objectively evaluates the effectiveness of the response. The aim is to allow lessons to be learned and shared with other parties involved.*

***NOTE 2** The employer or asset owner should specify how this obligation is cascaded through the supply chain and the responsibilities of the parties involved, and document it in the BASMP.*

***NOTE 3** The obligation to investigate security breaches or incidents is not intended to place unnecessary demands or burdens on the lower levels of the supply chain. However, it is important that these levels are not ignored or exempt, as they may often be involved in some of the more specialist and sensitive aspects of the design, construction, operation and maintenance of the built asset.*

9.4.2.2 Relevant policies, processes and procedures shall be updated to reflect the findings of the evaluation and to improve on the response to any future breach or incident.

***NOTE** Changes to prevent re-occurrence might involve re-training of personnel in the employer or asset owner and/or its supply chain, and revision of induction training for future personnel.*

9.5 Review of the SB/IMP

9.5.1 The employer or asset owner shall establish a suitable mechanism for performing periodic reviews of the SB/IMP across the lifecycle of the built asset to identify and assess any risks which have changed for political, economic, social, technological, legal or environmental reasons and which impact on the built asset, asset information and/or digital systems.

***NOTE** With the increased use of IT in construction and asset management, organizations may become more vulnerable to disruption due to failure of IT systems. It is recommended that any business continuity and disaster recovery measures that are set out in the SB/IMP are periodically reviewed and tested to ensure they are fit-for-purpose and effective.*

9.5.2 Reviews shall also be undertaken at major milestones in the built asset's lifecycle, e.g. when moving from design into build, and from build into operation.

9.5.3 The employer or asset owner shall establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on the built asset, asset information and/or digital systems. The triggers for initiating such a review, and the timetable for its completion, shall be set out within the SB/IMP documentation.

***NOTE** Events that might require event-triggered reviews, are listed in **5.1.1**, Note 1.*

[11] Available from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

10 Built asset security information requirements (BASIR)

10.1 The employer or asset owner shall develop, maintain and implement a BASIR for the lifecycle of the asset which sets out the specific information requirements around sensitive assets/systems based on the policies, processes and procedures contained in the BASMP.

10.2 The BASIR shall inform the asset information requirements (AIR) and, in a project, the EIR (see Figure 2).

10.3 The BASIR shall detail the employer or asset owner's requirements with regard to the arrangements for, and overseeing of, the secure capture, handling, dissemination, storage, access and use of all data and information pertaining to sensitive assets and systems, including:

a) conducting surveys;

   NOTE *Surveys, photographs or scans are capable of capturing sensitive operational information on fixtures and fittings, signs, boards or screens in the built asset. When arranging such surveys steps should be taken to mask or obscure such information prior to the survey taking place, or provide appropriate increased security to protect the captured information when the survey data is processed, stored or used.*

b) the arrangements for, and overseeing of, the secure storage of, and secure access to, all data and information pertaining to sensitive assets and systems retained for asset management purposes;

c) the arrangements for, and overseeing of, the secure storage of, secure access to, and ultimately secure disposal of, all project and/or asset information retained for the period required to comply with legal or other regulatory requirements together with any specific requirements of the employer, whichever is longer;

d) the maximum amount of information relating to sensitive assets or systems to be contained in model(s), the CDE, other databases and information exchanges;

e) the management and monitoring of access to information about sensitive assets and systems contained within any file or database by each organization with access to any of these files and/or databases;

f) the management of access to information relating to sensitive assets and systems to be on a need-to-know basis, with site contractors only having access to information that is relevant and necessary for the completion of their tasks;

   NOTE *During the build and commissioning activities, access to information should be managed as different suppliers interact with the construction of the built asset.*

g) the storing of operations and maintenance procedures for sensitive assets and systems in the CDE or asset management databases;

   NOTE *This should be based on a risk-based assessment which considers the impact of their loss or unauthorized access.*

h) notification of the requirement of any special handling or protection of information which has security sensitivity and has been provided to the employer or asset owner by an organization within the supply chain; and

i) within a project, the requirements for purpose-specific or volume-specific COBie files for security-related systems, and the need for these to be kept separate from the single coordinated COBie file.

   NOTE *The use of volume-specific COBie files is outlined in PAS 1192-2.*

NOTE *Where the circulation of sensitive information held in models needs to be managed during the design, construction or operation of an asset, the employer should communicate these requirements to the supply chain via the BASIR. The BIM protocol will enable these requirements to be contractually enforced.*

10.4 The BASIR shall be reviewed and updated to reflect any changes made to the BASMP.

11 Working with suppliers

11.1 Working outside formal contracts

The employer or asset owner shall take security-minded measures when working outside formal contracts (for example in pre-contract dealings) in relation to the access given to information relating to the built asset (see **11.2.1**).

11.2 Procurement

11.2.1 When tendering or re-tendering contracts relating to the procurement of:

- advisory/consultancy service;
- construction;
- facilities management (FM) and maintenance/ management; or
- other goods and services

and requiring the release of digital models and supporting data, the asset owner shall separate and suitably protect sensitive information and data while ensuring sufficient information is available to facilitate the transaction.

NOTE 1 *This separation and protection exercise might include: redaction or removal of space or room labels; removal of information regarding sensitive features, uses of protective measures; and provision of aggregated data, such as the number and type of objects, rather than providing access to all the detailed object information.*

NOTE 2 *The asset owner should ensure that tender agreements include appropriate confidentiality and security requirements that cover all parties, including sub-contractors and suppliers of a bidding supplier, associated in the preparation of a tender.*

11.2.2 Where the tender documentations contain sensitive information relating to the use of the asset, or high level information about the level of protection the asset requires, the employer shall require them to be subject to appropriate security measures. These measures shall be sufficient to:

a) limit access to this information to identified key roles;

b) exclude this information from any CDE;

c) exclude detailed requirements for any such physical asset security provisions from the tender documentation to be used by general contractors; and

d) enable general contractors to provide the correct infrastructure (for example, conduit and cable trays etc.), for the installation of sensitive assets or systems by specialist security-cleared contractors.

11.2.3 The employer or asset owner shall, as part of the supplier selection process, assess all tender documentation to establish how it is intended that the security requirements set out in the BASMP and BASIR would be met.

11.2.4 The employer or asset owner shall assess the security understanding, capability, competence and experience of the potential suppliers bidding for a contract, as well as any security training, coaching and support requirements.

11.3 Unsuccessful bidders

The employer or asset owner shall require that all relevant data or information is returned or destroyed. Where appropriate, the employer or asset owner shall require the supplier to verify that defined procedures have been completed.

11.4 Contractual measures

11.4.1 The employer or asset owner shall manage its supply chain security risks by having in place contractual provisions which support the security policies, processes and procedures contained within the BASMP.

NOTE 1 *The contractual terms should address the security requirements in a holistic manner by addressing people, process, physical and technology matters.*

NOTE 2 *Contractual provisions should be supported by the employer's ability to review the effectiveness of the supplier's security systems on a periodic basis. Employers with a greater security sensitivity should have developed standards and self-assessment systems which enable a supplier's capability and practice to be assessed on a regular basis.*

11.4.2 Where appropriate, the provisions shall include the flow down of contractual obligations from the primary professional advisors, contractors and suppliers, who are in direct contract with the employer or asset owner, through the layers of sub-contracts.

NOTE *It is not an acceptable security practice, at any level in the contract hierarchy, for the contracting party to pass, or to try to pass, all security responsibility to its sub-contractors or suppliers.*

11.4.3 The employer or asset owner shall insert a clause within the contractual documentation to enable adjustments in response to changes in the political, legislation or regulatory environment to be implemented.

NOTE *The employer or asset owner needs to be aware of the potential cost implications of any such changes.*

11.4.4 Where compliance with specific security standards is required (e.g. the provision of physical and technical protection for IT systems to a defined standard, the implementation of appropriate security regimes etc.), these shall be clearly identified in the contract along with any expected independent, third-party inspection or verification.

11.4.5 The employer or asset owner shall impose, through its contractual arrangements, a general obligation relating to acceptable use of models, data and information on all individuals with access to the built asset's systems and/or asset information.

11.4.6 To handle breaches caused by a professional advisor, contractor or supplier there shall be clear contractual provision for the reporting of the breach to the employer or asset owner, and for provision of assistance in the investigation and follow up actions.

11.4.7 The contractual measures shall include provisions that allow the employer or asset owner to review security measures and compliance with the relevant security policies, processes and procedures at any level in the contract chain.

NOTE *Depending on the sensitivity of the project or asset and the potential security threats, there might be a need for systems and personnel used by the professional advisors, contractors and suppliers to satisfy specific security requirements.*

11.4.8 The employer or asset owner shall monitor and enforce all security-related contractual provisions relating to its professional advisors, contractors and suppliers in order that they adopt an acceptable security-minded approach to the fulfilment of their contractual obligations.

NOTE *A balance should be struck between formal verification involving supplier audits and an honour/trust-based system of verification. The balance varies from project-to-project and supplier-to-supplier. Those suppliers handling sensitive information, or with access to sensitive parts of a built asset, should be subject to greater scrutiny than those involved in less sensitive roles. As part of this balance the employer or asset owner may consider it appropriate to advise suppliers that making false claims or statements about their security capability and/or adherence to required security controls can be treated as fraud.*

11.4.9 In a project the employer or asset owner shall input the necessary security and information delivery requirements for the built asset from the BASMP and BASIR into the EIR.

NOTE *In addition, the employer or asset owner may set out its information delivery requirements in an alternate form.*

11.4.10 Appropriate security measures shall be applied to the EIR where it contains sensitive information relating to the use of the asset, or high-level information about the level of protection the asset will require.

11.4.11 In a project, the employer or asset owner shall require that the supply chain proposals contained in the BIM execution plan (BEP) detail the secure processing and storage of, secure access to, and ultimately secure disposal of, all project information retained for the period required to comply with legal or other regulatory requirements, together with any specific requirements of the employer, whichever is longer.

11.4.12 Where any information is to be disposed of securely, the employer or asset owner shall require the proposals to detail the secure deletion and/or destruction of project or asset information, and removal of access to that information (e.g. where it is held in the CDE).

NOTE *In many projects utilizing digital technologies the employer or asset owner might not be interested in the large volume of planning and design information held in the CDE. The information that is being retained for the period required to comply with legal or other regulatory requirements together with any specific requirements of the employer, whichever is longer, should be appropriately stored and protected so as to prevent unauthorized access, to maintain availability, utility, integrity and authenticity. There will also be significant volumes of project related data on IT systems owned by the supply chain and stored in hard copy format in their premises.*

11.5 Post contract award

11.5.1 Within a project the employer shall:

a) check that the re-submitted BEP, master information delivery plan (MIDP) and task information delivery plan (TIDP) meet the employer's security requirements and provide sufficient information on security capabilities and responsibilities of the whole of the supply chain; and

b) work with the project delivery manager, the information manager, lead designer and other key roles to address any outstanding security issues.

11.5.2 The employer or asset owner shall require an organization's terms of reference for its personnel in key project, operational and asset management roles to identify the security responsibilities of each.

11.5.3 In defining the roles and responsibilities of each party in the supply chain, the employer or asset owner shall identify any high-risk positions and require that the relevant requirements of the BASMP are satisfied in the staffing of those roles.

11.5.4 The employer or asset owner shall require the advisory, consultancy and supplier organizations contracted by it, to manage all asset-related sensitive information they handle in accordance with the security policies, processes and procedures contained in the BASMP and the requirements of the BASIR.

NOTE 1 *Exchanges of project and asset information between professional advisors, designers, technical specialists and the supply chain might contain significant volumes of sensitive information, e.g. the detailed design and layout of security systems, analysis of protective measures, and pricing or contract-sensitive information. The handling and storage of such information should comply with the BASMP and BASIR, and the parties involved should manage access to this sensitive information on a strict need-to-know basis within their organizations.*

NOTE 2 *Team members should be cognisant that the aggregation of exchanged data could result in revealing sensitive information.*

11.5.5 The employer shall work with the design team to decide whether separate project volumes are required for aspects of the design relating to security systems (for example, routeing of infrastructure that supports sensitive systems and access routes) and implement accordingly.

NOTE 1 *In the example shown in PAS 1192-2, Figure 11, the employer may wish to restrict access to the communications and signalling volumes. For spatial coordination purposes a 3D zone may be allocated within the overall tunnel design, which allows for clash detection, but does not contain the detail of what cables, components, etc. are located within the allocated space. The detailed design of the communications and signalling systems would be held securely in separate models, accessible only to those personnel involved in their design, implementation and support. The exchange of information about these volumes would then be achieved through volume-specific COBie files.*

NOTE 2 *Further information on project volumes can be found in PAS 1192-2,* ***7.6****.*

11.6 End of contract

11.6.1 The employer or asset owner shall require any organization storing any data or information, to put procedures in place for the secure disposal of retained data at the end of the period required to comply with legal or other regulatory requirements, together with any specific requirements of the employer, whichever is longer, or when it is no longer required.

11.6.2 Upon the termination of a FM, maintenance or management contract, the employer or asset owner shall require that all relevant data or information is returned, destroyed or stored securely in accordance with contractual requirements. Where appropriate, the employer or asset owner shall require the supplier to verify that defined procedures have been completed.

NOTE *The FM, maintenance and management contract should define the procedures to be adopted for the post-contract management of information.*

11.6.3 The employer or asset owner shall require sufficient decommissioning and demobilization processes to be put in place to maintain the security of asset information.

12 Asset management

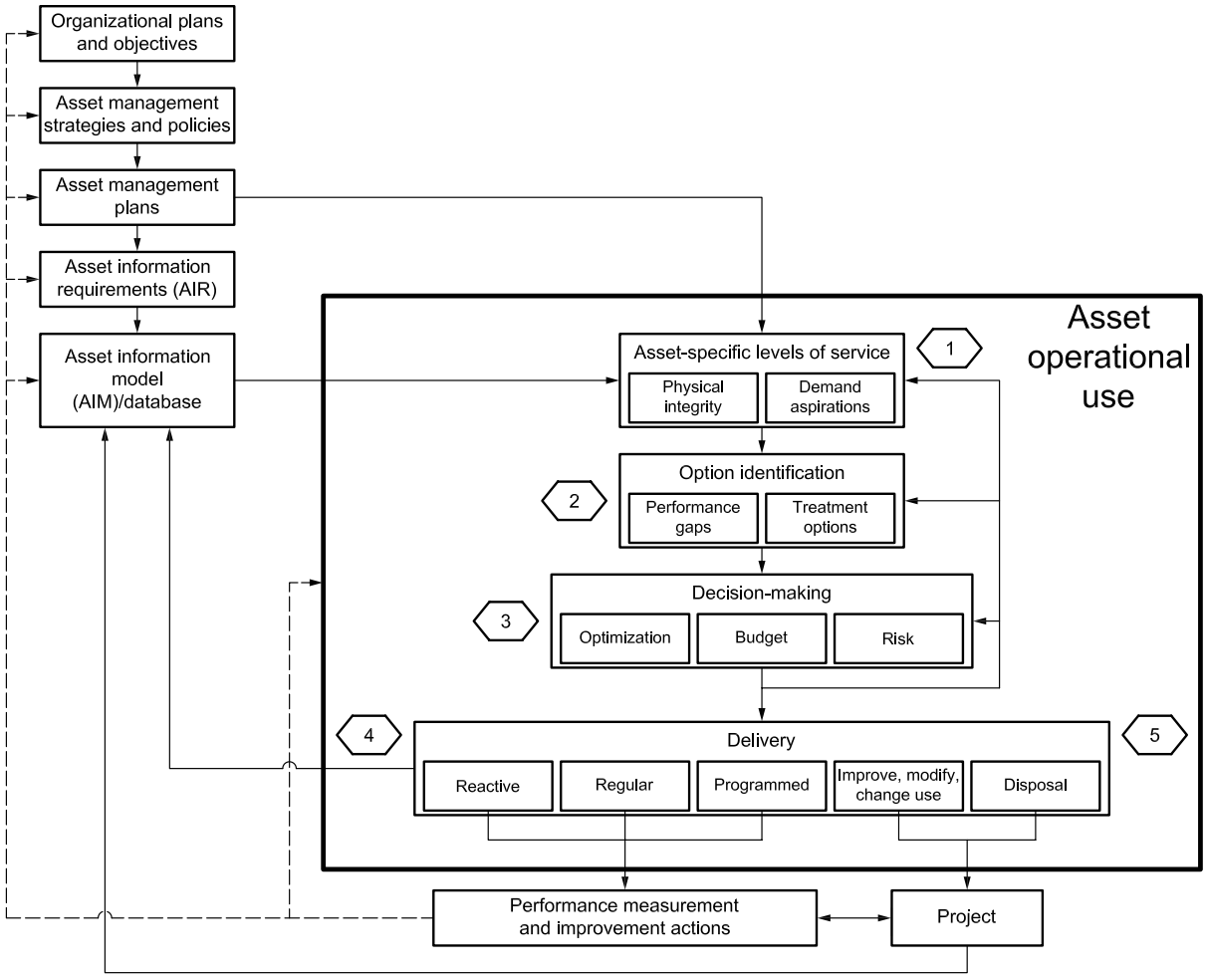
12.1 General

12.1.1 The asset owner shall create an information management role which assumes responsibility for maintaining, managing and providing appropriate security for the built asset information throughout its operational life.

NOTE *The asset management process is shown in Figure 8. A continuing information management role is essential for maintaining the security of asset information, both in terms of the cyber security of the systems and digital content, and managing the security threat that the data may pose to neighbouring built assets. The nature of the role and how it is delivered varies according to the procurement route used to create, operate and maintain the built asset.*

12.1.2 As part of the operational function, the information management role shall be responsible for the access permissions for those who can create, read, update and delete information. The control of access shall be in accordance with the BASMP and associated security policies, processes and procedures, including the requirements set out in the BASIR.

Figure 8 – The project work stages and decision points



NOTE *Reproduced with kind permission of CPNI and Alexandra Luck.*

NOTE 1 *The levels of service comprise the preservation of the integrity of the built asset and the service delivered by the asset in terms of use, e.g. safety, availability, accessibility, etc.*

NOTE 2 *Option identification is based on an assessment of the gaps between a built asset's current and desired performance and the options available for closing those gaps.*

NOTE 3 *Decision-making should be based on consideration of a combination of: the optimal regime for the operation and maintenance of the built asset; the available budget; and an assessment of risk.*

NOTE 4 *Non project-based delivery options comprise:*

- *reactive maintenance – undertaken as a priority in response to a defect in the built asset which poses an immediate or imminent hazard;*
- *regular maintenance – routine and cyclical maintenance work;*
- *programmed maintenance – includes preventative maintenance work, component renewal or replacement.*

NOTE 5 *The delivery options of improvement, modification, change of use or disposal of a built asset are likely to be managed through a project.*

12.2 Modification/change of use and end of life

12.2.1 When planning the change of use, modification, decommissioning or disposal of a built asset, the asset owner shall conduct a security risk assessment and put appropriate measures in place to protect valuable, attractive and sensitive items, including all physical or information assets.

NOTE *During the planning for the decommissioning or disposal of an asset, a risk assessment should be undertaken to identify any specific security measures and/or security requirements that should be addressed. The requirements may relate to the asset itself or the protection of associated or neighbouring built assets. For example, the analysis might identify valuable, attractive or sensitive items, including IT systems or information that should be protected, removed and where necessary, securely disposed of prior to implementation of the change/modification.*

12.2.2 The asset owner shall assess the security risks associated with any change of use during the asset's lifecycle and take appropriate steps to manage the security of asset information and of existing security systems.

NOTE *During the operational lifecycle of the built asset there can be a number of changes of use, where the asset remains in the ownership or occupancy of the same organization. Two specific scenarios that have security implications may need to be addressed when acquiring or designing and constructing the built asset:*

- *Change of use from less sensitive to more sensitive role/occupancy – there should be an assessment of what information is already publicly available and what is available within the supply chain, to assess the risk that the security of the new use may be compromised.*
- *Change of use from more sensitive to less sensitive role/occupancy – there should be an assessment of what information on sensitive security measures is contained within any CDE/asset management repository or held by the supply chain. There may also be sensitive security-related features or systems that are no longer required for the planned use. A risk assessment should be undertaken regarding the access to sensitive security information and systems. Depending on the results of the risk assessment it may be necessary to require removal of sensitive information, data sets, and security systems prior to use in a less sensitive role.*

12.3 Change of ownership or occupancy

12.3.1 On change of use or occupancy the asset owner shall undertake a risk-based review of the presence of sensitive security-related products and of sensitive and personally identifiable information held in the building systems.

12.3.2 Where the CDE, asset management database and/or facility management system contains:

a) commercially sensitive information about the previous owner or occupier;

b) operationally sensitive information about the previous owner or occupier;

c) information relating to security products or systems; and/or

d) personal or personally identifiable information about users and/or occupiers,

the asset owner shall take steps to remove or de-sensitise the information which is no longer required.

NOTE 1 *Where data needs to be retained for asset management and performance reporting purposes, an option that may be considered is the creation of anonymised data sets. However, this should be considered as part of a risk-based approach because there is potential for recovery of data that has been removed through correlation of multiple datasets, including those outside of the control of the asset owner.*

NOTE 2 *The employer or asset owner should be aware of potential issues around the change of ownership of a supplier or contractor and manage any associated risks in an appropriate and proportionate manner.*

13 Compliance with other legislation and standards

13.1 Legislation

NOTE *The information in this clause does not constitute legal advice. Users of this PAS should take appropriate legal advice where any of the legislation or regulations in this clause may or will apply to asset information under their control.*

13.1.1 Computer Misuse Act 1990 [6]

The employer or asset owner shall apply a security-minded approach in its specification, design, operation and maintenance of project and asset information systems so as to ensure that its personnel, professional advisors, contractors and suppliers do not inadvertently commit offences when fulfilling their contracted duties.

NOTE *Offences can arise where an individual accesses data or information where they lack the requisite privileges or authorization. The access may include viewing, printing, moving data or altering files or database records.*

13.1.2 Data Protection Act 1998 [1]

The employer or asset owner shall apply a security-minded approach to handling, storage and use of personal data held within the CDE.

NOTE *This Act regulates the use of personal data and could apply to asset information, whether held in electronic or paper form, where it includes any set of information relating to individuals. The employer or asset owner should be aware that personal data may be held within the CDE and put in place the required policies, processes and procedures so that it is in compliance with the requirements of this legislation.*

13.1.3 Environmental Information Regulations 2004 [2]

Where the employer or asset owner is a public authority, it shall release asset information, as part of its publication scheme and on request, on a risk-based, security-minded basis. It shall inform personnel handling such requests of the types of information that shall be withheld.

NOTE *The Environmental Information Regulations [2] provides public access to information about the environment held by public authorities by:*

a) obliging public authorities to proactively publish certain information about their activities in accordance with their publication scheme, and

b) entitling members of the public to request information from public authorities.

The Regulations cover any recorded information held by the public authority that falls within the definition of 'environmental information' and can also apply to environmental information that another person or organization holds on behalf of the public authority. It typically covers information about land development, pollution levels, energy production, and waste management, and includes financial information where it relates to the costs of redeveloping land and constructing a new built asset.

Where a public authority is an employer or asset owner with regard to a built asset, it should consider what, if any, asset information is to be published as part of its publication scheme, the extent to which members of the public may be provided with information in response to Environmental Information Regulations [2] requests, and the exemptions that exist.

13.1.4 Freedom of Information Act 2000 [3] and Freedom of Information (Scotland) Act 2002 [7]

Where the employer or asset owner is a public authority, it shall, on a risk-based, security-minded basis, consider what asset information may be released as part of its publication scheme and on request. It shall make the personnel handling such requests aware of the types of information that shall be withheld.

NOTE *The Freedom of Information Acts [3] provide public access to information held by public authorities, by:*

a) obliging public authorities to proactively publish certain information about their activities in accordance with their publication scheme, and

b) entitling members of the public to request information from public authorities.

Together they cover any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.

Where a public authority is an employer or asset owner with regard to a built asset, it should consider what, if any, asset information is to be published as part of its publication scheme, the extent to which members of the public may be provided with data in response to freedom of information requests, and the exemptions that exist.

13.1.5 Government Security Classifications

Where applicable, the employer or asset owner shall comply with the Government Security Classifications policy with regards to all information that it collects, stores, processes, generates or shares in order to own,

procure, operate or maintain a built asset, including information received from, or exchanged with, external parties both within and outside its supply chain.

NOTE *Compliance with this policy may require specific security measures to be imposed regarding the CDE, particularly where it contains significant volumes of official information or where some of the information requires specific controls and security measures.*

13.1.6 Official Secrets Act 1989 [5]

Where official information is held within the CDE, the employer or asset owner shall apply protective measures in accordance with the UK Government guidance on information security.

NOTE *The Official Secrets Act [5] applies to the protection of official information. Where the built asset is either a building owned or occupied by a public authority, or is part of the critical national infrastructure, there might be details of its design, construction, operation and use that are sensitive and might be covered by the Act.*

Where the CDE includes information covered by the Official Secrets Act [5], additional protective measures might be required in accordance with the Government's guidance on information security.

13.1.7 Planning and Compulsory Purchase Act 2004 [8]

In the event that the employer or asset owner submits a planning application which is handled by a planning inquiry, it shall request that the provisions of Section 80 of the Planning and Compulsory Purchase Act (2004) be applied to all security-sensitive information regarding the built asset or planned built asset.

NOTE *Section 80 of this Act deals with the arrangements for planning inquiries where matters of national security are at issue. Whilst, in general, all oral evidence at planning inquiries should be heard in public and all documents should be open to public inspection, there is an exception when there would be public disclosure of information relating to national security or to the security of any premises or property, and that disclosure would be contrary to the national interest.*

13.1.8 Privacy and Electronic Communications Regulations 2003 [9]

Where an employer or asset owner provides a public electronic communications service, for example guest access to the internet or an internet café on site, it shall consider whether the provisions of these regulations apply to the security of the service offered.

NOTE *The employer or asset owner should be aware of the Privacy and Electronic Communications Regulations and consider whether any of the provisions apply to the built asset and its systems, and if so implement appropriate measures to instil compliance.*

13.1.9 Public Records Acts 1958 and 1967 [10]

Where the employer or asset owner is a public authority, it shall consider what information is required to be retained for public record purposes. Where the built asset has a lifecycle greater than 30 years, the asset owner shall, on a risk-based, security-minded basis, consider what asset information may need to be sealed for a longer period to prevent compromising the security of the built asset.

13.1.10 Re-use of Public Sector Information Regulations 2005 [11]

Where the employer or asset owner is a public authority, it shall apply a security-minded approach when considering what information shall be made available for re-use, and the extent to which the asset information is exempt from re-use.

NOTE *Public authorities should carefully consider the security implications of making asset information available for re-use. Whilst individual items might not pose a threat, aggregation of data, including correlation of data supplied by different public bodies, could reveal sensitive operational information and capabilities. Where security considerations might be applicable, the public authority should not identify the information as available for re-use.*

13.1.11 Sensitive information in planning applications

Where a planning application contains sensitive information, the employer or asset owner shall apply a security-minded approach to submitting the application. The employer or asset owner shall work with the local planning authority to limit the information available on the open planning register, with sensitive information being subject to special handling arrangements.

NOTE *Planning applications from bodies such as the diplomatic community, defence, security and law enforcement organizations, and owners of critical national infrastructure might contain sensitive information which the local planning authority should consider, but which should not be made available on the planning register.*

Before submitting a planning application, the employer or asset owner should discuss the status of sensitive information relating to a proposed development with the relevant local planning authority[12)]*.*

[12)] Further information can be found at: http://planningguidance.planningportal.gov.uk/blog/guidance/crown-development/sensitive-information-in-planning-applications/

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 1192:2007, *Collaborative production of architectural, engineering and construction information – Code of practice*

BS 7858:2012, *Security screening of individuals employed in a security environment – Code of practice*

BS ISO 15686-4:2014, *Building Construction – Service Life Planning – Service Life Planning using Building Information Modelling*

BS ISO 29481-1:2010, *Building information modelling – Information delivery manual – Part 1: Methodology and format*

BS ISO 29481-2:2012, *Building information models – Information delivery manual – Part 2: Interaction framework*

BS ISO 55000:2014, *Asset management – Overview, principles and terminology*

BS ISO 55001:2014, *Asset management – Management systems – Requirements*

BS ISO 55002:2014, *Asset management – Management systems – Guidelines for the application of ISO 55001*

BS ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

PD ISO/TS 12911:2012, *Framework for building information modelling (BIM) guidance*

PAS 555:2013, *Cyber security risk – Governance and management – Specification*

PAS 754:2014, *Software Trustworthiness – Governance and management – Specification*

PAS 1192-2:2013, *Specification for information management for the capital/delivery phase of construction projects using building information modelling*

PAS 1192-3:2014, *Specification for information management for the operational phase of assets using building information modelling*

Other publications

[1] GREAT BRITAIN. The Data Protection Act 1998. London: The Stationery Office.

[2] GREAT BRITAIN Environmental Information Regulations 2004. London: The Stationery Office.

[3] GREAT BRITAIN Freedom of Information Act 2000. London: The Stationery Office.

[4] GREAT BRITAIN. Serious Organised Crime and Police Act 2005. London: The Stationery Office.

[5] GREAT BRITAIN Official Secrets Act 1989. London: The Stationery Office.

[6] GREAT BRITAIN Computer Misuse Act 1990. London: The Stationery Office.

[7] SCOTLAND Freedom of Information (Scotland) Act 2002. Edinburgh: The Stationery Office.

[8] GREAT BRITAIN Planning and Compulsory Purchase Act 2004. London: The Stationery Office.

[9] GREAT BRITAN Privacy and Electronic Communications Regulations 2003. London: The Stationery Office.

[10] GREAT BRITAIN Public Records Acts 1958 and 1967. London: The Stationery Office.

[11] GREAT BRITAIN Re-use of Public Sector Information Regulations 2005. London: The Stationery Office.

Further reading

BS 8541-2:2011, *Library objects for architecture, engineering and construction – Recommended 2D symbols of building elements for use in building information modelling*

BS ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*

IET Standards, *Resilience and Cyber Security of Technology in the Built Environment,* Institution of Engineering and Technology/CPNI, 2013

IET Standards, *Code of Practice for Cyber Security in the Built Environment*, Institution of Engineering and Technology, 2014

Building Information Modelling (BIM) Task Group http://www.bimtaskgroup.org

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)20 8996 9001 Fax: +44 (0)20 8996 7001

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)20 8996 7669 Fax: +44 (0)20 8996 7001
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)20 8996 9001 Fax: +44 (0)20 8996 7001
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 Fax: +44 (0)20 8996 7005
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)20 8996 7002 Fax: +44 (0)20 8996 7001
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

This page deliberately left blank.

Peter Hansford
Chief Construction Advisor

As our industry shifts into the digital arena we need to be more attentive to how we create and manage our construction information – with regard to people, process and technology.

PAS 1192-5 is a key constituent in the Level 2 BIM suite, and marks a significant milestone in the development of the BIM programme.

It underpins the advancement of future digital built environments and enables smart asset management, as well as incorporating full consideration of appropriate security processes and mind-set. It addresses the stages required to produce and promote a relevant security philosophy and culture which are vital to today's businesses – helping them to unlock new and more efficient processes and collaborative ways of working.

By applying appropriate security measures, organisations will be able to transact more securely in a safe, reliable and resilient digital built environment.

Mark Bew MBE
Chair of the HM Government BIM Task Group

In the short duration of the UK Level 2 programme we have seen dramatic changes to the political and social fabric of the world. Risks from terror attacks have changed dramatically as have methods of defence and protection. The built environment is a significant part of the material world in which we live today and is undergoing an enormous digital transformation. So we must ensure that we can adequately protect everyone from any unnecessary risk that this might entail.

PAS 1192-5 is a fundamental part of the Level 2 BIM portfolio and represents another international first for the UK Level 2 programme.

It offers practical advice for high and normal risk scenarios, to ensure we go about our work in an appropriate and sensible manner. It recognises the benefits of open sharing of information to enable collaborative behaviour. But it balances this by ensuring all these functions are carried out in a thoughtful, deliberate and efficient way, taking account of appropriate and proportionate security.

bsi.

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom

www.bsigroup.com

www.bimtaskgroup.org

9 780580 882579