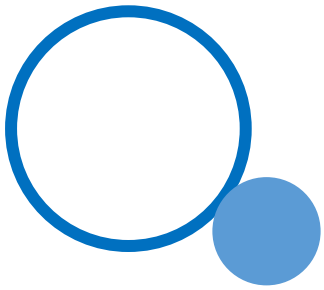


MINDFUL SECURITY GUIDANCE

NHSScotland

Contents

List of Figures

List of Tables

Acronyms

BARMS	Built Asset Risk Management Strategy
BASIR	Built Asset Security Information Requirements
BASMP	Built Asset Security Management Plan
BASS	Built Asset Security Strategy
BEP	BIM Execution Plan
CDE	Common Data Environment
CII	Critical Information Infrastructure
CIO	Chief Information Officer
COBie	Construction Operation Building information exchange
CPNI	Centre for the Protection National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
EIR	Employer's Information Requirements
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
NIS	Network Information Systems Regulation
OT	Operational Technologies
SB/IMP	Security Breach/Incident Management Plan

Introduction

Mindful security, especially information security is fundamental to the success of NHSScotland and their Boards. Security is not just in terms of the physical controls and guarding, or security-minded behaviour by personnel, but also in respect of how Boards manage risks arising from unauthorised access to, and manipulation or sharing of, data, information and systems. Cybercriminals often set their sights on large organisations such as healthcare providers. To physically protect sites and the related electronic data as well as the ability to share and use information in a secure way should be fundamental to any Board's asset management strategy.

The consequences of poor security should not be underestimated and could affect project financial margins, the construction programme, business reputation, the built asset itself and, worst of all, the lives of personnel.

Understanding a Board's or individual project's security risk profile and conducting effective planning for appropriate and holistic project security (encompassing personnel, physical and cyber security) is therefore essential and will help in enabling a safe and productive construction environment.

1 Building Information Modelling (BIM and Mindful Security)

Mindful security is also a key component of BIM Level 2 maturity (and in Scotland BIM Level 1) where PAS 1192-5:2015 Specification for security-minded building information modelling, digital built environments and smart asset management is a required standard. (Figure 1)

PAS 1192-5 specifies requirements for security-minded management of Building Information Modelling (BIM) and digital built environments. It outlines the cyber-security vulnerabilities to hostile attack when using BIM and provides an assessment process to determine the levels of cyber-security for BIM collaboration which should be applied during all phases of the site and building lifecycle.

The PAS addresses the steps required to create and cultivate an appropriate security mindset and secure culture within an organisation such as a Board, including the need to monitor and audit compliance.

PAS1192-5 can be downloaded at

https://bim-level2.org/en/standards/

Figure 1 PAS 1192-5

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

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

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

PAS 1192-5:2015 was commissioned by the Centre for the Protection of National Infrastructure (CPNI) to support growing BIM adoption and provide wider guidance than ISO 27001 and the implementation of an information security management system (ISMS) to protect corporate business systems. ISO 27001 sets out the information security requirements for an individual organisation however BIM and smart asset management involves an inherently collaborative process involving the sharing of large amounts of digital models, data and information between the broad range of organisations in a supply chain. Additionally, ISO 27001 may be too onerous for those involved in NHSScotland projects especially the SME organisations. A summary overview of the PAS 1192-5 standard is illustrated in Figure 2.

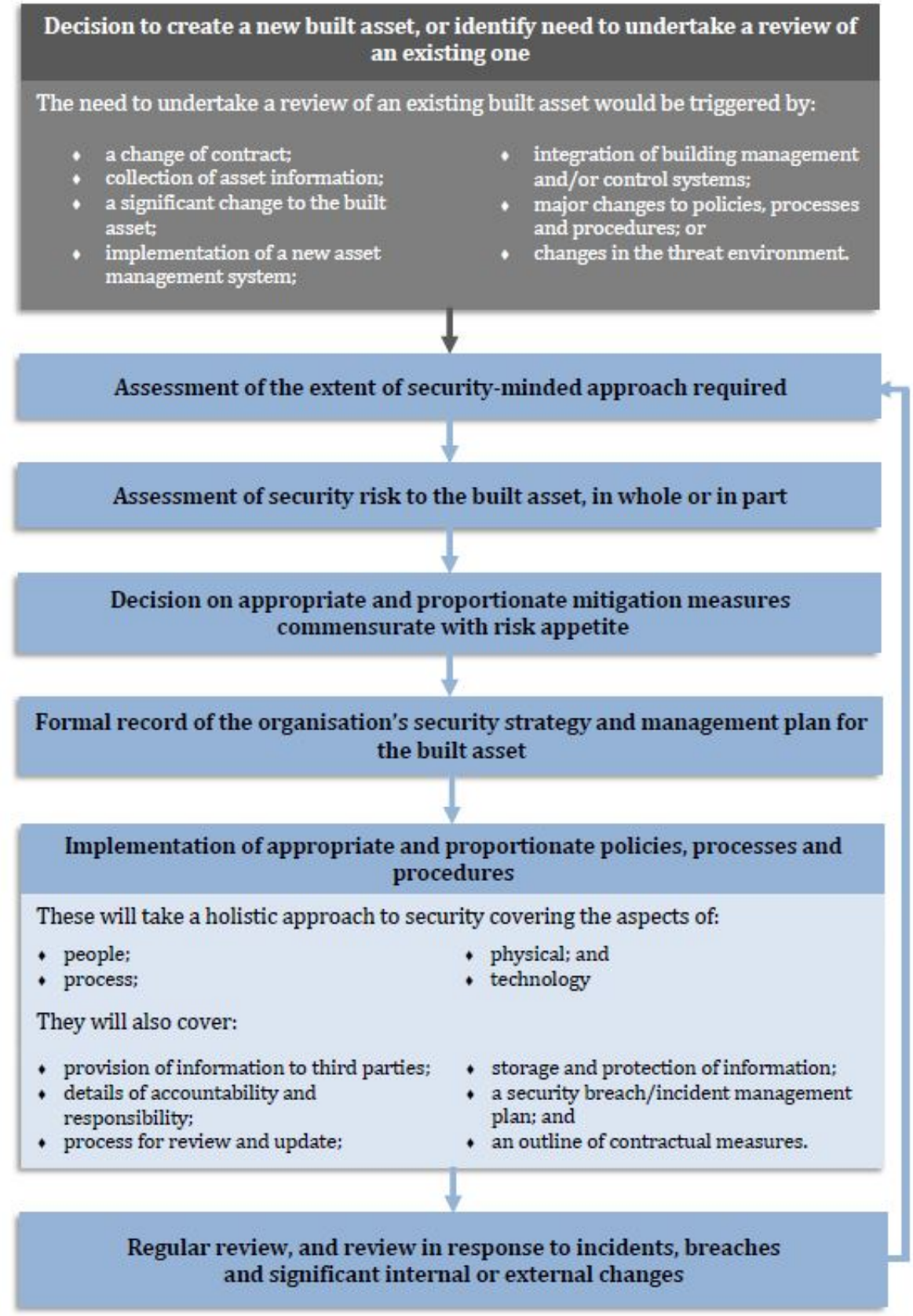


Figure 2 Summary overview of PAS 1192-5

To further help you consider your approach to security, The Centre for Digital Built Britain (CDBB) have outlined Ten Steps to security-mindedness as illustrated in Figure 3.

Figure 3 Ten steps to security-mindedness (Reference: Alexandra Luck, Centre for Digital Built Britain (CDBB))

2 Security Minded Approach – The Principles

Getting the security basics rights is vitally important and an NHSScotland Board should be able to demonstrate their understanding of, and ability in:

- Identifying;
- Assessing;
- Implementing; and
- Managing and communicating issues about security.

Additionally, Boards (their staff and their projects) should follow the six security minded principles set out below. These are based on those developed by the Engineering Council and tailored to NHSScotland. It is important that these principles are imbedded in the Board's standard procedures and training of staff:

PRINCIPLE ONE

ADOPT A SECURITY-MINDED APPROACH TO YOUR PROFESSIONAL AND PERSONAL LIFE

Be able to demonstrate an awareness of how behaviour and actions, including use of social media, can impact on the personnel security of their staff and that of others such as Principal Supply Chain Partners (PSCPS);

Identify potential threats and security vulnerabilities that exist at each stage of the NHSScotland SCIM process, suggesting potential measures to mitigate unacceptable risks;

- ✓ Appreciate how exploitation of a vulnerability may result in harm to people, a built asset, services provided by NHSScotland or data / information;
- ✓ Understand the importance of implementing a combination of physical, personnel and technological mitigation measures to address security risks;
- ✓ Demonstrate appropriate use of social media professionally and socially;
- ✓ Identify and oversee the implementation of security policies and processes appropriate to both the construction and operational phases.

PRINCIPLE TWO

APPLY RESPONSIBLE JUDGEMENT AND TAKE A LEADERSHIP ROLE

- ✓ Demonstrate working with other professionals to ensure informed, proportionate, holistic judgements;
- ✓ Demonstrate use of professional judgement in assessing security risks within a NHSScotland construction project;
- ✓ Able to challenge assumptions and proposals while seeking to improve practices, and empower others to do the same;
- ✓ Provide NHSScotland staff with the opportunity to maintain appropriate levels of security competence.

PRINCIPLE THREE

COMPLY WITH LEGISLATION AND CODES, UNDERSTAND THEIR INTENT AND BE PREPARED TO SEEK FURTHER IMPROVEMENTS

- ✓ Aware of security-related laws and policies that NHSScotland and their Boards have to comply with;
- ✓ Aware of, and acts in accordance with, security- related codes of practice relevant to construction activities;
- ✓ Able to identify the role of existing security guidance recognising any limitations in respect of construction, and suggest improvements where reasonably practicable.

PRINCIPLE FOUR

ENSURE GOOD SECURITY-MINDED COMMUNICATIONS

Able to identify the security policies and processes relevant to NHSScotland staff and other members of the supply chain, and communicate them clearly and effectively;

- ✓ Able to express clearly the balance of security risks and opportunities;
- ✓ Adopt an ‘open reporting’ approach to security risks, incidents and near-misses, coupled with a spirit of questioning and learning from others;
- ✓ Selective of the material used when publishing information at conferences, workshops and seminars or when writing in professional or trade publications to avoid releasing sensitive data and information.

PRINCIPLE FIVE

UNDERSTAND, COMPLY WITH AND SEEK TO IMPROVE LASTING SYSTEMS FOR SECURITY GOVERNANCE

- ✓ Demonstrate understanding of own role in contributing to the security of the built asset;
- ✓ Contribute to the development, implementation and review of Board security policies and processes;
- ✓ Ensure security-related roles and responsibilities are clearly assigned and understood by staff and members of the NHSScotland supply chain;
- ✓ Improve own understanding of security risks and mitigation measures that can be applied during construction;
- ✓ Contribute to the development and implementation of appropriate mechanisms for reporting and feedback on security incidents and issues;
- ✓ Contribute to the scrutiny and auditing of the security culture and implementation of security policies and processes.

PRINCIPLE SIX

CONTRIBUTE TO PUBLIC AND PROFESSIONAL AWARENESS OF SECURITY

- ✓ Able to engage in debate on security risks and benefits, especially in relation to new technologies and innovative developments;
- ✓ Able to recognise the social, political and economic implications of security risks and acknowledge these through appropriate channels;
- ✓ Honest and clear about uncertainties, and prepared to challenge misrepresentations and misconceptions;
- ✓ Contribute to public and professional awareness of security by appropriate sharing and promoting knowledge of effective solutions.

3 Implementing a Security Minded Approach

The following framework is designed to help NHSScotland Boards and their project teams create a security minded approach especially those that are executing BIM Level 2 methodology.

3.1 Understanding the overall security threat to your built asset

To ensure that each project adopts an appropriate level of a security minded approach to its built asset and associated asset information it is important to categorise in relation to their level of criticality. In support of this the project team shall apply a security triage process to help identify the need for an appropriate security minded approach to an asset for instance:

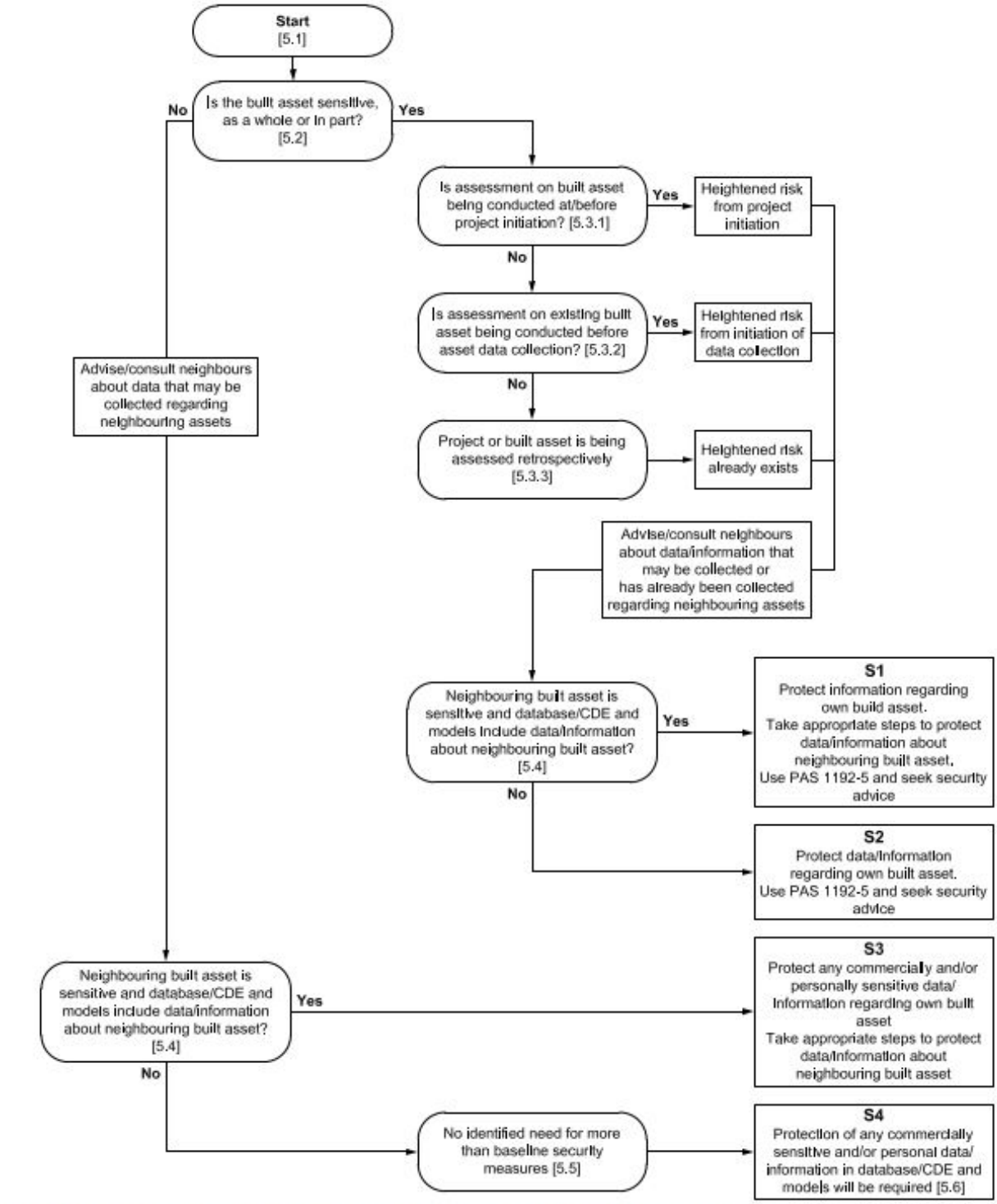
A. Where a new project investment is proposed;

B. Adaption or extension to an existing asset is planned;

C. Implementation of a new asset management system;

D. Changes to the operating environment which necessitate changes in the management of asset information.

PAS1192:5 illustrates a Security triage process to help identify an appropriate security level which is illustrated over. The triage process diagram should be read in the context of the wider PAS1192-5 document. The references such as Figure 5 are due to the diagram being extracted from the PAS. (Figure 4)



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

Figure 4 Security triage process to identify the need for a security-minded approach to the built asset and associated asset information (extracted from Figure 5 of PAS 1192-5)

Due to the nature of the work that NHSScotland and their Boards undertake, often storing significant volumes of pharmaceuticals, gases and/or chemicals, it is important that facilities be reviewed in relation to sensitivity in whole or in part.

Table 1 gives recommendation to sensitivity baselines for healthcare facilities – it is recommended that all hospital facilities be classified as sensitive in whole or in part. All other medium to low facilities should be assessed by the project team.

Themes to be considered as part of the assessment:

- Extent of pharmaceutical storage
- Extent of chemicals and medical gases to be stored
- Extent of operational technologies
- Sensitivity of facility including risk of activism
- Sensitivity of data and information relating to that facility

The triage process and its result should be completed using the CPNI template which can be found at:

https://www.cpni.gov.uk/system/files/documents/31/68/Application_of_the_Security_Triage_Process.pdf

Table 1 Recommendation to sensitivity baselines for healthcare facilities

Ref	Facility Classification	Baseline Sensitivity	Final sensitivity, post review	Notes
01	Acute Hospital	Sensitive in whole or part		
02	Children's Hospital	Sensitive in whole or part		
03	Maternity Hospital	Sensitive in whole or part		
04	Specialist Hospital	Sensitive in whole or part		
05	Mental Health Hospital	Sensitive in whole or part		
06	Community Hospital	Medium risk - Project to undertake assessment to determine.		
07	Older People Hospital	Medium risk - Project to undertake assessment to determine.		
08	Multi Service Hospital	Medium risk - Project to undertake assessment to determine.		
09	Health Centre	Medium risk - Project to undertake assessment to determine.		
10	Clinics (including Day Hospitals and Resource Centres)	Medium risk - Project to undertake assessment to determine.		

Ref	Facility Classification	Baseline Sensitivity	Final sensitivity, post review	Notes
11	Offices	Low risk - Project to undertake assessment to determine.		
12	Support Facilities	Low risk - Project to undertake assessment to determine.		
13	Staff Residential Accommodation	Low risk - Project to undertake assessment to determine.		
14	Patient Residential Accommodation	Low risk - Project to undertake assessment to determine.		
15	GP Practice	Low risk - Project to undertake assessment to determine.		
16	Dental Practice	Low risk - Project to undertake assessment to determine.		
17	Pharmacy	Sensitive in whole or part.		
18	Optician	Low risk - Project to undertake assessment to determine.		
19	Care Home	Low risk - Project to undertake assessment to determine.		
20	Non NHS functions	Low risk - Project to undertake assessment to determine.		
21	Non–Operational	Low risk - Project to undertake assessment to determine.		
22	Other	Project to undertake assessment to determine		

3.2 Appointment of a built asset security manager (BASM)

Built asset security manager (BASM) can be defined as – an individual reporting directly to, or employed by, the employer or asset owner and undertaking the role of security management [from BS 1192-5]

Where the security triage process identifies a need for a security-minded approach, the Board or project team shall nominate a suitably qualified and experienced individual to fulfil the role of BASM.

On most NHSScotland projects the BASM will be a part-time function and fulfilled by an individual who may undertake or be responsible for security and other duties within the Board or on a project.

It is important that the individual who fulfils the roles is however suitably qualified and experienced to undertake the role. On larger or more complex healthcare projects it may be necessary to seek the support of a specialist consultant.

The built asset security manager role shall typically encompass the following:

A. provide a holistic view of the project's security issues and the potential threats to be addressed;
B. offer the project team guidance and direction on the handling of risks;
C. take ownership, manage, and assist in the development of the built asset security strategy (BASS);
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);
F. take ownership, manage, and assist in the development of security breach/incident management plan (SB/IMP);
G. take ownership, manage, and assist in the development of the built asset security information requirements (BASIR);
H. assist in the development of security related 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: It is 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 Board's chief information officer (CIO), or chief digital officer, data protection officer, and asset management functions to the asset manager or facilities manager). However, the BASM shall remain responsible for the operational effectiveness of each of these aspects of security.

It important that the BASM works closely with those developing the project's BIM strategy and related documents such as the Employers Information Requirements (EIR) to ensure that all relevant security requirements are incorporated.

3.3) Develop a built asset security strategy (BASS)

Developing a protective BASS for mitigating identified risks will help a Board optimise the security implementation process. The BASS should be holistic, risk based and proportionate.

Leadership and governance will be key to the success of the BASS and it is important that the Board's leaders and project team demonstrate positive and visible support for protective security demonstrating to staff the value placed on personnel and people security policies and procedures.

In support of the foregoing the Board shall formally develop, record and maintain a security strategy for the project.

The BASS typically includes:

A. The security requirements determined through the security triage process;

B. The built asset risk management strategy;

C. A list of those to be informed about any residual risks; and

D. The mechanisms for reviewing and updating the BASS.

A template NHSScotland BASS is included in the Appendix of this guidance.

3.4) Develop a built asset risk management strategy (BARMS)

Effective security risk management requires a Board to have defined governance and oversight of protective security management systems. As risk owners, the Board's senior leaders need to be conversant with the key principles of protective security in order to guide their strategic decision-making.

Risks are essentially identified threats or vulnerabilities, aligned to assets that have been assessed for their likelihood and impact should that threat transpire. The ability to understand the uncertainties and confidence levels of assessments will help Board decision makers properly plan in their mitigation strategies.

Having undertaken a BASS for the project the next stage is to develop a built asset risk management strategy (BARMS) this has two key themes:

- Risk assessment
- Risk mitigation

All data gathered through this process should be recorded in a protective security risk register. The format of the register is a matter of preference e.g. either stand alone or incorporated in the overall Board or project risk register.

3.4.1 Risk assessment

The Board shall 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. The risk assessment shall identify and record the high-level security risks associated with:

- People;
- Process;
- physical;
- technological security (especially common data environment solutions); and
- sensitive data or information.

The assessment should consider these themes in the context of:

- Personnel and other users of the asset e.g. patients and visitors;
- The built asset itself;
- Asset information; and
- The service the built asset provides.

3.4.2 Risk Mitigation

The BARMS shall identify and record potential mitigation measures for each of the identified risks. The assessment of each mitigation measure should consider:

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 to the Board or project such as reducing business risks).

Having assessed the potential mitigation measures the project shall determine which countermeasures are proportionate and are to be adopted.

3.4.3) Residual Risks

Following the risk mitigation process, the project team shall identify and record and residual risks. These should be monitored across the project life-cycle until a point is reached when they are closed out.

3.5) Developing a built asset security management plan (BASMP)

The Board 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 as per the figure 5 extracted from PAS1192-5.

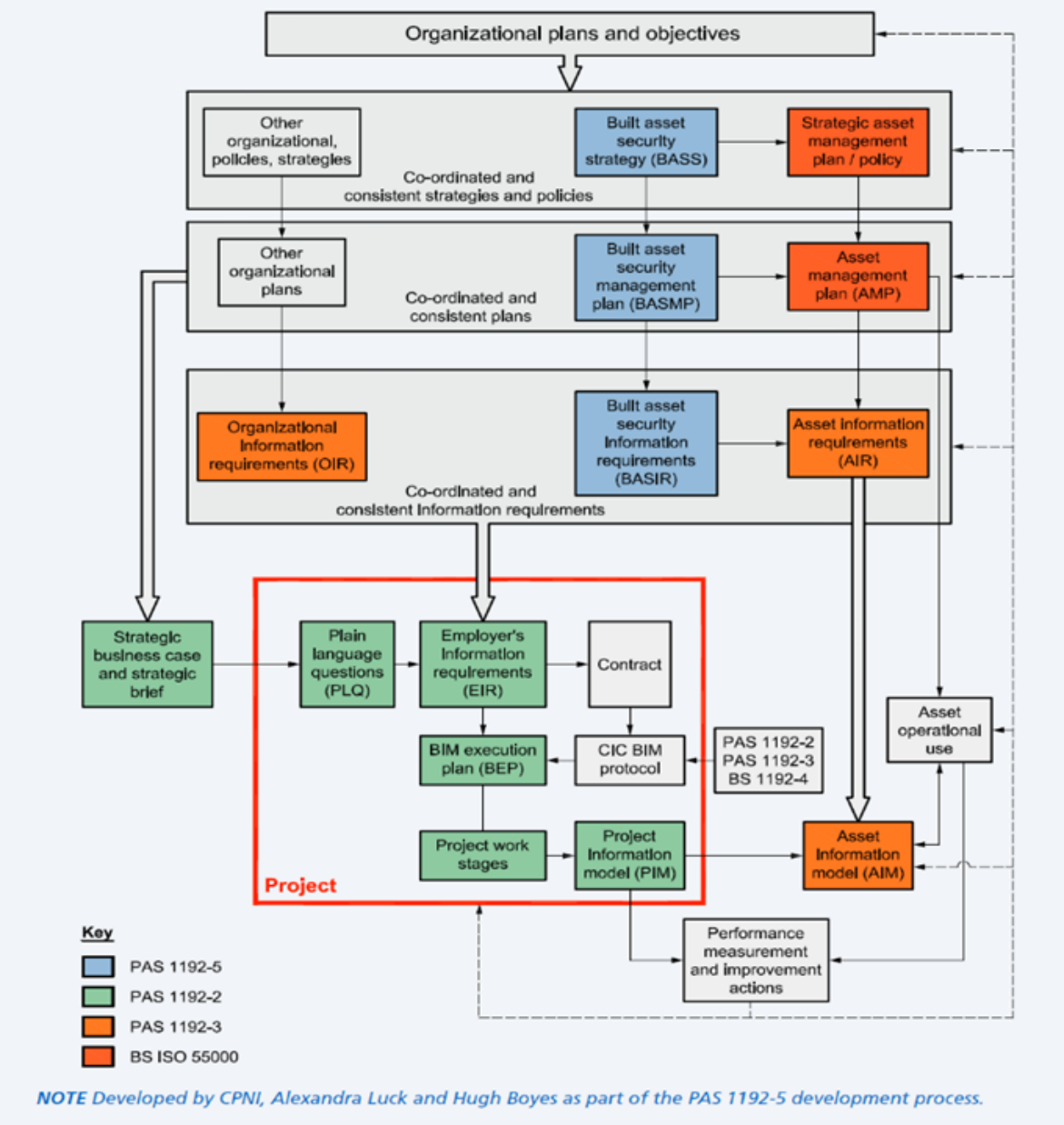


Figure 5 The integration of the Security-mined approach (taken from Figure 2 PAS 1192-5)

When undertaking a project, the team shall use the BASMP to help inform its strategic business case and strategic brief, and through those, its plain language questions (PLQs) and subsequent EIRs.

In compiling the BASMP the project team should consider the key aspects outlined in Table 2 which comprise the people, process, physical and technological aspects of the built asset, the related asset information, and building-related systems.

Table 2 BASMP key aspects

1.0	**Personnel Aspects**
1.1	Identification of high-risk positions within the project or Boards' organisation and any organisations employed on the contract or providing services to the Board. (High risk: 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);
1.2	security screening and vetting requirements for individuals employed on the contract, both in general and specific roles;
1.3	the security competence requirements of individuals in specific roles;
1.4	the general security awareness and training requirements to develop and promote a security minded culture for the project;
1.5	the role-based security training requirements in its supply chain (PSCPs etc) to facilitate the adoption and maintenance of a security-minded culture;
1.6	the induction of personnel and organisations joining the project delivery team or providing services to the Board so that they are appropriately briefed on their responsibilities and the required security-minded culture;
1.7	BIM: access requirements to models and associated asset information; and
1.8	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.

2.0	**Process Aspects**
2.1	granting individuals access to the common data environment (CDE);
2.2	handling asset information relating to neighbouring, separately-owned assets including utilities;
2.3	handling sensitive and/or classified information and documents;
2.4	version and change control processes and procedures for asset information.

3.0	Physical Aspects
3.1	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;
3.2	physical security measures required at the location of the new or existing built asset;
3.3	where appropriate, protection of neighbouring built assets not otherwise generally visible and/or accessible;
3.4	protective measures required for equipment comprising the CDE;
3.5	protective measures associated with the use of computing and electronic devices on the construction site; and
3.6	protective measures associated with the use of computing and electronic devices on, or in, the completed built asset.

4.0	Technical Aspects
4.1	measures related to the cyber security of systems processing and storing project information;
4.2	measures related to the cyber security of systems acquiring, processing and storing asset information;
4.3	the security of interconnections between such systems;
4.4	configuration management and change control processes and procedures for the systems processing and storing project and asset information;
4.5	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).
4.6	demobilisation of organisations who are leaving the project or asset management team, including the secure deletion and/or destruction of project or asset information held by those organisations, and/ or removal of access to that information; and
4.7	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.

5.0	Project logistical security requirements (where applicable)
5.1	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;
5.2	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;
5.3	the requirement for the PSCP or their 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;
5.4	appropriate and proportionate security measures around any sensitive assets which, for logistical reasons, have to be installed earlier than would generally be desirable; and
5.5	appropriate and proportionate measures to limit, or disrupt the success of, physical hostile reconnaissance.

6.0	Provision of data or information to third parties
6.1	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.
6.2	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.
6.3	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 organisation that is covered by Environmental Information Regulations or Freedom of Information legislation. This shall consider the impact of releasing the asset-related information, including the potential issues arising from data aggregation.
6.4	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.

7.0	**Managing accountability and responsibility for security**
7.1	detail the maintenance of security accountability within the employer or asset owner;
7.2	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;
7.3	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 organisation that has day-to-day responsibility for managing its delivery

8.0	**Monitoring and auditing**
8.1	The BASMP shall set out the appropriate and proportionate monitoring and auditing measures which shall take place across the lifecycle of the asset.

9.0	**Review of the BASMP**
9.1	The project team shall establish a suitable mechanism for performing periodic reviews of the BASMP to check that it remains fit-for-purpose;
9.2	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;
9.3	The project team 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.

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

If the provisions in the BASS and BASMP fail, the Board shall consider the business continuity and disaster recovery scenarios that may affect the operation and viability of projects utilising 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.

The Board 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. Types of security breaches/incidents 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 unauthorised access to information or data;

C. loss, compromise, unauthorised manipulation or change of project or asset information;

D. unauthorised 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. unauthorised access to, misuse of, or fraudulent use of IT systems.

3.6.1 Discovery of a breach or incident

The Board 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.

E. Containment and recovery:

The Board 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.

The SB / IMP should align with the Boards Major Incident Plan (MIP) to provide a framework and guidelines for an event or situation, with a range of serious consequences, which requires special arrangements to be implemented by one or more emergency responder agencies.

3.7) Built asset security information requirements (BASIR)

The project team 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.

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

The BASIR shall determine the employer'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 the items outlined in table 3.

Table 3 BASIR requirements

	Description
1	Conducting survey, photographs or scans are capable of capturing sensitive operational information on fixtures and fittings, signs, Boards or screens in the built asset;
2	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;
3	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 Board, whichever is longer;
4	the maximum amount of information relating to sensitive assets or systems to be contained in model(s), the CDE, other databases and information exchanges;
5	the management and monitoring of access to information about sensitive assets and systems contained within any file or database by each Board with access to any of these files and/or databases;
6	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;
7	the storing of operations and maintenance procedures for sensitive assets and systems in the CDE or asset management databases;
8	notification of the requirement of any special handling or protection of information which has security sensitivity and has been provided to the Board by an organisation within the supply chain; and
9	within a project, the requirements for purpose specific or volume-specific Construction Operation Building information exchange (COBie) files for security related systems, and the need for these to be kept separate from the single coordinated COBie file.

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

Typical sensitive information or volumes on an NHSScotland project will likely relate to:

- Door locking mechanisms;
- CCTV coverage;
- Security and Fire alarm systems;
- Medical gas systems;
- ICT systems;

- Lift systems;
- Building control systems, SCADA, BMS;
- Radiography spaces;
- Pharmaceutical / Drug storage spaces;
- Chemical storage spaces;
- Plant room spaces;
- ICT spaces;
- Roof voids;
- Location, routes, cabling, configuration;
- Identification and use of control systems;
- Location and identification of permanent plant and machinery;
- Structural design details;
- Location and identification of security or other control rooms;
- Location and identification of regulated spaces, or areas housing regulated substances (e.g. bio-hazards) or information; and
- technical specification of security products and features.

3.8) Working with suppliers

It is important that NHSS projects take security minded measures during any pre-qualification or tender period outside any formal contract or framework.

Where the tender documentation contains sensitive information relating to the use of the asset, or high-level information about the level of protection the asset requires, the Board shall require them to be subject to appropriate security measures.

The project 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.

The project 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.

Unsuccessful bidders: The project shall require that all relevant data or information is returned or destroyed. Where appropriate, the Board shall require the supplier to verify that defined procedures have been completed.

Contractual measures: The project 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.

The project team shall input the necessary security and information delivery requirements for the built asset from the BASMP and BASIR into the EIR.

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.

The project 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.

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).

The de-mobilisation of the project at the end of the capital stage is of particular importance and requires proper management and auditing.

4 The Common Data Environment (CDE)

Collaborative digital solutions and the nature of the technologies typically used to facilitate BIM and smart asset management create an increased risk of security breaches through widening access to asset information. Central to any NHSScotland BIM implementation strategy is the common data environment (CDE) and the Centre for the Protection National Infrastructure (CPNI) has created guidance has been written to support the implementation of the approach set out in PAS 1192-5:2015 to manage the risks that affect asset information that is created, processed or stored in cloud services or hosted outside the employer/asset owner's organisation. It sets out the best practice security requirements for implementation of a BIM Level 2 Common Data Environment (CDE) and is applicable to those operated within the design, construction and facilities management supply chains.

Guidance can be found at:

https://www.cpni.gov.uk/system/files/documents/8b/2b/20170309_Common_Data_Environments_A_Guide_for_BIM_Level_2.pdf

If hosting the CDE or document management system, it is essential that you:

- Apply access controls and permissions and monitor their use;
- Use file naming and information structure to manage data and protect file contents; and
- Plan for the transfer of project information in a secure manner.

5 Critical Information Infrastructure

The Board's critical information infrastructure (CII) especially that allied to operational technologies (OT) including Supervisory control and data acquisition systems, distributed control systems, and other control system configuration such as programmable logic controllers should be a key area of focus for the BASS.

Where appropriate a security by design framework should be created for the briefing of OT systems incorporating baseline security into an IT/OT system throughout its life-cycle, from creation to disposal and includes the identification, protection, detection, response and recovery capabilities for the cyber resiliency of the IT/OT systems. A vulnerability assessment and architecture secure review of the CII should be undertaken to identify security and control weaknesses.

Authorised personnel should be limited to areas where OT is located, and a log maintained of all access or attempts to access the systems.

Penetration testing including tests of the CII's hosts, networks and applications should be undertaken before the operational stage.

6 Compliance with other legislation and standards

The recommendations of this guidance do not supersede any of the current security legislation, frameworks and or standards that the Board and their projects follow and the BASS and BASMP should refer to all that currently apply.

This guide does not include security management or security service standards during the facilities management or operational stages and should be read in conjunction with HFS guidance on same.

Where a Board is currently using ISO 27001/2 this guidance should be used in conjunction with same to deal with the wider collaborative aspects that BIM necessitate.

This guidance should be read conjunction with the NHSS Information Security Policy Framework.

7 General Data Protection Regulation (GDPR)

At present patient identifiable information within NHSScotland is governed by the General Data Protection Regulation (GDPR) which forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018).

The introduction of Network Information Systems Regulation (NIS) in May 2018 placed legal compliance requirements on health Boards. NIS is intended to establish a common level of security for network and information systems and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks. Although NIS primarily concerns cyber security measures, it also covers physical and environmental factors.

Further information regarding GDPR can be found here:

https://ico.org.uk/for-organisations/

Scottish Ministers are the Competent Authority for Health in Scotland. An Information Security Policy Framework along with other guidance can be found at:

https://www.healthca.scot/

The GDPR and NIS require that appropriate technical and organisational measures are in place to safeguard individual rights and network and information systems. The Mindful Security Guidance can be embedded alongside these regulations to promote a security minded culture.

8 Mindful Security Framework – NHSScotland Compliance Checklist

This framework compliance checklist (Table 4) can be used to help an NHSScotland project team build a security-minded approach to a project either during the mobilisation or as a health check on a live-project.

Table 4 Framework compliance checklist

	Security Theme: Governance	
Ref	**Requirement**	**Project Action:**
G1	Has a security triage process been undertaken to help identify the need for an appropriate security minded approach to the project?	
G2	Has a BASM been appointed with appropriate experience plus clear roles and responsibilities?	
G3	Has a BASS been created which is risk based and propionate?	
G4	Has an effective BARMS been prepared?	
G5	Has a built asset security management plan (BASMP) been prepared?	
G6	Has a SB/IMP been prepared?	
G7	Have BASIR been identified and incorporated within the EIR?	
G8	Have the security minded requirements been incorporated within all relevant commissions and contracts for the project?	
G9	Have the supply chain been appropriately briefed on the project's security requirements?	
G10	Has the project CDE functionality been developed to consider a security minded approach?	
G11	Are there any other legal requirements to protect the Boards data and information or additional security requirements that need considered?	
G12	Are security inductions and training in place to communicate security requirements to staff and the supply chain?	

	Security Theme: Governance	
G13	Is monitoring and auditing of the implementation of the security requirements scheduled and undertaken?	
G14	Is there a process in place for checking data and information for sensitivities before it is sent to, or viewed by, third parties? Has this process been communicated to staff and the supply chain?	
G15	Is there a process in place for the demobilisation of staff and organisations working on the project? Have checks been carried out to ensure this process is being followed?	

	Security Theme: Personnel	
P1	Has a policy relating to the placing of work related information and images on social media been developed? Has this policy been communicated to staff and the supply chain? Have checks been carried out to ensure this policy is being followed?	
P2	Has guidance been provided to staff on actively managing their individual digital footprint?	
P3	Have high-risk positions on the project been identified (these positions are those that are likely to be the target of social engineering or external influence/pressure)?	

	Security Theme: Physical	
Ph1	Are physical security measures being implemented on site? Is compliance with physical security measures being monitored?	

	Security Theme: Physical	
Ph2	Has a policy relating to receiving personal deliveries at work been put in place? Has this policy been communicated to staff? Have checks been carried out to ensure this policy is being followed?	

	Security Theme: Technological and Cyber	
C1	Has a policy relating to the use of work devices for sending/receiving personal e-mails been developed? Has this policy been communicated to staff?	
C2	Has a policy relating to the gathering, processing and storing of work-related data and information on personal devices been developed? Has this policy been communicated to staff?	
C3	Is there a policy relating to the use of removable storage media? Has this policy been communicated to staff?	
C4	Is there a process for reporting and handling phishing e-mails? Has this process been communicated to staff?	

9 Appendices

9.1 NHSScotland Built Asset Security Strategy (BASS) Specimen template

Project details

Board:	[insert name of Board]
Project / Built Assets Covered:	[Insert name of project / built asset(s) covered by this BASS
For the purposes of this Strategy, neighbouring built assets are:	[insert name(s)]
Date Completed:	[Insert date completed by]
Completed by:	[insert name]
Proposed level of BIM Maturity (based on SFT BIM Grading Tool):	[insert level]

Sensitive Data and Information

The data and information that is classed as sensitive is that pertaining to:

Examples below, these should be tailored to meet the risks of the individual assets and be appropriate to the Board's risk appetite:

- Door locking mechanisms;
- CCTV coverage;
- Security systems;
- Medical gas systems;
- ICT systems;
- Lift systems;
- Building control systems, Supervisory control and data acquisition (SCADA), Building management system (BMS_;
- Radiography spaces;
- Pharmaceutical / Drug storage spaces;
- Chemical storage spaces;
- Plant room spaces;
- ICT spaces;
- Roof voids; location, routes, cabling, configuration;
- Identification and use of control systems;
- Location and identification of permanent plant and machinery;
- Structural design details;
- Location and identification of security or other control rooms;
- Location and identification of regulated spaces, or areas housing regulated substances (e.g. bio-hazards) or information; and
- technical specification of security products and features.

Legislation, Standards and Codes of Practice relevant to the built asset are:

Ref	Document	Date / Version

Built Asset Risk Management Strategy

Risk Assessment

Threat Agent	Motivation	Period in lifecycle of asset where threat may act	Potential action(s) of threat agent
T1	M1		Example: Hostile reconnaissance
T2			
T3			

Potential Action	Threat agent that may utilise action			Period in lifecycle					
	T1	T2	T3	IA	OBC	FBC	Construct	Handover	In-Use
A1 Hostile Reconnaissance	X	XX	X						

The number of crosses indicates the number of motivations of the threat agent to which the potential action is relevant.

For each of the potential actions of the threat agents, the vulnerabilities that could be exploited are:

Potential action	Potential vulnerabilities
A1 Hostile reconnaissance	

Summary of potential vulnerabilities against potential actions

Potential vulnerability	Potential Actions						
	A1	A2	A3	A4	A5	A6	A7
V1							

Summary of the vulnerabilities and potential impacts if exploited by a threat(s):

Ref.	Motivation that vulnerability could be exploited to help achieve	Compromise of, or harm caused to:	Impact of compromise or harm
V1	M1	E.g. Personnel and other users of the asset The built asset itself The services delivered from the built asset Personal data	E.g. Injury or harm caused to personnel Damage caused to the built asset Disruption of, or interruption to, service Inconvenience, delay and disruption to the wider aspects of the work of the organisation Breach of privacy Financial damage Reputational damage Compromise of national security

The risk associated with the potential of each vulnerability being utilised by a threat agent:

Ref	Motivation	Likelihood	Severity of impact	Resultant risk	Risk Ref	Notes
V1	M1				R1.1	
					R1.2	
					R1.3	
					R1.4	
					R1.5	

1.1.1.1 Risk Mitigation

For any risks that are not acceptable, the potential mitigation measures are:

Risk Ref	Mitigation Measures	Mitigation ref.
R1.1.-1.5		R1.M1
		R1.M2
		R1.M3

The assessment of each potential mitigation, is set out in the table below:

Mitigation ref.		Risk with measure in place	
R1.M1 – M3			

Mitigation measures to be implemented:

Mitigation ref.	Description	Measure to be implemented	If measure not implemented, record reasons
R1.M1			
R1.M2			
R1.M3			

1.1.2 General, reviews and updates to BASS

List of those to be informed of residual risks:	[Insert XXXX]
Details of when the BASS will be reviewed (including ad-hoc reviews)?	[Insert XXXX]
Those positions authorised to conduct a review are:	[Insert XXXX]
A review is to be undertaken after a trigger event within:	[Insert XXXX]
The timescale from completing a review is:	[Insert XXXX]
The timescale for updating the BASS, when a review finds this to be necessary, is:	[Insert XXXX]
The process for re-issue of the BASS and removal of the redundant version is:	[Insert XXXX]

Note: *Copies of all reviews should be stored in an Appendix to the BASS*

This document should be signed by an appropriate senior manager within the asset owner's organisation.

Signature:	Date:
Printed name and position within Board:	

9.2 NHSScotland Built Asset Security Management Plan (BASMP) Specimen template

1.0 Project details

Board:	[insert name of Board]
Project / Built Assets Covered:	[Insert name of project / built asset(s) covered by this BASS
For the purposes of this Strategy, neighbouring built assets are:	[insert name(s)]
Date Completed:	[Insert date completed by]
Completed by:	[insert name]
Proposed level of BIM Maturity (based on SFT BIM Grading Tool):	[insert level]

2.0 Checking Asset Information

Impact on other areas/security specialisms: HR / Physical / Technologically

2.1 Mitigation References:

[Insert mitigation references XXX]

[Insert mitigation references XXX]

2.2 Policy

2.2.1 E.g. Checks shall be in place to ensure that whenever asset information, including that pertaining to neighbouring sensitive assets, is sent to an individual or an organisation, it shall not contain that to which an individual or organisation has not been granted access.

2.3 Related Polices

2.3.1 This policy is reliant on the following policies also being in place:

[Insert policy name XXX]

[Insert policy name XXX]

[Insert policy name XXX]

2.3.2 If any of the above are altered, this policy shall be reviewed and any necessary alterations made to it in order to ensure essential risk mitigation measures remain in force.

2.3.3 Role responsible

[Insert role XXX]

2.4 Supporting Processes

2.4.1 [Insert processes XXX]

[Insert processes XXX]

[Insert processes XXX]

2.4.2 Role responsible

[Insert role XXX]

2.5 Monitoring and Auditing of Policy

2.5.1 Implementation of this policy shall be monitored and audited by:

- X
- Y

2.5.2 The supply chain shall collaborate with, and support, the X and Y in the monitoring and auditing process.

2.6 Mitigation References

- [insert mitigation references]
- [insert mitigation references]

2.6.1. Policy

- [Insert policies]

2.6.2 Related Policies

2.6.2.1 This policy is reliant on the following policies also being in place:

- [Insert policies]
- [Insert policies]
- [Insert policies]

2.6.2.2 If any of the above are altered, this policy shall be reviewed, and any necessary alterations made to it in order to ensure essential risk mitigation measures remain in force.

2.6.2.3 The following policies are dependent on this policy being in place:

- [Insert policies]
- [Insert policies]
- [Insert policies]

2.6.2.4 If this policy is altered, each of the above shall be reviewed and any necessary alterations made to them in order to ensure essential risk mitigation measures remain in force.

2.6.2.5 Role responsible:

- [insert]

2.6.3 Supporting Processes

2.6.3.1 [Insert processes]

2.6.3.2 Roles responsible:

- [Insert role]

2.6.4 Monitoring and Auditing of Policy

2.6.4.1 Implementation of this policy will be monitored and audited by:

- X [insert]
- Y [insert]

2.6.4.2 The supply chain shall collaborate with, and support, X and Y in the monitoring and auditing process.