CPNI
Centre for the Protection of National Infrastructure

COMMON DATA ENVIRONMENTS

A guide for BIM Level 2

March 2017

Introduction

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. This 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.

This guidance is based on *Implementing Cloud Security Principles* (NCSC, 2016), but tailored to address the requirements of a CDE accessed by users from both the employer/asset owner and by suppliers/contractors. It should be read alongside the PAS as both use a common set of terms and definitions.

Although targeted at public sector organisations, the framework is applicable to any UK-based construction project using externally hosted or cloud-based data storage, services or infrastructure. The following roles within the employer's/asset owner's organisation are referred to in this guidance:

- Senior Responsible Officer (SRO) - the individual responsible for making investment decisions on projects and for determining the asset management strategy for the built asset;
- Senior Information Risk Officer (SIRO) - the individual responsible for decisions regarding risks to the organisation's data and information;
- Built Asset Security Manager (BASM) - the individual responsible for managing the security aspects of a built asset, whose role is described in *PAS 1192-5:2015*, Clause 6.

Applicability

After applying the security triage process contained in *PAS 1192-5:2015*, the employer/asset owner should apply the guidance below to determine the security needs for its CDE.

Outcome of the triage process is S1 or S2:

- Taking into account the security requirements of the Built Asset Security Strategy (BASS), apply the guidance on the 14 security principles set out in the Appendix to this document;
- Contractual commitment to meet security requirements is essential;
- From an assurance perspective, independent validation of service provider assurances and certifications is essential.

Outcome of the triage process is S3 or S4:

- The SRO should consider whether business benefits will be derived from applying the guidance on the 14 security principles set out in the Appendix to this document.
- Contractual commitment to meet security requirements is desirable.
- From an assurance perspective, relying upon service provider assertion may provide sufficient, proportionate assurance.

Assurance

During the suitability assessment of a solution for use as a CDE, the supplier/service provider may make assertions about the solution or offer certification against specific standards.

The SIRO/BASM should generally not rely on any assertions without additional assurance provided through independent validation.

Where certification is offered against recognised standards, the SIRO/BASM should:

- recognise that the level of detail applied to individual controls varies between standards;
- determine whether the standard offered/achieved is acceptable for the storage, processing and management of the data;
- ensure that the scope of any certification offered has verified both the existence and use of appropriate controls as part of the assessment.

Independent verification should be sought to ensure that the scope and outcome of all certification assessments are correct.

Protecting project/asset-related personally identifiable information

Where the information created, stored or processed in a cloud service includes personally identifiable information, in addition to applying the 14 security principles the employer/asset owner should take into consideration advice given in *Guidance on the use of cloud computing* (ICO, 2012). This guidance sets out the need to clearly identify the data controller and data processor and highlights that additional security measures may be required to comply with the obligations of the employer/asset owner under the Data Protection Act 1998. The ICO guidance includes a checklist of points that are particularly relevant to the handling of personal data.

Appendix – CDE Implementation of Cloud Security Principles

Principle 1: Data in transit protection

The interfaces between the CDE and a user's device and any other systems should be protected using a Transport Layer Security (TLS) or Internet protocol security (IPsec) implementations as follows:

a) TLS (Version 1.2 or above) – access to the CDE employs TLS, configured to use the cipher suites and certificate sizes recommended in the National Cyber Security Centre (NCSC) TLS guidance[1] and not to allow security downgrade on handshake;
b) IPsec or TLS virtual private network (VPN) gateway – access to the CDE is via a TLS or IPsec VPN Gateway, which can be configured to support a strong cryptographic profile. See NCSC advice on IPsec[2] and TLS configuration to ascertain whether the gateway supports a good profile.

Principle 2: Asset protection and resilience

Physical location and legal jurisdiction

For each location where data is stored and/or processed, and from where the service is managed, the service provider should provide:

a) evidence of the physical security arrangements that are used to prevent unauthorised access to the data and IT equipment used to deliver the service; and
b) the physical address of all locations, including for locations outside of the UK, its latitude and longitude.

The service provider should be contractually committed to notify the SIRO/BASM in advance of any changes to this list and to do so with a specified notification period prior to implementation of the proposed change.

Based on a complete set of physical locations, the SIRO/BASM should understand:

a) the risks of unauthorised physical access to the asset data;
b) the countries in which the data will be stored, processed and managed;
c) the legal jurisdiction(s) within which the service provider operates and the impact on compliance with relevant legislation e.g. Data Protection Act (DPA).

The SIRO/BASM should consider whether the legal jurisdiction(s) are acceptable to the employer's/asset owner's organisation.

Data centre security

The service provider should:

a) provide information on the security controls around its (or its suppliers') data centres; and
b) have its data centre protections certified against a recognised and appropriate standard that covers physical security, e.g. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

[1] www.ncsc.gov.uk/guidance/tls-external-facing-services
[2] www.ncsc.gov.uk/guidance/using-ipsec-protect-data

v3.0 or SSAE-16/ISAE 3402. Where compliance with recognised standards is offered, the scope of the assessment must be relevant to locations where the data can be accessed by the service provider and its suppliers.

If the service provider does not refer to a recognised standard and/or is unable to provide appropriate independently verified certification, then a formal independent assessment should be made of the physical controls protecting the data centres.

Data at rest protection

The service provider should use encryption, physical security controls, or a combination of both, to protect data at rest within the service. Acceptable approaches are set out in the table below.

Approach	Description	Guidance
Physical access control	A number of standards are appropriate when validating physical access control protections. These are backed by a variety of certification schemes: • CSA CCM v3.0 • SSAE-16 / ISAE 3402	The scope of the assessment must be relevant to those locations where the data can be accessed by the service provider and its supply chain. See section on Assurance.
Encryption of all physical media	The service provider employs encryption to ensure that no data is written to disk in an unencrypted form.	Products that have been assessed against a NCSC approved standard are recommended. Depending on the nature of the data, the SIRO/BASM should determine whether encryption of all physical media is required or physical measures are sufficient.

The service provider may state that the use of obfuscation techniques, or data storage 'sharding'[3] make it infeasible for a determined attacker with physical access to a data centre to locate a specific customer's data. Without appropriate independent assurance, the SIRO/BASM should not accept this approach.

Note: Moving data between cloud service providers - to support on-boarding and off-boarding processes it may be necessary for storage media to be transferred between organisations and the service provider. If this is the case, the storage media should be appropriately protected using physical controls and/or encryption as set out in the table above.

Data sanitisation

The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data. Inadequate sanitisation of data could result in the data being:

a) retained by the service provider indefinitely;
b) accessible to other users of the service as resources are reused; or
c) lost or disclosed on discarded, lost or stolen media.

[3] Sharding is a type of database partitioning, where the contents of a very large database are split into smaller, faster, more easily managed parts called data shards, which can be spread across multiple servers.

When storage is no longer required, the service provider should sanitise it by explicitly overwriting the storage before reallocating it to another service user. This will help provide reassurance that another organisation could not gain unauthorised access to the data. Additional confidence may be gained if the service provider encrypts all stored data under user-specific keys, or if the data is encrypted (to an NCSC approved standard) before it is stored in the service.

The service provider should provide verifiable evidence to the SIRO/BASM of the process used to sanitise the storage before it is reallocated.

Equipment disposal

Once equipment used to deliver the CDE service reaches the end of its useful life, it should be disposed of in a way, which does not compromise the security of the service, or user data stored in the service. Acceptable approaches for the disposal of equipment are described below.

Approach	Description	Guidance
A recognised standard for equipment disposal is followed	A number of standards include controls, which cover the need for secure equipment disposal. These include: • CSA CCM v3.0 • ISO/IEC 27001	The standards referenced cover the need for secure equipment disposal, rather than validation of the process. See section on Assurance
A third-party destruction service is used	A destruction service, which specialises in secure disposal of equipment is used.	A number of these services have been assessed against a recognised standard, such as the CESG/NCSC Assured Service (Destruction) scheme.

Physical resilience and availability

Services have varying levels of resilience which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business. Services procured with 'best endeavours' support should be considered to have no guaranteed support.

The SIRO/BASM should evaluate whether the service provider can meet the availability and resilience requirements of the employer's/asset owner's organisation. The SRO should consider whether the business impact, including potential project delays and additional costs are adequately covered by any compensation arrangements available from the service provider in the event of service non-availability. Acceptable approaches are set out in the table below.

Approach	Description	Guidance
Review of historical data	The service provider may present evidence of service availability.	The SRO and SIRO/BASM should evaluate this evidence and consider whether this, together with the service provider's contractual commitments and reputation, represent acceptable operational and financial risks.
Analysis of the design	The service provider may be willing to share information on how they have designed their service to be resilient.	Have this information independently reviewed by a specialist security expert to provide additional confidence.

Note: A service provider may offer contractual commitments or Service Level Agreements (SLAs) regarding the level of service availability. However, whilst this approach may provide a mechanism for compensation in event of outages, such outages will not be prevented if the service design is inappropriate. The supplier's evidence of service availability should be reviewed so that the SIRO/BASM can assess the level of risk to service availability.

Principle 3: Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another. More information on the importance of separation requirements in cloud services can be found in the Separation Guide[4]. Acceptable approaches include:

a) use of virtualisation technologies (e.g. a hypervisor, network and storage virtualisation) to provide separation between users. Wherever possible, popular, and well-designed virtualisation technologies should be used, particularly those that have been assessed against well-defined security standards, such as the Certified Product Assurance scheme, and are subjected to appropriate regular penetration tests; and
b) use of software controls (e.g. operating systems, web servers or other applications) to provide separation between users. In this scenario, evidence is required of:
    i. regular penetration tests of infrastructure and any relevant web applications;
    ii. security reviews of the design of the service; and
    iii. an engineering approach that ensures security is a key consideration in developing the service.

The service providers should provide evidence that the approach adopted achieves reliable and effective separation between service users (i.e. different CDEs). This will allow the SIRO/BASM to:

a) understand the types of user that the CDE shares the service or platform with; and
b) have confidence that:
    i. the service provides sufficient separation of your data and service from other users of the service; and
    ii. the management of your service is kept separate from other users.

Note: Combinations of the two approaches can be complementary. When used in combination, they can provide greater confidence in the strength of separation within a service. However, this combined approach should be subject to independent validation and verification.

Principle 4: Governance framework

The service provider should have a security governance framework, which coordinates and directs its management of the service and information within it.

The service provider should provide the following information:

a) a clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service;
b) a documented framework for security governance, with policies governing key aspects of information security relevant to the service;

[4] www.ncsc.gov.uk/guidance/separation-and-cloud-security

c) financial and operational risk reporting mechanisms that ensure their board are kept informed of security and information risks; and
d) auditable processes to identify and ensure compliance with applicable legal and regulatory requirements.

The SIRO/BASM should require the service provider to demonstrate that the above requirements are being met by providing certified conformance with a recognised standard. Common security standards that include controls that cover how well a service provider's governance framework manages a particular service are CSA CCM v3.0 and ISO/IEC 27001. The scope of the supporting certification should be validated to ensure the governance framework goals set out above are covered.

Principle 5: Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

Configuration and change management

The service provider should:

a) provide an accurate picture of the IT assets, physical infrastructure and locations which make up the service, along with their configurations and dependencies;
b) demonstrate that its operational policies, processes and procedures ensure that the status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime;
c) demonstrate that changes to the service are assessed for potential security impact, then managed and tracked through to completion; and
d) ensure that unauthorized changes can be detected and investigated.

The SIRO/BASM should require the service provider to demonstrate that the above requirements are being met, by providing certified conformance with a recognised standard. Common security standards that include controls that cover how well a service provider's configuration and change management processes manages a particular service are CSA CCM v3.0 and ISO/IEC 27001. The scope of the certification should be verified to ensure that configuration and change management processes were covered as part of the assessment.

Note: Without good governance of the service (see Principle 4) it is likely that change and configuration management practices will be ineffective.

Vulnerability management

The service provider should demonstrate that appropriate policies, processes and procedures are in place to:

a) monitor relevant sources of information relating to threat, vulnerability and exploitation techniques;
b) identify and assess potential new threats, vulnerabilities or exploitation techniques that could affect its service;
c) ensure the severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations.; and

d) track known vulnerabilities until mitigations have been deployed.

The service provider should be contractually required to work to agreed timescales for implementing mitigations, based on the following good practice[5]:

a) 'critical' patches should be deployed within hours;
b) 'important' patches should be deployed within 2 weeks of a patch becoming available; and
c) 'other' patches should be deployed within eight weeks of a patch becoming available.

The SIRO/BASM should require the service provider to demonstrate that the above requirements are being met by providing certified conformance with a recognised standard. Common security standards that include controls that related to vulnerability management are ISO/IEC 30111:2013, CSA CCM v3.0 and ISO/IEC 27001. The scope of the certification should be verified to ensure that vulnerability management processes were covered as part of the assessment.

Note: The referenced standards do not explicitly set out acceptable timescales for mitigation. The above good practice timescales should be required as a minimum standard.

Protective Monitoring

The service provider should demonstrate that:

a) the service generates adequate audit events to support effective identification of suspicious activity;
b) these events are analysed to identify potential compromises or inappropriate use of the service; and
c) it takes prompt and appropriate action to address incidents.

The SIRO/BASM should require the service provider to demonstrate that the above requirements are being met by providing certified conformance with a recognised standard. Common security standards that include controls that address the need for effective protective monitoring processes are CSA CCM v3.0 and ISO/IEC 27001. The scope of the certification should be verified to ensure that protective monitoring processes are covered as part of the assessment.

Note: Standards differ in terms of the level of detail applied, and those referenced cover the need for effective protective monitoring, rather than validation of the controls in place.

Incident management

The service provider should demonstrate that:

a) incident management processes are in place for the service and are actively deployed in response to security incidents;
b) pre-defined processes are in place for responding to common types of incident and attack;
c) a defined process and contact route exists for reporting of security incidents by service users and external entities; and
d) security incidents of relevance to the employer's/asset owner's organisation will be reported in acceptable timescales and formats.

[5] See Principle 5 of the NCSC Cloud Guidance for further information

The SIRO/BASM should require the service provider to demonstrate that the above requirements are being met, by providing certified conformance with a recognised standard. Common security standards that include controls that address the need for effective incident management processes are ISO/IEC 27035:2011, CSA CCM v3.0 and ISO/IEC 27001. The scope of the certification should be verified to ensure that incident management processes were covered as part of the assessment.

Note: The standards referenced differ in terms of the level of detail applied. Some cover incident management controls in detail, whereas others simply require an incident management process to exist**.**

Principle 6: Personnel security

Where service provider personnel have access to an organisation's data and systems, a high degree of confidence in their trustworthiness is needed.

The service provider should:

a) subject these personnel to security screening and regular security training and ensure that they understand their security responsibilities;
b) explain how it screens and manages personnel within privileged roles; and
c) ensure the minimum number of people necessary have access to the data or it could affect delivery of the service.

Acceptable approaches are set out in the table below.

Approach	**Description**	**Guidance**
Personnel screening performed but does not conform with BS7858:2012 standard for personnel screening.	BS7858:2012 sets out a basic standard for personnel screening. Many multinational companies will perform background checks on staff that encompass the requirements of this standard, though in some countries it is not possible to perform all of the checks	In these cases, the service provider should describe the personnel security screening functions they carry out on staff with access to your data, or the ability to affect user services. The SIRO/BASM should consider whether this level of screening is acceptable.
Personnel screening performed which conforms to BS7858:2012	Personnel screening is in place which includes or exceeds the requirements of BS7858:2012.	Service provider personnel with privileged roles will be able to gain access to your data and/or affect the reliability of your service. The SIRO/BASM may find it valuable to understand the service provider's approach to detecting potential malicious insiders and use this information as part of the organisation's risk management decision.

Note:

1) Where a service provider is unable to verify the identity, check for unspent criminal convictions, and right to work of staff there is an increased risk of insider threat.
2) Where an organisation is unwilling or unable to perform personnel screening checks, unscreened individuals may have the ability to access the data or affect the service. This situation should not be accepted by the SIRO/BASM.

Principle 7: Secure development

The service provider should demonstrate that:

a) new and evolving threats are reviewed and the service improved in line with them;
b) development is carried out in line with industry good practice regarding secure design, coding, testing and deployment; and
c) configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

Acceptable approaches are set out in the table below.

Approach	Description	Guidance
Engineering approach adheres to a secure development standard or recognised good practice	A number of security standards or good practice guides exist which service providers could claim support their achievement of the goals outlined above. These include: • Safecode 'Fundamental Practices for Secure Software Development' • PAS 754:2014 • ISO/IEC 27034	Whilst the service provider's claim to implement one of these standards offers some assurance, without independent confirmation the SIRO/BASM should assess whether this provides sufficient confidence that all parts of the system are securely engineered. See section on Assurance
Independent review of engineering approach against recognised secure development standard	A number of security standards with supporting certification mechanisms exist which could be used to demonstrate conformance with the goals outlined above. These include: • CESG CPA Build Standard • ISO/IEC 27034 • ISO/IEC 27001 • CSA CCM v3.0	See section on Assurance Check that the scope of the assessment includes the incident management aspects required.

Principle 8: Supply chain security

The service provider should:

a) ensure that its supply chain satisfactorily supports all of the security principles, which the service claims to implement;
b) explain how the employer's/asset owner's information is shared with, or accessible to, third party suppliers and their supply chains;
c) demonstrate how its procurement processes place security requirements on third party suppliers;
d) explain how it manages security risks from third party suppliers and the conformance of its suppliers with any security requirements; and
e) explain how the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

The SIRO/BASM should require the service provider to demonstrate that security controls are implemented throughout the supply chain, by providing certified conformance with a recognised standard. Common security standards that include controls that address the need for effective incident management processes are ISO/PAS 28000:2007 and ISO/IEC 27001. The scope of the certification should be verified to ensure that required supply chain aspects were covered as part of the assessment.

Note: The standards referenced differ in terms of the level of detail applied. Some cover incident management controls in detail, whereas others simply require an incident management process to exist**.**

Principle 9: Secure user management

The service provider should make tools available for the employer/asset owner to securely manage its use of the service. Availability of secure management interfaces and supporting procedures is essential to prevent unauthorised access to and alteration of the employer's/asset owner's resources, applications and data.

Authentication of users to management interfaces and support channels

The service provider should provide evidence that:

a) the employer's/asset owner's organisation is aware of all of the mechanisms by which the service provider would accept management or support requests (e.g. telephone, web portal, email, etc.);
b) strong authentication is in place, so that only authorised individuals from the employer's/asset owner's organisation can use those mechanisms to affect the use of the service (Principle 10); and
c) regular testing is in place to verify its security via these channels (e.g. through using social engineering techniques).

The SIRO/BASM should assess the strength and effectiveness of user identification and authentication in each of these mechanisms.

Note: Exercising the strength of authentication provides confidence, about the authentication mechanisms in place at a given point in time.

Separation and access control within management interfaces

The service provider should:

a) demonstrate the measures that prevent users from other organisations from accessing, modifying or otherwise affecting your service management;
b) explain how it manages the risks of privileged access using the system(s);
c) assist the SIRO/BASM to understand how the service management interfaces are protected (see Principle 11) and what functionality they expose; and
d) support any independent penetration testing of the management interfaces.

Where the separation between users of digital service management interfaces is performed in software, regular testing, including penetration tests, should be used to assess the strength of separation within digital service management interfaces.

Penetration testing should be well scoped to ensure that it provides confidence in the security of the service management interfaces. The penetration testing should be designed to detect common or publicly known weaknesses at the time of the test, as well as allowing some time for investigation of novel and/or previously unknown classes of vulnerability.

Principle 10: Identity and authentication

All access to service interfaces should be constrained to authenticated and authorised individuals. Authentication should occur over secure channels, i.e. protected by TLS or with access via a VPN.

Acceptable approaches are set out in the table below.

Approach	Description	Guidance
Two factor authentication	Users authenticate with a username, password and either a hardware/software token, or 'out of band' challenge (e.g. SMS).	This approach is considered good practice, assuming that standard, and well tested, authentication schemes are used.
TLS client certificate	The service supports authentication over TLS using an X.509v3 client certificate that identifies an individual user.	This method provides strong cryptographic protection, but is dependent on the secure creation and management of certificates, and on the safeguards in place on end user devices to protect them. Processes will be needed to revoke lost or compromised credentials.
Identity federation with your existing identity provider	The service supports federating to another authentication scheme, such as a corporate directory, an OAuth or SAML provider.	Using federated identity approaches for public sector users has the benefit of only having to manage a single identity and authorisation scheme, rather than many.

If the service provider relies upon authentication solely via basic username and password any compromised credentials can be easily re-used by an attacker to gain access to the service. This is not an acceptable approach for access via the Internet.

Note: the service provider may support a combination of approaches, e.g. two factor authentication and/or TLS client certificate, and identity federation.

Principle 11: External interface protection

To ensure that all external or less trusted interfaces of the service are identified and appropriately defended, the service provider should provide information to allow the SIRO/BASM to:

a) understand what physical and logical interfaces service data may be available from, and how access to the data is controlled;
b) understand how the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10).

Acceptable approaches are set out in the table below.

Approach	Description	Guidance
Internet	Users connect to the service directly over the internet.	Since the service can be accessed from any internet-connected device, attacks can be launched from anywhere. External interfaces to the service should be robust to attack and subject to a regime of continuous testing to ensure they remain secure. See section on Assurance
Community network	Some cloud services (particularly community cloud services) may only connect directly to private community networks (e.g. the Public Services Network)	If the cloud service is only accessible via the community or private networks, the service is likely to be less exposed to remote attackers. However, this does not prevent attacks by insiders. Appropriate controls, access and usage logs and monitoring should be in place. If the service offers any internet connectivity to the data, then it should be treated as thought connected directly to the Internet.
Private network	Some services may provide dedicated connections in to your network.	

Principle 12: Secure service administration

The service provider should provide sufficient information to allow the SIRO/BASM to:

a) understand which service administration model is being used by the service provider to manage the service; and
b) be able to assess any risks the service administration model in use brings to the organisation's data or use of the service.

The service provider should identify which of the systems administration models[6] it uses to administer the service. The SIRO/BASM should assess the risks associated with implemented systems administration models. Independent assurance from a suitably qualified security architect may be required.

If the service provider asserts that their systems administration approach is not covered by one of the models, the SIRO/BASM should commission independent assurance from a suitably qualified security architect to assess the risks associated with the service provider's approach.

Note: An unknown service management architecture represents an unacceptable level of risk for systems processing BIM data and should not be accepted by the SIRO/BASM.

[6] Systems administration architectures – see www.ncsc.gov.uk/guidance/systems-administration-architectures

Principle 13: Audit information for users

Audit records are needed to monitor access to the CDE and data held within it. The type and scope of audit information available has a direct impact on the ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

If the service provider does not offer audit information this will prevent identification of misuse of the CDE service and asset data. The inability to determine how, when or where a service is accessed could result in legal or regulatory issues and should be regarded as unacceptable.

The SIRO/BASM needs to be confident that the audit information available will be suitable for investigating misuse or incidents. The service provider should be contractually required to make specific audit data available to authorised service users. The timetable, method, format and retention period of the data should be specified in the service contract.

Note: Provision of audit information does not in itself give any protection. The information will require analysis to uncover evidence of compromise or misuse.

Principle 14: Secure use of the service

Security of the CDE will be undermined if the service is accessed or used through poorly configured or compromised end user devices. The SIRO/BASM should require that the data is only accessed as follows:

a) by using enterprise managed devices that are under the control of the employer's/asset owner's organization. These devices should be configured securely applying the appropriate NCSC End User Devices Security Guidance; and
b) by using partner (Supplier) managed devices, for which a minimum standard of certification of compliance with the Cyber Essentials should be contractually required. For Tier One advisers and suppliers, and particularly for those working on sensitive aspects of the built asset or its design, it is preferable to require certification to Cyber Essentials Plus.

Given the need to rely upon contracts to enforce the employer's/asset owner's organisation's security requirements with partners/suppliers, it is essential that the security variant of the BIM protocol[7] is used as this includes cascading security provisions that can be applied to the supply chain.

[7] This is available from the CPNI website (www.cpni.gov.uk)