CPNI
Centre for the Protection of National Infrastructure

CLOUD-BASED BIM AND SMART ASSET MANAGEMENT: ADOPTING A SECURITY-MINDED APPROACH

March 2016

Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Background

Effective security is an essential element of safe and trustworthy delivery and management of digital built assets, be they buildings or infrastructure, as well as in protecting related intellectual property, commercial and personally identifiable information. All organisations therefore need to be aware of the risks associated with poorly configured and maintained systems, as well as the limitations of contractual arrangements with system providers. These issues are of increasing importance to the businesses that design, build, operate and use these assets with the proliferation of cloud-based services and Software as a Service (SaaS) systems.

This guidance has been written to support the implementation of the approach set out in PAS 1192-5 to manage the risks that can affect asset information that is created, processed or stored in cloud services. It should be read alongside the PAS as both use a common set of terms and definitions. It supplements existing UK Government guidance on cloud security[1] which provides a framework for determining security need against 14 principles. Although specifically targeted at public sector organisations, the framework is applicable to any UK-based construction project.

What are the cloud service security needs for my project/asset?

After applying the security triage process contained in the PAS, the Employer or Asset Owner should apply the guidance below to determine its cloud service security needs.

	Security-minded approach	**Cloud security requirements**
S1	Protect data/information regarding own built asset. Take appropriate steps to protect data/information about neighbouring built asset. Use PAS 1192-5 and seek security guidance.	Apply the 14 security principles in the UK Government cloud security guidance in line with the security requirements of the Built Asset Security Strategy (BASS). Contractual commitment to meet security requirements is essential - independent validation of service provider assurances should be considered and employed where appropriate.
S2	Protect data/information regarding own built asset. Use PAS 1192-5 and seek security guidance.	
S3	Protect any commercially and/or personally sensitive data/information regarding own built asset. Take appropriate steps to protect data/information about neighbouring built asset.	Consider whether business benefits will be derived from applying the 14 security principles in the UK Government cloud security guidance. Relying upon service provider assertion may provide sufficient, proportionate assurance.
S4	Protect any commercially sensitive and/or personal data/information regarding own built asset.	

[1] http://www.gov.uk/government/collections/cloud-security-guidance

Each of the 14 principles represents a fundamental security aspect that should be considered when determining the appropriate and proportionate level of security of data/information that is required of a cloud service. The Appendix to this document contains a set of due diligence questions regarding the use of cloud services for the creation, processing or storage of asset information.

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 or Asset Owner should also take into consideration the cloud computing guidance published by the Information Commissioner's Office (ICO)[2]. 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 or 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.

Notes:
Cloud computing removes the physical ties between software and the hardware platforms on which it runs, thus enabling ubiquitous, on-demand networked access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider intervention. This in turn enables the delivery of rapidly scalable processing and storage environments.

[2] https://ico.org.uk/media/1540/cloud_computing_guidance_for_organisations.pdf

Appendix – Due diligence questions regarding use of cloud services for creation, processing or storage of asset information

This Appendix contains a set of questions that asset owners should address when considering the use of cloud services for the creation, processing or storage of asset information. The answers to these questions should be used to inform the built asset risk assessment process. They should be checked when undertaking periodic reviews of the BASS or re-applying the triage process to the built asset.

Cloud security principles	Response to questions	Method of assurance
1. Data in transit protection		
1.1 How is the asset information protected in transit between the cloud service and the user's device (computer, laptop, tablet, etc.)?		
1.2 How is the asset information protected internally within the cloud service?		
1.3 How is the asset information protected between the cloud service and any other cloud service (e.g. where point cloud data is sent to a rendering engine)?		
2. Asset protection and resilience		
2.1 In what country or countries will the asset information be stored?		
2.2 What are the security arrangements for the data centre(s) used for the storage of the asset information?		
2.3 How is the storage media containing the asset information protected to prevent unauthorised access?		
2.4 What are the data sanitisation processes for provisioning, migration or de-provisioning of any storage media or processing resources that form part of the cloud service that handles the asset information?		
2.5 What are the processes for decommissioning and disposal of equipment used to deliver the cloud service?		
2.6 How resilient is/are the data centre environment(s) used to deliver the cloud service?		

Cloud security principles	Response to questions	Method of assurance
2.7 In what country or countries will the asset information be processed?		
2.8 What are the security arrangements for the data centre(s) used for the processing of the asset information?		
2.9 From which country or countries will the service be managed, supported and administered (i.e. the locations of service provider personnel and its support staff who are responsible for delivering and maintaining the service)?		
2.10 Under what legal jurisdiction(s) does the cloud service operate?		
3. Separation between consumers		
3.1 What other consumers/users/organisations are sharing the cloud service or cloud platform that is storing or processing the asset information?		
3.2 What confidence does the asset owner have that there is adequate separation between third party information and its asset information?		
3.3 What confidence does the asset owner have that there is adequate separation between the management of its service/platform and the management of third parties?		
3.4 What confidence does the asset owner have that the answers to the other separation questions in this section will not change adversely over time?		
4. Governance framework		
4.1 What confidence does the asset owner have that the governance framework (policies, processes and procedures) in place for the service is appropriate for its intended use?		
4.2 How often is the effectiveness and appropriateness of the governance framework reviewed?		
4.3 What processes are in place to identify and ensure compliance with applicable legal and regulatory requirements relating to the service?		

Cloud security principles	Response to questions	Method of assurance
4.4 What processes are in place to identify and ensure compliance with applicable security requirements relating to the service?		
5. Operational security		
5.1 What processes are in place to ensure that changes to the system do not unexpectedly alter security properties and have been properly tested and authorised?		
5.2 What processes are in place to ensure that security issues in constituent components are identified and mitigated?		
5.3 What processes are in place to ensure that effective measures are in place to detect attacks and unauthorised activity on the service?		
5.4 What confidence does the asset owner have that the service can respond to incidents and recover a secure available service in a timely manner?		
6. Personnel security		
6.1 Is there an acceptable level of security screening conducted by the service provider on all those staff with access to the asset information or with the ability to affect the service?		
6.2 What level of security screening is applied to systems administrators that are responsible for the service?		
7. Secure development		
7.1 Has the service been designed and developed to identify and mitigate threats to its security?		
7.2 Does the development of the software used by the service apply the trustworthy software principles set out in PAS 754, Software Trustworthiness - Governance and Management - Specification?		

Cloud security principles	Response to questions	Method of assurance
8. Supply chain security		
8.1 What confidence does the asset owner have that the service provider’s supply chain satisfactorily supports all of the security principles that the service claims to implement?		
8.2 To what extent is the asset information shared with, or accessible by, third party suppliers and their supply chains?		
8.3 How does the service provider manage security within its supply chain, in particular the handling of risks and conformance to standards by its third party suppliers and delivery partners?		
8.4 How does the service provider verify that hardware and software used in the delivery of the service is genuine and has not been tampered with?		
9. Secure consumer management		
9.1 What tools are provided to allow an asset owner to securely manage its service?		
9.2 What tools are used to ensure that only authorised individuals from the asset owner’s organisation and its supply chain are able to authenticate and access management interfaces for the service?		
9.3 What confidence does the asset owner have that only authorised individuals are able to perform actions affecting its service through support channels?		
10. Identity and authentication		
10.1 Are appropriate and proportionate measures in place to ensure access to all service interfaces is only available to properly authenticated and authorised individuals?		
10.2 Is the authentication handled over secure channels?		

Cloud security principles	Response to questions	Method of assurance
11.External interface protection		
11.1 Do users understand how to safely and securely connect to the service whilst minimising the risk to their own systems and devices?		
11.2 Does the asset owner understand what physical and logical interfaces its asset information is available from?		
11.3 Does the asset owner have sufficient confidence that appropriate and proportionate protections are in place to control access to its asset information?		
11.4 Does the asset owner have sufficient confidence that the service can determine the identity of connecting users and services to an appropriate level for the data or function that is being accessed?		
12. Secure service administration		
12.1 What methods are used by the service provider’s administrators to manage the operational service so as to mitigate any risk of exploitation that could undermine the security of the service?		
12.2 What confidence does the asset owner have that the technical approach the service provider employs to manage the service does not put the asset information or service at risk?		
13. Audit information provision to consumers		
13.1 Will the service provider provide all necessary audit records to the asset owner to permit monitoring of access to its service and the asset information held within it?		
13.2 How will the audit records be made available, in what format and what is the retention period associated with them?		
13.3 What confidence does the asset owner have that the audit information will allow it to meet its needs for investigating breaches and misuse incidents?		

Cloud security principles	Response to questions	Method of assurance
14. Secure use of the service by the consumer		
14.1 What end user devices will be used to access the service?		
14.2 What service configuration options are available to users and what are the security implications of choices they make?		
14.3 How can the asset owner ensure that service users, whether administrators or end users, understand how to use the service safely and securely?		
14.4 How do the service processes, uses and infrastructure relate to the use of the service and the asset owner's security requirements?		