UK BIM Alliance - Security Guidance

Understanding IT Resilience

Title of guidance:	*Understanding organisational IT resilience*
Author:	*Sarah Davidson*
Company:	*Gleeds*
Email:	*Sarah.davidson@gleeds.co.uk*
Objective of guidance:	*To provide guidance on schemes and standards that can help the Employer to understand their own plus project team member organisational resilience*

Abbreviations/acronyms	**Full name**
OIRs	*Operational information requirements*
AIRs	*Asset information requirements*
EIRs	*Employer's Information requirements*
BEP	*BIM Execution Plan*
AIM	*Asset information model*
CDE	*Common data environment*

Relevant/referenced sources	
PAS 1192-5:2015	*Specification for security-minded building information modelling, digital built environments and smart asset management*
	The Cyber Essentials Scheme
	10 Steps to Cyber Security
BS ISO 27001: 2013	*Information technology – Security techniques – Information security management systems - Requirements*

Keywords:	*Cyber Essentials,*

General notes to support the text/publication on the UK BIM Alliance website
[insert as applicable]

Briefing note text

Having an understanding of your own IT resilience and the IT resilience of the organisations that you are working with (all those storing information, including data hosts) is important. This will give you a picture of the measures and processes that are in place to protect organisational, asset and project data and information. In addition it will help expose potential operating risks whilst enabling monitoring and improvements to be put in place as needed.

There are a number of standards and schemes in place to assist in understanding IT resilience. They are geared towards the development and implementation of appropriate IT management strategies and include:

The Cyber Essentials Scheme

PAS 1192-5 notes a Government recommendation that all its suppliers should as a minimum meet the requirements of the Cyber Essentials scheme. It is designed to protect organisations from the most common internet threats and considers:

1. Boundary firewalls
2. Secure configuration
3. User access control
4. Malware protection
5. Patch management

There are two levels to the scheme:

1. Cyber Essentials
2. Cyber Essentials Plus

The first step for both levels is to complete a short self-assessment questionnaire. For Cyber Essentials, this questionnaire is independently reviewed by an external certifying body. For Cyber Essentials Plus tests of various systems are carried out by an external certifying body.

You can find out more at https://www.cyberaware.gov.uk/cyberessentials/

10 Steps for Cyber Security

The basic premise of 10 Steps is that an organisation has an effective risk management scheme (step 1) which is then supported by 9 elements of IT governance covering:

1. Security IT configuration
2. Network security
3. Managing user privileges
4. User education and awareness
5. Incident management
6. Malware prevention
7. Systems monitoring
8. Removable media controls
9. Home and mobile working policies and procedures

The National Cyber Security Centre provides detail behind 10 Steps along with other helpful guidance – their website is https://www.ncsc.gov.uk/ with 10 Steps information available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Cloud security principles

If you are going to be utilising cloud storage then it is worth looking at the Government's Cloud Security Principles to provide a means of evaluating how robust the storage service is. These principles may go beyond what is required of a construction project (whether private or public) but are a helpful reference point – see https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

Standards

BS ISO 27001: 2013 sets out requirements for IT systems. It covers establishing, implementing, maintaining and continually improving an information security management system. It is worth establishing the extent to which organisations work in compliance with or are certified to this standard. There are various elements to this standard and certification may be limited to certain aspects of it.

Industry collaboration – Cyber Aware

The Government's Cyber Aware campaigned is aimed at making sure that there are consistent and clear messages about the need to become resilient to cyber threat whilst getting the most out of

online systems. You can find out more about Cyber Aware and how to get directly involved at https://www.cyberaware.gov.uk/