Baseline security recommendations for projects that do not reach the requirement of PAS1192-5 and a Built Asset Security Manager Involvement (See note 1).
This flow chart may be followed/implemented by the project lead in collaboration with IT manager and CIO/Information Manager/Security manager etc

Potential Vulnerabilities

1. People – Consider staff training and regular awareness sessions using information from the National Cyber Security Centre (NCSC): **https://www.ncsc.gov.uk/guidance**
2. Un-authorised devices being allowed on network – this can be easily mitigated by port control and good and regular Wi-Fi password management.
3. Disgruntled employees – Awareness around the risks of a disgruntled employee leaving the organisation; theft of data is common.
4. Movement of information – how data is moved around both internally and externally via insecure email systems and/or un-encrypted media devices which are not controlled.
5. Password management – Regular password management and follow NCSC guidance : **https://www.ncsc.gov.uk/guidance/password-collection**
6. Suspicious emails – Suspicious emails with attachments or links; consider email naming policy. Look to NCSC for current threats - **https://www.ncsc.gov.uk/threats**

Assumptions

1. Your system has up-to-date Antivirus software and firewall; this includes servers, end user devices etc.
2. Your active equipment has physical LAN or VLAN management to segregate systems to stop the spread of an attack – particularly CCTV, BMS, Access control systems etc.
3. Access to business systems is routinely accessed which includes access to relevant folders.
4. You have a work from home policy.
5. You have policy on removable media devices.
6. Only authorised and official software in use.
7. Operating system is up to date and still supported by the originating software developer.
8. Server Room security is in place.

Considerations

1. Marketing – how you communicate your involvement with a project; particularly using internet tools i.e. websites or uncontrollable document like press releases.
2. Tendering and procurement – how you share information with the supply chain and retain control of it.
3. 'Sheep-Dip' - A stand alone (not networked) PC with up-to-date AV software that can be used to check for viruses on removable media prior to introducing to a networked device.
4. Network Access Control (NAC) – A procedure that can control how new devices join the network.
5. Those who have access to all project information i.e. Project Managers and Cost Managers; particularly from external sources.

Notes -

Note 1:

The Security triage from PAS 1192-5:2015 should be followed in the first instance to establish the level of security that is required around the project. If the result of this process is S3 or S4 (as described in Fig 5 of PAS 1192-5:2015) then the processes below may be followed in order to encapsulate project info with baseline security measures.

Note 2:

The Government Cyber Essentials (CE) scheme gives a confidence around cyber 'health'. Some frameworks (e.g. CCS) require CE+ accreditation to be on framework. More info can be found at **https://www.gov.uk/government/publications/cyber-essentials-scheme-overview**
ISO27001 may also be beneficial.

Note 3:

A Government scheme to highlight to 10 main areas where Cyber risks can be mitigated; more detail can be found on the info graphic on this document (info-graphic not controlled so subject to change) and at **https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary**

Note 4:

Common Data Environment (CDE) is a process where project data is available for collaborative use. The process can be carried out in a number of ways but the 2 most common are an Electronic Data Management System (EDMS) or utilising an organisations existing folder structure on a networked drive.

Note 5:

Whether cloud based or not, understand where the data is being stored (country) and what level of tier the data centre is; understand how/when data is being backed up, where back ups are stored, how often is data backed up, how long are back ups stored for etc.

Note 6:

If outsourcing data storage/hosting check any Service Level Agreements and ensure there is clarity on what you have procured; in particular, those captured under Note 5.

Note 7:

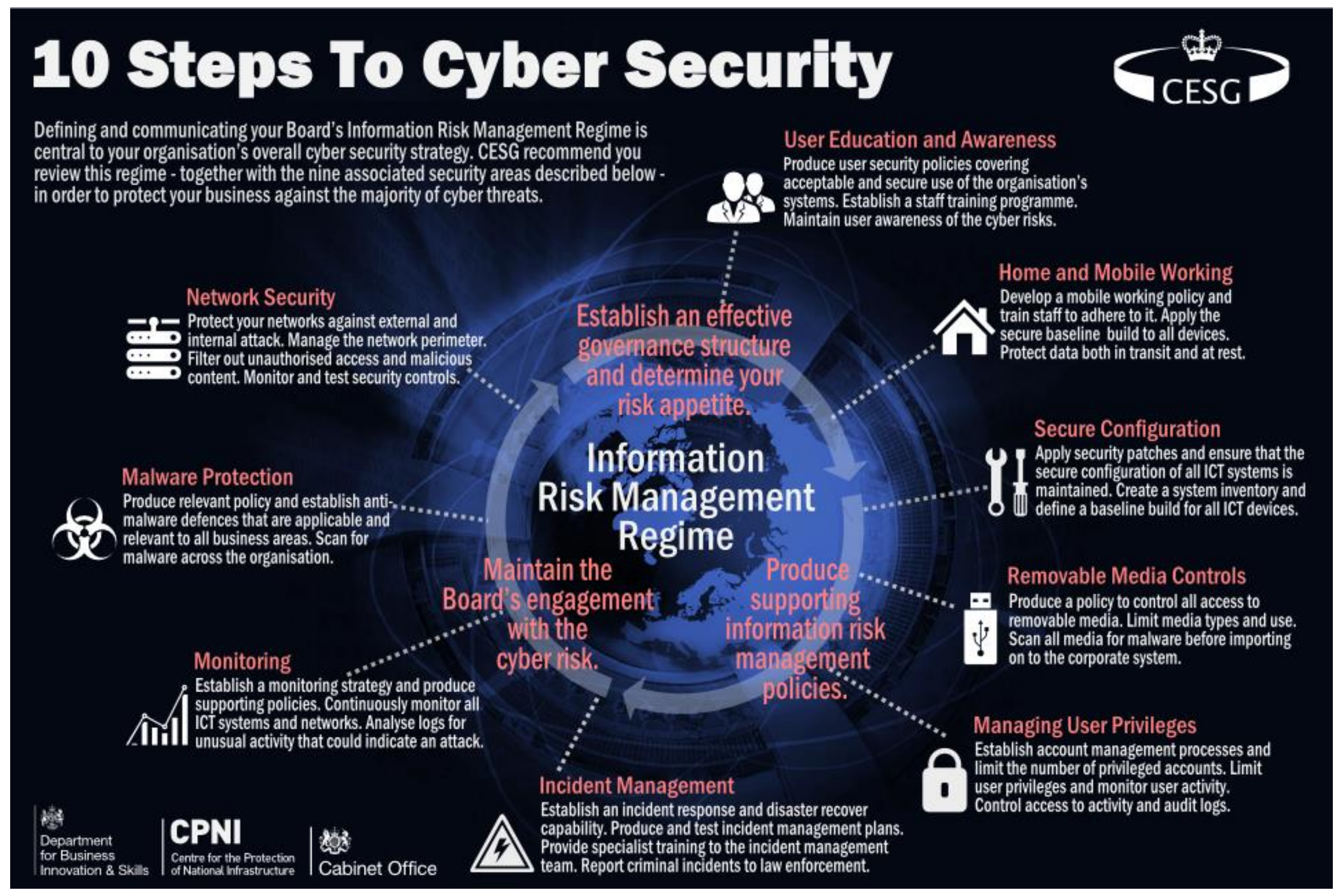
An Information Manager (IM) should be appointed by client/project owner.

Note 8:

The General Data Protection Regulation (GDPR) comes into force May 2018. Any personal data must be stored and accounted for throughout lifecycle of data. Loss needs to be reported. Seek specific GDPR guidance.

IMPORTANT

At the time of creation, information on GDPR and Network and Information Systems NIS (Directive) was either still out for consultation or awaiting clarification – independent advice should be sought as both of these legislations will become UK Law May 2018 and can incur significant fines (Min €20Mil).



10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

User Education and Awareness
Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration
Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Managing User Privileges
Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

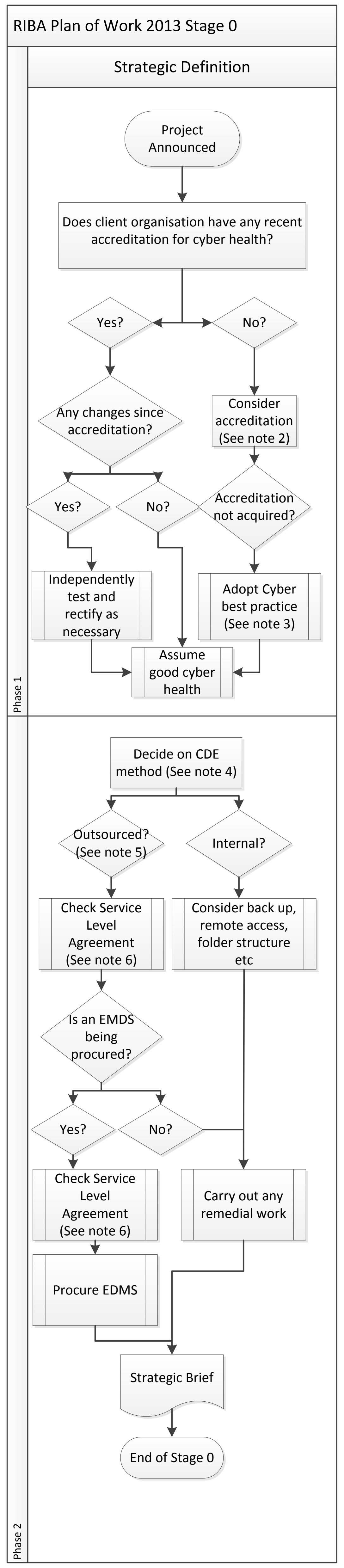
Incident Management
Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Malware Protection
Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Network Security
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Department for Business Innovation & Skills | CPNI Centre for the Protection of National Infrastructure | Cabinet Office



RIBA Plan of Work 2013 Stage 0

Strategic Definition

Phase 1

Project Announced

Does client organisation have any recent accreditation for cyber health?

Yes?

No?

Any changes since accreditation?

Consider accreditation (See note 2)

Yes?

No?

Accreditation not acquired?

Independently test and rectify as necessary

Adopt Cyber best practice (See note 3)

Assume good cyber health

Phase 2

Decide on CDE method (See note 4)

Outsourced? (See note 5)

Internal?

Check Service Level Agreement (See note 6)

Consider back up, remote access, folder structure etc

Is an EMDS being procured?

Yes?

No?

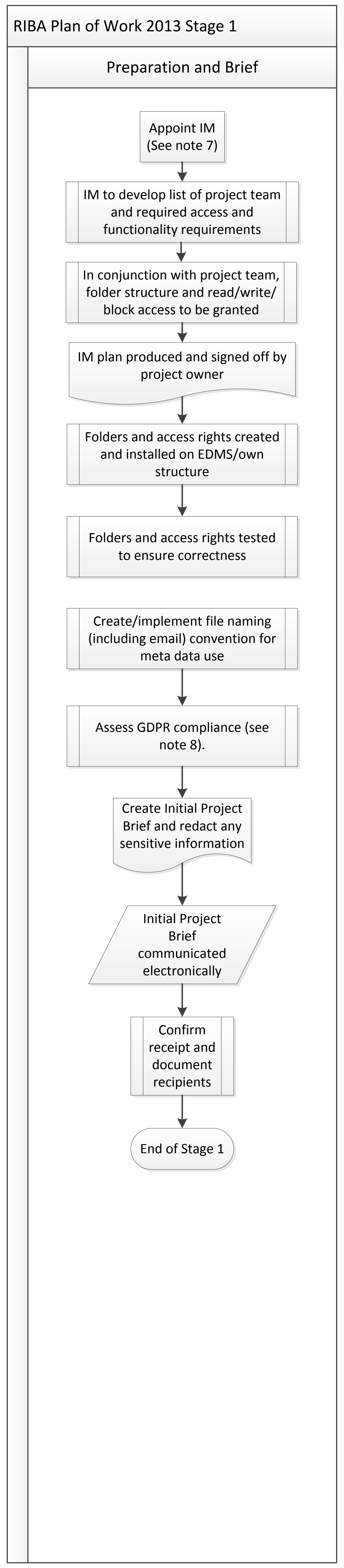
Check Service Level Agreement (See note 6)

Carry out any remedial work

Procure EDMS

Strategic Brief

End of Stage 0



RIBA Plan of Work 2013 Stage 1

Preparation and Brief

Appoint IM (See note 7)

IM to develop list of project team and required access and functionality requirements

In conjunction with project team, folder structure and read/write/block access to be granted

IM plan produced and signed off by project owner

Folders and access rights created and installed on EDMS/own structure

Folders and access rights tested to ensure correctness

Create/implement file naming (including email) convention for meta data use

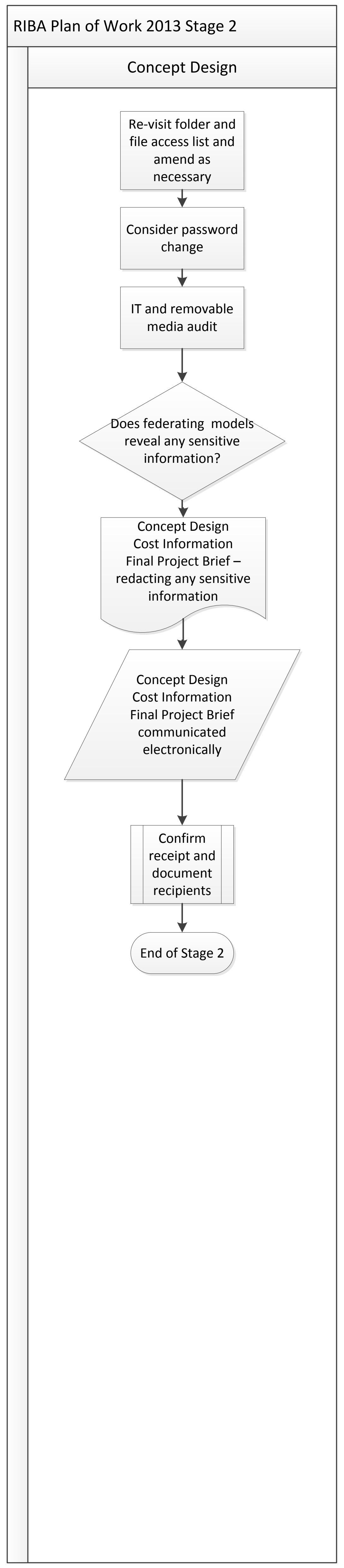
Assess GDPR compliance (see note 8).

Create Initial Project Brief and redact any sensitive information

Initial Project Brief communicated electronically

Confirm receipt and document recipients

End of Stage 1



RIBA Plan of Work 2013 Stage 2

Concept Design

Re-visit folder and file access list and amend as necessary

Consider password change

IT and removable media audit

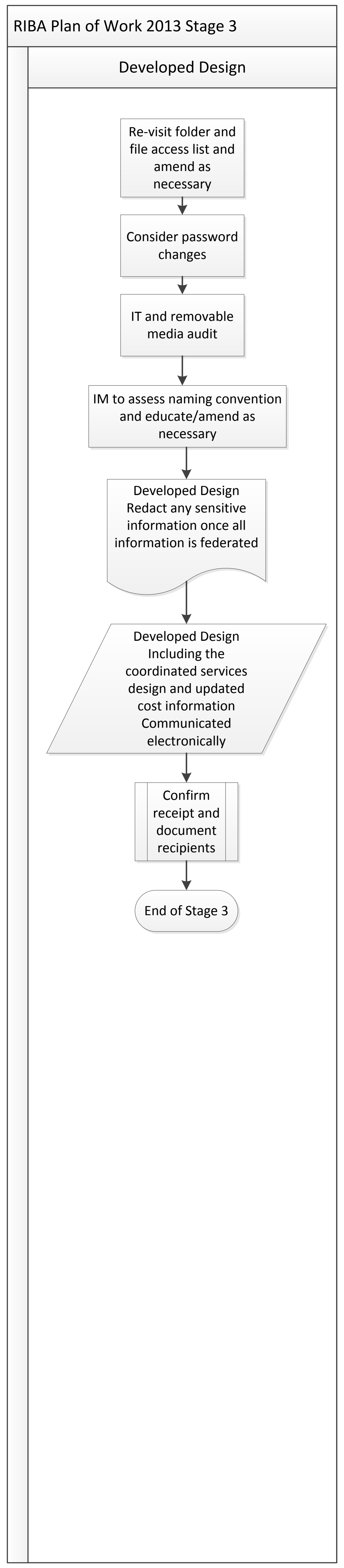
Does federating models reveal any sensitive information?

Concept Design Cost Information Final Project Brief – redacting any sensitive information

Concept Design Cost Information Final Project Brief communicated electronically

Confirm receipt and document recipients

End of Stage 2



RIBA Plan of Work 2013 Stage 3

Developed Design

Re-visit folder and file access list and amend as necessary

Consider password changes

IT and removable media audit

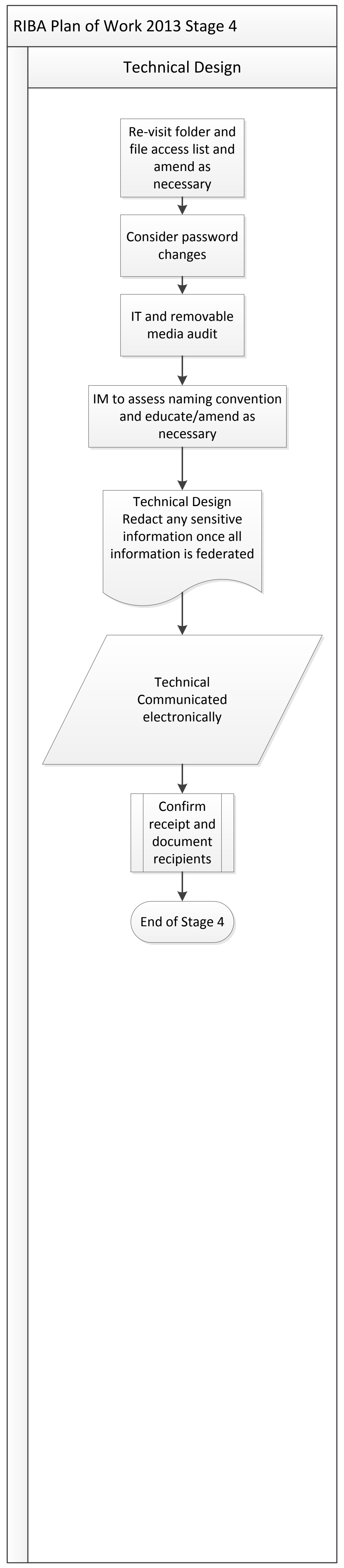
IM to assess naming convention and educate/amend as necessary

Developed Design Redact any sensitive information once all information is federated

Developed Design Including the coordinated services design and updated cost information Communicated electronically

Confirm receipt and document recipients

End of Stage 3



RIBA Plan of Work 2013 Stage 4

Technical Design

Re-visit folder and file access list and amend as necessary

Consider password changes

IT and removable media audit

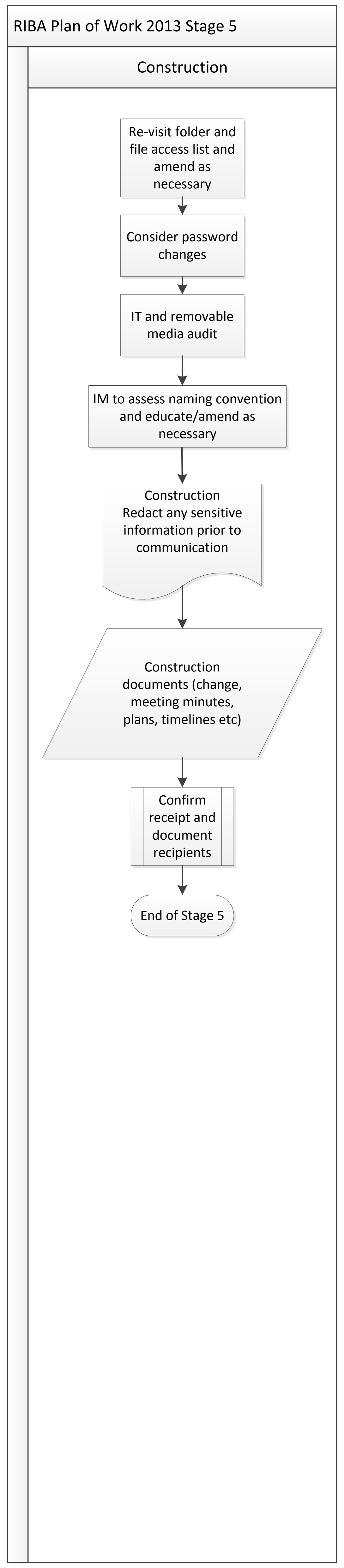
IM to assess naming convention and educate/amend as necessary

Technical Design Redact any sensitive information once all information is federated

Technical Communicated electronically

Confirm receipt and document recipients

End of Stage 4



RIBA Plan of Work 2013 Stage 5

Construction

Re-visit folder and file access list and amend as necessary

Consider password changes

IT and removable media audit

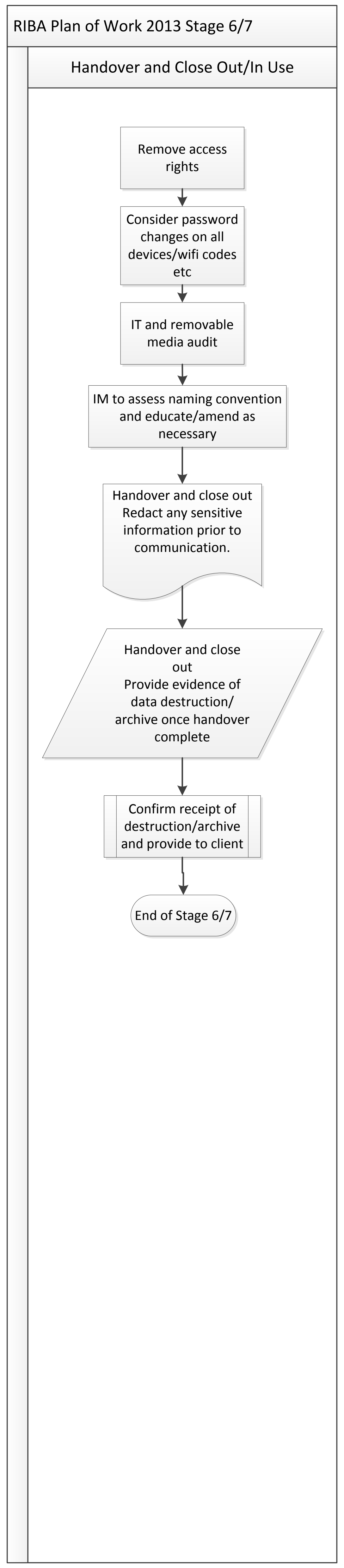
IM to assess naming convention and educate/amend as necessary

Construction Redact any sensitive information prior to communication

Construction documents (change, meeting minutes, plans, timelines etc)

Confirm receipt and document recipients

End of Stage 5



RIBA Plan of Work 2013 Stage 6/7

Handover and Close Out/In Use

Remove access rights

Consider password changes on all devices/wifi codes etc

IT and removable media audit

IM to assess naming convention and educate/amend as necessary

Handover and close out Redact any sensitive information prior to communication.

Handover and close out Provide evidence of data destruction/archive once handover complete

Confirm receipt of destruction/archive and provide to client

End of Stage 6/7