Check List

Maintaining Business Availability and Functionality

- How critical is the business data and functionality?
- What is the service providers business continuity and DR plan?
- What is your data back up plan?
- What is your business continuity and DR plan?
- Data restoration options?
- Scalability options?
- How robust is the network connectivity to the Cloud?
- Is there a service provider availability guarantee?
- How do you understand and quantify the impact of a potential outage?
- SLA's – are there scheduled outages?
- What monetary compensation is tied to the SLA for unplanned outages?
- What lock in or termination considerations are associated with a change of service provider?

Protection of data from unauthorised access

- What IT Security policies and procedures does the service provider have in place?
- What physical security arrangements are in place?
- How are the IT Security policies and procedures audited?
- What sovereignty and legal considerations do we need to consider?
- Security checking of staff
- Auditing of staff
- Non-staff access to data centres by visitors or contractors
- Data sensitivity
- Ownership of data
- What is the chosen cloud delivery or deployment model
- Are there software and hardware procurement requirements?
- What technologies does the provider use to secure access?
- Are there monitoring and management systems are in place for customers?
- Which remote monitoring and management systems does the provider use?
- What gateway technologies are deployed?
- User authentication is in place?
- Is there centralised control of data?
- Sanitisation of media
- What are the data encryption arrangements
- Data encryption key management plan
- Is email content filtered

Protect data from unauthorised access by customers of the same service provider

- Customer segregation process
- Dedicated Server infrastructure
- Sanitisation of media