

8. Business continuity / disaster recovery

Awarding bodies must have suitable measures in place to ensure the effective management of business continuity to address business interruption and the need for disaster recovery for their e-assessment services and systems, in the event of a system's failure. This management should be underpinned by measures to identify potential risks to those services and systems so that they can be managed to minimise disruption.

- 8.1. Awarding bodies must implement risk management procedures to provide early identification of risks to the operation of e-assessment systems and enable action to be taken to minimise the impact of those risks, in line with recognised standards of good practice (see Appendix 1 for a list of relevant standards of good practice).
- 8.2. Awarding bodies' service level agreements with service providers for their e-assessment systems must consider substantial interoperability with other systems and service providers, as far as is practicable, to enable adaptability in the contracting of services and to help manage risks and dependencies in the event of a system's failure.
- 8.3. Awarding bodies must put in place procedures to anticipate interruptions to the operation of their e-assessment systems and minimise the time needed for their recovery, while ensuring secure system back-ups are maintained, including the facility to enable off-site access.
- 8.4. Awarding bodies must put in place a disaster recovery programme that sets out how the operation of their e-assessment system and services will restart after a significant disruption.
- 8.5. Awarding bodies' disaster recovery programmes should determine how access to alternative, convenient, fully equipped services and facilities will be provided. This must include how service will be re-started in line with an awarding body's defined priorities and within identified timescales, after the disaster has occurred.
- 8.6. Awarding bodies must ensure that their centres have comprehensive strategies for back-up and contingency scenarios in the light of a system failure at the centre.