Standards – Guidance and Examples

Operational Controls and Procedures

Standard
3.2 Business Continuity/Disaster Recovery PASA expects administrators to have fully documented, tested and robust Business Continuity and Disaster Recovery plans in place in respect of their operation.

Rationale
Business continuity and disaster recovery plans which are documented and regularly tested provide assurance that services can continue to be delivered and services remain available should a disruptive incident occur. Business continuity and disaster recovery plans ensure that scheme data and records are secured, protected from destruction and continue to be available to enable services to be provided. Where administration services are provided (in whole or in part) by a third party then it is expected that Business Continuity and Disaster Recovery plans are in place for both the appointee and the delegating body.

General Principles
PASA believes that having documented procedures which are tried and tested is necessary to ensure continuity and consistency of service should a Business Continuity or Disaster Recovery incident arise. They help to ensure that all the necessary steps are taken to provide ongoing service in the event of a disaster, ensuring the staff and Governing Bodies[1] are aware of the situation. Where the Governing Body is applying for PASA accreditation, both the appointee and delegating body need to be able to demonstrate that their processes are clearly defined and maintained; that they are tested regularly and they are taking corrective action where procedures fail to work. Where

[1] Governing Bodies should include, as appropriate, Trustees, Trustee Boards, Governance Committees and Boards and others charged with the oversight of the administration service delivery

the administrator is seeking accreditation, it will need to be able to demonstrate that their processes are clearly defined and maintained; that they are tested regularly and they are taking corrective action where procedures fail to work.

It is expected that the audit of the Business Continuity and Disaster Recovery plan will be appropriate to the size and complexity of the providing organisation.

Outcomes

- Planned downtimes are known and communicated to governing bodies and scheme members;

- All services are recovered within a reasonable timescale in the event of a disaster/continuity issue;

- Key member processes such as pensioner payments, retirement processing and bereavement services are recovered within 24 hours

- Critical data not lost or permanently damaged;

- Governing bodies can be confident that services will continue to be provided.

Measures/Evidence

- The administrator (and in the case of a Governing Body applying for PASA accreditation) should have a documented business continuity plan that includes disaster recovery and which covers all of its locations, demonstrating:

    - Robust security, back-up and/or recovery procedures for paper files and all scheme records;

    - Recovery of all systems in an alternative location if the original location is unusable;

    - Alternative premises appropriate to the scale of the operation are available and the facilities are tested regularly;

    - A communication plan (internal and external) with an appropriate cascade of instructions;

- Disaster Recovery testing should be carried out at least annually;

- The results of the tests should be reported to governing bodies including as a minimum, the date of the test, the general results of the tests, whether there were any material failings identified and, if so, what corrective action is being taken and the date of the next planned test. Where online systems are in use this reporting also applies to any penetration testing undertaken;

- Exceptions identified in tests should be subject to a remedial action plan, with timelines and responsibilities identified and evidence that the action plan has been/is being fulfilled;

- The results of the testing should be communicated to the governing body in accordance with the agreed reporting standard.

Application to TPAs and Accreditation Approach

The accreditation team will randomly select procedures and test results looking for:

- Adherence to procedures during testing;

- Successful reinstatement of the service;

- Evidence of the process for ensuring procedures are maintained and updated as necessary or following testing outcomes;

- Evidence the controls in place for monitoring these are being followed;

- Evidence of the management reporting and escalation route for non-adherence to procedures;

- Where some services are outsourced to a third party, that reporting and control information is supplied by the appointed party at the same level as applies to the delegating party.

- Sharing of the BCP with trustees.

Application to In-House Teams and Accreditation Approach

PASA recognises that the in-house team may be covered by the employer's Business Continuity and Disaster Recovery plan and therefore will take this into account. The accreditation team will look for:

- Adherence to procedures during testing;

- Successful reinstatement of the service;

- Evidence of the process for ensuring procedures are maintained and updated as necessary or following testing outcomes;

- Evidence the controls in place for monitoring these are being followed;

- Evidence of the management reporting and escalation route for non-adherence to procedures;

- Where some services are outsourced to a third party, that reporting and control information is supplied by the appointed party at the same level as applies to the delegating party.

Application to Master Trusts and Accreditation Approach

The accreditation team will randomly select procedures and test results from both the administrator (in-house or external third party) and the Principal looking for:

- Adherence to procedures during testing;

- Successful reinstatement of the service;

- Evidence of the process for ensuring procedures are maintained and updated as necessary or following testing outcomes;

- Evidence the controls in place for monitoring these are being followed;

- Evidence of the management reporting and escalation route for non-adherence to procedures;

- Where some services are outsourced to a third party, that reporting and control information is supplied by the appointed party at the same level as applies to the delegating party.

Application to Annuity Providers and Accreditation Approach

The accreditation team will randomly select procedures and test results from both the administrator (in-house or external third party) and the Principal looking for:

- Adherence to procedures during testing;

- Successful reinstatement of the service;

- Evidence of the process for ensuring procedures are maintained and updated as necessary or following testing outcomes;

- Evidence the controls in place for monitoring these are being followed;

- Evidence of the management reporting and escalation route for non-adherence to procedures;

- Where some services are outsourced to a third party, that reporting and control information is supplied by the appointed party at the same level as applies to the delegating party.

Timelines

PASA expects these Business Continuity and Disaster Recovery procedures to be in place for all organisations seeking accreditation.