Standards – Business Continuity/Disaster Recovery

Sept 2024

PASA

Standard:

3.2 Business Continuity/Disaster Recovery

PASA expects appointed administrators to have fully documented, tested and robust business continuity and disaster recovery plans in place in respect of their operation (including consideration of cyber incidents).

Rationale:

Business continuity and disaster recovery plans which are documented and regularly tested provide assurance administration services can continue to be delivered and remain available should a disruptive incident occur (including a cyber incident). Business continuity and disaster recovery plans should include measures to prevent and manage a cybercrime incident and should meet any applicable laws and regulations. The FCA, the ICO, the NCSC and TPR have all issued guidance and commentary indicating their expectations around cyber security. Specific Guidance on cybercrime and fraud is published by PASA separately.

Business continuity and disaster recovery plans ensure scheme data and records are secured, protected from destruction and continue to be available to enable services to be provided. This should include instances where scheme data and records are subject to cybercrime. Any business continuity plan or cybercrime incident plan should include steps to mitigate any damage and ensure appropriate training for all staff occurs. The plan should also include steps to remediate an attack and assist Data Controllers to comply with their legal obligations to report data breaches.

Where administration services are provided (in whole or in part) by a third party then it's expected business continuity and disaster recovery plans (including consideration of cybercrime) are in place for both the appointee and the delegating body.

General Principles:

Having documented procedures which are tried and tested is necessary to ensure continuity and consistency of service should a business continuity, or disaster recovery (including cybercrime) incident arise.

They help to ensure all the necessary steps are taken to provide ongoing service in the event of an incident, ensuring the staff and Governing Bodies[1] are aware of the situation.

Where the Governing Body or appointed administrator is applying for PASA accreditation, both the appointee and delegating body, or administrator, need to be able to demonstrate:

- their processes are clearly defined and maintained
- their processes are tested regularly
- they're taking corrective action where procedures fail to work

It's expected the audit of the business continuity and disaster recovery plan (including cybercrime) 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 investing any DC contributions, pensioner payments, retirement processing and bereavement services are recovered within 24 hours
  - In the event of a cybercrime attack, key functions (such as those referred to above) should be restored as soon as practical
  - Critical data isn't lost or permanently damaged
  - Governing Bodies can be confident services will continue to be provided and they'll be supported in meeting their legal obligations to work with the relevant authorities as required

Measures/Evidence:

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

[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

    - 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
    - Remote operation is available if required, or 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
    - In the event of a cybercrime incident, key functions are restored quickly in line with the plans set out
- 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 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
- The business continuity plan should include measures to identify, mitigate and recover from a cyber incident, including the following:
    - Demonstrate an understanding of the risk you are exposed to
    - Ensure controls are in place to meet the risks you have identified (this might be evidenced by a formal certification such as cyber essentials or alignment to a widely recognised, risk-based Cyber Security or Information Security standard or framework (such as ISO27001, NIST or ISF)
    - How to identify a cyber incident is occurring and actions to take on discovery
    - A plan to recover from the attack and restore normal services
- A separate cyber incident response plan which supplements the business continuity and disaster recovery plan would also meet this requirement
- Conduct an annual review of vulnerability to cybercrime with an action plan prepared to ensure any gaps identified are resolved
- Given the inherent risks of a cyber incident, the appointed administrator should demonstrate staff are regularly advised of potential risks and understand what action to take if they become aware of a cyber incident
- It may also be appropriate to take input from external specialists, for example in using penetration testing, considering cyber insurance or consulting other experts regularly

Accreditation Approach:

For TPAs, in-house teams, Master Trusts and Annuity Providers:

- **The Accreditation team will randomly select procedures and test results looking for:**
  - **Documentation of the procedures (including regular review of cybercrime developments)**
  - **Evidence the risks of cybercrime have been assessed**
  - **Awareness of cyber risks amongst staff as appropriate**
  - **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, reporting and control information is supplied by the appointed party at the same level as applies to the delegating party**

In addition, for TPAs:

- **Sharing of the BCP with trustees**

For in house teams, PASA recognises the team may be covered by the employer's business continuity and disaster recovery plan and therefore will take this into account. For Master Trusts and Annuity Providers, the Accreditation team will randomly select procedures and test results from both the appointed administrator (in-house or external third party) and the Principal.

Timelines:

PASA expects these business continuity and disaster recovery procedures (including cybercrime) to be in place for all organisations seeking accreditation.

PASA

assess | aspire | achieve

Get in touch:

info@pasa-uk.com

www.pasa-uk.com

PASA is a Community Interest Company and our full name is Pensions Administration Standards Association CIC.

Company number: 6597097