Balancing and Settlement Code

BSC PROCEDURE

BSCP537 APPENDIX 3

QUALIFICATION PROCESS FOR SVA PARTIES, SVA PARTY AGENTS AND CVA MOAs

APPENDIX 3

GUIDANCE NOTES ON COMPLETING THE SELF ASSESSMENT DOCUMENT (SAD)

Version 3.0

Date: 28 February 2019

BSC PROCEDURE 537 Appendix 3

relating to

Guidance Notes on completing the Self Assessment Document (SAD)

1. Reference is made to the Balancing and Settlement Code for the Electricity Industry in Great Britain and, in particular, to the definition of "BSC Procedure".

2. This is BSC Procedure 537 Appendix 3, Version 3.0 relating to the Guidance Notes on completing the Self Assessment Document (SAD).

3. This BSC Appendix is effective from 28 February 2019.

4. This BSC Procedure Appendix has been approved by the BSC Panel.

AMENDMENT RECORD

Version	Date	Description of Changes	Changes Included	Mods/ Panel/ Committee Refs
1.0	23/07/07	P197 Release	P197	Panel 115/04
2.0	10/09/07	P207 Release	P207	Panel 127/04
3.0	28/02/19	28 February 2019 Release	P344	Panel 284C/01

GUIDANCE NOTES ON COMPLETION OF THE SAD

CONTENTS

Whilst guidance has been provided for each question in the SAD, there are a number of areas where further clarification may be required to ensure that responses are complete. The objective of this guidance note is to provide additional information on some of the more complex sections covered by the SAD. Should further guidance still be required, the Applicant should contact ELEXON to discuss further. This guidance is not intended to be part of the SAD nor is it an exhaustive list. Not all of the items identified will necessarily be applicable to, or cover, the circumstances of every Applicant.

1. Disaster Recovery planning and testing to ensure business continuity

Background information:

Qualified Persons do not work in isolation, but are highly dependent on other Parties and Party Agents in the electricity market to operate effectively. The existence of reasonable, comprehensive, written and fully tested disaster recovery plans is therefore essential to ensure the Trading Arrangements continue to operate effectively, as a whole, despite problems encountered by an individual Qualified Person. Consequently, services must meet the basic criteria of a reasonable, documented disaster recovery plan which has been fully tested.

Disaster recovery planning is not restricted simply to IT systems and hardware but extends to the necessary source documentation and surrounding procedures including telecommunications. For example, if Meter reading information is recorded and/or processed using a paper based system, then the disaster recovery plan should ensure that this information is accessible and that processing can continue in an emergency situation should this occur.

As part of the disaster recovery planning process, each Qualified Person will normally define what constitutes an emergency (disaster) situation dependent upon its own particular circumstances. Normal practice would be to analyse different types of emergency situation that could occur and to categorise these into different grades of emergency depending on severity. For example, failure of a computer disk may be an emergency situation which invokes a certain set of emergency procedures but would not be severe enough to invoke those procedures which require evacuation to a back-up computer facility. Similarly, what might constitute a disaster situation for one organisation may not constitute one for another organisation. Using the example of a computer disk failure, an organisation operating a large computer system would normally have the facilities to call an engineer to replace the disk unit and recover the information held on that disk. In this case the problem may be considered an exception condition rather than an emergency. However, for an organisation operating a single PC, a computer disk failure may well constitute an emergency situation (disaster) as the expertise to replace the disk unit and recover the lost information may not be readily available. The disaster recovery plan should not just consider IT risks but also environmental. For example, if there were to be a power failure, the water supply was switched off, or access to premises was denied.

Disaster recovery plans are perhaps best described as a series of pre-agreed procedures giving authority to a “disaster recovery team” to act to recover services in an emergency.

Completing the SAD

The following provides a cross reference between the Disaster Recovery questions covered in each section of the SAD and provides further guidance as to the areas that should be covered by the response. In summary:

- Disaster recovery and business continuity planning and testing is covered in questions **4.2.1, to 4.2.4 and 4.3.1 to 4.3.4** of the SAD.
- Testing of the disaster recovery plan is also referred to in **Section 3 Testing** but the Applicant is instructed to simply provide a cross reference to the questions in Section 4.

Question Number	Question	Further Guidance
4.1.3	What plans does your organisation have in place to address disaster recovery of all key data, systems and processes and how will you ensure business continuity considering the people, knowledge, resources and office space required to operate the service? (complex system question)	Effective disaster recovery plans must cover all critical components of the business processes which comprise the service you are providing. These must be based on your risk analysis of your requirements and assumptions made in writing your plan. You should explain how all these critical aspects have been addressed. Furthermore, you will need to show that you have omitted nothing essential from your plans. You should also provide a brief description of your disaster recovery facilities, including third party providers, arrangements for alternative office accommodation, re-routing of telecommunication links etc. The following areas should be considered in the development and documentation of a comprehensive disaster recovery plan: 1. Identification and documentation of all applicable business processes and supporting applications. 2. Identification and analysis of all threats to critical business processes and supporting facilities covering the service. These may include, but are not limited to bomb threats, fire, flood, power/utility outage, lottery wins by office syndicates, hurricanes etc. 3. Dependencies on internal and external business processes and other business support services (e.g. premises, hardware support, telecommunications support, systems support etc.) should be identified and documented for the service. These dependencies should be communicated to the relevant parties. 4 Identification of minimum recovery resources (such as critical personnel, hardware, software, workspace requirements, telecommunications etc.) and alternate facilities for the systems and supporting processes. There are plans to ensure that these resources and facilities are available to enable appropriate restoration of the service within required recovery timeframes. Controls over access to alternate facilities are established and properly documented to prevent unauthorised access during the operation of these facilities. 5. Development and documentation of recovery strategies for the resumption of critical business

Question Number	Question	Further Guidance
		support services (e.g. systems support, telecommunications support) and IT facilities. 6. Back up and restoration procedures for all applications and data necessary to support the service have been developed, documented and tested. 7. Recovery procedures are documented in detail, including: a. Notification of teams and users; b. Procedures to invoke the alternate site and relevant alternate site contacts; c. Operation of applications systems; d. Communications and systems software at alternate site; e. Testing of restored operations; f. Manual and/or interim processing procedures should be developed and documented to meet stated recovery time objectives wherever recovery time shortfalls exist between the restoration of appropriate IT facilities and the service requirements (e.g. the business unit needs to process Meter reads but the communications links to make such Meter reads are unavailable for several days); and g. Procedures are in place and documented for the recovery of incremental data lost between the last backup and the time of the disaster; and h. Vital records are stored off site; 8. Appropriate teams are established for the recovery of the service. The functions of these teams including responsibility for their overall management have been defined and documented. 9. A disaster recovery awareness programme has been developed aimed at communicating details of the plan to all staff, business units and other associates (where deemed appropriate).

Question Number	Question	Further Guidance
		10. The plan has been reviewed and approved by senior management. You should also provide information on the periods of time that each aspect of your service could be out of operation (outage) under your plans and demonstrate that these periods of outage are consistent with the service level standards as set out in the relevant BSCPs and PSLs. Examples of evidence that you would be expected to be able to provide to illustrate the controls and procedures that you have in place would be: • Formalised final version of your Disaster Recovery Plan (a draft is not acceptable). • Evidence of senior management sign-off. • Formal, documented, up to date procedures. • Formal, documented, evidence of roles and responsibilities. • Where a third party contractor is used for disaster recovery – evidence of a formal disaster recovery contract services being in place.
4.1.4	How have you tested your disaster recovery plans prior to go-live (or for a re-Qualification within the 12 month period prior to your re-Qualification application)?	This response should address the extent of the disaster recovery testing that you have already undertaken in order to support your Application. The response should demonstrate how your testing has demonstrated that the disaster recovery plans which you have in place will ensure that there will be no disruption to the day to day operation of the BSC Systems and that no other Party or Party Agent will be adversely impacted. Tests should cover both IT and operational aspects of the service, including: 1. Notification procedures and lines of communication; 2. Compatibility of alternate IT and workspace facilities (e.g. equipment, telecommunications); 3. Recovery of critical applications systems at alternate site; 4. Interim and manual processing procedures; and

Question Number	Question	Further Guidance
		5. Recovery of the systems. Examples of evidence that you would be expected to be able to provide to illustrate the controls and procedures that you have in place would be: • Disaster Recovery plan test plan • Disaster Recovery plan test results (satisfactory test results would be expected) results showing significant issues in recovery would indicate that the Disaster Recovery plan in place was not adequate and therefore did not support that the service had adequate recovery plans in place to mitigate risk to the service and all other participants operating in the market. • Disaster Recovery plan test result sign off by senior management
4.1.5	How will you ensure that your disaster recovery plans continue to be tested on an ongoing basis?	To be reasonably certain that your disaster recovery plan will work it must be tested and updated regularly. The plan should be tested fully at least once in a 12 month period, but often aspects of the plan are tested more frequently. Additional testing of the plan will need to be undertaken if significant changes have been made which would impact the Disaster Recovery plan. Good practice states that when Disaster Recovery plans are updated either due to organisational, location, third party disaster recovery services provider or IT operational change a full test should be undertaken to ensure that the updated plan will function as required. These changes may arise, for example, from the relocation of computer systems, migration to new hardware and software environments or as a result of significant modifications to data volumes being processed. Test planning, testing and post test evaluation procedures (this should include the establishment of frequency and trigger criteria for updating the plan(s)), formalised test schedules, procedures to ensure adequate post test evaluation is undertaken e.g. test results should be compared against predetermined test criteria and test objectives to determine the degree of success of the test, written evaluations of the test process, results and outstanding issues should be submitted by the test team

Question Number	Question	Further Guidance
		leaders and discussed with senior management, rectification procedures to ensure all testing issues are resolved, the plan updated (where applicable) and re-testing of the plan is undertaken. Examples of evidence expected to be in place to illustrate your controls and procedures in place would be: • Formalised final version of your Disaster Recovery schedule (a draft is not acceptable). • Evidence of senior management sign-off. • Schedule of tests to be performed / project plan detailing commitment to test every 12 months. • Where a third party contractor is used for disaster recovery – evidence of a formal disaster recovery service contract being in place which includes the facility to test on an ongoing basis.
4.1.12	How have you ensured that appropriate data back-up, archive and restoration arrangements have been established and operate effectively?	This question is not referring to the specific Disaster Recovery plans you have in place (4.2.1) but to daily operational back-up processes that should be being performed. Therefore submission of your Disaster Recovery plan as evidence to support a response to this question would not be sufficient. The aim of this question is to ascertain that there are appropriate operational day-to-day back-up procedures in place and that this can be demonstrated as working effectively. Examples of evidence expected to be in place to illustrate your controls and procedures in place would be: • Back-up schedule / IT Operations task schedule. • Completion of IT operations task list on a regular basis. • Documented back-up procedures in place, e.g. in IT Operations User Manual. In addition, good practice recommends regular testing of back-up tapes to ensure that back-up tapes are functioning as expected. This is to mitigate the risk that back-up tape failures would only be

Question Number	Question	Further Guidance
		recognised upon attempted recovery in the event of a disaster. Examples of evidence expected to be in place to illustrate your controls and procedures in place would be: • Documented back-up tape testing procedures e.g. in IT Operations User Manual. • Evidence of regular back-up tape testing (where applicable). It may be that back-up tape checks are automatically performed by some form of monitoring tool, eg. Redbox, which can notify the operatives of any failure in back-up. • Adequate security over back-up tapes.
4.2.2	What plans does your organisation have in place to ensure that the service can continue to operate in the event of a Disaster?(simple system question)	Whilst it is not expected that a service with a simple system would have as complex a Disaster Recovery plan as a service with complex systems, the requirement to have an appropriate level of Disaster Recovery cover still applies albeit of a less complex nature. A service with simple systems still needs to be able to demonstrate the thought processes that have gone into Disaster Recovery planning and that the Applicant has implemented adequate documented procedures and has adequate controls in place to mitigate against loss of service in the event of a disaster. Consideration should be given to the same points (1-7) as noted in the guidance in 4.2.1 above. However, this should be in the context of the simple systems in use. Additional consideration should be given to: • All paper based information. • Up to date, off-site storage of all paper based data required to operate your service and meet minimum audit trail requirements as set out in the PSLs. Illustrative example: If your system was a simple system based on: • The utilisation of one key spreadsheet only.

Question Number	Question	Further Guidance
		• Formal records being faxed from other services. Adequate Disaster Recovery may constitute having an up to date copy of the key spreadsheet stored on disk securely off site. In addition, where paper records are your key source of information a duplicate copy of these would also be expected to be held somewhere other than your key operating location. This could involve holding a duplicate set of paper copies securely offsite, or scanning all records onto CD and holding a copy of the CD in a secure offsite location. Consideration should also be given to your ability to operate from (and have access to) an alternate location. For example if your operations primarily require the use of a telephone, PC and fax machine, consideration should be given to where these services can be obtained and how quickly. The primary objective is to demonstrate that you can recover your service (which in the case of a simple system should be much simpler than a complex system with multiple IT requirements) within sufficient time, so as not to impact on Settlement. Consideration should be given to the recovery of the service within periods of time that meet the requirements of the BSCPs and PSLs. Examples of evidence expected to be in place to illustrate your controls and procedures in place would be: • Formalised final version of your Disaster Recovery plan (a draft is not acceptable). • Evidence of senior management sign-off. • Formal, documented, up to date procedures. • Formal, documented evidence of roles and responsibilities. • Where a third party contractor is used for disaster recovery – evidence of a formal disaster recovery services contract being in place. **Testing of your Disaster Recovery plans** The methods of testing your Disaster Recovery plan may vary depending on the structure and key components of the simple system in place. A test of the illustrated system above may constitute

Question Number	Question	Further Guidance
		relocation to another office / building and using the back-up discs of the key spreadsheet and data flow records to demonstrate it is possible to continue operation. If the telephone and fax are your key means of communicating with other parties, then it would be key to demonstrate that you not only had all up to date contact details for internal staff in the Disaster Recovery plan, but also up to date contact details for all relevant external parties, so that you can contact them and provide them with your temporary alternate telephone and fax numbers to ensure that they can continue to communicate with you as required. **Ongoing Testing** In terms of testing a simple Disaster Recovery plan – the requirement still stipulates that this should be every 12 months. Where changes have occurred, you should be ensuring that these are incorporated in an updated Disaster Recovery plan and tested to ensure that the plan still operates satisfactorily.