BCDR Testing

An overview of the approach to testing and customer communication

Version: 0.2
Date: November 2024
Author: BCDR

Document control heading

Revision history

Revision date	Summary of changes	Changes marked	Version number
July 2024	Draft document, 1st Version	No	V0.1
November 2024	Minor clarification edits from initial feedback	No	V0.2

Reviews

Name	Title / Responsibility	Release Date	Version number
BCDR Team	BCDR Testing	July 2024	V0.1
BCDR Team	BCDR Testing	November 2025	V0.2

Approvals

Name	Title / Responsibility	Release Date	Version number
Bilal Ali	Head of Service Management	July 2024	V0.1
Gareth Swift	BCDR Testing Manager	November 2024	V0.2

Table of Contents

1.   Introduction

1.   Business Continuity Disaster Recovery (BCDR) is a vital part of DCC services that ensures resilience to unforeseen outages which ensures services can continue to be provided with as little disruption for DCC customers and consumers as possible.

2.   In addition, the Smart Energy Code (SEC) requires that DCC has in place BCDR procedures and to test those procedures. Testing often results in downtime where the Services, or more often a subset of them, are unavailable for the duration of the test and so there can be an impact to users. Over time DCC has changed the approach to BCDR Testing in response to User feedback where those changes have been targeted at reducing the impact on customers.

3.   BCDR Testing is a key part of ensuring and proving DCC System resilience so that the services can continue to be provided in the event of an unplanned outage or disaster.

4.   The content of this document is centred on the approach to BCDR testing on live, production and disaster recovery environments. Alternative methods of testing and exercising methods are discussed for the purposes of comparison and substitution where a Live Exercise may not be the appropriate approach.

2.   Background

5.   The most important purpose of completing BCDR Tests is to prove system resilience and that services to DCC customers can continue or be recovered in a timely manner in the event of an unplanned outage. There are also regulatory requirements for DCC to consider in completing testing.

6.   Smart Energy Code (SEC) H10.9 requires DCC to have BCDR Procedures in place to ensure that in the event of a disaster there is no significant disruption to Services and that Services can be restored as soon as possible.

7.   SEC H10.11 places an obligation on DCC to periodically test, at least annually, the BCDR arrangements in order to assess whether they remain suitable for achieving the objectives set out in SEC H10.9.

8.   DCC is required to comply with, and be certified for, ISO22301:2019 the international standard for Business Continuity Management Systems which provides a level of assurance that DCC is compliant with industry and best practise requirements. As part of ISO 22301, clause 8.5 covers how a BCDR testing and exercising programme is a key component of maintaining the standard and demonstrating best practice.

9.   SEC H10 requires that DCC consult with Parties and SEC Panel before completing any BCDR Testing and to provide Parties with 60 working days' notice of any test.

10.   BCDR Testing results in downtime of DCC services, and DCC is aware of the need to keep downtime to a minimum so as to reduce service disruption for customers. Overall downtime can be impacted by other activities such as Planned and Unplanned Maintenance.

3.   DCC Resilience

3.1.   DCC Network Complexity and Capability

11.   DCC's network is provided by multiple Service Providers and has been designed for resilience, comprised of individual, inter-operable, geographically separated solutions to isolate the service impact of any failures or downtime.

12. Each individual component solution has the capability to respond to faults with localised redundancy within its primary, Production environment, e.g. paired network devices, to provide service continuity.

13. Additionally, each component solution can respond to a major disaster within its primary infrastructure, by moving all its services to a secondary instance of Production.

14. BCDR testing is focused on proving the capability of each component solution to move services to its secondary environment, whilst maintaining interoperability across the network.

15. To minimise the impact of disruption, BCDR testing is usually conducted to avoid the colder winter months, outside normal office hours, where the volume of critical services on DCC systems is at its lowest, and the procedures invoked are designed to protect critical data.

3.2. Benefits of BCDR Testing

16. With individual component technologies evolving and changing, regular BCDR testing on the 'live' environments provides confidence that a service can be restored within acceptable timeframes, minimising potential disruption across the ecosystem should a real world disaster occur.

17. Ultimately, BCDR testing provides assurance and mitigation that the risk of disruption is being effectively controlled across the DCC network in the event of an unplanned outage.

18. Other benefits of testing include:

- Validation that secondary infrastructure is maintained in line with primary infrastructure and in a ready state.

- Development of the competence and skill required to respond to incidents or disasters effectively and efficiently and learn from unexpected scenarios so that improvements to the process and planning can be made.

- Identification of improvements to BCDR plans, runbooks, and recovery solutions.

- Capture of learnings and knowledge for future reference and adaptation e.g. in a different failure scenario.

- Insight to system behaviours and alerts so that these are known and expected ahead of an incident.

- A greater understanding of how interrelated response plans should function alongside each other in a larger scale disruptive incident or crisis

- Supports continued ISO22301 and ISO27001 certification and is aligned with the BCI Good Practice Guidelines.

3.3. Disadvantages of BCDR Testing

19. Most of the DCC's network solutions are deployed in an Active/Standby configuration, requiring service downtime during testing, impacting multiple service users and service providers.

20. To manage risk and protect data, testing is often carried out gracefully[1], but a graceful failover is not always fully representative of an invocation or disaster and can also extend the time required from outage windows.

21. Preparation, governance and execution of live tests on Production environments is time and resource intensive. If service is not recovered at the end of testing, incident management will consume further time and resource.

22. Service disruption exceeding RTOs is unacceptable to DCC and its customers, may harm end users and harms the reputation of smart metering.

23. Not all parties can support testing outside normal working hours, leading to a delay in the identification of post-test issues.

24. Absence of Pre-Production environments to simulate testing, introduces unpredictability to every test due to the rate or volume of change of solutions in the period between tests.

25. Testing can challenge customers own change management and DR testing plans.

26. Potential for loss of knowledge and experience in between tests, e.g. a key SME leaves the service provider.

27. If testing does not go to plan, confidence in the resilience of the solution is reduced and testing failover may not be trusted as a robust incident response until retested.

## 3.4. BCDR Testing Constraints and Restrictions

28. With no SEC requirement for Pre-Production environments testing opportunities are limited to live Disaster Recovery testing on Production environments, or paper-based desktop exercises.

29. DCC work to reduce the impact of testing and SEC obligations in respect of maximum tolerance to Disruption, Recovery Time Objectives and Recovery Point Objectives ensure that outage windows are kept to a minimum.

30. The degree of inter-dependency between solutions requires a co-ordinated approach and forward planning between multiple solution Service Providers to agree an annual schedule.

31. To support Customers the annual schedule is planned to avoid the winter months, quarterly tariff events and major change and release activities.

32. Any BCDR Test must be consulted on by DCC and customers provided with 60 working days notification. DCC chooses to complete an annual BCDR testing schedule and issue a single consultation to cover the full 12-month schedule.

33. Where amendments are required DCC will aim to consult and provide the 60 working day notice period. Where that cannot happen as much notice as is possible will be provided and DCC will consider the impact of a shorter notice period before scheduling the test.

34. Where additional testing is agreed to as part of a new services go Live Service Criteria DCC will consult with customers and issue the required 60 working days notice.

35. A planned BCDR test will not proceed if, during Planning (see below), a solution review and risk assessment concludes that proceeding is outside of DCC Operations and Security risk appetite.

---

[1] A graceful failover requires that both primary and secondary infrastructure are confirmed as synchronised prior to failover, before service traffic or processing is stopped, and all systems brought up online in the secondary instance or location. Service traffic or processing will recommence as soon as all SMEs have completed the agreed system health checks. If there are no processing errors, a formal return to service is communicated.

4. BCDR Testing Approach

4.1. Planning and Approval

36. The planning cycle for each component solution test commences eight to twelve weeks in advance of an individual test date, in line with the BCDR Annual Testing Schedule.
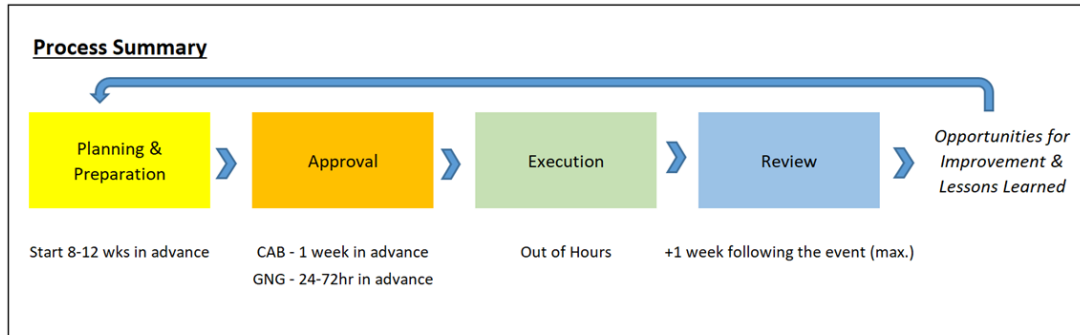
37. A standard approach is taken to planning all BCDR tests, including but not limited to:

- Engagement of all Service Providers impacted, or required to support, the BCDR test in weekly planning meetings and during the actual test event on bridge calls.

- Engagement of a multi-disciplined DCC team across Operations, CTO and Security in planning and execution.

- Requests for voluntary participation from DCC Users in conducting health checks post-exercise.

- A full solution review and risk assessment for the period since the last BCDR Test based on:

  - Service impacts.

  - Incidents.

  - Problems (especially where there is no known root cause).

  - Changes.

  - Learnings and performance from the last BCDR test.

  - Service Provider performance.

  - Other environmental impacts e.g. material changes in volumes.

- Desktop reviews of the BCDR plan, test plan and runbook procedures to ensure that the target Recovery Time and Recovery Point Objectives are achievable, and that testing will be completed within the agreed Outage Window.

- Development and execution of checklists for critical pre and post-test activities such as health-checks.

- Delivery of Communications to ensure that DCC Users are aware of the test date, outage window and services impacts, with the opportunity to raise queries in advance.

- DCC Problem Management raise a proactive Problem record for each BCDR test event to ensure that issues and lessons learned are captured and tracked to conclusion.

- ▪ Approval from the DCC Change Approval Board (subject to DCC Senior Leadership Team final approval).

- ▪ Final approval from the DCC Senior Leadership Team (SLT), 24-72 hours prior to the test date, taking into account the risk assessment outcomes, weather warnings and confirmation that the testing documentation and resource is in place.

- ▪ A formal communication will be sent from DCC Service Desk to confirm the decision to proceed or stand down.

4.2. Execution

38. To minimise disruption, BCDR testing usually occurs at the weekend or overnight, when volumes of critical service requests are typically at their lowest. Refer to Appendix 2 for information on current volumes for installations.

39. There is a final Go-No Go decision prior to the start of the Outage Window, and the decision to proceed with the test will be dependent on the results from pre-test checks, latest weather warnings, resource availability and wider network health. A formal communication will be sent from DCC Service Desk to confirm the decision to proceed of stand down.

40. Evidence of the implementation of the BCDR test runbook and procedures will be captured, including any unexpected behaviour, delays or issues for inclusion in the final BCDR Test Report.

41. Post-test checks are completed by all impacted service providers and DCC Operations and Security personnel and if all health-checks return the expected response, formal approval is given for the return to service communications to be distributed by DCC Service Desk.

4.3. Review and Reporting

42. Evidence of the execution of the testing procedures is captured by the Service Provider as agreed in each test runbook.

43. Service Providers are required to submit a Test Report to provide an assessment of the test outcomes against test objectives and identify any learnings to be carried forward. The Test Report is available for DCC's review within 20 working days of the BCDR test completion date.

44. DCC's Technical Operations Centre will provide an event report to show the actual impact of testing on critical service requests for internal review.

45. If there is an incident following, or because of a BCDR test, the incident will be managed in accordance with DCC's Incident Management, Major Incident Management and Problem Management procedures.

- DCC BCDR will report the outcome of each test and provide an annual summary of BCDR testing outcomes to the SEC Panel.

4.4. Testing of New Services Pre and Post Go Live

46. New Services and solutions are resilience tested before go-live, with BCDR test outcomes included in the Live Service Criteria for final approval to transition to Production.

47. BCDR testing on new Services and solutions once they are in Production, is often agreed to be conducted within three months of go live, subject to consultation and a 60-day notice period, and standard planning and execution processes, as outlined.

48. BCDR testing of new Services and solutions will form part of the Annual Outage schedule once the first Production test has completed and met defined testing objectives.

5. Future Considerations and Opportunities

5.1. Alternative Methods of Testing or Proving Resilience

- Where a live test on Production environments is assessed as outside of DCC's risk appetite, or resilience can be proven via other means, alternative methods of testing and exercising will be considered. Once controls or mitigating actions have been implemented live tests will be considered.

49. The decision to select an alternative method of testing in place of an annual, live BCDR event will be made on a solution-by-solution basis.

50. Alternatives are:

- **Desktop walkthrough of BCDR Plans and disaster recovery (DR) runbooks**. This is already conducted as part of the planning activity prior to any BCDR test and would be the minimum requirement in respect of testing.

- **Desktop scenario exercises**. As a follow on from the desktop walkthrough of BCDR Plans and DR runbooks, it is beneficial to run a scenario exercise to introduce variety and breadth to testing. A scenario exercise has the potential to engage a wider audience in preparing to respond to disruption, without impacting service.

- **Planned maintenance activities** i.e., where a solution is failed over and back to implement a change, there should be no requirement to plan towards a standalone BCDR test. Evidence of capability can be captured during the maintenance window and reported to DCC. This method is already being adopted with Service Providers.

- **Live incidents requiring a failover of a solution**. If successful, a live invocation may replace the contractual requirement to complete an annual BCDR test.

- **Cloud environment Fault-Injection service (AWS) and Chaos Laboratory (Azure) exercises, or cloud provider documented assurance**. These can be used to prove cloud solution resilience or assurance, especially for availability zone resilience or cloud-managed services.

- **Pre-Production environment BCDR testing**. Pre-Production is not currently available for solutions within the DCC network.

5.2. Assessing the need for live BCDR testing in Production

51. In addition to conducting solution reviews and risk assessments there are other factors which will influence the design of an annual BCDR test:

- **Outcomes from the last BCDR test or invocation**, e.g. a successful outcome and low volume of change may mean that an alternative method to live testing can be considered to minimise service impact and deferral of a live test to the next annual cycle.

- **Solution design improvements** provide opportunities conduct testing as part of the implementation programme, or as part of business-as-usual planned maintenance.

- **Technology constraints** requiring an alternative approach to live testing.

- **ISO22301:2019** supports testing and exercising over time to ensure that solutions are tested at both '*planned intervals and when there are significant changes*'.

- **Consolidated testing** opportunities are identified, either for complementary or non-conflicting solutions, requiring a single outage window, rather than multiple windows.

6. Customer engagement with Planning

52. Customers currently inform DCC of their own planned maintenance or testing and submit queries via email if they have concerns about any conflicts with DCC planned outages.

53. In addition to the annual consultation process for the BCDR Test Schedule and confirmation of the testing schedule at least 60 working days in advance of the fist test, customers are notified monthly, at least 28-days in advance, about the combined outages that will arise from both Planned Maintenance and BCDR testing.

54. Via these advanced, monthly notifications, DCC provides specific information to parties, which will include, but not be limited to:

- Dates and times of the scheduled Outage Windows.

- Services to be impacted, by region and by cohort (where applicable)

- DCC contact details for parties to raise queries to about the testing and impacts.

55. Examples of the current format of communications is supplied in Appendix 1.

56. Customers are actively engaged in the planning of a BCDR test if they are required to make changes, and invited to perform health checks post-test, subject to their availability outside of normal office hours.

6.1. Future Opportunities to Engage DCC Customers

57. Customers provided feedback to DCC in Q1 2024 that improvements in BCDR test communications are required to ensure that all parties understand the service impacts of planned testing. Customers have expressed a particular interest in testing which affects meter installations and prepayment activities.

58. See Appendix 3 for details on the impact of different BCDR tests, including those anticipated to impact customers' ability to install meters.

59. Real world service impact data is being captured and planned improvements to communications will be shared with the SEC and customers at the earliest opportunity in 2024. The current format of relevant communications is supplied in Appendix 1.

7. Continuous Improvement and Review

7.1. Commitment to review

60. DCC strives for continuous improvement and the BCDR Testing approach document will be reviewed at least annually, with input requested from key stakeholders, including those engaged with the annual BCDR Test Schedule consultation process.

61. In addition to the review of the document, DCC will endeavour to make regular requests for parties to ensure that relevant contact details are supplied to DCC for inclusion in all future communications for BCDR testing.

As new DCC network solutions are introduced, DCC will work with Service Providers to ensure that designs and BCDR testing requirements are aligned with the objective of minimising service disruption and planned annual downtime. Where this objective is

challenged, DCC will assess the impact and risk and consult with customers on the BCDR testing approach to be adopted.

8.   Glossary

The capitalised terms in this document are either defined in the SEC or in the table below.

Term	Definition
Active/Standby	When systems are deployed in an active/standby configuration, there are pairs (or identical clusters) of devices and infrastructure deployed within environments, with only one of the pair receiving and processing traffic, while the other remains ready to take over processing if the 'active' one fails.
	There are different forms of 'standby' modes in terms of readiness. Some standby devices or infrastructure will be ready to failover to automatically, whilst others will be identical but require manual intervention to bring into service.
	Planned maintenance must ensure that both Active and Standby infrastructure is kept in alignment.
Live Test	A live test requires that a service provider proves that if the primary infrastructure for a solution is unavailable, the service can be recovered to an alternative location and/or set of infrastructure within agreed recovery targets.
Primary Environment / Primary Infrastructure	The primary environment or infrastructure is usually where service traffic is routed to and processed, as well as replicated to the secondary environment or secondary infrastructure.
Production Environment	A Production environment is where real-time data is processed and managed to meet operational and service requirements.
Secondary Environment / Secondary infrastructure	A secondary environment or infrastructure is sometimes described as the disaster recovery environment. Unless any components are deployed as 'Active', the secondary environment will be maintained in a standby mode.

9.   Appendices

9.1.   Appendix 1: BCDR Testing Service Impact Communications

9.1.1. Monthly Maintenance and BCDR Communication (extract)

Below is an extract from the 'DCC Monthly Maintenance and BCDR Communication' that is issued by DCC Service Centre at least one-month in advance.

Planned BCDR activities (June 2024)	
6th June 2024 20:00 to 7th June 2024 02:00	BT (TSP) BCDR Event – Failover from Production to DR. During the event the following services will be unavailable: For SMETS 2 across all regions, the following services will be unavailable for the times specified: **SMKI Internet Portal & SMKI Portal**
13th June 2024 20:00 to 14th June 2024 02:00	BT (TSP) BCDR Event – Failback from DR to Production. During the event the following services will be unavailable: For SMETS 2 across all regions, the following services will be unavailable for the times specified: **SMKI Internet Portal & SMKI Portal**

If you have any queries regarding this then please email them to: ServiceCentre@SmartDCC.co.uk.

9.1.2. Individual Test Communication (example)

Below is an example of the service impact table that is issued by DCC Service Centre at the start of any planned maintenance or BCDR test.

DCC – Business Continuity Disaster Recover Test: Due to Start

Change Start: 23/09/2023 20:00 – Change End: 24/09/2023 02:00

Key Services – SMETS 2	Current Service Status	Impacted Region
DSP CSS Gateway	Available	UK Wide
Install & Commissions	Available	UK Wide
AD1 Power Outage Alerts	Available	UK Wide
Prepayment	Available	UK Wide
Service Requests Scheduled	Available	UK Wide
On Demand Service requests	Available	UK Wide
Transitional Change of Supply (TCOS)	Available	UK Wide
Enduring Change of Supply (ECOS)	Available	UK Wide
OTA Firmware Updates	Available	UK Wide
SMKI Repository	Available	UK Wide
SMKI Internet Portal	Available	UK Wide
SMKI Portal	Available	UK Wide
Post Code Lookup	Available	UK Wide
Key Services – SMETS 1	**Current Service Status**	**Impacted Cohort**
S1SP Gateway	Unavailable	MOC
Service Requests Scheduled	Unavailable	MOC
On Demand Service Requests	Unavailable	MOC
Prepayment	Unavailable	MOC
Transitional Change of Supply (TCOS)	Unavailable	MOC
Enduring Change of Supply (ECOS)	Unavailable	MOC
OTA Firmware Updates	Unavailable	MOC
Shared Services	**Current Service Status**	**Impact**
DCC Service Management Tool (Remedy)	Available	UK Wide
Comms Hub Diagnostics	Available	UK Wide
SSI/SSMI	Available	UK Wide

9.2. Appendix 2: BCDR Testing Potential Impact - Installations

Below is an illustration of actual meter installations in early 2024 to show typical weekday and weekend volumes.
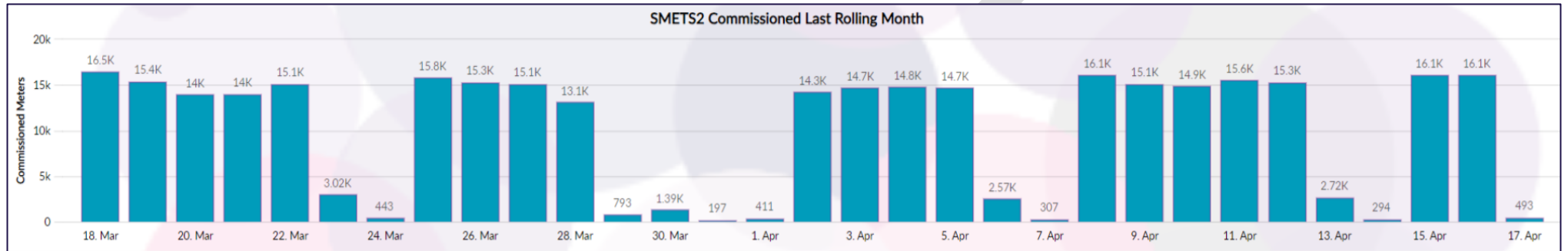
Observations:

- Weekend installs volumes are significantly lower than weekday volumes.

  - Sunday volumes in January/February 2024 averaged c.500 installations (across 8 dates).

  - Sunday dates (volume of installations) in the above chart were impacted by the Easter period:

    - 24th March (443), 31st March (197) – Easter weekend, 7th April (307), 14th April (294).

- Assuming the above installation volumes are representative, the DCC BCDR Annual Testing Schedule 2024/25 has the potential to impact four days' worth of Customers' ability to install meters – equivalent to c2,000 meters. Please see Appendix 3 for an Impact Matrix of individual tests.

9.3. Appendix 3: BCDR Testing Service Impact Matrix

Outage Windows:	2 x Sundays (09:00-15:00)	2 x Sundays (09:00-15:00)	2 x Thursday nights (20:00-02:00)	2 x Sundays (09:00-15:00)	2 x Saturday nights (20:00-02:00)	2 x Sundays (09:00-17:00)	Consolidated Testing on 2 x Sundays (09:00-15:00)		
BCDR Event: Service Impact	**Arqiva (CSP N failover)**	**DXC / Trilliant (Resilience & SFTP failover)**	**BT (SMKI failover)**	**Accenture (ECoS failover)**	**Secure Meters (DR failover)**	**CGI (DSP Total System failover)**	**Capgemini (CP SMETS 1)**	**Capgemini (DCO)**	**CGI (SIE IOC DR test)**
SMETS 2									
DSP CSS Gateway	Available	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
Install and Commissions	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
AD1 Power Outage Alerts	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
Prepayment	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
Scheduled Service Requests	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
On Demand Service Requests	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
Transitional Change of Supply (TCOS)	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
Enduring Change of Supply (ECOS)	Unavailable for North	Available	Available	Unavailable UK Wide	Available	Unavailable UK Wide	Available	Available	Available
OTA Firmware Updates	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
SMKI Repository	Available	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
SMKI Internet Portal	Available	Available	Unavailable UK Wide	Available	Available	Available	Available	Available	Available
SMKI Portal	Available	Available	Unavailable UK Wide	Available	Available	Available	Available	Available	Available
Postcode Lookup	Unavailable for North	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
SMETS 1									
S1SP Gateway	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
Schedule Service Requests	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
On Demand Service Requests	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
Prepayment	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
Transitional Change of Supply (TCOS)	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
Enduring Change of Supply (ECOS)	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
OTA Firmware Updates	Available	Unavailable for FOC	Available	Available	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
Migrations	Available	Unavailable for FOC	Available	Unavailable UK Wide	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for MOC	Unavailable for IOC, MOC and FOC	Unavailable for IOC
SSI/SSMI	Available	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
DCC Service Management Tool (Remedy)	Available	Available	Available	Available	Available	Unavailable UK Wide	Available	Available	Available
Comms Hub Diagnostics	Unavailable for North	Available	Available	Available	Available	Available	Available	Available	Available

Observations & Rationale for BCDR testing at weekends or outside normal office hours:

- Installations:
    - Of the fourteen dates on which testing is planned to occur in 2024/25, only four events will impact DCC's customers' ability to install meters on Sundays.
    - Based on current volumes, as at April 2024 (see Appendix 2), these four events represent c.2,000 meters which could have been installed if testing did not take place. (As a point of reference, installations for a single, typical weekday range 15,000-17,000.)
- Prepayment activities:
    - DCC recognises that BCDR testing is impactful for prepayment activity and avoids testing during the winter months (November to March).
    - 'Non-disconnection hours' are applied to most prepayment meters at weekends, on Bank Holidays and between 18:00-11:00 on weekdays.
    - End users who top-up their prepayment meters during BCDR testing at weekends will not therefore be disconnected and their meter will update as soon as the service is available.

9.4. Appendix 4: ISO22301:2019 (clause 8.5 extract)

8.5 Exercise programme

The organization shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions.

The organization shall conduct exercises and tests that:

a) are consistent with its business continuity objectives;

b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives;

c) develop teamwork, competence, confidence and knowledge for those who have roles to perform in relation to disruptions;

d) taken together over time, validate its business continuity strategies and solutions;

e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements;

f) are reviewed within the context of promoting continual improvement;

g) are performed at planned intervals and when there are significant changes within the organization or the context in which it operates.

The organization shall act on the results of its exercising and testing to implement changes and improvements.