



Test Coverage Document

Future Service Management

Version: 1.4

Author: DCC Test Assurance

Classification: **DCC Confidential – SEC RED**

Document Control

Revision history

Revision date	Summary of changes	Changes marked	Version number
07/11/2024	First Draft Issues for internal reviews	N/A	0.3
13/11/2024	Issued to TAG for review at TAG120 (27/11/24)	N/A	1.0
29/11/2024	Issued Iteration 1 to TAG for ex-committee Baselining	Yes	1.1
03/12/2024	Issued Iteration 1 to TAG121 for Review includes Removal of 2.2.3 Device Manager Functional testing, Revision of 2.2.4 CH manufacturer Functional Testing, Revision of 2.3.1.2 Coverage of FSM & OMS interfaces	Yes	1.2
19/12/2024	Issued to Iteration 2 TAG122 for Review and Approval includes revision of; 2.2.3 Comms Hub Manufacturer Functional Testing, 2.2.5 Logistics Functional Testing	No	1.3
17/02/2024	Iteration 1.4 issued for TAG for approval at TAG123 No change to iteration 1.3		1.4

Reviews

Name	Title / Responsibility	Release Date	Version number
Paul Macintosh	Test Assurance Manager	07/11/2024	1.3
Chris Rowell	Test Governance Manager	07/11/2024	1.0
Tom Burke	Test Governance Lead	03/12/2024	1.3

Table of Contents

1	Introduction.....	4
1.1	Project Background.....	4
1.2	Purpose	4
1.3	Approval and Revision.....	4
2	Scope and Coverage.....	5
2.1	Coverage Traceability Documents.....	5
2.2	Pre-Integration Test.....	9
2.3	Systems Integration Test.....	19
3	Devices For Use in Testing.....	28
3.1	Functional Testing	28
3.2	System Integration Test.....	28
3.3	Regression Testing	29
	SMETS1.....	29
	SMETS2.....	30
4	Security Testing.....	31
5	Risks	31
6	Appendices	33
6.1	Service Now PIT CTD.....	33
6.2	SIT CTD.....	33

1 Introduction

1.1 Project Background

The Future Service Management (FSM) programme is a new IT Service Management capability that replaces the existing DCC Service Management System (DSMS) BMC Remedy.

This is to ensure continuity of a SEC compliant Service Management System to raise Production incidents, as the current DSMS has approached End-of-Life.

FSM Programme will be delivered using ServiceNow, which will have a mix of Commercial-Off-The-Shelf (COTS) deliveries alongside customised deliveries that are catered specifically to the DCC needs.

For the full Project Background, please refer to the LC13b Plan & the Project Brief.

1.2 Purpose

As per SEC Appendix AQ - SEC Variation Testing Approach Document for the FSM Arrangements (the FSM SVTAD), the purpose of the Test Coverage Document is to document:

- the scope (breadth) and coverage (depth) of testing against requirements for the relevant Sub-System (in the case of PIT) and the Modified DCC Total System (in the case of SIT), identified as groupings of functional and non-functional requirements.
- whether the identified requirement shall be tested in PIT or SIT
- where a changed interface is to be tested, all associated or impacted interfaces shall also be tested.
- any perceived risks associated with the scope and coverage of testing and the proposed mitigations.

Similarly, testing should account for all elements of the Modified DCC Total System.

1.3 Approval and Revision

Approval and revision of this document shall be as per Clauses 5.2 (approval) and 5.4 (revision) of the FSM SVTAD.

2 Scope and Coverage

In this section, the scope and coverage of testing undertaken in PIT and SIT shall be explained, including information on the types of testing undertaken.

Section 2.1 provides an explanation of the Coverage Traceability Documents which contain the granular detail of how coverage across the various Testable Requirements is achieved and can be found as appendices to this Test Coverage Document.

Section 2.2 PIT defines the scope of testing for each Sub-System.

Section 2.3 defines the scope of testing undertaken in SIT, where testing of the Modified DCC Total System will occur.

2.1 Coverage Traceability Documents

Coverage Traceability Documents are Excel documents contained in the Appendices of this Test Coverage Document and are the main vehicle through which the following requirements of the FSM TCD (as per the FSM SVTAD) are met:

- “the scope (breadth) and coverage (depth) of testing against requirements for the relevant Service Provider (in the case of PIT) and the Modified DCC Total System (in the case of SIT), identified as groupings of functional and non-functional requirements”;
- “any perceived risks associated with the scope and coverage of testing and the proposed mitigations”.

They form the basis upon which Service Providers will design their testing.

The following sections describe the content and use of the workbooks contained within the Coverage Traceability Document.

2.1.1 Control Sheets

Control sheets provide a view on requirements derived from high level design and procurement documentation, against which the FSM Solution shall be tested. The functional and non-functional high-level requirements contained in the Control Sheets are mapped to Testable Requirements on the Coverage Workbook. Each Control Sheet is validated against the Coverage Workbook to ensure that every high-level requirement is covered in the Coverage Workbook.

The following artefacts have been covered by virtue of Control Sheets for each Sub-System:

Artefact	ServiceNow ITSM	DSP Access Layer	Device Manager	Comms Hub	OMS	Logistics
FSMS & OMS Interface Catalogue	X	X	X	X	X	X
Device Manager High Level Architecture	N/A	N/A	X	N/A	X	X
FSM High Level Architecture Document	X	X	X	X	X	X
Future Service Management RTM V3.1	X	X	X	X	X	X

2.1.2 Coverage Workbook

The Coverage Workbook contains Functional and Non-Functional Testable Requirements which are traced back to high level requirements identified through the various control sheets. The Testable Requirements are written in such a way that they clearly articulate a Testable Requirement, drawn from multiple sources where those sources approach the same requirement in a subtly different way.

The Coverage Workbook indicates the type of testing expected against a particular requirement through the use of Focus Areas and Acceptance Criteria. The fields contained in the Coverage Workbook are summarised below:

Group	Item	Use
Version Control	Major / Minor Change	This column indicates if a Change to the Testable Requirement since the last issued version is “Major” or “Minor”, where: “Major” is a change to any of the following columns: • Status • Reference • Testable Requirement • Focus Area Reference • Focus Area • Acceptance Criteria “Minor” is a change to any other column.
	Comment on Changes	This column contains an audit trail of the reason each change has been made. Where a Testable Requirement has been updated across multiple versions the audit trail shall detail all changes.
	Version Last Updated	The version that a Testable Requirement was last updated, which can be as a consequence of being added, updated or removed.
Testable Requirement	Status	The status of a Testable Requirement, which will be one of “Baseline” or “Removed”.
	Reference	A unique reference assigned to each Testable Requirement
	Category	Groups Testable Requirements at a high level
	Sub-Category	Groups Testable Requirements within a Category into more distinct groups
	Testable Requirement	The requirement to be tested, derived from requirements of artefacts, for example Service Provider’s Low Level Design document or RTM

Group	Item	Use
	Focus Area Reference	A unique reference identifying a particular Focus Area. Each Testable Requirement considered a part of a particular Focus Area will hold the Focus Area Reference for that Focus Area, allowing the Focus Area to be filtered. These can be filtered within the CTD in order to view the complete list of Testable Requirements assigned to a Focus Area
	Focus Area	Describes an area of functionality or grouping of non-functional characteristics which is assigned a common Focus Area Reference.
	Acceptance Criteria	Describes the breadth of testing which is required against all Testable Requirements captured in a specific Focus Area.
Reference Docs	Interface Command	A Reference to one or more Interface Commands drawn from the FSMS & OMS Interface Catalogue, which are covered by the Testable Requirement
	RTM Reference	A Reference to one or more sections of the RTM, which are covered by the Testable Requirement

2.2 Pre-Integration Test

The Pre-Integration Test Phase consists of two Test Stages. These are:

1. Unit Testing – the earliest test stage, where individual components of a Sub-System are tested in the PIT environment
2. System Testing – where the interactions of components within the same Sub-System are tested within the PIT environment

Unit and System testing may be executed in parallel.

2.2.1 ServiceNow DCC Specific (PIT) Functional Testing

The testable requirements of the ServiceNow DCC specific delivery are derived from FSMS & OMS Interface Catalogue as well as business requirements drawn from the RTM.

In this section of the document, the key functional, testable requirements of ServiceNow are drawn out. Following table shows the high-level focus areas of each sub-system. Granular level details are provided in the Coverage Traceability Document. Note that the Acceptance criteria for ServiceNow DCC specific PIT for some Focus areas in the below table are identical, however, presented here for reference.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-19	FSMS interface to Arqiva for the following: • Create Incident from Arqiva • Update Incident from Arqiva • Create/Update from Arqiva • Send Return to Arqiva	• Valid structural variances of the interface command • Post command / response processing (Data Updates, Workflows, Event Logging, and Timestamps) • Exception path conditions including all HTTP Response codes • Retries where applicable
FSM-Func-20	FSMS interface to Arqiva or VMO2 to send the "Update Comms Hub Faults Analysis Report"	• Valid structural variances of the interface command • Post command / response processing (Data Updates, Workflows, Event Logging, and Timestamps) • Exception path conditions including all HTTP Response codes • Retries where applicable
FSM-Func-21	FSMS interface to Cloud Enterprise Data Analytics Repository (CEDAR) to send Data Feed	• Received as per schedule • Data type, formatting and special characters are as expected • Range of data is aligned to the rules per report • Valid data reports are generated. • Reports are produced within acceptable latency.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-24	FSMS interface to Email Server - Send outbound emails from FSMS - Receive inbound emails into FSMS	- Valid structural variances of the interface command - Post command / response processing (Data Updates, Workflows, Event Logging, Timestamps) - Exception path conditions including all HTTP Response codes - Retries where applicable
FSM-Func-25	FSMS interface to SOC to send following requests: "Security Logs – FSMS" "Security Logs – IDP Hub" "Security Logs – Integration Layer" "Security Incidents"	- Valid structural variances of the interface command - Post command / response processing (Data Updates, Workflows, Event Logging, Timestamps) - Exception path conditions including all HTTP Response codes - Retries where applicable
FSM-Func-27	FSMS interface to VMO2 for the following: - Create Incident Request from/to VMO2 - Update Incident Request from/to VMO2 - Create Problem Request from/to VMO2 - Update Problem Request from/to VMO2 - Create Work Order Request from/to VMO2 - Update Work Order Request from/to VMO2 - Create/Update Return request from VMO2 - Send Return to VMO2	- Valid structural variances of the interface command - Post command / response processing (Data Updates, Workflows, Event Logging, Timestamps) - Exception path conditions including all HTTP Response codes - Retries where applicable

2.2.2 ServiceNow Functional Testing

The testable requirements of the ServiceNow functionality are derived from business requirements drawn from the RTM. These testable requirements are not connected via interfaces, however, form part of the core functionality.

In this section of the document, the key functional, testable requirements of ServiceNow are drawn out. Following table shows some examples from different ITSM functionality for each category. Granular level details are provided in the Coverage Traceability Document.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-01	Access Management with a sub-category: "Assign Role Based Permissions in the Future Service Management System"	- An FSM admin user is able to create new RBAC permissions. - An FSM admin user is able to assign a new RBAC permission to a user group or job type that defines the level of access to functionality of the FSM system.
FSM-Func-03	Asset & Configuration Management with a sub-category: "Asset & Configuration Management - Communication Hubs"	- The FSM system begins to track the Comms Hub throughout its lifecycle upon its delivery to the appropriate customer, and all details are viewable within the FSM system. - An FSM user that has permission to return Comms Hubs is able to view all Comms Hubs of all generations as assets. - An FSM user with permission is not able to view Comms Hubs as part of asset management upon their decommissioning. - The FSM system tracks Comms Hubs throughout their lifecycle when they have been refurbished.
FSM-Func-04	Authentication with a sub-category: "Identity Management Service Inactivity Timeout"	- An FSM user is inactive for 15 minutes and is logged out from the FSM system. - An FSM user that attempts to login with an expired session ID is not permitted entry to the FSM system. - An FSM user that reauthenticates themselves after their session is timed out is able to access the FSM system.
FSM-Func-05	Change Management with a sub-category: "Raise Change - Expedited"	- An FSM user with permission is able to raise a new change request and provide all relevant details, before submitting. - An FSM DCC admin user is alerted. - The FSM system starts the SLA and the change is assigned to an appropriate FSM DCC admin user. - An audit log associated to the change request is updated accordingly.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-08	Diagnostics with a sub-category: "Service Availability"	- An FSM user with permission is able to view the DCC System Component status. - An FSM user with permission is able to view a list of all Smart Metering activities and is able to highlight service alerts using RAG status. - An FSM user with permission is able to open service alerts and view their details. - An FSM user with permission is able to raise an incident against a specific component within the 'DCC Components Status' module, and the FSM system suggests the incident type based on the component selected. - An FSM user with permission is able to open service alerts and view a list of the most recent service alerts that have been raised across the DCC Total System."
FSM-Func-09	FSM Admin with a sub-category: "FSM Admin User - Roles and Permissions"	- An FSM DCC admin user is able to view all users, user roles, and RBAC permissions of the FSM system. - Data is able to be extracted for business use. - An FSM DCC admin user is able to make updates to users and their RBAC permissions and an audit log is maintained.
FSM-Func-11	Problem Management with a sub-category: "Search Problem"	- FSM user is able to login to the system successfully. - FSM user is able to search using specific unique identifiers and view a list of all open problems with all relevant details that match the search criteria.
FSM-Func-13	Incidents with a sub-category: "Create Major Incident- User Driven"	- The system should have error handling for mandatory field validation - Dropdown list for incident type should dynamically show available options - Notifications should be sent to Smart DCC automatically upon incident creation - Confirmation email and/or system notification should be sent to the user and relevant parties - SLAs and escalation workflows must be triggered when the major incident is created - Smart DCC must be able to approve or reject the incident, and the system must handle both outcomes appropriately. - An audit log must be maintained for all incidents raised, capturing all user actions and system generated actions (like notifications sent/received/approval received, etc) - Reporting functionality should track the timeline of the major incident from creation to closure
FSM-Func-14	FSM Data with a sub-category: "Manage Data across DCC System - DCC Operational Dashboard"	- FSM user successfully logs into FSM. - FSM user has permission to configure their dashboard against various metrics across the DCC Landscape. - FSM user can edit their dashboard view at any time.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-28	Knowledge Management with a sub-category:: “Create and Publish Knowledge Management Article”	• An FSM user that is a Knowledge Manager is able to create knowledge articles and publish these to the FSM system. • An FSM user that is a Knowledge Manager is able to create knowledge articles and assign them to SMEs for review. • An FSM user that is an SME is able to approve a knowledge article and the Knowledge Manager is notified that the article has been published. • An FSM user that is an SME is able to reject a knowledge article and the Knowledge Manager is notified and is able to amend and resubmit. • An FSM user is able to create a knowledge article request and this can be approved by a Knowledge Manager or an SME for publishing.
FSM-Func-30	Personalised Landing Page with a sub-category: “A Personalised Landing Page Across Interfaces”	• An FSM user, upon logging into the FSM system, is presented with a personal landing page with information on recent tickets raised and other tailored information related to the user (or their party). • An FSM user is able to customise the layout of their personal landing page, and upon submitting the amendments, is presented with this upon logging into the FSM system going forward.
FSM-Func-31	Release Management with a sub-category: “Plan Releases”	• FSM user is able to access the release module of the FSMS. • Release Plan can be created and populated with details in relation to the planning of a release/update to the DCC Total System. • A release is able to be approved. • The Release Plan can be executed.
FSM-Func-32	Reporting with a sub-category: “Age of a Ticket”	• FSM user is able to login to the system successfully. • FSM reports and data can be reported/have SLAs against Business Days (including UK Bank Holidays) and against Calendar Days.
FSM-Func-33	FSM Service Catalogue	• Smart DCC admin user has permission to build and update the Service Catalogue. • Smart DCC admin user builds the Service Catalogue in a customer focussed design. • FSM user has permission to view the Service Catalogue. • FSM user is presented with a Service Catalogue of key business services.
FSM-Func-34	Service Level Management with a sub-category: “Adjudicate Service Level Outcomes and Breaches - View/Close/Pause Tickets”	• The FSM system changes the status/workflow step based on the rules of an SLA, when an SLA has been breached for a ticket. • When a ticket enters one status/workflow step, the ticket enters one SLA period (e.g. five days) and the ticket has five days to be resolved. • A ticket has multiple SLAs across workflows and steps. • A ticket has split SLAs across workflows and steps. • An SLA is paused on a ticket and the SLA remains on hold for the ticket until it is restarted. • An FSM user is able to view the SLA attached to a ticket when opened. • SLAs are reportable.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-35	Service Requests with a sub-category: "Raise Service Requests"	• FSM user is able to login to the system successfully. • FSM user can search for specific service requests. • FSM user logs and submits a service request with all of the necessary information. • Service request is assigned to appropriate FSM user, and user that submitted request is notified
FSM-Func-37	Ticket Management with a sub-category: "View Tickets"	• FSM user is able to login to the system successfully. • FSM user is able to view a list of all open tickets, with all relevant details.

2.2.3 Comms-Hub-Manufacturer Functional Testing

The testable requirements of the ServiceNow are derived from FSMS & OMS Interface Catalogue as well as business requirements drawn from the RTM.

In this section of the document, the key functional, testable requirements of Comms Hub Manufacturer are drawn out. Following table shows the high-level focus area of Comms Hub Manufacturer sub-system. Granular level details are provided in the Coverage Traceability Document.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-26	FSMS interface to Comms Hub Manufacturer for the following: • SendDisposalCertificate - From Comms Hub Manufacturer • Send RMA Details - To Comms Hub Manufacturer • Request exception ORR - From Comms Hub Manufacturer • Update RMA Details- From Comms Hub Manufacturer • Notify CH Delivery - From 3rd Party Logistics • Notify FAR Acceptance - To Comms Hub Manufacturer • Move CH to Forward Logistics - To Comms Hub Manufacturer • Upload R-ASN- From Comms Hub Manufacturer • Accept R-ASN - To Comms Hub Manufacturer • Update Preliminary Fault Assessment - From Comms Hub Manufacturer • Fault Analysis Report (FAR)- From Comms Hub Manufacturer • Notify FAR Action- From Comms Hub Manufacturer • Update Refurbishment Status- From Comms Hub Manufacturer • Notify CH Disposal- From Comms Hub Manufacturer • Share Rfb-ASN -To Toshiba	• All structural variances, including boundary value analysis of data items, Timestamping in UTC • Post command / response processing (Data Updates, Workflows, Event Logging, Timestamping in UTC) • Exception path conditions including all HTTP Response codes • Retries where applicable

2.2.4 DSP Integration Layer Functional Testing

The testable requirements of the ServiceNow are derived from FSMS & OMS Interface Catalogue as well as business requirements drawn from the RTM.

In this section of the document, the key functional, testable requirements of DSP Integration Layer are drawn out. Following table shows the high-level focus area of DSP Integration Layer sub-system. Granular level details are provided in the Coverage Traceability Document.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-23	FSMS interface to DSP Integration Layer for the following: • Read Inventory - Request - To DSP • Device Ownership - Request - To DSP • Device Interested Parties - Request - To DSP • Retrieve Service Audit Trail - Request - To DSP • Coverage Check (Postcode) - Request - To DSP • Coverage Check (District) - Request - To DSP • CSP Comms Hub Database - Request - To DSP • Comms Hub Diagnostics - Request - To DSP • Retrieve Traffic Management Data - Request - To DSP • Retrieve Firmware Distribution Device Data - Request - To DSP • Retrieve Firmware Distribution Data - Request - To DSP • Manage DCC Service User Suspension - Request - To DSP • Manage Corporation - Request - To DSP • Manage SEC Party - Request - To DSP • Manage DCC Service User - Request - To DSP • Manage Manufacturer - Request - To DSP • File Uploads - Request - To DSP on below ○ Manage Quarantine Release ○ Manage Anomaly Detection Parameters ○ Manage Certified Product List ○ Manage Organisation Compromise ○ Manage Anomaly Detection Attributes ○ Manage Meter Point Supplier Lookup ○ Manage Comms Hub Logistics Data • Manage Communications Hub - Request - To DSP • Manage Comms Hub Channel Configuration - Request - To DSP • DSP Component Health Status - Request - To DSP • DUIS Version of the Interested Party - Request - To DSP • All Interested Parties - Request - To DSP • Create Incident - Request - From DSP • Create Comms Hub Returns Record - Request - From DSP • Reset Firmware Distribution Device Data - Request - To DSP • Coverage File Download - Request - To DSP • Manage Device Status - Request - To DSP • FSM Report Request - to DSP • FSM Report Request - Response from DSP • FSM Report - Device Certificate Report	• All structural variances, including boundary value analysis of data items, Timestamping in UTC • Post command / response processing (Data Updates, Workflows, Event Logging, Timestamping in UTC) • Exception path conditions including all HTTP Response codes • Retries where applicable

2.2.5 Logistics Functional Testing

The testable requirements of the Logistics are derived from business requirements drawn from the RTM and associated Interface Specifications.

In this section of the document, the key functional, testable requirements of the Logistics are drawn out.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-26	FSMS interface to 4G OMS Forward Logistics for the following: - Notify Receipt of CH Shipment at TPL Warehouse -From Comms Hub Manufacturer - Delivery Acceptance/Rejection for M-ASN -From Comms Hub Manufacturer - Update Shipment of CH to SU From 3rd Party Logistics	- All structural variances, including boundary value analysis of data items, Timestamping in UTC - Post command / response processing (Data Updates, Workflows, Event Logging, Timestamping in UTC) - Exception path conditions including all HTTP Response codes - Retries where applicable

2.2.6 OMS Functional Testing

The testable requirements of the OMS are derived from business requirements drawn from the OMS HLD, RTM and associated Interface Specifications

In this section of the document, the key functional, testable requirements of the OMS are drawn out.

<u>Focus Area Reference</u>	<u>Focus Area</u>	<u>Acceptance Criteria</u>
FSM-Func-22	DCC TOC interface to DCC OMS to send “ShareCHInstalledPerDay” “ShareChangeOfSupplyData”	- All structural variances, including boundary value analysis of data items, Timestamping in UTC - Post command / response processing (Data Updates, Workflows, Event Logging, Timestamping in UTC) - Exception path conditions including all HTTP Response codes - Retries where applicable

2.2.7 System Capacity Testing

The FSM system capacity testing will baseline the performance of new cloud-based solution.

In absence of end-to-end integrated test environment, DCC will take a risk-based approach for system capacity testing. The system capacity testing utilised isolated component-based PIT environment to assure that the solution can operate at the requisite level of traffic.

The test environment will be scaled version of potential production environment. The test environment will be supported by simulators to generate the payloads.

The testable non-functional requirements are derived from the current production volume and has been covered as part of CTD. The following table covers the key measurement for the system capacity testing:

Focus Area Reference	Focus Area	Acceptance Criteria
NFR-01	Transaction Volume	System Capacity Test Completion Report showcasing solution: Achieving specified transaction volume during the tests for an agreed duration whilst maintaining the availability, concurrency hardware utilisation and agreed response time SLAs. Scaling up and scaling down of resources in line with design expectations.

The above focus area will utilise following, but not limited to, types of tests to assure:

- Load Test: Short duration average volume test
- Stress Test: High volume test to stretch the solution and trigger autoscaling
- Soak test: long duration a day-in-life test

2.2.8 Security Testing

Security Testing will be performed during PIT and SIT.

The DCC shall ensure that an organisation which is a CHECK approved service provider or a CREST certified tester carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

1. in respect of each DCC System, on at least an annual basis;
2. in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and
3. on the occurrence of any Major Security Incident in relation to the DCC Systems”.

For the Security governance approach for FSM, the outcome of Non-Functional security testing will be assured by DCC Security Assurance and an independent auditor, who will engage with Security Sub Committee where necessary. The outcome will be reported to TAG for information. Functional Security testing including User Authentication and RBAC will be Assured by DCC Test Assurance with TAB governance for PIT and TAB/TAG for SIT.

Functional Security testing including User Authentication and RBAC will be Assured by DCC Test Assurance. PIT Test Completion shall be approved by TAB. SIT Test Completion shall be approved by TAB and agreed by TAG.

2.3 Systems Integration Test

2.3.1 Functional Testing

2.3.1.1 Input Documents

The testable requirements for Systems Integration Testing (SIT) have been derived from the following documents:

- **FSMS & OMS Interface Catalogue v3.2** – a list of all the external interfaces of FSMS and OMS with other components within the DCC Total System. SIT shall cover these interfaces.
The **FSM API Interfaces List Sheet** within the Future Service Management CTD measures the coverage of each interface against the **Coverage Workbook**. This provides evidence that all new FSMS & OMS interfaces delivered by this project are covered within the SIT scope. The **Coverage Workbook** details for each testable requirement whether they are cover by PIT, SIT or both PIT & SIT.
- **Future Service Management RTM V3.1** – that describes all the functional and non-functional requirements of FSMS & OMS. SIT shall cover all the functional requirements for which there is an integration between FSMS or OMS and another component within the DCC Total System. SIT shall not cover the non-functional requirements.

The **Functional Requirements RTMv3.1 Sheet** within the Future Service Management CTD measures the coverage of each functional requirement against the **Coverage Workbook**. This provides evidence that all FSMS & OMS functional requirements are covered. The **Coverage Workbook** details for each testable requirement whether they are cover by PIT, SIT or both PIT & SIT.

2.3.1.2 Coverage – FSM & OMS Interfaces

The main SIT test objective is to demonstrate that all the FSM and OMS interfaces with other components in the DCC Total System work correctly. The table below provides a summary of all the FSM and OMS interfaces that shall be tested as part of the SIT scope:

Item Ref.	Interface Summary	Originating System	Destination System
IC-001	Read Inventory	FSMS	DAL
IC-002	Device Ownership	FSMS	DAL
IC-003	Device Interested Parties	FSMS	DAL
IC-004	Retrieve Service Audit Trail	FSMS	DAL
IC-005	Coverage Check (Postcode)	FSMS	DAL
IC-006	Coverage Check (District)	FSMS	DAL
IC-007	CSP Comms Hub Database	FSMS	DAL
IC-008	Comms Hub Diagnostics	FSMS	DAL
IC-009	Retrieve Traffic Management Data	FSMS	DAL
IC-010	Retrieve Firmware Distribution Device Data	FSMS	DAL
IC-011	Retrieve Firmware Distribution Data	FSMS	DAL
IC-012	Manage DCC Service User Suspension	FSMS	DAL
IC-013	Manage Corporation	FSMS	DAL
IC-014	Manage SEC Party	FSMS	DAL
IC-015	Manage DCC Service User	FSMS	DAL
IC-016	Manage Manufacturer	FSMS	DAL
IC-017	File Uploads	FSMS	DAL
IC-018	Manage Communications Hub	FSMS	DAL
IC-019	Manage Comms Hub Channel Configuration	FSMS	DAL
IC-020	DSP Component Health Status	FSMS	DAL
IC-021	DUIS Version of the Interested Party	FSMS	DAL
IC-022	All Interested Parties	FSMS	DAL
IC-023	Create Incident	DSP Data Systems	FSMS
IC-026	Create Comms Hub Returns Record	DSP Data Systems	FSMS
IC-027	Reset Firmware Distribution Device Data	FSMS	DAL
IC-028	Coverage File Download	FSMS	DAL
IC-029	Manage Device Status	FSMS	DAL
IC-032	FSMS Data Feed	FSMS	CEDAR
IC-033	SendEOLReport	OMS	Device Manager

Item Ref.	Interface Summary	Originating System	Destination System
IC-034	EOLReportResponse	Device Manager	OMS
IC-035	SendPreNotification	OMS	Device Manager
IC-036	NotifyCHReturnsInitiated	Device Manager	OMS
IC-038	NotifyFARStatus	OMS	Device Manager
IC-039	NotifyCHDisposal	OMS	Device Manager
IC-040	ShareAggregatedCHForecast	OMS	Test Bench Warehouse Management System
IC-041	ShareMasterOrder	OMS	Test Bench Warehouse Management System
IC-042	AcceptOrRejectMasterOrder	Test Bench Warehouse Management System	OMS
IC-043	SendEOLReport	Test Bench Warehouse Management System	OMS
IC-044	EOLReportResponse	OMS	Test Bench Warehouse Management System
IC-045	UploadMasterASNFile	Test Bench Warehouse Management System	OMS
IC-046	NotifyCommsHubShippingStatus	Test Bench Warehouse Management System	OMS
IC-047	SendDisposalCertificate	Test Bench Warehouse Management System	OMS
IC-048	Send RMA Details	OMS	Test Bench Warehouse Management System
IC-049	Request exception ORR	Test Bench Warehouse Management System	OMS
IC-050	Update RMA Details	Test Bench Warehouse Management System	OMS
IC-051	Notify CH Delivery	Test Bench Warehouse Management System	OMS
IC-052	Notify FAR Acceptance	OMS	Test Bench Warehouse Management System

Item Ref.	Interface Summary	Originating System	Destination System
IC-053	Move CH to Forward Logistics	OMS	Test Bench Warehouse Management System
IC-054	Upload R-ASN	Test Bench Warehouse Management System	OMS
IC-055	Accept R-ASN	OMS	Test Bench Warehouse Management System
IC-056	Update Preliminary Fault Assessment	Test Bench Warehouse Management System	OMS
IC-057	Fault Analysis Report (FAR)	Test Bench Warehouse Management System	OMS
IC-058	Notify FAR Action	Test Bench Warehouse Management System	OMS
IC-059	Update Refurbishment Status	Test Bench Warehouse Management System	OMS
IC-060	Notify CH Disposal	Test Bench Warehouse Management System	OMS
IC-061	Order Firming	OMS	Test Bench Warehouse Management System
IC-062	M-ASN Notification	OMS	Test Bench Warehouse Management System
IC-063	Notify Receipt of CH Shipment at TPL Warehouse	Test Bench Warehouse Management System	OMS
IC-064	Delivery Acceptance/Rejection for M-ASN	Test Bench Warehouse Management System	OMS
IC-069	Upload SU-ASN	Test Bench Warehouse Management System	OMS
IC-070	Confirm SU-ASN Acceptance Status	OMS	Test Bench Warehouse Management System
IC-071	Update Shipment of CH to SU	Test Bench Warehouse Management System	OMS
IC-072	Upload Proof Of Delivery	Test Bench Warehouse Management System	OMS
IC-073	Reject Delivery by SU	OMS	Test Bench Warehouse Management System

Item Ref.	Interface Summary	Originating System	Destination System
IC-074	Collected the Rejected Delivery	Test Bench Warehouse Management System	OMS
IC-076	Share R-ASN	OMS	Test Bench Warehouse Management System
IC-077	ShareCHInstalledPerDay	TOC	OMS
IC-078	ShareChangeOfSupplyData	TOC	OMS
IC-080	Security Logs - FSMS	FSMS	SOC
IC-081	Security Logs - Integration Layer	FSMS	SOC
IC-082	Security Logs - IDP Hub	FSMS	SOC
IC-084	Security Incidents	SOC	FSMS
IC-085	Create Incident	Service Management System	FSMS
IC-086	Update Incident	Service Management System	FSMS
IC-087	Create/Update Return	Service Management System	FSMS
IC-088	Send Return	FSMS	Service Management System
IC-089	Update Comms Hub Fault Analysis Report	Service Management System	FSMS
IC-091	Create Incident	Service Management System	FSMS
IC-092	Update Incident	Service Management System	FSMS
IC-093	Create Problem	Service Management System	FSMS
IC-094	Update Problem	Service Management System	FSMS
IC-095	Create Incident	FSMS	Service Management System
IC-096	Update Incident	FSMS	Service Management System
IC-097	Create Problem	FSMS	Service Management System
IC-098	Update Problem	FSMS	Service Management System
IC-099	Create Work Order	FSMS	Service Management System
IC-100	Update Work Order	FSMS	Service Management System
IC-101	Update Work Order	Service Management System	FSMS
IC-102	Create/Update Return	Service Management System	FSMS

Item Ref.	Interface Summary	Originating System	Destination System
IC-103	Send Return	FSMS	Service Management System
IC-104	Update Comms Hub Fault Analysis Report	File Server	FSMS
IC-106	Outbound Emails	FSMS	Email Server
IC-107	Inbound Emails	Email Server	FSMS
IC-108	Report Request	FSMS	DSP
IC-109	Deliver Report	DSP Data Systems	DCC
IC-110	RSMI_007	FSMS	DSP

2.3.1.3 Coverage – High Level Requirements

The table below provides a summary of all the FSM high level requirements that shall be tested as part of the SIT scope:

High Level Requirement Title
SAML (Security Assertion Markup Language) Authentication for Self Service Interface
Security Logs
Replication of the Smart Metering Inventory
Diagnostics
Communication Hub Return Request
Communication Hub Return Record
Communication Hub Return Update
Firming Notification
Details of the Upcoming Shipment
Order Delivery
Consignment Delivery
Aggregated Forecast to CHM
Raise an Incident
Assign an Incident Category
Update an Incident
Complete an Incident
Major Incident
Security Incident
Raise a Problem
Update a Problem
Ticket Management - Integrated Partner
Inventory Reports
Service Audit Trail Reports
CSP SMWAN Network Coverage
OMS Reports
Future Service Management Data into the DS&A Data Portal
Manage Data into and out from the Future Service Management System
Data Migration for Launch (DSMS)
User Migration
Data Migration for Launch (OMS)
Data Migration for Launch (SMI)
FSM and DSP Bi-Directional Integration
FSM and CSP Bi-Directional Integration
FSM (OMS) and Comms Hub Ordering Component Bi-Directional Integration
FSMS Integrations with SOC

High Level Requirement Title
FSMS Integrations with DS&A (CEDAR)
FSMS (OMS) integration with TOC
Bidirectional Connectivity Between Supported Components of the End To End FSMS
FSMS Non-API Interfaces Integration

2.3.1.4 Coverage - Device Set Configurations

The FSM scope does not require end to end testing of device sets, however device sets are required to demonstrate some FSM & OMS behaviours.

CHM2 - CSP C&S

CHM3 (2G/3G) - CSP C&S

CHM1 - CSP N

CHM3 (4G) - CSP C&S

DCC will utilise HAN devices and/or emulators to attach to the CHs to enable CH diagnostics - these HAN devices will have the GBCS version most prevalent in production for each CSP. The FSM solution does not reach or impact the HAN devices.

2.3.2 Regression Testing

The System Regression Scope shall include:

- testing of SMETS1 & SMETS2 SRV testing on existing DUIS interfaces and GBCS versions
- Functional Regression testing, post defect fixes found during Functional Testing

2.3.3 Final Regression Cycle

A regression test run will take place against the version of the solution that is planned to exit SIT.

The scope of the Final Regression Cycle will comprise of a subset of the Functional Testing scope. The principles used in selecting the scope for Final Regression Cycle are as follows:

- Tests will be a subset of the tests from the functional test phase
- Maximise the testing of FSM interfaces with other components in the DCC Total System
- OMS Forward Logistics process to be executed for an order
- Reverse Logistics process to be executed.

2.3.4 System Capacity Testing

The system capacity testing in SIT will take place to measure the end-to-end response time. The objective of the test will be to establish a baseline for end-to-end response time for completing a single transaction. These tests will help in understanding latency, packet loss, etc. however, these tests will not be subjected to high volume of transactions.

3 Devices For Use in Testing

PIT and SIT phases will be driven by Test Data. Where real devices are used to support testing of business process in the SIT phase a device selection methodology is not required, the Device selection will be representative of SMETS2 CH Manufacturers.

Functional Testing shall be conducted on real Devices; however, this Test Coverage Document recognises that there are test scenarios where it is not possible or prudent to utilise real Devices. In these instances, the use of a Device Emulator is permitted. Examples of test scenarios where this may be the case are provided below;

- Where functionality is not yet available on a real Device.
- Exception scenarios, where a Device is required to exhibit incorrect behaviour in order to trigger a failure condition, which may not be possible on a real Device.

3.1 Functional Testing

No devices are required for PIT testing.

3.2 System Integration Test

The following Device Models (or Device Model Combinations in the case of SMETS1) are included in the scope of Systems Integration Testing.

CHM2 - CSP C&S

CHM3 (2G/3G) - CSP C&S

CHM1 - CSP N

CHM3 (4G) - CSP C&S

DCC will utilise HAN devices and/or emulators to attach to the CHs to enable CH diagnostics - these HAN devices will have the GBCS version most prevalent in production for each CSP. The FSM solution does not reach or impact the HAN devices.

3.3 Regression Testing

Regression Testing scope shall include a suite of tests which exercises the current baseline of functionality which already exists in Production. This will include 4G CH devices, as the programme will be live in production too.

The following Device Models or Device Model Combinations have been identified for use in regression testing undertaken during the SIT Phase of testing, out of which 3 SMETS1 sets, one for each of the S1SP and 2 SMETS2 sets, one for each CSP will be available on a regular basis.

SMETS1

Manufacturer	Device Manufacturer	Device	Firmware
MDS	ELSTER	CHF	2EDBEB09
	ELSTER	GPF	2EDBEB09
	ELSTER	ESME	0401EB5B
	ELSTER	GSME	0025DBC6
	Chameleon	PPMID	26301
MDS	ELSTER	CHF	2EDBEB09
	ELSTER	GPF	2EDBEB09
	ELSTER	ESME	0401EB5B
	ELSTER	GSME	0025DBC6
	Chameleon	PPMID	21101
	Chameleon	IHD	26301
Elster 12g	ELSTER	CHF	2EDBEB09
	ELSTER	GPF	2EDBEB09
	ELSTER	ESME	0401EB5B
	ELSTER	GSME	446
	STI	PPMID	014F0000
Elster 13g	ELSTER	CHF	2EDBEB09
	ELSTER	GPF	2EDBEB09
	ELSTER	ESME	0401EB5B
	ELSTER	GSME	0025DBC6
	STI	PPMID	1430000
Itron	ITRON	CHF	3345337
	ITRON	GPF	3345337
	ITRON	ESME	3475317
	ITRON	GSME	029310D6
	GEO	PPMID	10310915
Itron	ITRON	CHF	3345337
	ITRON	GPF	3345337
	ITRON	ESME	3475317
	ITRON	GSME	029310D6
	GEO	PPMID	10310915
Aclara	ACLARA	CHF	30309
	ACLARA	GPF	30309
	ACLARA	ESME	30304
	ACLARA	GSME	25B3062A
	Chameleon	PPMID	11200
Aclara	ACLARA	CHF	30309
	ACLARA	GPF	30309
	ACLARA	ESME	630304
	ACLARA	GSME	25B3062A
	Chameleon	PPMID	11100
Secure	Secure Meters	CHF	C7A10001
	Secure Meters	GPF	C7A10001
	Secure Meters	ESME	C0A10001
	Secure Meters	GSME	C4A10001

Manufacturer	Device Manufacturer	Device	Firmware
	Secure Meters	PPMID	C6A20001
Secure	Secure Meters	CHF	C7A1E001
	Secure Meters	GPF	C7A1E001
	Secure Meters	ESME	C0A1E001
	Secure Meters	GSME	C4A10001
	Secure Meters	PPMID	C6A20001
	Secure Meters	PPMID	C6A20001
BG1	Trilliant	CHF	220A0000
	Trilliant	GPF	220A0000
	Landis+Gyr	ESME	23070101
	Landis+Gyr	GSME	3000168
	GEO	PPMID	20210900
BG1	Trilliant	CHF	220A0000
	Trilliant	GPF	220A0000
	Landis+Gyr	ESME	23070101
	Landis+Gyr	GSME	3000168
	GEO	PPMID	20210900
NP1	Trilliant	CHF	22500000
	Trilliant	GPF	22500000
	Landis+Gyr	ESME	23070101
	Landis+Gyr	GSME	3022168
	GEO	PPMID	4040001
NP1	Trilliant	CHF	22080000
	Trilliant	GPF	22080000
	Landis+Gyr	ESME	23070101
	Landis+Gyr	GSME	3022168
	GEO	PPMID	2001093D

SMETS2

CH	CSP / S1SP	ESME	GSME	PPMID	DUIS Version	Notes/Coverage
SET A SBCH-GBCS V3.2 TOSH 13.6	VMO2	L&G SMETS2V4.2 F/W 38.04.04.04	L&G SMETS2v4.2 F/W 03.03.32.54	GEO - 2.4 GHz F/W 5.8.0	4.0	1. Install & Commission 2. Daily System Regression 3. Decommissioning
SET B DBCH-GBCS V3.2 EDMI 3.11.X	ARQ	L&G SMETS2V4.2 F/W 38.04.04.04	L&G SMETS2v4.2 Sub GHz F/W 15.01.91.31	GEO - Sub GHz F/W 5.8.0	5.2	1. Install & Commission 2. Daily System Regression 3. Decommissioning

4 Security Testing

Security Testing will be performed during PIT and SIT.

The DCC shall ensure that an organisation which is a CHECK approved service provider or a CREST certified tester carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

4. in respect of each DCC System, on at least an annual basis;
5. in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and
6. on the occurrence of any Major Security Incident in relation to the DCC Systems”.

For the Security governance approach for FSM, the outcome of Non-Functional security testing will be assured by DCC Security Assurance and an independent auditor, who will engage with Security Sub Committee where necessary. The outcome will be reported to TAG for information. Functional Security testing including User Authentication and RBAC will be Assured by DCC Test Assurance with TAB governance for PIT and TAB/TAG for SIT.

Functional Security testing including User Authentication and RBAC will be Assured by DCC Test Assurance. PIT Test Completion shall be approved by TAB. SIT Test Completion shall be approved by TAB and approved by TAG.

5 Risks

Reference	Description	Mitigation
TBC	DCC does not have a stand-alone Performance test environment	As part of the shift left approach Performance testing will be run as part of the PIT test phase to find early Testing Issues. The system capacity testing will utilise isolated component-based PIT environment to assure that the solution can operate at the requisite level of traffic. A further measurement of end-to-end response time will be observed during SIT phase to provide confidence in the solution.

Reference	Description	Mitigation
R6856	PIT Completion is scheduled for 21st February 25 which is shortly post approval of the Test approach Documents and TCD. As a result, PIT will run Oct 24 to Jan 25 without formal agreement of its scope and completion criteria. If TAG, its members, and/or the SVTAD consultation responses were to state that the current test scope is insufficient or incorrect then further testing would be needed. This would delay the planned PIT exit and the associated SIT Entry with further downstream impact to programme timelines.	DCC presented the test approach docs to TAG119 (30 October 2024) for Review. DCC will return to TAG120 (27 November 2024) having addressed TAG feedback where DCC will ask for the TAD to be conditionally approved. The TCD will be shared in the TAG collaboration space w/c 11 November 2024, in order to facilitate a review discussion at TAG 120, with approval then being sought at TAG 121 (11 December 2024) Should any additional uplift be required as a result of the SVTAD consultation, DCC would return the documents to TAG to seek approval of the uplift. Conditional approval of the FSM test documents will be requested at TAG 122 (Jan 25) post the SVTAD designation.

6 Appendices

6.1 Service Now PIT CTD

6.2 SIT CTD

This will be provided, once all the SIT testing is determined.