RETAIL ENERGY CODE

This document is classified as **WHITE**.
Information is for public, unrestricted dissemination and publication.

01	Initial Assessment Report
02	Preliminary Change
03	Final Change Report

INITIAL ASSESSMENT REPORT

R0048 – DCC SERVICE ORGANISATIONAL CONTROL 2 (SOC2) ASSESSMENTS

DOCUMENT VERSION	V1.0
DATE ISSUED	09/12/2022
DOCUMENT APPROVAL STATUS	APPROVED

RESPONSIBLE COMMITTEE	TECHNICAL EXPERT PANEL	CHANGE PATH	SELF GOVERNANCE
PRIORITY STATUS	LOW	URGENCY	STANDARD

DEADLINE FOR ALTERNATIVE CHANGE PROPOSALS	17/02/2023

LEAD CHANGE ANALYST



George Barnes

Click to send an email

02045668350

CHANGE OVERVIEW

Currently within the Central Switching Service (CSS) Service Definition document there is a requirement for the CSS Provider to arrange for and undertake system organisation control type 2 (SOC2) assessments on the CSS's cloud-based infrastructure.

This Change Proposal seeks to determine if it is appropriate for the requirement for assurance on the CSS's cloud-based infrastructure to be changed from 'SOC2 Type 2' to 'independently assessed'.

	High Impact: N/A
	Medium Impact: Switching Service Provider
	Low Impact: N/A

1 BACKGROUND

Within the CSS Service Definition, there is currently a requirement for the CSS Provider to arrange for and undertake SOC2 assessments on the CSS. SOC2 assessments are a cyber security compliance framework, which focuses on the principles of security, availability, processing, integrity, confidentiality, and privacy. SOC2 assessments are often used where a third-party Service Provider is responsible for collecting and storing sensitive information.

The CSS Provider has raised this Change Proposal with the intention of removing this requirement and replacing it with a suitable alternative which will be less labour intensive and potentially provide better value for money.

The Smart Energy Code (SEC) has accepted that there was felt to be a lack of flexibility in SOC2 assessment frameworks, making it difficult to adapt them to meet the obligations placed on the Service Provider by the Code. For this reason, the requirement for the DCC to undertake SOC2 assessments was removed from the SEC in MP103, implemented in 2019.

The requirement for the CSS Provider to acquire SOC2 security certification originally came from the Code of Connection (CoCo) as a result of the output of the Information Risk Assessment (IRA) conducted by the CSS Provider as part of their Switching Programme activity. Any changes made to the requirement for security certification would need to be assessed against the output of the IRA to ensure that the alternative arrangement adequately mitigates the risks to information security highlighted within it.

2 PROBLEM STATEMENT

The CSS Provider asserts that SOC2 assessment does not provide a proportionate level of assurance or the best value for money, which based on their experience, they believe they have a better understanding of the CSS's risk profile. However, the use of SOC2 assessments is currently defined within the CSS Definition document, which means an alternative assurance regime cannot be used.

3 USER STORIES

REF.	USER STORIES
MARKET PARTICIPANT USER STORIES	
M1	As the Code Manager, I want REC Service Providers to obtain and maintain appropriate security certification, so I have confidence that the Service Providers security, processing integrity, confidentiality and privacy controls are assessed, and any risks are identified and addressed.
M2	As the CSS Provider, I want to be able to obtain an appropriate security certification, so I can demonstrate security compliance in a proportionate and cost-effective approach.

4 IMPACTS

REC DOCUMENTS / PRODUCTS
Central Switching Service (CSS) Service Definition

REC SERVICE PROVIDERS
Central Switching Service (CSS) Provider
Electricity Retail Data Agent (ERDA)
Gas Retail Data Agent (GRDA)

Central Switching Service (CSS) Service Definition – This Change Proposal seeks to make amendments to the CSS Definition document.

If this Change is approved, the legal text of paragraph 11.3. will be updated to change the requirement for the CSS Provider to use SOC2 Type 2 assurance.

The Proposer has provided draft legal text which can be found here.

Central Switching Service Provider – Should this Change Proposal be implemented; the CSS Provider will be impacted. This is because they will be able to procure a more appropriate assurance regime. The scale of this impact will be assessed through a Service Provider impact assessment.

Electricity Retail Data Agent & Gas Retail Data Agent – Whilst not directly impacted by this Change Proposal, the Code Manager will validate impacts to ERDS and GRDS caused consequentially by the audit arrangements with the CSS Provider being changed.

5 CHANGE PATH AND RESPONSIBLE COMMITTEE

CHANGE PATH	SELF GOVERNANCE

RESPONSIBLE COMMITTEE	TECHNICAL EXPERT PANEL

The Responsible Committee for this Change Proposal is the Technical Expert Panel (TEP), as the only document identified as being impacted is the CSS Definition which is a Category 2 document under the responsibility of the TEP.

We have classified this change as a Self-Governance change as we do not believe that this change will have material or discriminatory impacts on any REC Parties, competition, or Consumers.

6 PRIORITY STATUS AND URGENCY

RETAIL ENERGY CODE

PRIORITISATION MATRIX

Category	Significance / Resource impacts / Urgency	Further selection / breakdown	Score (0-3)	Weighting	Weighted Score
Impacts	Consumer Impact		0	25	0
	Retail Markets Impact		0	15	0
	RECCo / REC Party / REC Service Provider Impact	Operational Effectiveness and Efficiencies	2	5	10
		Legal and Regulatory Compliance	1	13	13
Resource	Complexity / Effort / Duration		3	8	23
Strategic Alignment	Contribution to/ Alignment with the objectives of the REC		0	15	0
	Contribution to/ Alignment with RECCo's Forward Work Plan		0		0
Urgency *(The need to progress a change to meet a targeted date)*			2	20	40
				Overall Priority Score (rounded)	85

Priority Status	LOW
Change Proposal Type	STANDARD

This Change Proposal has a low priority based on a priority score of 85.

Urgency – a score of 2 has been given to acknowledge that this Change Proposal needs to be implemented ahead of August 2023 which is the beginning of the first audit, and the CSS Provider will require time to ensure they have contracts in place to obtain the audit. This change is being progressed now despite it having a low priority to meet this date. (Please see R0048.CPP.D001 in section 2.1.5 of the Change Proposal Plan).

Impacts – a score of 2 for operational effectiveness and efficiencies and a score of 1 for legal and regulatory compliance. This Change Proposal will enable the CSS Provider to procure assurance that is appropriate and proportionate for the service they are providing. This is expected to improve effectiveness and efficiency of the assurance activity for the CSS Provider.

Resource – A score of 3, to reflect that the Code Manager anticipates minimal resource requirements to develop and implement any proposed solution.

7 SUMMARY OF CHANGE PROPOSAL PLAN

Whilst a solution was proposed with this Change Proposal, the Code Manager believes that further work is required to ensure that the security audit requirements within the Central Switching Service Definition document are robust and mitigates the risks to information. As such, the plan begins with a period of solution analysis and development, containing an impact assessment which will be targeted at the CSS Provider to understand the impacts of the solution, as well as provide information to build the case for change.

Following this, the plan shows the dates that consultations will be issued, as well as when the Code Manager will issue a consultation to seek wider feedback on the proposed solution.

	FROM	TO
SOLUTION ANALYSIS AND DEVELOPMENT	21/12/2022	10/02/2023
SERVICE PROVIDER IMPACT ASSESSMENT	16/01/2023	06/02/2023
PRELIMINARY CHANGE REPORT AND CONSULTATION ISSUED	17/02/2023	10/03/2023
FINAL CHANGE REPORT ISSUED	17/03/2023	17/03/2023
RESPONSIBLE COMMITTEE DECISION	29/03/2023	29/03/2023
APPEAL WINDOW CLOSURE	12/04/2023	12/04/2023

8 GLOSSARY

TERM	DEFINITION
Central Switching Service (CSS)	means the Systems and processes provided or procured by the CSS Provider for the purpose of providing the Address Management Service and the Registration Service.
Central Switching Service Provider (CSS Provider)	means the DCC when performing functions under or in relation to this Code (but always excluding its functions under the Smart Energy Code and its roles as CSS Systems Integrator, SI Provider and Switching Operator), including in respect of the Central Switching Service and including in effecting the design, build and testing of any System that will allow it to perform functions under this Code after the CSS Go-Live Date. This role is the CSS Procurer and Manager function as described in the E2E Data Migration Plan, E2E Integration Plan, E2E Post Implementation Plan, E2E Testing Plan, E2E Transition Plan: Implementation Approach and E2E Transition Plan: In-Flight Switches Approach.

TERM	DEFINITION
Data Communications Company (DCC)	means the person holding the DCC Licence.
Design Baseline	means the suite of documents, collectively known as Design Baseline 4, published by the Authority on 22 June 2018, as updated or superseded from time-to-time (including by the Technical Specification).
REC Service Provider	means the provider of each REC Service.
Smart Energy code (SEC)	means the code of that name maintained pursuant to the DCC Licence
Switching Programme	means the programme established by the Authority to implement new switching arrangements in retail energy markets
System and Organisation Control Type 2 (SOC2)	SOC2 assessments are a cyber security compliance framework, they focus on the principles of security, availability, processing, integrity, confidentiality, and privacy and are often used when a third party Service Provider is responsible for collecting and storing sensitive information. It originates from the United States of America Statement on Auditing Standards 70 (SAS70) financial audits. As such proves difficult to align the requirements of a SOC2 audit with more various requirements for security.