RETAIL ENERGY CODE

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

01	Initial Assessment Report
02	Preliminary Change Report
03	Final Change Report

CHANGE REPORT

R0048 – DCC SERVICE ORGANISATION CONTROL 2 (SOC) ASSESSMENTS

CHANGE REPORT	FINAL
DOCUMENT VERSION	1.0
ISSUED DATE	13/06/2024
DOCUMENT APPROVAL STATUS	PRE-VOTE

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

DEADLINE FOR ALTERNATIVE CHANGE PROPOSALS	11/04/2024

LEAD CHANGE ANALYST



Caroline Freimuller

Click to send an email

020 3923 9765

ASSURANCE LEAD

Anton Moden

Click to send an email

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 (SOC) 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 'SOC Type 2' to 'independently assessed'.

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

RETAIL ENERGY CODE

CODE MANAGER'S RECOMMENDATION

The Code Manager recommends Change Proposal R0048 is **REJECTED**.

CONTENTS

BACKGROUND		
1.	Summary	**3**
2.	Problem Statement	**3**
3.	User Stories	**3**
PROPOSAL		
4.	Summary of Analysis Undertaken	**4**
5.	Proposed Solution	**4**
6.	Draft Legal Text	**4**
7.	Summary of Impact Assessment Activity	**4**
8.	Delivery Against Change Proposal Plan	**5**
9.	Key Risks, Assumptions, Issues and Dependencies	**5**
10.	Summary of Consultation Responses	**6**
11.	Business Case Assessment	**6**
12.	Case for Change	**8**
13.	Code Manager's Recommendation	**8**
14.	Appendix	**8**
15.	Glossary	**99**

BACKGROUND

1 SUMMARY

Within the CSS Service Definition, there is currently a requirement for the cloud base infrastructure to be assured. Many cloud services are on shared infrastructure (e.g. a public cloud), and it is often neither possible nor practical for the organisations using the service to assure that the service is operating to the appropriate standards. SOC assessments exist for this purpose, allowing the cloud service provider to deliver independent assurance that can be shared with their customers, without the need to manage multiple requests from their customers and the confidentiality requirements associated with them.

SOC assessments over cloud services focus on internal controls over security, confidentiality, processing integrity, privacy, and availability of data. Type 2 refers to the assessment covering controls over a specified timeline, instead of a point in time (Type 1).

The CSS Provider has raised this Change Proposal with the intention of removing this requirement and replacing it with a suitable alternative.

The requirement for the CSS Provider to acquire SOC 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 assurance 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 SOC 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 SOC 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 assurance, 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 assurance, so I can demonstrate security compliance in a proportionate and cost-effective manner.

RETAIL ENERGY CODE

PROPOSAL

4 SUMMARY OF ANALYSIS UNDERTAKEN

This Change Proposal has run alongside a derogation exempting the DCC, in its role of CSS Provider, from Paragraph 11.3 of the CSS Service Definition whilst this change is progressed and a decision is made.

As part of this derogation the DCC provided a Competent Independent Organisation (CIO) assessment report to the REC Performance Assurance Board (PAB) and the Change Team. The CIO report focused on the activities of Landmark, the organisation that manage the CSS. Landmark do not provide the cloud base infrastructure, which is separately procured from Microsoft. The CIO report provides no assurance, or other commentary on the cloud base infrastructure. It has been determined this is therefore not a suitable replacement for the SOC report.

5 PROPOSED SOLUTION

The proposed solution is achieved through legal text changes to the CSS Service Definition clause 11.3, removing the requirement for the cloud-based infrastructure to be assured specifically via SOC assessment.

As the Proposer, DCC suggested the replacement of the wording SOC to “independently assured” to remove this requirement as they felt SOC was an over application of assurance within the CSS now that DCC have a better understanding of the risk profile.

6 DRAFT LEGAL TEXT

The legal text changes to deliver the proposed solution to R0048 can be found here.

It proposes the amendment of clause 11.3 in the CSS Service Definition from “The CSS’s cloud base infrastructure shall be assured with SOC Type 2 security certification” to “The CSS’s cloud base infrastructure shall be assured with an independently assured security certification”.

7 SUMMARY OF IMPACT ASSESSMENT ACTIVITY

7.1 SERVICE PROVIDER IMPACT ASSESSMENTS

The CSS Service Provider was asked to complete an Impact Assessment for this change.

CSS SERVICE PROVIDER	• DCC, in their role as the CSS Service Provider, propose to use an expert independent assurance provider to assess Landmark’s activity rather than specifically a SOC assessment over the cloud base infrastructure. • They suggest this assurance will be aligned to industry standard security assessments, which are broadly aligned to SOC and ISO27001 processes, but no further detail was provided.

	• No costs or savings were specifically called out, although the CSS Service Provider expects to make savings if able to procure from a selection of vendors. • There is not expected to be a lead time required for the implementation of this solution. • The only assumption made during the impact assessment is that there will be a variety of expert independent assurance providers available to request quotes and availability from, in order to competitively select a supplier to perform the assurance.

8 DELIVERY AGAINST CHANGE PROPOSAL PLAN

The Change Proposal Plan was removed until the outcome of the derogation, where DCC submitted a CIO assessment for comparison with a SOC assessment, could be received for analysis.

As soon as this was received and reviewed, the Code Manager made the decision to progress to Preliminary Change Report as soon as possible rather than submitting a new Change Proposal Plan.

9 KEY RISKS, ASSUMPTIONS, ISSUES AND DEPENDENCIES

9.1 RISKS AND ISSUES

No.	RISK	NOTES	MITIGATION
R1	Without a specified assessment, different controls could be evaluated between years and items missed.		A specific assessment is required. SOC has been determined as the best type for the assurance required by the REC.
R2	Microsoft are unlikely to agree to another assessment type as common practice is to use SOC reports.	Microsoft are the Cloud Service Provider, vs Landmark who are the Cloud Service Customer.	

10 SUMMARY OF CONSULTATION RESPONSES

A consultation was circulated on 25 April 2024 to obtain views on the Preliminary Change report. In total 2 responses were received from an Energy Supplier and from a Distribution Network Operator (DNO). The responses have been consolidated and comments provided by the Code Manager. This can be found here.

The key themes from these responses have been summarised and set out below.

10.1 SUMMARY OF RESPONSES

10.1.1 COMMENTS ON THE SOLUTION AND LEGAL TEXT

Both respondents did not support the removal of the current requirement for a SOC Type 2 security certification, to be replaced with an independently assured security certification.

They confirmed they saw no benefit from the implementation of the change and agreed that the proposed legal text would weaken the controls in place for the CSS. The need for adequate assurance of the CSS was called out throughout the responses, with the Energy Supplier placing emphasis on the need for maintaining Consumer trust that their data is handled securely.

10.1.2 CASE FOR CHANGE AND CODE MANAGER'S RECOMMENDATION

Both respondents agreed with the Code Manager's recommendation for rejection based on the Business Case Assessment and the Case for Change presented in the change report.

The DNO in particular agreed with the Code Manager's assessment of the benefits and risks associated with this Change Proposal and agreed that the risks outweighed any potential benefits. It was also noted that while there may be cost savings available to the Service Provider, these would need to be passed back to the industry for these organisations to see any benefit.

11 BUSINESS CASE ASSESSMENT

11.1 COSTS

	DESIGN/ DEVELOPMENT COSTS	IMPLEMENTATION COSTS	ONGOING OPERATIONAL COSTS
CSS SERVICE PROVIDER	N/A	£0	£0 PER ANNUM

11.2 BENEFITS

INTANGIBLE BENEFITS	BENEFITS DESCRIPTION
REDUCTION IN PROCUREMENT COSTS	The CSS Service Provider has stated they expect procurement to be at a reduced cost compared to SOC. Without needing a specified assessment type, they will be able to tender with a wider range of vendors, however it is not possible to confirm this or how much of a saving could be possible.

11.3 COST BENEFIT ANALYIS SUMMARY

While there are no implementation or on-going costs associated with the Change Proposal and there is the potential for savings dependent on the assessment provider procured, the Code Manager does not feel the benefits outweigh the risks associated with this solution.

In summary these risks are:

- Controls applicable to the Cloud Service Provider (as opposed to the Cloud Service Customer) are not monitored appropriately, meaning areas that are at risk are not flagged to the CSS Provider/RECCo.
- Controls may not be correctly carried through year on year and items could be missed as there would not be a defined list of items to be assured.

Due to the nature and volume of data processed by the CSS, the Code Manager rates these risks to the service as high. In July 2023 there was a major incident with the CSS that was due to the cloud base infrastructure, so it is critical that this is appropriately assured.

As stated in section 4, this Change Proposal has had a derogation running alongside it to allow DCC to complete a CIO assessment rather than SOC for the REC PAB and Change team to evaluate the outcome of that assessment and determine if it still covered everything required by the REC for assurance purposes. As the CIO assessment focuses on the Cloud Service Customer rather than the Cloud Service Provider, there were controls that were flagged as not applicable. To ensure the integrity of the CSS, these controls are required by the REC and the Performance Assurance team so there can be confidence that the Cloud Service Provider is secure.

The Code Manager recognises that while SOC is an American driven assessment, it is an internationally accepted assurance standard for system security, availability, processing integrity, confidentially and privacy controls. As the CSS processes a huge amount of Consumer data on a daily basis and is a pivotal industry system, it is appropriate for strict controls to be in place to ensure the security of that information and system. It is also vital to provide public confidence in the energy industry as a whole.

12 CASE FOR CHANGE

The Code Manager does not consider there to be a robust positive case for change.

While there are no implementation or on-going costs associated with the Change Proposal and there is the potential for savings dependent on the assessment provider procured, there are risks to the assurance of the CSS.

Some crucial items would not be in scope of the assessment that are key due to the nature and volume of data handled by the CSS. It is key that there is adequate assurance in place to ensure the integrity of the CSS and public confidence that data is being handled appropriately and securely. There is also concern that without a specific assessment type, controls may not be correctly carried through year on year and items could be missed as there would not be a defined list of items to be assured. Lastly, the Code Manager believes that Microsoft would not agree to use another assessment type to assure the cloud base infrastructure as common practise is to use SOC reports.

Due to the undeterminable cost savings to the CSS Service Provider and the potential risks associated with the proposed solution (which could impact Consumers), the Code Manager cannot recommend approval of this Change Proposal at this time. This position will be reviewed post industry consultation and, if appropriate, a revised case for change will be presented in the Final Change Report.

13 CODE MANAGER'S RECOMMENDATION

The Code Manager recommends that the Technical Expert Panel **REJECT** the proposed change solution.

14 APPENDIX

CHANGE PROPOSAL	Link
LEGAL DRAFTING	Link

RETAIL ENERGY CODE

15 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.
Consumer	means any person supplied (or seeking a supply) of Energy at an RMP (whether or not that person also exports or is seeking to export electricity at an RMP).
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.
Data Communications Company (DCC)	means the person holding the DCC Licence.
Performance Assurance	means the activities undertaken by the Code Manager and the REC PAB in accordance with the Performance Assurance Schedule.
RECCo	means the company established under Clause 5 of the main body of this Code.