RETAIL ENERGY CODE

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

NON-CONFIDENTIAL CONSOLIDATED CONSULTATION RESPONSES

R0048 – DCC SERVICE ORGANIATION CONTROL 2 (SOC2) ASSESSMENTS

On 25 April 2024 the Code Manager issued a consultation to industry to seek feedback on the Preliminary Change Report for R0048 – DCC Service Organisation Control 2 (SOC2) Assessments.

The purpose of this document is to consolidate the responses and for the Code Manager to answer any questions raised within those responses.

DOCUMENT VERSION	1.0
RESPONSE TYPE	NON-CONFIDENTIAL
DATE ISSUED	
RESPONSIBLE COMMITTEE	Technical Expert Panel
LEAD ANALYST	Caroline Freimuller

DATE CONSULTATION ISSUED	25/04/2024
RESPONSE DEADLINE	20/05/2024

Question 1:	Do you agree with the Code Manager's assessment of the benefits and drawbacks of the R0048 solution? Do you have any further comments on the solution?	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	Given that the CSS is a core system of the industry, we believe that it is of critical importance for all the relevant essential parts of its infrastructure to be assured to an appropriately high standard. The CSS processes a large volume of data which are sensitive and, in that light, the integrity of its systems should be a paramount concern and international standards should be used to assure that integrity. We recognise the role of data security in maintaining consumer trust in the industry as a whole and it is imperative to have adequate assurance that the CSS Provider handles data appropriately and securely. We note that the CSS Service Definition currently specifies that a System and Organisation Controls Type 2 (SOC 2) assessment of the cloud-based infrastructure be undertaken. We believe that the current assurance standard is appropriate. We do not believe that this requirement should be downgraded and we do not support the proposal to remove it from the Service Definition.	Thank you for your comments, noted.
National Grid Energy Distribution (Distribution Network Operator)	Yes we agree with the Code Manager's assessment of the benefits and drawbacks of the R0048. Whilst we understand DCC wishing to have a proportionate level of assurance and best value for money, we do not feel that DCC have been able to demonstrate that an alternative assurance arrangement adequately mitigates the risks to information security.	Thank you for your comments, noted.

	Any replacement of the current requirements of a SOC Type 2 security certification by an independent assessment of CSS's cloud base infrastructure would have to be of a standard to comply with ISO/IEC 27001, which CSS has to be certified against. We do not see that DCC have been able to demonstrate that they will be able to provide that level of assurance under "an independently assessed" security certification.	

Question 2:	Do you agree that the proposed solution resolves the problem statement?	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	We do not agree with the proposal to remove the SOC 2 assessment requirement for the CSS's cloud-based infrastructure. We are concerned that its removal from the Service Definition would create unnecessary risk as, without a specific assessment type, controls may not be consistently assessed or applied to the degree necessary to assure an essential part of the CSS. In addition, the CSS Provider's proposal to replace the SOC 2 requirement with "independently assessed" in the Service Definition is excessively vague and does not offer the necessary clarity on the methodology and standards of assessment. We welcome the fact that the Type 2 assessment covers a defined timeframe, providing greater assurance that controls on how data is stored in the cloud are not only designed and implemented, but also whether they have operated effectively and as intended over that period. We note the Code Manager's statement that the CSS Provider delivered a "Competent	Thank you for your comments, noted.

	Independent Organisation" (CIO) assessment report as proposed alternative to a SOC 2 assessment report, and that the CIO report covered only the cloud service customer (Landmark – which manages the infrastructure) but not the cloud service provider (Microsoft – which provides the infrastructure). We do not believe that an assessment report which does not and cannot give assurance on the CSS's cloud-based infrastructure is an acceptable alternative to a SOC 2 assessment – nor do we believe that such a weaker assessment should replace the existing requirement of the Service Definition. In any event, we see no compelling rationale or evidence from the Data Communications Company, as proposer, for this change. We note that the terminology of "Competent Independent Organisation" is employed in connection with the Smart Energy Code, under which the DCC also provides services. Regardless of any potential desire by some for synergies, we believe that the assurance standard established in the CSS Service Definition for its cloud-based infrastructure is appropriate for the CSS.	
National Grid Energy Distribution (Distribution Network Operator)	No we do not agree that the proposed solution resolves the problem statement. As stated above any replacement of the current requirements of a SOC Type 2 security certification by an independent assessment of CSS's cloud base infrastructure would have to be of a standard to comply with ISO/IEC 27001, which CSS has to be certified against. We do not see that DCC have been able to demonstrate that they will be able to provide that level of assurance under "an independently assessed" security certification.	Thank you for your comments, noted.

Question 3:	Do you have any comments on the proposed legal text which sets out the proposed solution?	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	We note that this proposal consists of a simple, yet consequential change to the CSS Service Definition – replacing "'SOC Type 2'" with "independently assured" in Paragraph 11.3. However, we have substantial reservations about this replacement. It is unclear to us what "independently assured" would mean in practice, given that the change would replace a specific assurance standard with a vague statement. Given the importance of the CSS, we believe that the assurance standard for its cloud-based infrastructure should remain specified in the Service Definition and that it should be both robust and consistent. In turn, we do not believe that it would be appropriate for the CSS Provider to be given the discretion to set the assurance standard or to vary the standard. In our view, the SOC 2 assessment is the appropriate assurance standard for the CSS's cloud-based infrastructure.	Thank you for your comments, noted.
National Grid Energy Distribution (Distribution Network Operator)	The legal text changes need to reflect that an independently assessed security certification will be of a standard to comply with ISO/IEC 27001 for which CSS has to be certified against. Prior to any legal text changes DCC would need to demonstrate that an independent assessment adequately mitigates the risks to information security.	Thank you for your comments, noted.

Question 4:	Do you anticipate any benefits to your organisation or to the industry as a result of this change? If so, please provide details.	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	We recognize that there might be a savings benefit for the service provider. However, any savings will be outweighed by the risks the service and its users will be exposed to. Therefore we do not envisage any benefits to the CSS or service users by downgrading the assurance standard for the service's cloud-based infrastructure. Instead, we are concerned that the removal of the SOC 2 standard from Paragraph 11.3 would demonstrably weaken the controls of an essential part of a core system of the industry, which we do not believe would be prudent or appropriate.	Thank you for your comments, noted.
National Grid Energy Distribution (Distribution Network Operator)	As there has been no cost v benefit analysis made available, we are unable to fully answer this question. However, unless any achieved savings were passed back to industry we see no benefit.	Thank you for your comments, noted.

Question 5:	Do you agree with the Code Manager's assessment of the Change Path, that this Change Proposal should be subject to Self-Governance approval by the Technical Expert Panel?	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	We have no comments to make at this stage on the change path for this change proposal. However, given the vital nature of the CSS to the retail energy market, and the fact that this change proposal would weaken the assurance standard for an essential part of that service, we believe that RECCo and the Authority should be made aware of this proposal, if they have not been already.	Thank you for your comments, noted.
National Grid Energy Distribution (Distribution Network Operator)	Yes we agree.	Thank you for your comments, noted.

Question 6:	Do you agree with the Code Manager's recommendation, that the Change Proposal should be rejected by the Technical Expert Panel? If not, please explain why.	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	We believe that this proposal should be rejected, for the reasons that we have outlined elsewhere. No compelling rationale for this change has been provided, nor has a suitably clear definition of "independently assessed" been offered, and we see no justification for deviating from the currently established SOC 2 assessment requirement for the CSS's cloud-based infrastructure. It is a matter of concern to us that, due to the derogation granted to the CSS Provider as a consequence of raising this change proposal, a SOC 2 assessment of the cloud-based infrastructure has apparently not been undertaken. We recall the major incident affecting the CSS in July 2023 which involved its cloudbased infrastructure. Should this proposal be rejected, as we believe it should be, we hope and expect that the CSS Provider will deliver a SOC 2 assessment of this infrastructure as soon as possible.	Thank you for your comments, noted.
National Grid Energy Distribution (Distribution Network Operator)	Yes we agree that the Change Proposal should be rejected by the Technical Expert Panel. Any replacement of the current requirements of a SOC Type 2 security certification by an independent assessment of CSS's cloud base infrastructure would have to be of a standard to comply with ISO/IEC 27001, which CSS has to be certified against. We do not see that DCC have been able to demonstrate that they will be able to provide that level of assurance under "an independently assessed" security certification.	Thank you for your comments, noted.

Question 7:	Do you have any other comments relating to this Change Proposal?	
RESPONDENT DETAILS	**RESPONSE**	**CODE MANAGER COMMENTS**
Scottish Power Energy Retail (Energy Supplier)	No additional comments.	N/A
National Grid Energy Distribution (Distribution Network Operator)	No.	N/A