This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

DP103 'DCC SOC2 Assessments' Problem statement – version 0.1

About this document

This document provides a summary of this Draft Proposal, including the issue or problem identified, the impacts this is having, and the context of this issue within the Smart Energy Code (SEC).

Proposer

This Draft Proposal has been raised by Gordon Hextall on behalf of the Security Sub Committee (SSC).

What is the issue or problem identified?

What are SOC2 assessments?

Currently, SEC Sections G9.2-G9.7 requires the Data Communications Company (DCC) to undertake an annual Systems Organisation Controls 2 (SOC) 2 assessment to gain independent assurance of its compliance with the SEC security obligations and the security controls in place at DCC and its Service Providers.

Section G9.2 requires that the SOC2 assessment covers:

> *(a) all security risk assessments undertaken by the DCC in relation to itself and any DCC Service Providers;*
>
> *(b) the effectiveness and proportionality of the security controls that are in place in order to identify and mitigate security risks in relation to the DCC Total System; and*
>
> *(c) the DCC's compliance with:*
>
> > *(i) the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;*
> >
> > *(ii) the requirements of Sections G2 and G4 to G6 or any CPA Certificate Remedial Plan;*
> >
> > *(iii) such other requirements relating to the security of the DCC Total System as may be specified by the Panel (having considered the advice of the Security Sub-Committee) from time to time."*

SOC2 is a USA security audit standard that originates from the earlier USA SAS70 financial audits. As such it has proved difficult to align with the SEC security obligations. SOC2 provides no calibration of findings (i.e. observations are binary and are not related to risk or impact); this requires a great deal of subsequent investigation and follow-up.

Equally, since it is a fixed audit framework it is inflexible and therefore has proven extremely difficult to adapt to the DCC and its Service Providers. This leads to unnecessary and costly procedures e.g. for Assertion Statements from Service Providers. SOC2 does not provide the SSC with an equivalent assurance of DCC security compliance as User Security Assessments provide for Users.

The DCC is currently subject to the third such SOC2 assessment and the SSC considers that an alternate assessment methodology will provide greater value and assurance to the SSC and to Users.

What is the impact this is having?

The SOC2 Assessment is a burdensome assessment which provides no benefit to the DCC nor the SSC and does not provide adequate assurance for the wider Users who are dependent on the DCC meeting its SEC security obligations. Unnecessary cost is incurred in both undertaking the assessment and in complying with an assurance framework that does not relate to the SEC provisions.