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.

Paper Reference:	**SECP_76_1701_21**
Action:	**For Decision**

DP103 Problem Statement

1. Purpose

Draft Proposal DP103 'DCC SOC2 Assessments' was raised by the Security Sub-Committee (SSC) and has undergone the Development Stage. The Change Sub-Committee believes this Draft Proposal is ready to be converted to a Modification Proposal.

This paper sets out our proposed approach for progressing this modification for the Panel's approval. We are recommending that this modification be progressed to the Refinement Process, and that the Panel agrees the first package of work to be undertaken.

This paper provides a high-level summary of the key points. A copy of the problem statement submitted by the Proposer can be found in Appendix A.

2. Summary of the issue

SEC Sections G9.2-G9.7 require that the Data Communications Company (DCC) undertake an annual SOC2 assessment to gain independent assurance of its compliance with the SEC security obligations and the security controls in place at the DCC and its Service Providers.

However, SOC2 is a USA security audit standard that originates from financial audits. As such it has proven difficult to align with the SEC security obligations. SOC2 provides no calibration of findings which requires a great deal of subsequent investigation. Since it is a fixed audit framework it has also proven extremely difficult to adapt to the DCC and its Service Providers, leading to unnecessary and costly procedures.

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

3. Proposed progression

The Change Sub-Committee has agreed that this Draft Proposal is ready to be converted to a Modification Proposal. We believe that this modification should be progressed to the Refinement Process to allow for the development and assessment of a solution to the agreed issue.

The SSC has been working with the DCC to develop a suitable assessment methodology, but this will require a formal impact assessment from the DCC to confirm any costs or operational implications.

Work package and timetable

We propose the following first package of work to be undertaken during the Refinement Process:

Activity	Date
Document new assessment methodology with SSC and DCC	Jan 20 – Feb 20
DCC Preliminary Assessment	Feb 20
Discuss at March Working Group meeting	4 Mar 20
Update Panel on Progress	17 Apr 20

Areas of assessment

We do not believe there are any further questions that need to be considered in addition to the standard assessment areas.

4. Recommendations

The Panel is requested to:

- **AGREE** that DP103 is ready to be converted to a Modification Proposal;
- **AGREE** that MP103 should be progressed to the Refinement Process; and
- **AGREE** the first package of work and the timetable for MP103.

Adam Lattimore

SECAS Team

10 January 2020

Attachments:

- **Appendix A:** DP103 problem statement

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 1.0

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.