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.

MP103

‘DCC SOC2 Assessments’

Modification Report

Version 0.2

About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

If you have any questions on this modification, please contact:

Emmanuel Ajayi

020 8132 4134

emmanuel.ajayi@gemserv.com

1. Summary

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

Currently, SEC Sections G9.2-G9.7 require the Data Communications Company (DCC) to undertake an annual Systems Organisation Controls 2 (SOC2) assessment. The purpose of this is to gain independent assurance of compliance with the SEC security obligations and the security controls in place at the DCC and its Service Providers.

Since it is a fixed audit framework it is inflexible and therefore has proven extremely difficult to adapt to the SEC obligations for DCC and its Service Providers. The SOC2 assessment is a burdensome assessment which provides little benefit to the DCC nor the SSC. It does not provide adequate assurance for the wider Users who are dependent on the DCC meeting its SEC security obligations.

Changes to the legal text in Section G would enable the DCC to make necessary changes to replace SOC2 assessment with a more effective assurance regime.

This modification will not impact any SEC Parties other than the DCC and will have no costs to Parties. If approved, we recommend this modification should be implemented in the November 2020 SEC Release.

2. Issue

What are the current arrangements?

Section G9.2-G9.7 requires the DCC to undertake an annual SOC2 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."*

What is the issue?

Service Organisation Control 2 (SOC2) is a security audit standard that originates from the United States of America (USA) Statement on Auditing Standards 70 (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.

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 appropriate assurance of DCC security compliance.

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 little 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 and therefore delivers little value.

3. Solution

Proposed Solution

The SSC considers a more meaningful assessment would be the User Security Assessment process that applies on an annual basis for all Suppliers, Network Operators, Other Users and Shared Resource Providers. This would be a better measure of compliance against the specific SEC security obligations than can be achieved by a SOC2 audit with its fixed global structure of assessment that isn't tailored to the SEC.

The Security Assessment process for Users also allows for a Follow-up Assessment of aspects of non-compliance to ensure they have been satisfactorily addressed but this option does not exist for SOC2.

The proposed solution is therefore to retain the approach that requires the DCC to procure a DCC Security Assessment (whereby the procurement effort and cost of the assessment is for the DCC to bear) but to emulate the User Security Assessment process by adopting much of the legal text in Section G8 that applies to Users.

Such changes to the legal text in Section G9 would require the DCC to make necessary arrangements for the DCC to be assessed on an annual basis by a DCC Competent Independent Organisation (CIO) with the same characteristics of a User CIO. The SSC will develop a DCC Security Controls Framework (SCF) similar to the Users' SCF that sets out specifically what evidence the DCC CIO will look for to assess compliance against the SEC security obligations.

This solution will emulate the User Security Assessment process and:

- ensure a much more meaningful security assessment of the DCC and its Service Providers against specific SEC security obligations by a DCC CIO;
- provide more meaningful DCC CIO reporting of non-compliances for review by the SSC in the same way that applies to Users;
- allow for the DCC to produce a Management Response to any findings of actual or potential non-compliances;
- ensure that a DCC remediation plan is required as necessary and is monitored and reviewed by the SSC;
- allow for a Follow-up Security Assessment to be carried out where SSC considers it necessary to be satisfied that one or more non-compliances have been rectified; and
- ensure that any outstanding non-compliances are reported to the SEC Panel to consider whether there has been an Event of Default.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
	Large Suppliers		Small Suppliers
	Electricity Network Operators		Gas Network Operators
	Other SEC Parties	✓	DCC

The DCC will be the only party impacted as the modification aims to measure the operational effectiveness of the DCC's security controls.

DCC System

There is no impact on DCC systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section G 'Security'

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

Consumers

There is no impact on consumers.

Other industry Codes

There is no impact identified on other Codes.

Greenhouse gas emissions

There is no impact identified on greenhouse gas emissions.

5. Costs

DCC costs

There are no implementation costs to implement this modification.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

There will be no cost on SEC parties.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **5 November 2020** (November 2020 SEC Release) if a decision to approve is received on or before 22 October 2020
- **25 February 2021** (February 2021 SEC Release) if a decision to approve is received after 22 October 2020 but before 11 February 2020.

The November 2020 SEC Release is the first possible Release that this modification could be implemented.

7. Assessment of the proposal

Observations on the issue

The SSC and Working Group agreed on the initial assessment of the issue in the current SOC2 arrangements needing replacement.

Solution development

The solution proposed by the Proposer and explained in Section 3, is to adopt the User Security Assessment approach set out in SEC Section G8. This will be applied to the DCC security obligations in SEC Section G9. Once the SEC changes are implemented, the DCC will be obliged under the SEC to procure a DCC CIO with the assessment scope and the quality and independence characteristics agreed by the SSC. The SSC will also develop a DCC Security Controls Framework in the same way that currently applies to Users. The DCC will be subject to an annual independent assessment by a DCC CIO against their compliance with specific SEC security obligations in the same way that applies to Users.

Support for Change

The SSC facilitated the development of the legal text changes required. The Working Group agreed with the changes to the legal text.

Views against the General SEC Objectives

Proposer's views

Objective(f)[1]

The Proposer believes that this modification will better facilitate SEC Objective (f) as the implementation of a more appropriate audit will better ensure security.

[1] (f) ensure the protection of data and the security of data and systems in the operation of the SEC.

Appendix 1: Progression timetable

This Modification was presented to the Panel on 13 March 2020 and converted to a Modification Proposal. Following the Refinement Consultation, the Modification Report will be presented to Panel.

Timetable	
Event/Action	**Date**
Draft Proposal raised	18 Dec 19
Presented to CSC for final comment and recommendations	02 Jan 20
Panel converts Draft Proposal to Modification Proposal	17 Jan 20
Modification discussed with SSC	25 Mar 20
Modification discussed with Working Group	01 Apr 20
Refinement Consultation	11 May 20 -1 Jun 20
Update Panel	12 Jun 20
Modification Report Consultation	15 Jun 20 – 3 Jul 20
Change Board Vote	22 Jul 20

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CIO	Competent Independent Organisation
CPA	Commercial Product Assurance
CSC	Change Sub-Committee
DCC	Data Communications Company
SAS70	Statement on Auditing Standards 70
SCF	Security Controls Framework
SEC	Smart Energy Code
SOC2	Systems Organisation Controls 2
SSC	Security Sub-Committee
USA	United States of America