

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 1.0

19 June 2020



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.

Contents

1. Summary.....	2
2. Issue.....	4
3. Solution	5
4. Impacts	6
5. Costs	7
6. Implementation approach	8
7. Assessment of the proposal	9
Appendix 1: Progression timetable	10
Appendix 2: Glossary	11

This document also has two annexes:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex B** contains the full responses received to the Refinement Consultation.

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, this modification is targeted for implementation 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 will:

- 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; or
- **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 SEC Release that this modification could be implemented in.

7. Assessment of the proposal

Observations on the issue

The SSC and the 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. The Working Group had no comments on the solution.

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

Support for Change

The Working Group and the SSC supported the proposed solution.

A Network Party in the Refinement Consultation noted the change has no impact on them and should be implemented as possible to address the issue. Furthermore, the Network Party noted the legal text present is adequate to facilitate the change and added the Modification should be approved.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that this modification will better facilitate SEC Objective (f) ¹ as the implementation of a more appropriate audit will better ensure security.

Refinement Consultation Respondents' views

A SEC Party confirmed in the Refinement Consultation that the modification better facilitates SEC Objective (f) to ensure an auditable way of ensuring the protection of data and the security of the systems.

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 Report will be presented to the Panel on 19 June 2020 and then be issued for Modification Report Consultation.

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	19 Jun 20
Modification Report Consultation	22 Jun 20 – 10 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

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’

Annex A

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Section A ‘Definitions and Interpretation’

These changes have been drafted against SEC Section A Version 8.0.

Amend Section A as follows:

Certified Cyber Security Consultancy (CCSC)

means the scheme of that name which is administered by NCSC or any successor to that scheme.

DCC Independent Security Assessment Service Provider

has the meaning given to that expression in Section G9.3 (Procurement of the DCC Independent Security Assessment Service Provider).

Follow-up Security Assessment

has the meaning given to that expression in Section G8.19 (Categories of Security Assurance Assessment) for a User Security Assessment and in Section G9.17 for a DCC Security Assessment.

Section G ‘Security’

These changes have been drafted against SEC Section G Version 8.0.

Amend Section G7 as follows:

G7. **SECURITY SUB-COMMITTEE**

Establishment of the Security Sub-Committee

- G7.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section G7, to be known as the **“Security Sub-Committee”**.
- G7.2 Save as expressly set out in this Section G7, the Security Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub- Committees).

Membership of the Security Sub-Committee

- G7.3 The Security Sub-Committee shall be composed of the following persons (each a **“Security Sub-Committee Member”**):
- (a) the Security Sub-Committee Chair (as further described in Section G7.5);
 - (b) eight Security Sub-Committee (Supplier) Members (as further described in Section G7.6);
 - (c) two Security Sub-Committee (Network) Members (as further described in Section G7.8);
 - (d) one Security Sub-Committee (Other User) Member (as further described in Section G7.10);
 - (e) one Security Sub-Committee (Shared Resource Provider) Member (as further described in Section G7.12);
 - (f) one representative of the DCC (as further described in Section G7.15).
- G7.4 Each Security Sub-Committee Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Security Sub-Committee Member at the same time.
- G7.5 The **“Security Sub-Committee Chair”** shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:
- (a) the candidate selected is sufficiently independent of any particular Party or class of Parties;
 - (b) the Security Sub-Committee Chair is appointed for a [three-year] term (following which he or she can apply to be re-appointed);
 - (c) the Security Sub-Committee Chair is remunerated at a reasonable rate;
 - (d) the Security Sub-Committee Chair’s appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members); and

- (e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.
- G7.6 Each of the eight **“Security Sub-Committee (Supplier) Members”** shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):
- (a) be appointed in accordance with Section G7.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);
 - (b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and
 - (c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Supplier) Member”, references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.
- G7.7 Each of the eight Security Sub-Committee (Supplier) Members shall (subject to Section G7.14) be appointed in accordance with a process:
- (a) by which six Security Sub-Committee (Supplier) Members will be elected by Large Supplier Parties, and two Security Sub-Committee (Supplier) Members will be elected by Small Supplier Parties; and
 - (b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).
- G7.8 Each of the two **“Security Sub-Committee (Network) Members”** shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):
- (a) be appointed in accordance with Section G7.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);
 - (b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and
 - (c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Network) Member”, references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.
- G7.9 Each of the two Security Sub-Committee (Network) Members shall (subject to Section G7.14) be appointed in accordance with a process:

- (a) by which one Security Sub-Committee (Network) Member will be elected by the Electricity Network Parties and one Security Sub-Committee (Network) Member will be elected by the Gas Network Parties; and
- (b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.10 The **“Security Sub-Committee (Other User) Member”** shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

- (a) be appointed in accordance with Section G7.11, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);
- (b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and
- (c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Other User) Member”, references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

G7.11 The Security Sub-Committee (Other User) Member shall (subject to Section G7.14) be appointed in accordance with a process:

- (a) by which he or she is elected by those Other SEC Parties which are Other Users; and
- (b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.12 The **“Security Sub-Committee (Shared Resource Provider) Member”** shall:

- (a) be appointed in accordance with Section G7.13, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);
- (b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and
- (c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Shared Resource Provider) Member”, references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

G7.13 The Security Sub-Committee (Shared Resource Provider) Member shall (subject to Section G7.14) be appointed in accordance with a process:

- (a) by which he or she is elected by those Other SEC Parties which are Shared Resource Providers; and
- (b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.14 The following shall apply in respect of all candidates nominated or re-nominated for election as a Security Sub-Committee (Supplier) Member, Security Sub-Committee (Network) Member, Security Sub-Committee (Other User) Member or Security Sub-Committee (Shared Resource Provider) Member:

- (a) the Security Sub-Committee may, by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations, reject a candidate (by notifying the candidate of such rejection) where the Security Sub-Committee determines that the candidate does not satisfy one or more of the following requirements:
 - (i) the candidate must have been nominated by a company or other organisation, and the individual who submitted the nomination on behalf of the organisation must hold a senior position within the organisation;
 - (ii) the organisation which nominated the candidate must have confirmed that it is satisfied that the candidate has the relevant security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;
 - (iii) the organisation which nominated the candidate must have confirmed that the candidate has successfully completed a BS7858 security assessment (or a security assessment named by such organisation which the organisation confirms to be equivalent); and
 - (iv) the candidate must have sufficient security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;
- (b) a candidate who is rejected under paragraph (a) above shall not (subject to paragraph (c) below) be an eligible candidate for the relevant election;
- (c) where a candidate disputes a rejection notification under paragraph (a) above, the candidate shall have 3 Working Days following receipt of such notification to refer the matter to the Panel for its final determination of whether the candidate satisfies the requirements set out in paragraph (a) above; and
- (d) where necessary, the Secretariat shall delay giving notice of the names of eligible candidates pending expiry of the time periods set out in paragraph (a) and/or (c) or determination by the Panel under paragraph (c) (as applicable).

G7.15 The DCC may nominate one person to be a Security Sub-Committee Member by notice to the Secretariat from time to time. The DCC may replace its nominee from time to time by prior

notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation).

Proceedings of the Security-Sub Committee

G7.16 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section G7.17:

- (a) a representative of the Secretary of State and a representative of the Authority shall be:
 - (i) invited to attend each and every Security Sub-Committee meeting;
 - (ii) entitled to speak at such Security Sub-Committee meetings without the permission of the Security Sub-Committee Chair; and
 - (iii) provided with copies of all the agenda and supporting papers available to Security Sub-Committee Members in respect of such meetings;
- (b) the Security Sub-Committee Chair shall invite to attend Security Sub-Committee meetings any persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters.

G7.17 Subject to Section G7.16, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the Security Sub-Committee, for which purpose that Section shall be read as if references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

Duties and Powers of the Security Sub-Committee

G7.18 The Security Sub-Committee:

- (a) shall perform the duties and may exercise the powers set out in Sections G7.19 to G7.23; and
- (b) shall perform such other duties and may exercise such other powers as may be expressly ascribed to the Security Sub-Committee elsewhere in this Code.

Document Development and Maintenance

G7.19 The Security Sub-Committee shall:

- (a) develop and maintain ~~a documents~~, to be known as the "Security Controls Framework", which shall set out the appropriate User and DCC Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance) and be designed to ensure that such security assurance assessments are proportionate; and:
 - (i) achieve appropriate levels of security assurance in respect of different Users and different User Roles, and the DCC set out the appropriate User Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance); and

- (ii) ~~in the case of User related assessments are be designed to ensure that such security assurance assessments are proportionate;~~ consistent in their treatment of equivalent Users and equivalent User Roles, and ~~achieve appropriate levels of security assurance in respect of different Users and different User Roles;~~
- (b) carry out reviews of the Security Risk Assessment:
 - (i) at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System; and
 - (ii) in any event promptly if the Security Sub-Committee considers there to be any material change in the level of security risk;
- (c) maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;
- (d) maintain the End-to-End Security Architecture to ensure that it is up to date;
- (e) develop and maintain a document to be known as the "**Risk Treatment Plan**", which shall identify the residual security risks which in the opinion of the Security Sub-Committee remain unmitigated taking into account the security controls that are in place; and
- (f) liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs and HCALCs that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment.

Security Assurance

G7.20 The Security Sub-Committee shall:

- (a) periodically, and in any event at least once each year, review the Security Obligations and Assurance Arrangements in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;
- (b) exercise such functions as are allocated to it under, and comply with the applicable requirements of Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance);
- (c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of the Security Obligations and Assurance Arrangements;
- (d) keep under review the NCSC CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;
- (e) to the extent to which it considers it appropriate, in relation to any User (or, during the first User Entry Process, Party) which has produced a User Security Assessment Response that sets out any steps that the User proposes to take in accordance with Section G8.24(b):
 - (i) liaise with that User (or Party) as to the nature and timetable of such steps;

- (ii) either accept the proposal to take those steps within that timetable or seek to agree with that User (or Party) such alternative steps or timetable as the Security Sub-Committee may consider appropriate; and
 - (iii) take advice from the User Independent Security Assurance Service Provider; and
 - (iv) where the Security Sub-Committee considers it appropriate, request the User Independent Security Assurance Service Provider to carry out a Follow-up Security Assessment;
- (f) provide advice to the Panel on the scope and output of the independent security assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;
- (g) to the extent to which it considers appropriate, in relation to the DCC which has produced a DCC Security Assessment Response that sets out any steps that the DCC proposes to take in accordance with Section G9.24(b), provide advice to the Panel on the scope and output of the SOC2 assessment of the DCC Total System;
- (i) liaise with the DCC as to the nature and timetable of such steps;
 - (ii) either accept the proposal to take those steps within that timetable or seek to agree with the DCC such alternative steps or timetable as the Security Sub-Committee may consider appropriate;
 - (iii) take advice from the DCC Independent Security Assessment Service Provider; and
 - (iv) where the Security Sub-Committee considers it appropriate, request the DCC Independent Security Assessment Service Provider to carry out a Follow-up Security Assessment;
- (h) provide advice to the; Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance; and
- (i) Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance; and
 - (ii) DCC in relation to the appointment of the DCC Independent Security Assessment Service Provider, monitor the performance of the person appointed to that role and provide advice to the DCC in respect of its views as to that performance;
- (i) provide advice and information to the Authority in relation to any actual or potential non-compliance with the CPA Security Characteristics of any Device or apparatus in respect of which a CPA Certificate is issued or required.

Monitoring and Advice

G7.21 The Security Sub-Committee shall:

- (a) provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of security incidents and the management of vulnerabilities on their Systems;
- (b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;
- (c) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Security Obligations and Assurance Arrangements;
- (d) provide the Panel, the Change Sub-Committee, the Change Board and any relevant Working Group with support and advice in relation to any Draft Proposal or Modification Proposal which may affect the security of the End-to- End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;
- (e) advise the Authority of any modifications to the conditions of Energy Licences which it considers may be appropriate having regard to the residual security risks identified from time to time in the Risk Treatment Plan;
- (f) respond to any consultations on matters which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;
- (g) act in cooperation with, and send a representative to, the SMKI PMA, the Technical Architecture and Business Architecture Sub-Committee and any other Sub-Committee or Working Group which requests the support or attendance of the Security Sub-Committee;
- (h) (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the At HAN Forum on matters relating to the Alt HAN Arrangements which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;
- (i) provide such further support and advice to the Panel as it may request; and
- (j) provide the Authority with such information and documents as it may reasonably request in relation to any matter referred by a Party to the Authority for determination pursuant to Section F2.7B.

Modifications

G7.22 The Security Sub-Committee shall establish a process under which the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:

- (a) are likely to affect the Security Obligations and Assurance Arrangements; or
- (b) are likely to relate to other parts of the Code but may have a material effect on the security of the End-to-End Smart Metering System,

and the Code Administrator shall comply with such process.

G7.23 Notwithstanding Section D1.3 (Persons Entitled to Submit Draft Proposals):

- (a) the Security Sub-Committee shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where the Security Sub-Committee considers it appropriate to do so; and
- (b) any Security Sub-Committee Member shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where he or she considers it appropriate to do so (where the Security Sub-Committee has voted not to do so).

G7.24 Notwithstanding and subject to the provisions of the Working Group Terms of Reference, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

G7.25 For the purposes of Section D7.1 (Modification Report):

- (a) written representations in relation to the purpose and effect of a Modification Proposal may be made by:
 - (i) the Security Sub-Committee; and/or
 - (ii) any Security Sub-Committee Member (either alone or in addition to any representations made by other Security Sub-Committee Members and/or the Security Sub-Committee collectively); and
- (b) notwithstanding Section D7.3 (Content of the Modification Report), the Code Administrator shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.

Amend Section G8.6 as follows:

Suitably Qualified Service Provider

G8.4 The User Independent Security Assurance Service Provider shall be treated as suitably qualified in accordance with this Section G8.4 only if it satisfies:

- (a) one or more of the requirements specified in Section G8.5; and
- (b) the requirement specified in Section G8.6.

G8.5 The requirements specified in this Section G8.5 are that the User Independent Security Assurance Service Provider:

- (a) is a CTAS provider;
- (b) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or

- (c) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Panel substantially equivalent in status and effect to one or more of the arrangements described in paragraphs (a) and (b).
- G8.6 The requirement specified in this Section G8.6 is that the User Independent Security Assurance Service Provider:
- (a) employs consultants who are members of the Certified Cyber Professional (CPP) and the Certified Cyber Security Consultancy (CCSC) schemes at the 'Lead' or 'Senior Practitioner' level in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
 - (b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Amend Section G9 as follows:

G9. DCC SECURITY ASSURANCE

The DCC Independent Security Assessment Arrangements

~~G9.1~~—The DCC shall establish, give effect to, maintain and comply with arrangements, to be known as the "DCC Independent Security Assessment Arrangements", which shall:

~~(a)~~—have the purpose specified in Section G9.2; and

~~(b)~~—make provision for the DCC to take the actions specified in Section G9.3.

~~G9.1~~ The purpose specified in this Section G9.2 shall be the purpose of procuring the services of a DCC Independent Security Assessment Service Provider to undertake security SOC2-assessment services, of:

Scope of Security Assessment Services

~~G9.2~~ The security assessment services specified in this Section G9.2 are services in accordance with which the DCC Independent Security Assessment Service Provider shall:

~~G9.2~~—

(a) carry out DCC Security Assessments at such times and in such manner as is provided for in this Section G9; all security risk assessments undertaken by the DCC in relation to itself and any DCC Service Providers;

(b) produce DCC Security Assessment Reports in relation to the DCC that have been the subject of a DCC Security Assessment; 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) receive, consider and validate DCC Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee; the DCC's compliance with;

- (d) otherwise, at the request of, and to an extent determined by, the Security Sub-Committee, carry out an assessment of the compliance of the DCC with its obligations under:
 - (i) 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; and where:
 - (iii) following either a DCC Security Assessment, any material increase in the security risk relating to the DCC has been identified; or
 - (iv) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;
- (e) at the request of the Security Sub-Committee, provide to it advice in relation to:
 - (i) the compliance of the DCC with its obligations under Sections G or any CPA Certificate Remedial Plan; and
 - (ii) changes in security risks relating to the Systems, Data, functionality and processes of the DCC which fall within Section G5 (Information Security: Obligations on the DCC);
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);
- (e)(g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
 - (i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G9; the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
 - (i)(ii) assess the DCC's compliance with 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 Security Sub-Committee or the Panel (having considered the advice of the Security Sub-Committee) from time to time.

G9.3 The actions specified in this Section G9.3 shall be actions taken by the DCC to:

- (a) procure the provision of security ~~assurance-assessment~~ services by the DCC Independent Security ~~Assurance Assessment~~ Service Provider (as further described in Section G9.4);
- (b) ensure that the DCC Independent Security ~~Assurance Assessment~~ Service Provider carries out ~~SOC2-Security A~~ssessments for the purpose specified in Section G9.2:
 - (i) annually;
 - (ii) on any material change to the DCC Total System; and

- (iii) at any other time specified by the Security Sub-Committee or the Panel;
- (c) ~~consult with the~~ comply with the arrangements set out by the Panel, and obtain its approval, in respect of the scope of each such assessment before that assessment is carried out Security Sub-Committee in a Security Controls Framework;
- (d) in line with the methodology and processes set out in the Security Controls Framework:
 - (i) procure that the DCC Independent Security ~~Assurance Assessment~~ Service Provider produces a DCC Security Assessment Report following each such assessment that has been carried out;
 - (ii) ensure that the ~~DCC Independent Security Assessment Service Provider provides Panel~~ and the Security Sub-Committee ~~are provided~~ with a copy of each such DCC Security Assessment Report;
 - (iii) produce a DCC Security Assessment Response in relation to each such report; and
 - (iv) provide to the Panel and the Security Sub-Committee a copy of each DCC Security Assessment Response and, as soon as reasonably practicable thereafter, a report on its implementation of any action plan that is ~~required by the Security Sub-Committee~~ set out in that DCC Security Assessment Response.

The DCC Independent Security ~~Assurance Assessment~~ Service Provider

G9.4 For the purposes of Section G9.3, the "**DCC Independent Security ~~Assurance Assessment~~ Service Provider**" shall be a person who is appointed by the DCC to provide security ~~assurance assessment~~ services ~~and who~~:

- (a) ~~of the scope specified in Section G9.2 is qualified to perform SOC2 assessments;~~
- (b) ~~from a person who has been approved by the Security Sub-Committee, following consultation with it by the DCC, as otherwise being suitably qualified to provide security assurance services for the purposes of this Section G9; and~~
 - (i) is suitably qualified in accordance with Section G9.5;
 - (ii) is suitably independent in accordance with Section G9.8.

~~G9.5 The independence requirement specified in this Section G9.5 is that the DCC Independent Security Assurance Service Provider must be independent of the DCC and of each DCC Service Provider from whom the DCC may acquire capability for any purpose related to its compliance with the obligations referred to at Section G9.2(c) (but excluding any provider of corporate assurance services to the DCC).~~

Suitably Qualified Service Provider

G9.5 The DCC Independent Security Assessment Service Provider shall be treated as suitably qualified in accordance with this Section G9.5 only if it satisfies:

- (a) one or more of the requirements specified in Section G9.6; and

~~the requirement specified in Section G9.7 satisfies the independence requirement specified in Section G9.5.~~

(b) _____

G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:

(a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or

(b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to one or more of the arrangements described in paragraphs (a) and (b).

G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:

(a) employs consultants who are certified under the Certified Cyber Security Consultancy (CCSC) scheme and have experience of operating at the 'Lead' or 'Senior Practitioner' level in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and

(b)) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

Independence Requirement

G9.8 The DCC Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G9.8 only if it satisfies:

(a) the requirements specified in Section G9.9; and

(b) the requirement specified in Section G9.10.

G9.9 For the purposes of Sections G9.9 and G9.10:

(a) the DCC must be independent from the DCC Independent Security Assessment Service Provider in carrying out functions under this Section G9; and

(b) all of the DCC's Service Providers must be independent from the DCC Independent Security Assessment Service Provider in carrying out its functions to assess the DCC's compliance with its obligations as the DCC under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.10 The requirements specified in this Section G9.10 are that:

(a) neither the DCC or any of its subsidiaries, and no DCC Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assessment Service Provider;

- (b) no director of the DCC and no director of any DCC Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assessment Service Provider; and
- (c) the DCC Independent Security Assessment Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC or any of the DCC's Service Providers. (for these purposes references to the DCC's Service Providers shall not include the DCC Independent Security Assessment Service Provider where it acts in that capacity).

G9.11 The requirement specified in this Section G9.11 is that the DCC Independent Security Assessment Service Provider is able to demonstrate to the satisfaction of the Security Sub-Committee that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with the DCC or the DCC's Service Providers (and for these purpose a 'commercial relationship' shall include a relationship established by virtue of the DCC Independent Security Assessment Service Provider itself being a DCC Service Provider to the DCC).

Compliance of the DCC Independent Security Assessment Service Provider

G9.12 The Security Sub-Committee shall advise the DCC of any performance failures or non-compliance with the SEC obligations on the part of the DCC Independent Security Assessment Service Provider to enable the DCC to ensure that the DCC Independent Security Assessment Service Provider carries out its functions in accordance with the provisions of this Section G12.

DCC: Duty to Cooperate in Assessment

G9.13 The DCC shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the DCC Independent Security Assessment Service Provider), for the purposes of facilitating an assessment of the DCC's compliance with its obligations under Sections G2 and G4 to G6 or DCC Licence Condition 8 (Security Controls for the Authorised Business) or SEC Appendix Z Sections 6 and 7 and any CPA Certificate Remedial Plan.

G9.14 For the purposes of Section G9.13, the DCC shall provide the DCC Independent Security Assessment Service Provider with:

- (a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;
- (b) all such other forms of cooperation as may reasonably be requested, including in particular:
 - (i) access at all reasonable times to such parts of the premises of the DCC or its Service Providers as are used for, and such persons engaged by the DCC as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7; and
 - (ii) such cooperation as may reasonably be requested by the DCC Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G9.

Categories of DCC Security Assessment

G9.15 For the purposes of this Section G9, there shall be the following two categories of security assessment:

- (a) a Full DCC Security Assessment (as further described in Section G9.16);
- (b) a Follow-up DCC Security Assessment (as further described in Section G9.17).

G9.16 A "Full DCC Security Assessment" shall be an assessment carried out by the DCC Independent Security Assessment Service Provider in respect of the DCC and its Service Providers to identify the extent to which the DCC is compliant with each of its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.17 A "Follow-up DCC Security Assessment" shall be an assessment carried out by the DCC Independent Security Assessment Service Provider, following a DCC Security Assessment, in accordance with the provisions of Section G9.25.

DCC Security Assessments: General Procedure

DCC Security Assessment Methodology

G9.18 Each DCC Security Assessment carried out by the DCC Independent Security Assessment Service Provider shall be carried out in accordance with the Security Controls Framework developed as defined in G7.19(a).

The DCC Security Assessment Report

G9.19 Following the completion of a DCC Security Assessment, the DCC Independent Security Assessment Service Provider shall, in discussion with the DCC, produce a written report (a "DCC Security Assessment Report") which shall:

- (a) set out the findings of the DCC Independent Security Assessment Service Provider on all the matters within the scope of the DCC Security Assessment;
- (b) specify any instances of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 which have been identified by the DCC Independent Security Assessment Service Provider;
- (c) specify any instances of actual or potential non-compliance of the DCC with its obligations under DCC Licence Condition 8 (Security Controls for the Authorised Business);
- (d) specify any instances of actual or potential non-compliance of the DCC with its obligations under SEC Appendix Z, Sections 6 and 7; and
- (e) set out the evidence which, in the opinion of the DCC Independent Security Assessment Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified;

G9.20 The DCC Independent Security Assessment Service Provider shall submit a copy of each DCC Security Assessment Report to the Security Sub-Committee and to the DCC.

The DCC Security Assessment Response

G9.21 Following the receipt by the DCC of a DCC Security Assessment Report which relates to it, the DCC shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

- (a) produce a written response to that report (a "DCC Security Assessment Response") which addresses the findings set out in the report; and
- (b) submit a copy of that response to the Security Sub-Committee and the DCC Independent Security Assessment Service Provider.

G9.22 Where a DCC Security Assessment Report following a Full DCC Security Assessment, specifies any instance of actual or potential noncompliance of the DCC with its obligations under Sections G2 and G4 to G6 and / or with DCC Licence Condition 8 (Security Controls for the Authorised Business) and / or with SEC Appendix Z, Sections 6 and 7, the DCC shall ensure that its DCC Security Assessment response includes the matters referred to in Section G9.23.

G9.23 The matters referred to in this Section are that the DCC Security Assessment Response:

- (a) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assessment Service Provider and, where it does not, explains why this is the case;
- (b) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the DCC Security Assessment Report; and
- (c) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.

G9.24 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), the Security Sub-Committee (having considered the advice of the DCC Independent Security Assessment Service Provider) shall review that response and either:

- (a) notify the DCC that it accepts that the steps that the DCC proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the DCC Security Assessment Report; or
- (b) seek to agree with the DCC such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G9.25 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the DCC in accordance with Section G9.24(b), the DCC shall:

- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) report to the Security Sub-Committee on:

- (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;
- (ii) the completion of those steps in accordance with the timetable; and
- (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G9.26 Where a DCC Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G9.24(b), the DCC Independent Security Assessment Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the DCC to:

- (a) identify the extent to which the DCC has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) assess any other matters related to the DCC Security Assessment Response that are specified by the Security Sub-Committee.

DCC Security Assessments: Further Provisions

G9.27 The DCC Independent Security Assessment Service Provider may, in carrying out any DCC Security Assessment, take into account any relevant security accreditation or certification held by the DCC.

Setting the Compliance Status

G9.28 Following the completion of a Full DCC Security Assessment, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Security Assessment Response.

G9.29 The Security Sub-Committee shall identify whether any remaining non-compliances that exist with Section G2 or G4 to G6 and / or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and / or SEC Appendix Z, Sections 6 and 7 and shall, where appropriate:

- (a) note and record that there are no non-compliances; or
- (b) note and record the specific non-compliances that need to be addressed.

G9.30 Where the Security Sub-Committee identifies remaining non-compliances that exist with Section G2 and G4 to G6 and / or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and / or SEC Appendix Z Sections 6 and 7, it shall:

- (a) require the DCC to take the steps set out in Section G9.24: or
- (b) require a Follow-up Security Assessment as set out in Section G9.26.

G9.31 Where the Security Sub-Committee identifies any remaining non-compliances with Section G2 or G4 to G6 and / or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and / or SEC Appendix Z, Sections 6 and 7, it shall notify the Panel as required by G9.37(b).

CPA Certificate Remedial Plan Preparation

G9.32 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans. The DCC Independent Security Assessment Service Provider will assess the DCC's compliance with Appendix Z Section 6 and Section 7.

Disagreement with Security Sub-Committee Decisions

G9.33 Where the DCC disagrees with any decision made by the Security Sub-Committee in relation to it under Section G9.28 to G9.31, it may appeal that decision to the Panel. If the DCC disagrees with any decision made by the Panel, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

~~G9.6 For the purposes of Section G9.5, the DCC Independent Security Assurance Service Provider is to be treated as independent of the DCC (and of a relevant DCC Service Provider) only if:~~

- ~~(a) neither the DCC nor any of its subsidiaries (or such a DCC Service Provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assurance Service Provider;~~
- ~~(b) no director of the DCC (or of any such DCC Service Provider) is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assurance Service Provider;~~
- ~~(c) the DCC Independent Security Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC (or in any such DCC Service Provider); and~~
- ~~(d) the DCC Independent Security Assurance Service Provider is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has or may in future have with the DCC.~~

DCC Security Assessment Reports and Responses

~~G9.7 For the purposes of this Section G9:~~

- ~~(a) a "DCC Security Assessment Report" means a written report produced by the DCC Independent Security Service Provider following a SOC2 assessment carried out by it for the purpose specified in Section G9.2, which:~~
 - ~~(i) sets out the findings of the DCC Independent Security Assurance Service Provider on all the matters within the scope of that assessment;~~
 - ~~(ii) specifies any instances of actual or potential non-compliance of the DCC with the obligations referred to at Section G9.2(c) which have been identified by the DCC Independent Security Assurance Service Provider; and~~

- ~~(iii) — sets out the evidence which, in the opinion of the DCC Independent Security Assurance Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified; and~~
- ~~(b) — a "DCC Security Assessment Response" means a written response to a DCC Security Assessment Report which is produced by the DCC, addresses the findings set out in the report and, where that report specifies any instances of actual or potential non-compliance of the DCC with the obligations referred to at Section G9.2(c);~~
- ~~(i) — indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assurance Service Provider and, where it does not, explains why this is the case;~~
- ~~(ii) — sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance specified in the DCC Security Assessment Report; and~~
- ~~(iii) — identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.~~

Events of Default

~~G9.8~~G9.34 In relation to an Event of Default which consists of a material breach by the DCC of any of the obligations referred to at Section G9.2(c), the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G9.~~935~~ to G9.~~1541~~.

~~G9.9~~G9.35 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section G9.~~834~~, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any of the obligations referred to at Section G9.2(~~ed~~) (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

~~G9.10~~G9.36 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any of the obligations referred to at Section G9.2(~~ed~~), it shall refer the matter to the Security Sub-Committee.

~~G9.11~~G9.37 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "Security Sub-Committee".

~~G9.12~~G9.38 Where the Security Sub-Committee has:

- (a) carried out an investigation in accordance with Section M8.3; or
- (b) received a DCC Security Assessment Report concluding that the DCC is in actual or potential non-compliance with any of the obligations referred to at Section G9.2(c),

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any of the obligations referred to at Section G9.2(c) has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

~~G9.13~~G9.39 Where the Panel determines that an Event of Default has occurred, it shall:

- (a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and
- (b) determine the appropriate steps to take in accordance with Section M8.4.

~~G9.14~~G9.40 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

~~G9.15~~G9.41 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

CPA Certificate Remedial Plan Preparation

~~G9.16~~G9.42 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

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 ‘SOC2 Assessments’

Annex B

Refinement Consultation responses

About this document

This document contains the full non-confidential collated responses received to the MP103 Refinement Consultation.

Question 1: Do you agree with the solution put forward?

Question 1			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	Yes	We believe that this solution addresses the issue identified and will better facilitate SEC Objective (f) to ensure an auditable way of ensuring the protection of data and the security of the systems

Question 2: Will there be any impact on your organisation to implement MP103?

Question 2			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	No	-

Question 3: Will your organisation incur any costs in implementing MP103?

Question 3			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	No	-

Question 4: Do you believe that MP103 would better facilitate the General SEC Objectives?

Question 4			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	Yes	We believe that this modification will better facilitate SEC Objective (f) to ensure an auditable way of ensuring the protection of data and the security of the systems.

Question 5: Noting the costs and benefits of this modification, do you believe MP103 should be approved?

Question 5			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	Yes	-

Question 6: How long from the point of approval would your organisation need to implement MP103?

Question 6			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	N/A	This modification doesn't impact us and therefore we do not require any lead time, however we feel that this modification should be implemented as soon as possible to address this issue.

Question 7: Do you agree with the proposed implementation approach?

Question 7			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	Yes	-

Question 8: Do you agree that the legal text will deliver MP103?

Question 8			
Respondent	Category	Response	Rationale
Western Power Distribution	Network Party	Yes	-

Question 9: Please provide any further comments you may have.

Question 9		
Respondent	Category	Comments
Western Power Distribution	Network Party	-