Consultation

Retail Energy Code: Technical Specification approach consultation

APPENDIX 3: Security and data protection approach

Publication date:	29 November 2019	**Contact:**	Rachel Clark, Programme Director
		Team:	Switching Programme
Response deadline:	24 January 2020	**Tel:**	020 2901 3901
		Email:	switchingprogramme@ofgem.gov.uk

Any enquiries related to the text of this publication should be sent to Ofgem at:
10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at **www.ofgem.gov.uk**. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

1. Security approach

Section summary

This appendix sets out the proposed approach for managing security and data protection for the arrangements governed by the enduring REC. It incorporates the agreed Switching Programme requirements for communicating with the Central Switching Service as well as the requirements for non-switching arrangements that will be introduced through the Retail Code Consolidation (RCC) Significant Code Review (SCR).

Questions

Question 1: Do you agree with the approach set out in this document for developing the REC security and data protection arrangements?

Question 2: Do you agree with our approach to translating the CSS CoCo into the REC and, in particular, how we propose to establish obligations on both REC and non-REC parties?

Question 3: Do you agree that the requirements set out in 5.11 are set at the appropriate level and should be met by parties that want to access the REC enquiry services?

Question 4: Do you agree with our proposed approach to have a single assessment of a Market Participant's compliance with the information security and data protection requirements across all relevant REC services (prior to access being granted and on an ongoing basis)?

Question 5: Do you agree with our proposals to place requirements for maintenance of the DPIA and IRA, and implementation of the information security and data protection requirements and associated assurance, on the Code Manager?

1. Introduction

1.1. The June 2019 Switching Programme and Retail Code Consolidation (RCC) consultation[1] described the REC Security Operating Framework, stating that it would include details of:

- Roles and responsibilities – setting out the key roles required for the management of security in relation to all aspects of the end-to-end switching arrangements (and all other services included in the REC).
- Access control – for relevant parties able to use the systems and any communications channels, including the provision of user accounts to individuals.
- Security procedures – to prevent unauthorised access to the systems, the steps in place to prevent access to any communications between the relevant parties by any specified communications, and the procedures to follow in the event of a breach.
- Data retention – specifying the information to be retained as an audit trail with respect to receipt of transactions from relevant parties/users.

1.2. The June consultation envisaged a single document covering all aspects of the end-to-end switching arrangements, with core security requirements included in the main body. At the time it was acknowledged that security provisions relating to non-switching services would be included in service specific service definitions.

1.3. Further work has now been carried out to define the switching related security and data protection provisions based on recognised best practice standards, which has highlighted differences between each of the different Switching Data Services.[2] This has resulted in a change to our approach to developing the REC security and data protection provisions to reflect the fact that security requirements should be risk based and proportionate to the service in question, with a view that information relating to service specific access controls and other security measures to protect data held by the service should be included in the individual service definitions i.e. the process for assigning user names. It is also proposed that any obligations on users of the services should be included in a relevant REC schedule or a separate contractual agreement e.g. the enquiry service third party data access agreements. This is covered further in Sections 4 – 7 which set out proposals in relation to each of the key Switching Data Services.

1.4. The June consultation also highlighted the potential to include additional security arrangements in REC v1.1 to cover any requirements during the design, build and test

[1] https://www.ofgem.gov.uk/system/files/docs/2019/06/june19_switching_programme_and_retail_code_consolidation_consultation_final2.pdf

[2] Means each of the Central Switching Service, the Gas Retail Data Service, the Electricity Retail Data Service, the Smart Meter Data Service, the Smart Meter Comms Service, the Electricity Enquiry Service, the Gas Enquiry Service and the REC Data Service.

phase. This discussion is ongoing and has not been included in this paper, which focuses on the enduring provisions.

1.5. The high-level proposals in this paper, which includes an update on development of security provisions that have been delivered to date; and proposals for development of enduring security requirements, associated assurance provisions and overall governance arrangements have been reviewed by the Switching Programme Security Advisory Group (see Section 9 for further information on the governance groups), the Regulatory Design User Group (RDUG) and the REC Steering Group ahead of this consultation. This appendix contains our further thinking following these reviews.

2. Current REC Data Protection Provisions

2.1. REC v1.0 became effective in February 2019.[3] Section 19 includes general data protection provisions applicable to all REC parties, together with specific requirements placed on the CSS Provider as a Data Processor in Section 20.

2.2. It also acknowledges that the CSS Provider and each Energy Supplier, Gas Transporter and Distribution Network Operator is likely to process personal data as a Data Controller, and in some limited cases as joint Data Controllers with one or more other parties, including personal data concerning Consumers.

2.3. The REC provisions require each party to comply with the current Data Protection Legislation in the performance of the REC and specifically in relation to sharing personal data, including ensuring that it has a lawful basis for sharing personal data with another party.

2.4. In addition, specific requirements are placed on the CSS Provider in its role as a Data Processor, including a requirement to implement appropriate technical and organisational measures to protect that personal data against accidental or unlawful loss, destruction, damage, alteration or disclosure.

2.5. These provisions will need to be reviewed prior to the implementation of the RCC and Switching SCRs, to ensure that they adequately reflect all REC services (not just the CSS) taking into account the latest position held by the Security Board (see Section 9 for further information on the governance bodies) in line with the Information Risk Assessment (IRA) and Data Protection Impact Assessment (DPIA).[4]

3. Proposed Security and Data Protection Provisions

3.1. As highlighted in Section 2 above, there is an assumption that all REC parties and service providers will be required to process personal data and will need to comply with the Data Protection Legislation. It is therefore important to ensure that robust

[3] https://www.ofgem.gov.uk/system/files/docs/2019/02/retail_energy_code_designation.pdf

[4] The Switching Programme has developed and is maintaining an Information Risk Assessment and a Data Protection Impact assessment.

information security and data protection provisions are in place to minimise the risk of security breaches and information being accidently or deliberately compromised.

3.2. This includes:

- Requirements on users to have in place robust information security and data protection arrangements, to minimise the risk of security breaches;
- Controls to ensure data is only provided to appropriately authorised users; and
- Assurance arrangements to test the effectiveness of these controls.

3.3. We believe the level of requirements placed on users should be proportionate, based on the associated risks and mitigate3d through the application of recognised best practice methods. The sections below therefore explain the analysis that has been delivered since the June 2019 consultation, and our proposed approach for developing the required REC provisions in relation to each Switching Data Service.

Question 1: Do you agree with the approach set out in this document for developing the REC security and data protection arrangements?

4. Central Switching Service (CSS)

4.1. The CSS will receive data from Energy Suppliers and other Switching Data Services and provide data to all Market Participants and Switching Data Services (defined as CSS User). A key focus of the Switching Programme has been consideration of the information security and data protection risks associated with exchange of data between these organisations. This analysis has been supported by the Security Advisory Group (SAG) comprised of representatives from BEIS, DCC and other code bodies; with oversight from the Security Board, who has overall responsibility for the IRA and DPIA developed in relation to the CSS arrangements.

4.2. One of the main outputs of these considerations is the CSS Code of Connection (CoCo). DCC developed the CSS CoCo for approval by the Switching Programme Design Authority in September 2019. The CSS CoCo defines the responsibilities for the CSS and CSS Users relating to the exchange of data.

4.3. Much of the information within the CoCo provides useful background to the design decisions and guidance to CSS Users on the options available to them; however, it will not be required within formal REC documentation on an enduring basis5. Other information within the CSS CoCo places requirements on REC Parties and other CSS Users that will need to be captured within enduring REC provisions.

[5] It is proposed that this information be incorporated within guidance documentation maintained by DCC as the Switching Operator.

4.4. This section summarises the information set out within the CSS CoCo and details the proposed approach to reflecting this in the enduring REC provisions. Categories of provisions include:

- Requirements that CSS Users must meet before access will be granted;
- Access controls and onboarding requirements in place to prevent security breaches;
- Background information and guidance to support CSS Users understanding the overall approach and how it impacts them.

Requirements on CSS Users

4.5. Throughout the CoCo there are references to requirements that CSS Users must meet in order to gain access to interact with the CSS. As the CSS CoCo is not intended as an enduring document, a clear set of party obligations should be extracted from the CSS CoCo and included within the REC governance framework.

4.6. Where the requirements are placed on REC Parties, it is proposed that these requirements are incorporated within a relevant REC Schedule. We have considered whether this could be part of the Entry Assessment and Qualification Schedule, overseen by the Code Manager or a separate REC Onboarding and Maintenance Schedule with its own defined process.

4.7. The situation is more complicated for non-REC Parties such as Shippers, MAPs and Supplier Agents that receive messages from the CSS. Although these organisations are not required to accede to the REC in its entirety, we believe obligations should be placed on these organisations via a standalone schedule / agreement to ensure all CSS Users meet the agreed requirements. This would be a similar approach to the existing data access arrangements, where UNC and MRA Parties gain access to data held by the Enquiry Services as part of their accession to the relevant Code, whilst non-parties are required to sign a Third Party Data Access Agreement.

4.8. We believe that it is more efficient for the onboarding requirements to be included within the same place for REC Parties and non-REC Parties; and have therefore concluded that requirements on CSS Users will be specified in a REC Onboarding and Maintenance Schedule, rather than the Entry Assessment and Qualification Schedule. Non-REC Parties will be required to sign up to this schedule via a standalone agreement before receiving information via CSS messages. This agreement will incorporate legal obligations relating to, for example, confidentiality, liabilities and third-party rights.

4.9. In terms of the specific requirements that will be placed on CSS Users within the REC Onboarding and Maintenance Schedule; the CSS CoCo identifies a requirement for CSS Users to complete a registration process (to be determined during the Design Build and Test phase of the Switching Programme) and apply for the relevant certificates and digital signatures to ensure data exchange is secure.

4.10. We propose that this registration process will form the basis of the requirements set out within the REC Onboarding and Maintenance Schedule and will be developed in Q1

2020, alongside the non- party agreement, for inclusion in the Spring 2020 consultation.

4.11. The remaining question is who administers this process and how it fits in with the entry assessment provisions. This question has been considered further in Section 8.

Service Definition

4.12. Most of the remaining provisions in the CoCo which are required to form part of the enduring REC framework will be included in the CSS Service Definition. The provisions in the CSS Service Definition will include high level information defining the CSS and demonstrating how the CSS controls access to the service.

4.13. A summary of the key provisions includes:

- A description of the CSS users and associated interfaces.
- High level information on the options for sending and receiving CSS messages i.e. via the public internet or a private network utilising Microsoft ExpressRoute.
- The authentication requirements including the establishment of a secure communications channel and the application of digital signatures to CSS messages. This process requires CSS Users to apply for security certificates. The actual process will be reflected in the REC Onboarding and Maintenance Schedule and will be delivered by a Certificate Authority, explained further in paragraph 4.15.
- Information regarding back up facilities in place to ensure a robust business continuity approach.
- Information regarding the CSS security measures, including the fact that CSS itself is certified against ISO/IEC 27001 and is subject to certification using a UKAS-certified auditing body.
- Non-functional requirements reflected within the CSS service levels.

4.14. These CSS provisions have been included within the draft CSS Service Definition See Annex 2 of Appendix 2.

4.15. The CSS CoCo also references the requirement for a CSS Certificate Authority (CCA) to provide each CSS User with new and updated security certificates, together with the associated public and private keys to enable the exchange of data with CSS. A procurement exercise for the CCA is expected to progress in parallel with this consultation. Once the procurement is complete, a CCA Service Definition will be developed which will incorporate the relevant provisions from the CSS CoCo.

Background and Guidance

4.16. A large part of the CoCo covers background information setting out the rationale for the security and onboarding requirements. For example, information regarding the options for CSS Users to use internet access or a private network to exchange data with the CSS; and consideration of additional options open to CSS Users deciding how to deliver their REC obligations, such as the use of a switching adaptor services.

4.17. Whilst this information is not required within the REC itself, it does provide useful guidance for new entrants to understand the different options available to them and the rationale for the existing provisions. It is therefore proposed that a guidance document is developed covering CSS access arrangements. This should be developed and maintained by the DCC as part of the wider knowledge base products, defined within the Baseline Statement as Category 3 documents (see main body of the consultation for further information on the change management approach).

Question 2: Do you agree with our approach to translating the CSS CoCo into the REC and, in particular, how we propose to establish obligations on both REC and non-REC parties?

5. Gas and Electricity Enquiry Services (GES and EES)

5.1. The GES as defined in the REC, is the equivalent to the existing gas Data Enquiry Service (DES) as defined in the UNC; and the EES as defined in the REC, is the equivalent to the existing Electricity Central Online Enquiry Service (ECOES) as defined in the MRA.

5.2. Existing UNC and MRA provisions relating to these services define requirements on users to ensure data accessed via the enquiry services is managed appropriately. Third Party Access Agreements are utilised for non-UNC / MRA Parties, which reflect the requirements on users relating to the handling of data and associated liabilities should security breaches occur. This section explains our proposed approach to developing the enduring REC provisions.

Requirements on Enquiry Service Users

5.3. The work we have undertaken to transfer the existing provisions into the relevant REC Schedule (the Data Access Schedule) and the GES / EES Service Definitions has raised concerns that there are currently different arrangements in gas and electricity with a lack of transparency over the specific requirements that organisations have to comply with before being granted access to data.

5.4. Bringing both the EES and GES within a single governance regime enables greater harmonisation between the two services and has highlighted this inconsistency as a point that warrants further consideration. Having assessed the two services, we do not believe the risks associated with data access under the separate services are different and therefore we see no justification for different requirements to be included on Enquiry Service Users. We also believe the requirements on REC Parties should not differ from the requirements on non-REC Parties.

5.5. We proposed in the June 2019 consultation that a dual fuel access agreement template should be included as an appendix to the Data Access Schedule, ensuring clear, consistent and transparent requirements are placed on all gas and electricity Energy Service Users. Work is progressing with the development of this template, in consultation with Xoserve and Gemserv; with the aim of including this in an updated Data Access Schedule in the Spring 2020 consultation.

5.6. In order to determine the specific requirements that should be placed on Enquiry Service Users, we note the work completed under the midata project which has considered the level of risk associated with access to Consumer data and sought to determine both an acceptable level of security requirements (referred to as accreditation) and also a robust and proportionate assurance regime (covered further in Section 8). Whilst the midata analysis focused on the implementation of a midata solution including access to tariff data which is not currently held within the existing enquiry services; we believe the principles set out within this analysis equally apply to the existing enquiry services which are expected to form part of any enduring midata solution. Further detail of the midata analysis and conclusions is therefore set out below and in Annex 1.

5.7. The midata analysis recognised that the development of an accreditation and assurance mechanism does not take place in a policy vacuum. Any potential requirements should be cognisant of, and not duplicate nor 'gold plate', the range of existing legislative requirements[6] on parties that access and handle data. The Information Commissioner's Office (ICO) (as the Competent Authority for data protection) has produced extensive guidance[7] to help organisations understand their legal obligations and develop compliant processes in line with good practice.

5.8. The primary objective for any accreditation and assurance framework, is ensuring, in a manner that delivers robust value for money and without unnecessary gold plating, that data is used only with a sound legal basis, such as with verified Consumer consent; and in a manner which is legally compliant, to minimise risk of data breach & data misuse.

5.9. Whilst the realisation of data protection risks, such as data breaches and subsequent misuse, could have significant, detrimental and long-lasting impacts on stakeholder confidence in energy market data access; regulatory enforcement of legislative data protection breaches is the remit of the relevant competent authority, in this case the ICO. It should therefore be noted that the proposed accreditation and assurance framework is not in any way duplicating the activities of other competent authorities in enforcing legislative compliance. The framework is establishing a series of requirements for users to access the data, which provide a proxy for legal and good practice compliance, and a mechanism to assure their compliance with such requirements.

5.10. It is recognised that any accreditation framework needs to balance the rigor of the requirements that applicants have to meet prior to gaining access to the ecosystem and the assurance regime that checks compliance on an initial and enduring basis.

5.11. The detailed analysis of accreditation and assurance options carried out by the midata team has been included in Annex 1. The conclusions from this work are that each user would have to meet the following requirements before gaining access to data:

[6] For example, General Data Protection Regulation 2018, Data Protection Act 2018, Privacy & Electronic Communications Regulations (PECR) and Security of Network & Information Systems Regulations 2018

[7] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

- Compliance with the ICO's checklists as evidenced by a statement signed by a company director;
- Evidence of payment of the relevant fee to the ICO where they are expecting to be a Data Controller[8];
- Demonstrate compliance with the best-practice Cyber Essentials[9] standard (self-assessment version) developed by the UK's National Cyber Security Centre (NCSC) – which helps organisations guard against the most common cyber threats and demonstrate their commitment to cyber security; and
- Have appropriate training mechanisms for personnel with access and appropriate controls to ensure data was only used within the terms of their access arrangements.

5.12. Although this work focused on the midata solution, it was acknowledged that access to the majority of data required under the initial midata use case (tariff comparison) was already available via ECOES and DES and that this proposed accreditation and assurance regime could therefore apply to those services.

5.13. We therefore propose that the enduring REC enquiry service provisions should include requirements on Enquiry Service Users in line with those descried in paragraph 5.11 above. These requirements would be included within the Data Access Schedule as part of the proposed Data Access Agreement.

Question 3: Do you agree that the requirements set out in 5.11 are set at the appropriate level and should be met by parties that want to access the GES and EES?

Service Definition

5.14. Draft GES and EES Service Definitions have been included in Annex 5 and 6 of Appendix 2 based on existing service documentation, which has been adapted to reflect the REC structure and take into account new service levels required following CSS go-live. These sit alongside the Data Access Schedule which defines the process by which users gain access to data and the Data Access Matrix which sets out the data that different types of party can access.

5.15. The GES Service Definition has therefore been drafted based on existing DES documentation included within the Security Operating Framework which forms part of the UK Link Manual (alongside information relating to other aspects of the service delivered by Xoserve as the Central Data Service Provider (CDSP)). Similarly the EES Service Definition is based on the existing ECOES provisions included in MRA Agreed Procedure 15 and the User Requirements Specification (URS).

[8] Note – further consideration of whether different categories of Enquiry Service User will be a Data Controller is required.
[9] https://www.cyberessentials.ncsc.gov.uk/

5.16. Both of these service definitions include the following provisions relating to information security and data protection:

- Access controls which limit data available based on user type as reflected in the Data Access Matrix;
- User authentication based on provision of a username and password to ensure only authorised users can access the data;
- Encryption of data accessed via the API service using a common standard;
- Data handling provisions including data retention and system audit;
- Information regarding back up facilities in place to ensure a robust business continuity approach.
- Non-functional requirements reflected within the relevant service levels.

6. Gas and Electricity Retail Data Service (GRDS and ERDS)

6.1. The key function of the GRDS and ERDS is to provide an interface between various Market Participants and REC / non-REC services. The approach to delivering each of these interfaces, and therefore the associated security arrangements, is set out below:

- CSS Provider– the main ERDS and GRDS interface is between itself and the CSS. For this purpose the ERDS and GRDS are both classified as CSS Users and the CSS security requirements apply, as reflected in Section 4 above.
- Distribution Network Operators (DNOs) and Independent DNOs (iDNOs) – the ERDS is a service delivered by individual DNOs and iDNOs, therefore there is no physical interface.
- Supplier Meter Registration Agent (SMRA) – the SMRS is also a service delivered by individual DNOs and iDNOs, therefore there is no physical interface required between the ERDS and the SMRS.
- Supplier Volume Allocation Agent (SVAA) – the ERDS receives electricity Market Participant Data from the SVAA via a data flow transferred via the Data Transfer Network which requires the ERDS to have a DTN connection. The associated security requirements form part of the Data Transfer Service Agreement.
- Central Data Service Provider (CDSP) - the CDSP delivers the central data service on behalf of Gas Transporters (GTs) and Independent GTs (iGTs), therefore there is no physical interface required between the GRDS and the CDSP.

- Smart Data Service Provider (DSP) – the interface with the Smart DSP is defined within the Smart Energy Code; therefore, the security requirements in relation to this interface reflect SEC requirements.

- Green Deal Central Charge Database Provider (GDCC) - the interface with the GDCC utilises the DTN, with security information reflected in the DTSA as per the SVAA interface detailed above.

- Electricity Supplier – the interface with Electricity Suppliers utilises the DTN, with security information reflected in the DTSA as per the SVAA interface detailed above.

6.2. It is not anticipated that the ERDS / GRDS service definitions will include any specific security provisions relating to data in motion. However, they will include provisions relating to data handling activities such as data retention and system audits.

7. Other Switching Data Services

Switching Operator Service

7.1. The Switching Operator Service has been defined as a separate service to the CSS itself and is delivered by DCC to reflect its responsibilities in relation to the overall switching arrangements. The service utilises two main applications: the Switching Portal which enables Market Participants and other interested parties to access information relating to the switching arrangements and raise incidents or service requests for action; and also the Switching Service Management System which stores and manages all incidents, requests, changes and queries for the switching arrangements.

7.2. The expectation is that a Service Management CoCo will be developed setting out the access requirements relating to both the switching portal and the service management system. As with the CSS CoCo, these provisions will be included within the Switching Operator service definition and potentially the proposed new REC Onboarding and Maintenance Schedule if obligations are placed on users.

7.3. At present, high level details of the access arrangements have been included in the Switching Operator Service Definition (see Annex 1 of Appendix 2).

Smart Meter Data Service

7.4. This service is delivered by the DCC action as the smart Data Service Provider. Given the level of security requirements associated with the smart metering provisions, the interfaces with the CSS will be required to meet the smart metering security requirements as defined in the SEC.

REC Data Service

7.5. This service, delivered by the Code Manager, will be responsible for provision of REC Governance Data to Market Participants and Switching Data Services. Interfaces with the CSS are expected to be covered by the provisions within the CSS CoCo / CSS service definition as set out in Section 4. Interfaces with industry will be developed following procurement of the service.

Non Switching Services

7.6. In addition to the switching services detailed above, the REC will include non-switching services e.g. the Energy Theft Tip Off Service. Security requirements will be included within each individual service definition, where relevant. Consideration will also be required on the security and data protection requirements for the Code Manager, PAB and any other governance groups that are managing sensitive data.

8. Assurance Provisions

8.1. In addition to requirements placed on service users and controls included within the services themselves; we have also considered the requirements for assurance arrangements to assess user's compliance with the information security and data protection requirements prior to access being granted to relevant REC service and on an ongoing basis. This consideration has focussed on the CSS and Enquiry Services as we are expecting to include a clear set of user requirements for these services, as set out in Sections 4 and 5 above.

Initial Assessment

8.2. The CSS CoCo requires CSS Users to provide evidence of compliance with the CoCo directly to the DCC security team before connection is permitted. Similarly, requirements are placed on Enquiry Service Users before access to data via the EES and GES is granted. Rather than new entrants being subject to multiple information security audits under the REC, we believe that there should be a single information security and data protection assessment, to be delivered by the Code Manager (or a service provider on their behalf) as part of the overall REC entry assessment arrangements.

8.3. It is acknowledged that the information security requirements for the CSS, EES and DES may be slightly different; however, these specific requirements would be clearly set out within the relevant REC schedule or access agreements. An independent audit would validate that each of these requirements have been met with a report available that the applicant could provide to the CSS, EES and GES Providers as part of the onboarding activities e.g. in order to receive the required keys / user login details.

8.4. This approach minimises duplication across multiple services within the REC; whilst still enabling each service provider to gain comfort that users of its service have robust information security provisions in place e.g. the relevant service provider will identify specific requirements that must be in place, such as systems and processes being as a minimium compliant with ISO/IEC 27001 requirements; and the assessment will confirm whether these requirements are being met.

8.5. In delivering this assessment, the Code Manager will be required to take into account assurance activities undertaken outside of the REC, for example reliance could be placed on the SEC information security audit; or where a user has ISO/IEC 27001 accreditation and has been certified under this mechanism, the REC information security assessment will place reliance on this certification process.

Ongoing Assessment

8.6. Where there are requirements for ongoing assessment, then this will also be delivered by the Code Manager (or a service provider on their behalf) based on the schedule of assessments required for each service.

8.7. Further detail regarding enduring CSS assurance requirements will be developed during Q1 2020.

8.8. With regards to the EES and GES, the processes in place to assess ongoing compliance with the terms of access differ: in electricity, users are required to undergo an initial audit before access is granted, with annual audits thereafter; whereas, in gas, there is no requirement for regular audits, although Xoserve does have a right to audit if there are data protection or information security concerns.

8.9. In order to determine the appropriate level of ongoing assurance, we have considered the analysis undertaken by the midata team (as set out in Section 5 and Annex 1).

8.10. The midata work concluded that ongoing assurance should be accomplished via an annual audit consisting of an internal assessment with director level self-certification of compliance each year, with an external audit every three years. The reflects a mid-point between the existing arrangements and would effectively reduce the level of assurance currently delivered under the MRA, with internal audits for two out of every three years; whilst increasing the assurance for gas users who have no annual audit requirements.

8.11. Although this work focused on the midata solution, the principle equally applies to the enquiry services. We therefore believe that the proposed midata assurance model should be adopted for the enquiry services under the REC.

Question 4: Do you agree with our proposed approach to have a single assessment of a Market Participant's compliance with the information security and data protection requirements across all relevant REC services (prior to access being granted and on an ongoing basis)?

9. Enduring Governance

9.1. The Switching Programme has established a Security Advisory Group to advise on security issues; and a Security Board to determine the acceptable level of risk and maintain the CSS DPIA and IRA. We believe that the DPIA and IRA are key documents that should be maintained following CSS go live; and extended beyond the CSS itself, to cover the Enquiry Services and any other services handline personal data e.g. theft provisions.

9.2. We have therefore been considering the requirements for ongoing security governance provisions. Three options have been identified:

- Option 1: Establish an enduring Security and Data Protection Board with responsibility for establishing and maintaining a DPIA and IRA across the whole suite of REC services (noting that a switching specific DPIA and IRA has already been developed). This Security and Data Protection Board would also be responsible for defining the scope of the information security and data protection audit and considering changes to specific system onboarding provisions included in the relevant service definitions, operational schedules and access agreements;

- Option 2: Include information security responsibility within the scope of the Performance Assurance Board (PAB) with support provided by the relevant technical group and legal advisors; or

- Option 3: Place requirements for maintenance of the DPIA and IRA, and implementation of the information security and data protection requirements and associated assurance, on the Code Manager; noting that the Code Manager may procure specialist resource to support these activities.

9.3. Given the scope of the work already assigned to the PAB and the specialist knowledge and expertise required to consider security and data protection issues; we do not believe that maintenance of DPIA and IRA should be included within its scope. However, we do believe the PAB should have a role in overseeing the assurance arrangements delivered by the Code Manager as part of the overall entry assessment and ongoing assurance requirements under the REC.

9.4. One of the key principles of the enduring REC governance framework is to place less reliance on standing groups, to ensure industry, and other procured resource, is used effectively. We therefore believe that Option 3 should be introduced, and the Code Manager should have overall responsibility for maintaining the DPIA and IRA rather than establishing a standalone Security and Data Protection Board. A technical working group could be established as and when required to review the DPIA and IRA. Given the importance of these documents, it is proposed that they should be classified as Category 1 products requiring RECCo Board approval.[10]

Question 5: Do you agree with our proposals to place requirements for maintenance of the DPIA and IRA, and implementation of the information security and data protection requirements and associated assurance, on the Code Manager?

[10] See main body of the consultation for further information on the proposed REC change management arrangements.

10. Development Roles and Responsibilities

10.1. This approach document highlights a number of deliverables / activities that must be developed during 2019 / 2020. This section summarises each of the key deliverables and the organisation(s) responsible for delivery:

- Security and Data Protection Approach – (This paper) sets out the proposed approach to security and data privacy consideration, covering both CSS and non-CSS requirements. Ofgem's Switching Programme has developed this document with proposals reviewed by the Security Advisory Group and RDUG and presented to the REC Steering Board prior to this consultation.

- Service Definition Documents – service definitions for each switching and non-switching service have been developed by the relevant service provider in accordance with the Service Definition Approach. These service definitions will include relevant security provisions defined in accordance with the overall security approach e.g. the CSS service definition should be consistent with the CSS CoCo. Ofgem's Switching Programme is responsible for the overall delivery of the service definitions, with drafting developed by the individual service providers. Several service definitions have been developed for consultation (see Appendix 2). Others will be developed for consultation in Spring 2020. Prior to consultation they will be reviewed by RDUG and the Regulatory Group.

- REC Onboarding and Maintenance Schedule – This paper proposes that specific requirements on CSS Users are included in a REC Onboarding and Maintenance Schedule. Subject to responses to this consultation, the development of the REC Onboarding and Maintenance Schedule will commence in 2020. The Ofgem Switching Programme is responsible for developing the schedule in consultation with DCC and the Security Advisory Group. The draft schedule will be reviewed by the RDUG and the Regulatory Group prior to the Spring 2020 consultation.

- Ongoing Assurance Provisions – This paper sets out a proposed approach to enduring assurance. Subject to responses to this consultation, development of the assurance provisions will commence in 2020 and may include, for example, a service definition for an information security audit, or separate service definitions if separate audits are required under each service. The Ofgem Switching Programme is responsible for setting the scope of the enduring assurance provisions and developing the required documentation in consultation with the RECCo Board, relevant service providers and the Security Advisory Group. The output will be reviewed by the RDUG and the Regulatory Group / REC Steering Board prior to the Spring 2020 consultation.

- Ongoing Governance Arrangements – This paper sets out proposals in relation to enduring governance. If, taking into account responses to this consultation, it is determined that an enduring Security and Data Protection Board is required, the Ofgem Switching Programme will define the terms of reference in consultation with the RECCo Board and the SAG. The terms of reference would be reviewed by the RDUG and the Regulatory Group / REC Steering Board prior to the Spring 2020 consultation.

10.2. Although the delivery of some activities for RCC and Switching go live will be the responsibility of code bodies and / or the RECCo Board, Ofgem will retain oversight of each element to ensure delivery in line with the proposed timeline set out in Section 11.

11. Proposed Timeline

Date	Activity
Summer 2019	Development of Security and Data Protection Approach.
Summer 2019	Development of CSS CoCo.
Autumn 2019	Industry consultation on overall approach and enduring assurance and governance arrangements.
Feb 2020	Ofgem decision on way forward post consultation.
Jan – April 2020	Development of required REC provisions e.g. REC Onboarding and Maintenance Schedule, information security audit requirements, Security Board terms of reference (if required).
Spring 2020	Ofgem consultation on REC provisions.
Q3 2020	Baseline REC drafting
Nov 2020	REC SCR changes finalised for approval
Apr 2021	RCC SCR implemented with appropriate security arrangements
CSS go live	Full enduring switching security provisions effective

Annex 1 – Midata Accreditation and Assurance Analysis

1. Accreditation options

1.1. The range of options considered by this analysis span the spectrum of current accreditation regimes within the energy sector and wider industries. The options have been considered within the relevant context, e.g. the new data protection regime, the need to be cognisant of impending strategic regulatory shifts in the sector and developments of cross-sectoral accreditation regimes under BEIS' Smart Data Review. The options have been developed in the context of the midata project. We think that there is a strong case for adopting equivalent proposals for the enquiry service provisions under the REC. However, work will be undertaken in Q1 2020 to define the enquiry service requirements, taking into account responses to this consultation.

1.2. Five options were considered, each building on the design elements of the previous options and escalating the requirements on users in steps by referencing external checklists and standards. The options focus on the desired management controls, and their integration into the third parties' business as usual activities, to manage data protection and cyber security risks.

- **Option 1** – 'do nothing'; under this option no bespoke compliance requirements are introduced on users. Access will be underpinned by a base expectation of compliance with relevant legislative requirements and would effectively be open access to users that complete the registration process. Whilst this expectation should ensure suitable management controls to deliver legal compliance, there is no mechanism to verify an organisation's understanding of their obligations nor of their management of such obligations.

- **Option 2** – 'risk based ICO self-assessment'; under this option a population of higher risk users, identified on the basis of either historic enforcement action in the data protection sphere or expected/actual number of data calls under the framework, would be required to certify via a company director their 'successful implementation', or 'not applicable', of all the points on the relevant ICO self-assessment checklists[11], depending on their business model.

  This approach is proposed to mitigate the data protection risks associated with higher risk organisations through the use of the regulator's 'good practice' checklists and utilising the gravitas of directors' compliance statements which are subject to the provisions of the Fraud Act (2006) and Companies Act (2006). The ICO's checklists should be considered a mix of legislative compliance and industry good practice, effectively establishing a baseline for stakeholders' expectations of well-run organisations active in this area. It should be noted, however, that some legally compliant organisations may not be able to positively answer all the checklist questions, but this should be a relatively small proportion. The checklists are centrally maintained by the ICO

[11] ICO self-assessment checklists - https://ico.org.uk/for-organisations/data-protection-self-assessment/

in line with evolving regulatory requirements, thereby removing the need for the detailed requirements to be managed within the Code

In addition, all users who are acting as Data Controllers would be required to be listed on the ICO's Register of Fee Payers (as evidence of having paid the relevant data protection fee to the ICO). This is required as a high-level proxy for organisations understanding their data compliance obligations.

Whilst this option mitigates Consumers' exposure from higher risk organisation, through the lens of the ICO's checklists, the broader narrative about enabling the majority of users to access data without undertaking any form of additional assessment compromises market desirability and Consumer confidence.

- **Option 3** – 'ICO & cyber self-assessment'; under this approach all users would be required to submit directors' compliance statements with the ICO's checklists and evidence payment of the relevant fee to the ICO, where they are acting as a Data Controller. This approach builds on the benefits of utilising the ICO's checklists, described in option 2.

  In addition, organisations would be required to demonstrate compliance with the best-practice Cyber Essentials[12] standard (self-assessment version) developed by the UK's National Cyber Security Centre (NCSC) – which helps organisations guard against the most common cyber threats and demonstrate their commitment to cyber security.

  There would be additional requirements on users to have appropriate training mechanisms for personnel with access and appropriate controls to ensure data was only used within the terms of their data access arrangements.

  This option would mitigate Consumers' risk exposure through self-assessment and declarations against good and best practice requirements.

- **Option 4** – Information Security Management Systems (ISMS) principles; in addition to previous requirements, users would be required to have implemented a formal ISMS that covered their end-to-end enquiry service interactions, that demonstrates compliance with the principles of ISO27001[13]

  This approach is proposed to ensure that organisations accessing the data ecosystem are able to demonstrate a structured and disciplined approach to the management of information security that met the rigor of the International Standards Organisation's (ISO) 'Plan-Do-Check-Act' approach and commitment to continuous improvement. The requirements operate at the strategic level and do not, in itself, impose any more stringent day to day control requirements than the previous option.

[12] https://www.cyberessentials.ncsc.gov.uk/
[13] https://www.bsigroup.com/en-GB/iso-27001-information-security/

- **Option 5** – Information Security Management Systems (ISMS) certification; this option builds on option 4 by requiring the external certification of users' ISMS to the ISO27001 standard or the SME equivalent. The actual compliance requirements for this option are equivalent to those under option 4 but with the additional rigor associated with achieving external certification for their approach. It should be noted that this external assurance associated with achieving ISO certification would not be directly related to, or managed through, the REC assurance framework, but does provide an approach upon which the REC assurance can build as necessary.

2. Assurance options

2.1. The second key element of the framework is the assurance protocol that checks whether any organisation wishing to access, or already has access to, the data ecosystem is compliant, at that particular point in time, with whichever proposed requirements are stipulated in the access arrangements. The assurance protocol will focus on verifying procedural and systemic compliance, rather than spot output compliance, so as to give confidence of the user's enduring compliance.

2.2. Four assurance options are presented for consideration, with each option building on the requirements of the earlier options and increasing the degree of external scrutiny for both the enrolment stage (i.e. confirming compliance prior to having initial data access) and post-enrolment/annual review basis.

- **Option A** 'do nothing'; under this approach no enrolment verification checks are undertaken on the user save for checking registration details (e.g. company registration number and address, corporate website URL). Post-enrolment checks are focused on reviewing regulatory compliance checks (for example, any ICO '72 hour breach notifications'). This option is considered to offer the weakest protection to Consumers.

- **Option B** 'self-assurance'; this option utilises directors' compliance statements with the proposed requirements for both the enrolment stage and annual review stage. For the enrolment stage checks would also be undertaken to confirm the user's registration with the ICO and any historic data breaches or ICO enforcement action involving the organisation.

  Post enrolment, the user may be subject to unscheduled 'right to' external audits at the discretion of the enquiry service administrator. These are likely to be determined on a risk-basis, potentially referencing the expected/actual number of API calls, Consumer feedback or broader regulatory activity. Whilst the 'right to' audits help mitigate the gaming potential associated with the predictability of scheduled audits, it does not offer as robust Consumer protection as subsequent options.

- **Option C** 'self-assessment plus'; this option utilises a mix of self-assessment and scheduled external verification. Users, for both the enrolment and annual review stages, would be required to submit their self-assessment documentation from their internal governance processes which enabled their director's compliance statement regarding the proposed requirements.

For the enrolment stage this self-assessment would be accompanied by the administrator's right to audit, potentially on a risk basis. The post-enrolment stage would have a cyclical triennial external audit of data protection and cyber security compliance, overlaid with the administrator's right to audit at other times; an approach analogous to the Data Communications Company (DCC) 'other user' approach under the SEC. Whilst more complex than previous options, it does offer robust Consumer protection at reasonable value for money.

- **Option D** 'external assurance'; this option entails the highest degree of external scrutiny through both an enrolment audit and post-enrolment annual audits – though with significant cost implications.

3. Evaluation Criteria

3.1. The table below shows the generic midata evaluation criteria:

Impacts on Consumers		
1	**Data protection & security**	Secure, reliable, GDPR-compliant solution with minimal vulnerabilities and protected data transfer functionality
2	**Consumer trust**	Understand and address Consumer concerns on the midata service and more generally data sharing, to ensure they are comfortable and confident in using midata to share their data
3	**Consumer-centred design**	All Consumers who wish to use midata should be able to, regardless of who their current supplier is or their technical abilities. Service design should ensure that all Consumer touchpoints are as clear, simple, intuitive, quick & easy as possible.
Impacts on Industry (suppliers and third parties)		
4	**Robustness & proportionality**	The end-to-end solution should be technically robust and integrate efficiently with other related systems, with clear documentation and governance to ensure sufficient standardisation as to minimise subjective interpretation.
5	**Flexibility & scalability**	Iterative delivery with supporting governance arrangements, so that the service can change in line with user needs and may also support additional use cases and

		functionality in line with evolving market & future business models.
6	**Market desirability**	Functionality will be sustained with monitoring and enforcement in cases of industry non-compliance and inconsistency. Conversely, access and assurance arrangements to the service for third parties will be robust, yet proportional.
7	**Digitally enabled**	Enable and facilitate digital, real-time products and services (e.g. API enabled with near real-time query response)
Impact on delivery, costs and risks		
8	**Solution cost/benefit**	The new arrangements should be designed and implemented so as to maximise the net benefits for customers and minimise cost for third parties seeking to access the service.
9	**Implementation & risk consideration**	The plan for delivery should be robust, and provide a high degree of confidence, taking into account risks and issues. It should have clear and appropriate allocation of roles and responsibilities and effective governance. Where possible an Agile approach should be taken to test and prototype early.

4. Options Appraisal

4.1. For the purposes of this assessment option 1 (“do nothing”) has been taken as providing a baseline of the current regulatory landscape and for most criteria calibrated at zero. **Such a score does not, therefore, indicate a poor or unacceptable position, and was calibrated as such to enable the relative benefits of wider options to be shown on the same metric.**

Evaluation Criteria	Option 1 – do nothing	Option 2 – risk-based ICO self-assessment	Option 3 – ICO & cyber self-assessment	Option 4 – ISMS principles	Option 5 – ISMS certification

Data protection & security	**0** – no additional benefits over legal minimum	**2.5** – additional rigor through formalised self-assessment for higher risk populations	**5** – additional rigor for all participants through formalised self-assessment & Cyber Essentials compliance	**7.5** – additional rigor through structured approach and commitment to continuous improvement	**10** – additional rigor through externally audited compliance
Consumer trust	**0** – no trust enrichment as reliant on status quo legislative compliance	**2.5** – minor enhancement through focus on higher risk populations	**7.5** – significant trust enhancement through formalised self-assessment	**7.5** – significant trust enhancement through compliance with external standards	**10** – significant trust enrichment through formal compliance with external standards
Consumer-centred design	**N/A** – accreditation is a 'backroom function' which does not influence consumer touchpoints				
Robustness & proportionality	**5** – reliance on wider legislative requirements maximises integration potential but minimises risk mitigation potential	**5** – semi-proportionate approach, through the focus on higher risk population, offers an acceptable balance between risk mitigation and integration	**10** – use of the ICO and Cyber Essesntials' frameworks provides a proportionate approach to both risk mitigation and integration potential without raising barriers to entry	**7.5** – reliance on external standards reinforces risk migitation through a structured approach but poses integration issues with existing systems and raises potential barriers to entry	**5** – robust, yet dispropotionate, approach underpinned by the utilisation of external standards which maximises risk mitigation potential but compromises the integration potential through administrative complexity and degree of specification and raises potentially significant entry barriers
Flexibility & scalability	**10** – the lack of midata specific requirements enables maximum flexibility and scalability	**7.5** – reliance on the ICO's framework for the higher risk population enables a high degree of	**5** – reliance on the ICO and Cyber Essentials frameworks will ensure the proportionate	**2.5** – the prescriptive requirements of ISO certification limits the flexibility and	**2.5** – the prescriptive requirements of ISO certification limits the flexibility and

	(relying on legislative requirements to ensure data protections)	flexibility & scaleability	adjustment of requirements	scaleability of the option	scaleability of the option
Market desirability	**0** – reliance on wider legislative requirements does not provide any additional market reassurance	**5** – the focus on the higher risk population provides only limited market reassurance	**10** – utilisation of the framework approach provides wide market reassuarance as to the calibration of accreditation requirements without presenting barriers to entry to legitimate third parties	**5** – overall, the specification of external standards weakens market reassurance as to the accreditation design (on account of disproportionality and barrier to entry)	**5** - overall, the specification of certification to external standards weakens market reassurance as to the accreditation design (on account of disproportionality and barrier to entry)
Digitally enabled	**N/A** – it is the architectural design for checking a party's registration status that will influence the degree of digital enablement & not the actual accreditation requirements				
Solution cost/benefit	**5** – administratively simple and low cost implementation option presents relatively low levels of consumer protection	**7.5** – offers a relatively low cost implementation option for enhanced, but not sector-wide, benefits	**10** – presents an optimal balance between implementation costs, administrative complexity and consumer protection benefits	**7.5** – relative to previous options this offers a more complex and costly solution for only limited additional consumer benefit	**5** - Offers the greatest level of consumer benefits but disproprotionate to the complexity and cost of the option
Implementation & risk consideration	**10** – very light touch approach presents a low implementation risk profile	**7.5** – focusing requirements on a (small) high risk population presents a relatively low implementation risk profile	**5** – introduction of broad requirements on applicants presents a medium implementation risk profile	**2.5** – specification of external standards presents a higher implementation risk profile	**2.5** – highest implementation risk profile due to the external standards certification requirement
Overall Score	**30**	**37.5**	**52.5**	**40**	**40**

4.2. The assessment above suggests that option 3 represents the optimal combination of desirable characteristics across the evaluation criteria and has therefore been assessed against each of the four assurance options (A-D) in the table below.

4.3. For the purposes of assessing the combination of the proposed requirements and the assurance regime, any vestige scores from the earlier assessment of the standalone proposed requirements have been reset to enable a fuller assessment of the combinations.

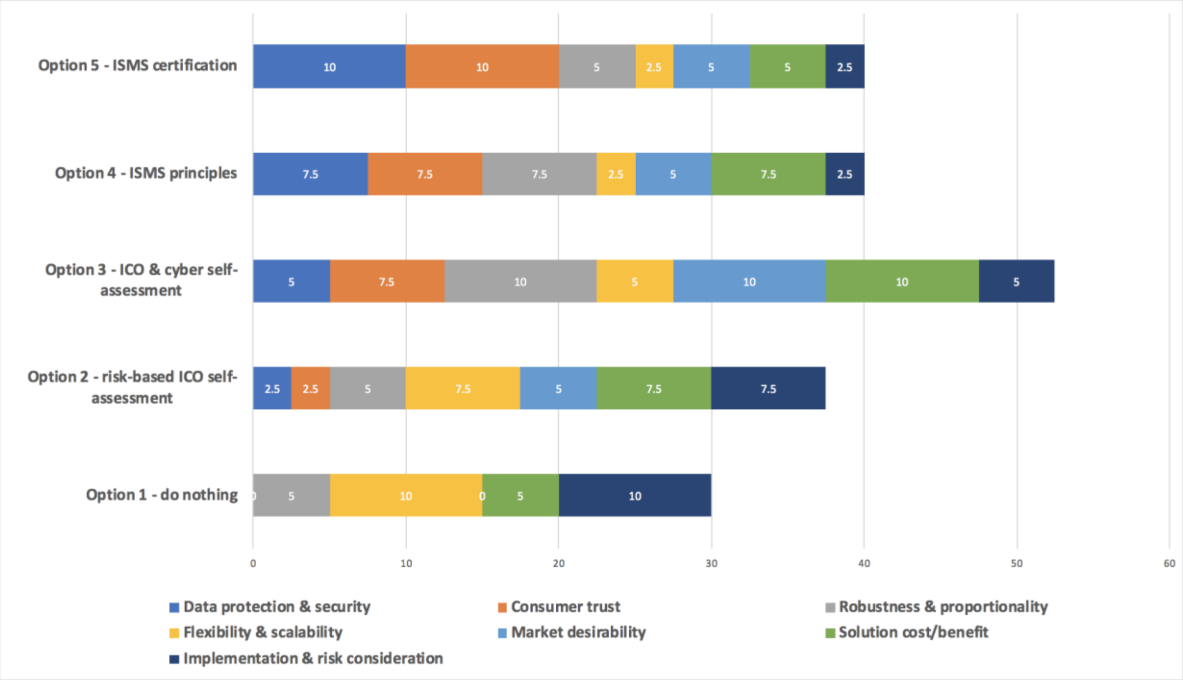
Evaluation Criteria	Option 3A – do nothing	Option 3B – self-assurance	Option 3C – self-assurance plus	Option 3D – external assurance
Data protection & security	**2.5** – this combination is considered to present legally robust yet relatively weak data protection (relative to the other options) at both the enrolment and post-enrolment stages given there is no external scrutiny or ongoing directors' declaration of compliance	**5** – this option presents an acceptable approach to data protection, combining a reliance on directors' declarations at all stages with the external scrutiny of a post-enrolment 'right to' audit – with the 'randomness' of the 'right to' audits helping to mitigate gaming potential associated with scheduled audits	**7.5** – the combination of directors' declarations, submission of self-assessment documentation and the external scrutiny associated with a 'right to' audit and post-enrolment triennial audits presents effective data protection risk management	**10** – external scrutiny through the inclusion of pre-enrolment audits and scheduled post-enrolment audits presents strong data protection controls
Consumer trust (N.B. indirect – supporting midata messaging)	**0** – this option is not considered to provide any enhancements to consumer trust	**5** - consumer trust is enhanced through compliance declarations and the external scrutiny associated with a post-enrolment 'right to' audit (which help to mitigate gaming potential associated with scheduled audits)	**7.5** – significant trust enhancement associated with self-assessments, evidence backed compliance declarations and external scrutiny through a mix of scheduled and 'right to' audits	**7.5** – significant trust enhancement through the external scrutiny associated with the inclusion of annual scheduled audits (although consumer trust is considered to have plateaued under option 3C & this option is not considered to add to it any further)

Consumer-centred design	**N/A** – accreditation is a 'backroom function' which does not influence consumer touchpoints			
Robustness & proportionality	**5** – has a high integration potential with existing systems, and low administrative complexity, but lacks robustness and proportionality so as to fully address the risks that would compromise stakeholder confidence	**7.5** – offers a semi-robust and prortionate approach to risk mitigation through compliance declarations and 'right to' audits, whilst presenting only limited implementation issues	**10** – presents the most appropriate balance between robustness, risk mitigation, frequency of external scrutiny, integration potential and proportionality	**7.5** – option presents the most robust approach to risk management, yet the frequency of external scrutiny (including administrative overheads and complexity) is disproprtionate and presents integration issues with existing systems
Flexibility & scalability	**7.5** – all the proffered options have comparable levels of flexibility and scalability (as the core reliance on the ICO's checklist should scale to meet future data protection requirements)	**7.5** – all the proffered options have comparable levels of flexibility and scalability (as the core reliance on the ICO's checklist should scale to meet future data protection requirements)	**7.5** – all the proffered options have comparable levels of flexibility and scalability (as the core reliance on the ICO's checklist should scale to meet future data protection requirements)	**7.5** – all the proffered options have comparable levels of flexibility and scalability (as the core reliance on the ICO's checklist should scale to meet future data protection requirements)
Market desirability	**2.5** – reliance on wider legislative requirements & lack of external scrutiny does not provide any additional market reassurance	**7.5** – market reassurance is provided through compliance declarations, 'right to' audit external scrutiny and good integration potential	**10** – significant market reassurance is provided through the balance and proportionality of evicence based declarations, external scrutiny and resultant access requirements	**7.5** – enhanced market reassurance through the reliance on external scrutiny, compromised by integration issues and the resultant cost/benefits
Digitally enabled	**N/A** – it is the architectural design for checking a party's registration status that will influence the degree of digital enablement & not the actual accreditation requirements			
Solution cost/benefit	**5** – relatively small net benefits due to low implementation costs and relatively low levels of consumer protection and benefits	**7.5** – relatively large net benefits due to relatively small implementation costs and large consumer benefits	**7.5** – relatively large net benefits due to medium costs, due to the option's administrative complexity, and large consumer benefits, associated	**5** - offers relatively small net benefits due to delivering the highest level of consumer benefits but at a disproportionate cost due to the frequency

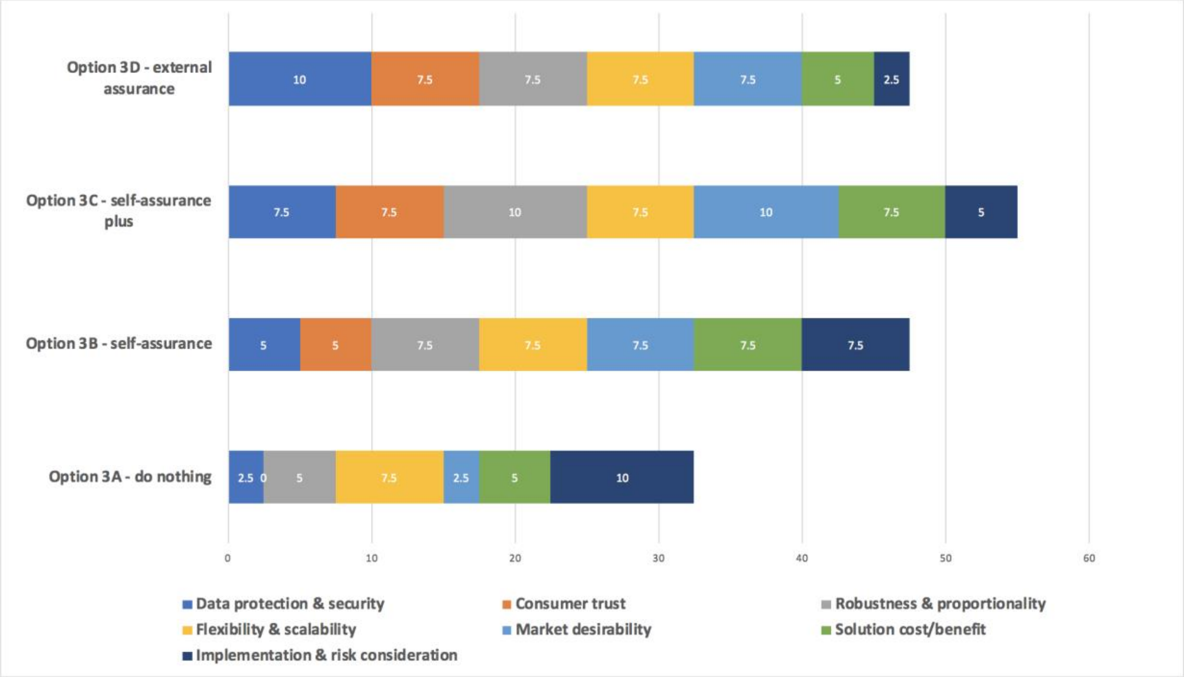
			with evidence backed compliance declarations and external scrutiny	of external scrutiny, administrative complexity and implementation issues
Implementation & risk consideration	**10** – very light touch approach presents a low implementation risk profile	**7.5** – reliance on compliance declarations and 'right to' audits presents a relatively low risk implementation profile	**5** – increased administrative complexity, associated with evidence backed compliance declarations and external scrutiny, increases the implementation risk profile for this option	**2.5** – the administrative complexity associated with this option presents the highest implementation risk profile
Overall Score	**32.5**	**47.5**	**55**	**47.5**

5. Midata Conclusions

5.1. The five proposed requirements options have been qualitatively assessed against the agreed and relevant evaluation criteria (listed above) as per the following graph. Each option has been scored from zero to ten inclusive by policy officials working on the accreditation piece, with each criterion being considered across the full range of its description. For example, with the 'robustness and proportionality' criterion an option may be scored highly for the robustness element but low for the proportionality aspect, resulting in a medium overall ranking. It should be noted that a couple of the criteria (consumer centred design and digital enablement) are not of relevance to the accreditation regime and therefore not shown on this graph.



5.2. The assessment of accreditation options indicates that option 1 presents the weakest combination of desirable characteristics. Whilst this should ensure compliance with legislative requirements, at a low cost and in a flexible and scalable manner and with low implementation risk, it is weaker than subsequent options utilising good practice risk management to deliver consumer protection, market desirability and stakeholder confidence. As noted above, the assessment suggests option 3 represents the optimal combination of desirable characteristics across the evaluation criteria and has therefore been assessed against each of the four assurance options (A-D) in the table below.



5.3. It is recognised that an audit function is an essential component of any management system, highlighting those control systems operating below the expected efficiency. The frequency of any auditing activity needs to consider i) the complexity of the processes being reviewed, with higher risk/more complex processes requiring more frequent review ii) the maturity of the processes, with new or unstable processes also requiring more frequent review, and iii) any historic breaches/problems involving the processes.

5.4. Whilst some of the constituent data streams are already accessible, via ECOES etc, the nature of the enduring data framework, which may enable third parties to access a more complete data profile on consumers than presently, combined with the potential sensitivity of future data streams and likely media spotlight on any breaches, would suggest a minimum of an annual audit cycle is most appropriate for delivering wider stakeholder confidence in the mechanism.

5.5. Using an internal self-assurance mechanism for this audit function should dovetail more easily with a user's existing management systems than an external audit regime, minimising costs and disruption, and enabling the audit to be undertaken by personnel with a detailed understanding of the organisation. It is recognised, however, that such internal reviews may be biased, especially where internal conflicts arise and may do little to reinforce stakeholder confidence in the process. As such a hybrid approach utilising internal self-assurance, supported by evidence backed directors' declarations, and a mix of scheduled and random external auditing is recommended to deliver the benefits of both approaches. The mix of scheduled and random audits has been proposed so as to mitigate the gaming risk associated with scheduled compliance audits.

5.6. These considerations, when combined, would suggest that stakeholder benefits and value is maximised through i) a scheduled annual review of user compliance ii) utilising a mix of internal and external assurance measures with iii) a right to external audit option overlaid to the internal assurance process and the scheduled external audits. **It is proposed that the '3C' combination represents the optimal combination of proposed requirements and assurance level.**