Proposed CCS ISDP Assessment Approach

It is proposed that all CCS applicants requiring an ISDP will be required to respond to the questions applicable to their role and proposed use of REC Data. However, the level of evidence required will depend on the applicant's individual risk profile. Applicants will be classified as low, medium or high.

Where a question is not relevant to the applicant's role or processing arrangements, it will not be required to provide evidence against that question. Where RECCo already holds equivalent and sufficiently current assurance or evidence, applicants will not be required to resubmit the same information.

The high, medium and low risk criteria set out below indicate the expected level and nature of evidence. They are not intended to prescribe particular technical solutions where an applicant can demonstrate equivalent controls and outcomes.

- whether the organisation is seeking to qualify as an EDH or ATP - the assessment will reflect the different risks associated with each role, including the greater focus on downstream data management for ATPs and the relevant CCS-specific security and data-sharing responsibilities of EDHs.
- the type of user and the purpose for which they are seeking to access data - including the nature and sensitivity of the data being accessed and the scale and purpose of the proposed access.
- the maturity of the applicant's information security and data protection arrangements, including its experience of managing comparable data and the evidence available to demonstrate that relevant controls are operating effectively.
- whether the applicant is accessing data for its own purposes or is expecting to pass consumer data to other downstream organisations - where downstream data sharing is expected, assurance will include the controls in place in place to manage the associated data protection and information security risks.
- the number of data access requests that the applicant is expecting to make, or is making, on an annual basis when considering ongoing maintenance of qualification assessments, together with the overall scale of data access.
- the extent of reliance on third-party processors, subcontractors or other service providers.
- any relevant history of information security incidents, personal data breaches or regulatory enforcement activity - the impact this has on the organisation's risk profile will recognise the nature of the incident, any remediation undertaken and the controls implemented to address identified weaknesses.

RECCo has reviewed these factors with the REC Performance Assurance Board and continues to consider how these factors should be weighted and whether any additional criteria should be incorporated into the assessment framework. The final approach will be informed by stakeholder feedback received through this consultation.

For the avoidance of doubt, organisations qualifying solely as Registered Tariff Interoperability Users to access account-specific tariff information will not be required to complete an ISDP and will instead complete the applicable registration and qualification requirements for that role.

In addition, organisations who have already qualified as an energy supplier or network operator will have completed comprehensive qualification activities and existing assurance evidence will be relied upon where it provides equivalent assurance. Any ISDP assessment required to qualify as a CCS User will therefore focus on CCS-specific risks and controls that have not already been adequately assessed.

Other existing enquiry service users that wish to qualify as a CCS User in order to access half hourly metered data will be required to complete a streamlined assessment. This reflects the need to assess the additional CCS-specific and half-hourly metered data risks that are not already addressed through their existing enquiry service qualification, while avoiding duplication of existing assurance activity.

Question	Criteria	Risk Category
Section 1: Company information		
1.1	Company name and number	Applicable to all.
1.2	Provide your Information Commissioner's Office (ICO)registration number	Applicable to all.
1.3	Registered Address	Applicable to all.
Section 2: Understanding how you will use the CCS		
2.1	Please indicate the expected maximum number of unique data access records your organisation plans to hold or access through the CCS within a 12-month period. This refers to the number of individual consumers for whom your organisation will either manage consent (as an A Data User) or facilitate data transfer (as a Data Holder). *For maintenance of qualification, please also identify any material change in the scale or frequency of data access since the previous assessment.*	Applicable to all.
2.2	Which systems or applications within your organisation will access or process REC Data? Please include a description or diagram of how REC data flows through your systems, including any integration points (e.g. Application Programming Interfaces (APIs), third parties, or external platforms).	High Risk: Require detailed diagram of internal systems, integrations, security boundaries and any third parties & external platforms. Medium risk: description or diagram illustrating the flow of personal data. Low risk: description or high-level diagram.
2.3	Will REC data obtained be stored within your systems, or processed only temporarily? If so, where will this data be stored or processed (including by any hosting provider)? Please identify the country or countries involved.	High Risk & Medium Risk: Detailed description of large-scale storage, especially if distributed or involving multiple third-party providers. Low Risk: Clear statement of location and basic security measures e.g. if they use a well-known, certificated cloud provider.

2.4	Have you reported any personal data breaches to the ICO in the past 12 months? If yes, provide a brief description and actions taken.	Applicable to all.
2.5	Confirm that the systems used to access or process REC data are within the scope of a current Cyber Essentials Plus or ISO27001 certification. Please provide the certification date, scope and Statement of Applicability (SoA).	Cyber essentials + is a requirement for all applications.
Section 3: Data handling and protection		
3.1	For what specific business purpose(s) will your organisation use the REC data? This purpose must directly align with the consent obtained from the consumer.	Applicable to all.
3.2	How do you ensure REC data is only accessed by staff or systems that require it for their role?	High Risk: Access Control Policy demonstrates robust, automated access control mechanisms, role-based access, and regular access reviews with audit trails. Medium risk: Access control policy, Role-Based Access Control (RBAC)implemented for staff and systems. Low risk: Statement of "need-to-know" principle and basic access controls.
3.3	What is your data retention policy specifically for REC data, and how is data securely deleted when no longer required or when consent is revoked?	High & Medium Risk: Demand robust, automated, and auditable processes for secure deletion/anonymisation of large data volumes, with operational evidence. Low Risk: Clear, documented policies and procedures for retention and disposal.
3.4	Please provide a redacted copy of your Data Protection Impact Assessment (DPIA)for this data processing. This should detail the key data protection risks identified, and the measures implemented to mitigate those risks. It should also detail how you ensure data accessed under REC services is only used in line	High & Medium Risk: Comprehensive, detailed DPIA covering all aspects of their large-scale data processing, with thorough risk assessments and mitigation strategies. Identified risks could touch on main risks with CCS including public trust, regulatory breaches, consumer safety/targeted fraud and discrimination).

	with the authorised purpose and consumer consent provided, and describe the controls in place to prevent unauthorised or inappropriate use of such data	Low Risk: A simpler, proportionate DPIA that clearly identifies risks and mitigations proportionate to their smaller-scale processing activities. High Risk: Technical controls, automated audit logs of data access and usage. DPIA mentions profiling/Automated Decision-Making (ADM)risks including a thorough assessment of potential for bias and discrimination, clear information provided to consumers about their right to human intervention with documented processes for handling these requests. Medium risk: documented procedures and controls to prevent authorisation / inappropriate use. Response shows they have considered and mitigated these discrimination and ADM risks. Low risk: statement that the organisation does not engage in profiling of ADM.
3.5	How do you ensure that only the minimum necessary REC data is requested and processed, strictly in line with the consumer's consent and stated purpose?	High Risk: Automated systems and controls to enforce data minimisation at scale including real-time consent validation, data subject verification, audit logs for consent checks, with evidence of regular review. Medium Risk: Process for updating consumer consent, consent validation log, description of data subject verification methods. Low Risk: Demonstrates adherence to data minimisation, policy outlining checks for valid consent and data subject verification.
3.6	Do you have a documented process in place to handle data subject rights requests (e.g., access, rectification, erasure, portability, object and restriction) for the personal data you hold? Please describe how this process ensures responses are provided without undue delay.	High Risk: Require scalable, automated systems and processes to handle a potentially high volume of Data Subject Rights (DSRs)within timeframes, with evidence of performance e.g. average response time, evidence of staff training. Medium Risk: Detailed DSR procedure document, records of past DSRs, communication paths and clear process management. Low Risk: A clear, documented process for handling DSRs, even if manual, demonstrating understanding of timeframes.

3.7	If REC data is transferred internationally (outside the UK), how do you ensure that data subjects' rights and the level of data protection are maintained in accordance with UK GDPR requirements (e.g., mechanisms included the use of a transfer risk assessment, reference to adequacy decisions, Standard Contractual Clauses (SCCs), or other appropriate safeguards)?	High & Medium Risk: If applicable, require detailed legal and technical documentation of safeguards (e.g., Transfer Impact Assessments for SCCs) and robust controls to maintain data protection levels. Low-Risk: Documented process which confirms they follow GDPR requirements for international transfers.
3.8	What controls are in place to prevent secondary use, profiling, or onward sharing of data accessed under REC services beyond the stated purpose and consent provided?	High Risk: System configurations designed to prevent profiling, technical controls e.g. data loss prevention tools, logs data access and usage. Medium Risk: Data usage clearly defined, logging and monitoring of data usage. Low Risk: A clear, documented statement that they do not engage in profiling, onward sharing or secondary use.
3.9	Describe your process for handling requests from consumers to withdraw their consent for data sharing, ensuring all relevant data is managed appropriately (in accordance with data retention policies) to enable notification to be provided to CCS in accordance with REC requirements .	High Risk: Robust, automated, and auditable processes for managing data post-withdrawal for large volumes touching on how they verify the data subject and remove data. Medium risk: Documented procedures, updating internal systems. Low Risk: A documented process for handling withdrawals e.g. a mailbox or designated contact person.
Section 4: Security Controls & Assurance		
4.1	How is personal data accessed via the CCS protected against unauthorised access, loss or disclosure once it is stored, processed or accessed within your organisation's environment, including where it is stored, processed or accessed through servers, databases, cloud services or end-user devices? Please describe relevant controls, including where applicable encryption, data loss prevention, monitoring and other measures not already evidenced through your Cyber Essentials Plus or ISO 27001 certification.	High Risk: Detailed evidence of the controls used to protect REC Data across the relevant processing environment, including encryption, access controls, monitoring and, where appropriate, data loss prevention measures, together with evidence that those controls are operating effectively. Medium Risk: Documented and implemented controls proportionate to the processing undertaken, including relevant encryption, access-control, monitoring and data-loss prevention arrangements. Low Risk: Clear policies and proportionate preventative measures appropriate to the nature and scale of the applicant's processing. (e.g., strong access controls, user training, basic technical controls).

4.2	How does your data classification scheme inform and dictate the security controls applied to different types of consumer/customer energy data you process?	High Risk: Well-defined, granular data classification scheme that dictates security controls across diverse datasets and systems. Medium risk: Data classification policy and corresponding security measures. Low Risk: A simpler, fit-for-purpose classification approach that demonstrates understanding of data sensitivity.
Section 5: Security Governance (not required for organisations with applicable ISO27001 certification)		
5.1	Please describe your organisation's data governance framework, including the roles, responsibilities, and meetings involved, specifically concerning REC data.	High Risk: Data Governance Framework or policy, a formal Data Governance Committee, recent meeting minutes from relevant committee, formal role descriptions (potentially a Responsible, Accountable, Consulted and Informed (RACI) matrix), evidence of communication plan for data governance policies and updates. Medium Risk: Data Governance Policy, highlighting individuals responsible for data protection. Low Risk: concise, written description outlining their approach to data governance.
5.2	Who within your organisation is responsible for information security and data protection?	Applicable to all.
5.3	How does your organisation identify and manage information security risks related to the processing of REC data accessed via the CCS?	High-Risk: Evidence of a sophisticated risk management methodology and Information Security Risk Management Policy, regular risk assessments, and a comprehensive risk register for all relevant systems and data. Evidence of continuous monitoring/reviews. Medium risk: Risk management framework, Information Security Risk Management Policy, principles from ISO27001 covering identifying, assessing and determining risk levels and identifying and evaluating risk treatment. Low-Risk: A written description of their risk management process for identifying and managing risks, with a basic risk register.
5.4	What training do staff receive specifically on handling REC data, and adhering to consent requirements?	High Risk: Evidence of mandatory, regular, and role-specific training with completion tracking, effectiveness measurement, and refresher training.

		Medium risk: Training policy or procedure, dedicated training modules on GDPR, incident reporting procedures etc. Low Risk: Clear policies for training and evidence of basic staff awareness.
Section 6: Security Incident Management		
6.1	What process does your organisation follow to detect and respond to security incidents affecting REC data or services?	High Risk: Detailed incident response framework and policy, evidence of regular testing and robust detection capabilities for large-scale operations. Medium Risk: Clearly defined Incident Response Policy and Plan (IRP), centralised logging and monitoring tools, defined escalation paths, staff training on incident identification, periodic review of IRP. Low Risk: A documented incident response policy, general staff awareness and system logging.
6.2	In line with the REC obligations, how would any compromise of REC data be notified to RECCo (and the Information Commissioner's Office if required) of a security incident, data breach or vulnerability affecting REC data or REC services, including expected timeframe?	Applicable to all.
Section 7 - Regulatory Compliance		
7.1	Confirm that your organisation complies with applicable UK data protection legislation (UK GDPR and Data Protection Act 2018) when processing REC data.	Applicable to all.
Section 8: Third party and operational controls		
8.1	Do any subcontractors or service providers support the systems used to access or process REC data? If yes, please list them and briefly describe their role.	High Risk: These applicants may have numerous third parties - data flow diagram, register of processes (GDPR Article 28), contracts are in place, detailed description of their specific role and data they are processing. Medium Risk: A comprehensive list with clear description of specific role and contracts in place.

		Low Risk: A list and brief description of applicable parties.
8.2	Do you share REC data with any third parties or service providers? If yes, please provide a list of the third parties used and describe the purpose of this sharing for each party	Applicable to all.
8.3	Please describe the mechanisms in place to ensure consistent and robust data security and protection throughout the entire data processing chain? How do you gain assurance over these third parties by assessing and monitoring them to ensure they comply with the consumer's consent and data protection requirements?	High & Medium Risk: Third-Party Risk Management Policy outlining onboarding and due diligence, Data Processing Agreements (DPAs), comprehensive monitoring of third-party compliance. Low Risk: Strong contractual controls, basic due diligence, and periodic reviews.
8.4	What physical or hosting environment protections exist for the systems processing REC data (e.g. office controls, secure hosting provider)?	High Risk: Detailed Physical and Environmental Security Policy and Procedures. Medium Risk: Physical security policy, environmental controls and access controls. Low Risk: Description of physical security measures for any data centres/sites and may refer to their provider's certifications.