REC Maintenance of Qualification Guidance

May 2022

V3.0

RETAIL ENERGY CODE

Contents

CHANGE HISTORY

Version	Status	Issue Date	Author	Comments
0.1	Created	11 May	Anton Moden	Disaggregation of pre-existing product
1.0		19 May 2021	Eliana Campbell	Final version agreed with RECCo
2.0	Final	February 2022	Adam Blair	Minor updates to guidance – system or process change disclosure
3.0	Final	May 2022	Adam Bamigbade	CSS Update

DOCUMENT CONTROLS

Reviewer	Role	Responsibility	Date
Walter Carlton	RPA Partner		10 May2021
Walter Carlton	RPA Partner		24 May 2022

Maintenance of Qualification

BACKGROUND

Each organisation that has been Qualified under the REC, including those under CMEC, is responsible for ensuring that it continues to meet its obligations under the REC, or as the case may be, its Access Agreement. A key element of this is maintaining qualification.

You are required to:

- Provide a Maintenance of Qualification Submission annually. You will be notified of this requirement in advance, through the REC Portal.
- Provide a Maintenance of Qualification Submission should a material event that could impact your ability to meet your REC obligations occur, or you reasonably foresee it could occur. Examples of this could be major systems and process change, or the implications of mergers and acquisitions activity.
- Promptly notify the Code Manager of any security breaches that could compromise the security or integrity of any REC Service, or any other REC Service Users.
- If you are a Qualified Energy Supplier or a Distribution Network Operator, inform the Code Manager of any changes to systems and/or processes that may impact interfaces with other Market Participants. Please refer to Section 8 for further guidance on disclosure requirements.

If you fail to submit your Maintenance of Qualification Submission, or the Code Manager believes you are in breach of the Code, this may be escalated to the Performance Assurance Board (PAB). The PAB will consider the escalation, such as whether it constitutes an Event of Default, and reserves the right to revoke your access to REC Services if it determines that you are in breach of the Code.

1. Maintenance of Qualification Submission

The Maintenance of Qualification Submission takes the form of 4 different types of submission:

Annual Statement

Compliance Statement

External Assessment

System or Process Change Disclosure

Which of these apply to you will vary based on your role in the market and the services to which you have access. Details of this can be found in the REC Service User Categorisation and Assessment Document. If you need to make an ad hoc submission related to a material event you can do this using the Ad-hoc System or Process Change Disclosure form, available on the REC Portal.

The Code Manager will communicate when Systems or Process Change Disclosure are due. Submissions are required for each Party acceded to the REC, as set out in the Party Register. You will also be notified 30 days before you are required to complete the submission.

2. Annual Statement

Required for all REC Parties and Non Party REC Service Users.

You will be required to submit an Annual Statement via the REC Portal to self-certify your continued qualification under the REC. The Annual Statement must be approved by a Director (or equivalent representative) and submitted to the Code Manager to be assessed.

If you are an Energy Supplier or DNO you must also highlight any changes or forthcoming changes and categorise the risks associated with the change. This Annual Statement will be assessed by the Code Manager.

The Annual Statement submission involves you completing the Annual Statement on the REC Portal, self-certifying that you meet the requirements to remain Qualified.

If you are implementing any changes you may request guidance on adherence to the Code through raising a request within the REC Portal to the Code Manager.

The Annual Statement and, where applicable, the underlying questions that accompany any change can be found within Appendix 1.

3. Annual Statement Outcome

The Code Manager will assess your Annual Statement return and will request further information from you, where required.

If, during the assessment of the Annual Statement, the Code Manager does not gain the necessary level of confidence required, additional information may be requested in order to assess your ongoing compliance with the REC.

If you are an Electricity Supplier or DNO making a change, dependant on the nature of the change and your responses, the Code Manager may recommend further testing. This will be arranged through messages in the REC Portal.

4. Compliance Statement

Required if you are an Electricity Supplier, DNO or Non-Party REC Service User. Post go-live this may apply to additional parties, e.g. Gas Suppliers, GES Users and CSS Users.

Compliance Statements are required for users of EES, GES and CSS. How often these are required depends on your user category and is set out in the REC Service User Categorisation and

Assessment Document. If you are required to provide a Compliance Statement, this will be submitted alongside your Annual Statement submission on the REC Portal.

The Compliance Statement requires you to self-certify your Information Security and Data Protection (ISDP) arrangements. You are expected to have adhered to those process and controls you have put in place to protect against ISDP risks that you may face and by completing the Compliance Statement you are confirming you have abided by your ISDP requirements.

The Compliance Statement must be approved by a Director (or equivalent representative) and submitted to the Code Manager to be assessed.

An example Compliance Statement can be found within Appendix 2.

5. Compliance Statement Outcome

The Code Manager will confirm you have submitted your Compliance Statement, and if the Code Manager does not gain the necessary level of confidence that it requires, the Code Manager may request additional information to assess your ongoing compliance with the REC.

6. External Assessment

Required if you are an Electricity Supplier, DNO. Some categories of Non- Party REC Service Users also require this assessment.

External Assessments are required for REC Parties and some Non-Parties, and are typically required once every three years. Which Non-REC Party Service Users will be requested to do External Assessments is set out in the REC Service User Categorisation and Assessment Document. If you are required to undergo an External Assessment, this will start with you answering a series of questions submitted alongside your Annual Statement submission on the REC Portal. The External Assessment must be approved by a Director (or equivalent representative) and submitted to the Code Manager to be assessed.

The External Assessment requires you to answer questions and provide evidence around your ongoing ISDP arrangements. You are expected to have adhered to those process and controls you have put in place to protect against ISDP risks that you may face and in completing the External Assessment you will document how you have adhered to your ISDP requirements. Evidence will also be required to support the External Assessment, referred to as ‘REC Service User Assurance Evidence’. This REC Service User Assurance Evidence will be assessed by the Code Manager. Guidance on completing the External Assessment, including what questions will be asked, how to answer those questions, and what evidence you need to provide can be found within Appendix 2.

7. External Assessment Outcome

The Code Manager will assess the REC Service User Assurance Evidence you have submitted, performing a review of submitted policies and procedures and sample checking adherence and compliance to the requirements.

If, during the assessment, the Code Manager does not gain the necessary level of confidence required, additional information may be requested to be uploaded via the REC Portal to assess your ongoing compliance with the REC.

The Code Manager will produce an evaluation report setting out any issues identified. You will be required to provide applicable rectification steps for any issues raised, which will be included within the evaluation report.

8. System or Process Change Disclosure

Required for Suppliers and DNOs.

Should you make, or intend to make, significant changes to your systems or processes you are required to disclose this and provide additional information for assessment by the Code Manager. You can access this at any time on the REC Portal by completing an 'Ad-hoc System or Process Change Disclosure' return, or declare when completing your Annual Statement.

Examples include (not exhaustive):

- a major change to core systems, including data migrations.
- significant business process changes that could impact market participants (e.g. following business growth).
- corporate or operational restructure, (e.g. following merger and acquisition activities, or as a result of SOLR);
- change of ownership.
- a significant outage or incident.
- an information security event, including all ICO reportable incidents.
- change of material outsourced providers that support your market role.

The Code Manager expects the Party to perform an Impact Assessment to ascertain whether a change has the potential to materially impact your ability to meet REC obligations. Management should document any changes to systems or processes that may impact interfaces with other market participants, made since the last Annual Statement or are it planned to be made in the next 12 months. Management are expected to self-certify the categorisation of risks associated with any changes.

Required for all REC Parties and Non-Parties

Under the REC, all Parties and Non-Parties are required to make this disclosure following a material event (e.g. a security breach) that could impact your ability to meet your current or future REC obligations, or impact interfaces with other market participants, REC services or central services.

Guidance on completing this disclosure, including what questions will be asked, how to answer those questions, and what evidence you need to provide can be found within Appendix 4.

If you would like to discuss the nature of any planned change, or significant event, and whether this would impact your Maintenance & Qualification Submission, please contact: enquiries@recmanager.co.uk

Appendix 1 - Maintenance of Qualification - Annual Statement

The below statement is the Annual Statement which must be completed on the REC Portal and submitted by a Director, or equivalent representative.

- I confirm, to the best of my knowledge based on reasonable enquiry, as an organisation Qualified under the REC, that:
- Management have understood the applicable requirements under the Retail Energy Code, including any obligations that have changedsince qualification;
- Management are not aware of any non-compliance to maintain being Qualified under the REC;
- Management have reported any system or technical issues reported to them by their prepayment meter infrastructure provider to theCode Manager (Suppliers only);
- Management have accurately reported all known Confirmed Energy Thefts to the Code Manager, as defined under the REC (Suppliersonly);
- Management have put in place processes for providing supporting evidence of compliance with theft reporting requirements if requestedby the Code Manager (Suppliers only);
- Management currently is compliant with all elements of the Smart Metering Installation Schedule, processes are in place that can demonstrate evidence of compliance in relation to this schedule and this can provided if requested by the Code Manager (Suppliersonly); and
- The operational contacts on the REC Portal are up to date and accurate.

For Energy Suppliers and DNOs only. Have you made any changes to systems or processes that may impact interfaces with other MarketParticipants, REC Services or other central services, since the last Annual Statement or are planned to be made in the next 12 months to the best of your knowledge?

If you answered NO to the above, you may stop the Annual Statement here, otherwise you will be required to complete the system andprocess change disclosure form (Refer Appendix 4).

Appendix 2 - Maintenance of Qualification – Compliance Statement

The below statement is the Compliance Statement which must be completed on the REC Portal and submitted by a Director, or equivalent representative:

I confirm, to the best of my knowledge having made all due inquiries and based on the sources of evidence, as [role] of [Enter MarketParticipant Company Name Here], that:

- We have maintained an up-to-date risk assessment covering information security and data protection risks associated with obligationsunder the REC Code, taking into account any significant change to our circumstances and whether there have been any security breaches;
- We have a complete and up-to-date relevant ICO Checklist;
- There have been no significant changes in our circumstances that would give rise to an increase in security or privacy risk, or wherethere has been a change, the appropriate mitigations have been put in place;
- We have appropriate information security accreditation reflective of the risks applicable to our organisation; and
- There have been no security breaches or ICO reportable data incidents, or if there have been such incidents detail the nature of such incidents.

Appendix 3 - Maintenance of Qualification – External Assessment

Once you have completed your response, please upload the completed form, along with the required supporting material into the REC Portal. To upload files into the REC Portal, please navigate to Party Operations, then Performance Assurance, and click ‘Your Files’. As you will have multiple files to upload, please zip your files relating to this application, naming each file with the reference number relating to the question below where relevant.

Please note that not all questions are applicable to every Market Role, or REC Service User category.#	**Item to be assessed**	**Your Response**	**REC Service User Assurance Evidence**
1.1	Please specify the architecture ofyour in-scope systems.	Please provide sufficient information to enable RECCo to understand the overall structure of your systems including the type of gateway, routing and validation mechanisms, applicable security systems and applications. Please also include a list of all systems utilised. Please highlight any changes you have made to the systems since your last ISDP assessment. In-scope systems means any systems used for generating, sending, receiving, storing (including for the purposes of back-up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and data associated with such activities in relation to the REC Service, which are operate by, or on behalf of, your organisation.	Schematic diagram to show components and relationships, with annotation showing where data flowsare processed. Indicate the type of gateway, whether it is high or low volume,remote, and/or shared with otherorganisations (who should be identified). List of all systems
1.2	Are you making use of any subcontractors, third parties or service providers to provide the operation of the service or developand manage any of the technical solution?	Yes / No	
1.2.1	Please provide a list of all subcontractors, third parties or service providers, including what activity they are performing.	Details of all subcontractors, third partiesand/or service providers that you intend to rely on in operating the service once you have acceded and their role in operating the service. In addition please detail any service providers who are supporting you through the assessment process.	List of all subcontractors, third parties or service providers includingdetails of what they are providing.
1.3	How have you been accessing thedata for the REC Service you have access to?	Details of how you have been accessing the data on the relevant REC Service, suchas if it is via the web portal, APIs or report.	

1.4	Have you made any changes to how you identify and appropriately assess all information security anddata protection risks relating to your business operations?	Detail any changes to your risk methodology, alignedto a recognised risk framework, including any changes to how the organisation managements' security and data risks which may include organisations risk appetite, risk and threat identification processes, risk scoring and treatment criteria and how risks are addressed and governed. Detail any new risks within the risk register, includingrisk scoring, owners, applicable controls and mitigating actions. Where applicable, detail any new risk treatment plans detailing the response to any risks identified.	Risk Methodology Risk Register Risk Treatment Plans (whereapplicable)
1.5	Have you maintained any information security accreditationthat you hold to mitigate the applicable risks to your organisation?	Details of any current or new relevantinformation security or data protection accreditation covering all or elements of your architecture and organisation.	Including but not limited to: ISO27001 certificate Cyber Essentials Plus CertificationIASME Governance Standard ISO27701 certificate
1.6	How have you ensured that you have appropriate risk, security andcontrol arrangements in place thathave been reviewed on a regular basis?	Please confirm how risk has kept under review,including items that may include triggers, threatsources and the frequency of reviews.	Risk Methodology Governance review minutes
1.7	How have you ensured that thereis appropriate governance, oversight and right tone from the top in relation to Information Security and Data Protection?	How have you obtained Management commitment to developing and embedding Information Security, including areas that may include appropriate levels ofgovernance, within the organisation? How have you assigned accountable owners for Information security.	Policy document detailingresponsibilities Governance committee TOR, agenda and minutes detailing Information security Audit/review documentation
1.8	How has your business taken steps to ensure appropriate information security and control procedures are in place?	Details of how you have taken steps to ensure appropriate information security and controls are inplace, such as the embedding of an Information Security Policy that complies with good industry practice such as ISO27001. Formal procedures and schedules in place for reviewing the Security Policy and adherence thereto, and reporting findings to Senior Management.	Information Security Policy Statement of Applicability Audit/review documentation

1.9	How has your business taken steps to ensure appropriate physical security and environmental control proceduresare in place?	Details of how you have taken steps to ensure appropriate physical security and environmental controls are in place, such as adherence to a documented procedure which details all expectedcontrols around both physical and environmental security which may include how premise are physically secure and access restricted and appropriate environmental controls for all relevant hardware such as servers.	Physical and environmental securitypolicy Audit/review documentation
1.10.	How has your business taken steps to ensure appropriate user access security and control procedures have been developed with respect to your service to guard against unauthorised logicalaccess to data and programs?	Details of how you have taken steps to ensure appropriate user access security and controls are in place, such as adherence to a documented procedure which details all expected user access controls which may include: A User access matrix detailing what all access all roles have, highlighting any roles where segregation of duties is required. Regular performance of User access reviews to all relevant systems. Details around password requirements and Multi- factor authentication. Sign off for new user access and removal of users who no longer require access.	Access controls policy Access control matrix Audit/review documentation

1.10.1	How does your business keep track of all access attempts and activities within the system?	Details of the solution(s) used to collect the audit logs, what audit and security event log activity is collected and how long this information is retained for?	The REC Service User should detail solutions that capture activity for all components of the CSS interface, i.e. not just the interface itself but any firewalls that act as part of the interface. This could be done with one solution or multiple. The records retained should include all log-in activity, be it successful or unsuccessful, log off activity, what systems have been accessed, and the actions taken. For example, security events could include instances such as: multiple failed log-ins, attempts to access sections that aren't permitted for that user role, log-ins during non-standard working hours. The REC Service User should assess events they have identified as sensible to track. The REC Service User should then detail how long this log information is stored for. Note that the REC requires the REC Service User to store this information for a minimum of six months, so they must state this as a minimum; otherwise, this section should be deemed non-compliant if they are unwilling to commit to this timeframe.

1.11	How has your business taken steps to ensure that credentials used to access services are heldin a secure and confidential manner, and any relevant secret key material is secured throughout its lifecycle.	Please provide details of how you have taken steps to ensure appropriate confidential credential management controls are in place, such as adherence to: A documented procedure detailing how different access credentials are held securely. A documented procedure detailing the lifecycle of any secret key material used, which may include details around: generation, registration, distribution, installation, storage, renewal and destruction and how this is being performed securely Please provide details of: any good practice or regulatory policies your process adheres to. How you have deemed that based on the confidentiality of the keys and secrets, the security measures in place have been deemed sufficient to protect them. How you look to securely manage each step of a key's lifecycle, such as the accurate generation of certificates, secure and restricted storage and secure destruction and or deletion.	Access controls policy Cryptographic lifecycle policySecret Key Register Audit/review documentation CSS Users must: detail how your process meets the requirements of the CSS Certificate Policy; articulate how you have assessed the appropriateness of the security module you are using to generate and store key pairs; certify that all of the information provided in this application (or any other accompanying or required documents) is correct, accurate and complete to the best of your knowledge, e.g. reviewing the received certificate before it is utilised; ensure that you have referenced security measures at all steps of a key in its lifecycle, from generation to destruction.
1.11.1	Have you had to follow your process to report any compromise or suspected compromise of the private keys associated with any of your certificates to the CSS Certificate Authority? If Yes what information did you provide and in what timeframe?	Please provide details of the process you follow to notify the CSS Certificate Authority if your private keys are compromised or suspected to be compromise, including how you will notify them, who performs this, what information will be provided and the relevant timeframe of the notification. If you have had to enact this process please provide details of this.	The REC Service User should define a process that clearly details how on the suspicion or actual compromise of their Private Keys, the steps taken through to notifying the CSS Certificate Authority. They should have a clear individual who's responsibility is to notify, should include how they would notify, i.e. via an online form or the email address they would pass details to, the timeframe to notify, which should be a reasonable period of time as soon as the event occurs, i.e. 24 hours, and also note what information will be provided, such as details around the event, what is being done to mitigate and remediate it, what they have suspected may have been compromised etc.

1.12	What steps has your businesstaken in relation to Human Resource Security, such as appropriate screening and relevant training?	Details of how you have taken steps to ensure appropriate Human Resource Security is in place, such as adherence to a documented procedure whichdetails all expected human resource security detailingappropriate screening of employees and information security training requirements.	Human resource security policy Screening and Training matrix Audit/review documentation
1.13	How has your business ensured that any unauthorised activity within your relevant systems is monitored for, and if detected hasbeen appropriately prevented and/or rectified?	Details around adherence to all security controls in place in relation to the monitoring systems for unauthorised activity which mayinclude: Firewalls, including configuration, monitoring andreview; Virus detection; Configuration change monitoring; Software installation monitoring. Time synchronisation monitoring.	System monitoring policy Operational evidence Audit/review documentation For CSS Users only, they must detail how the system detects any misalignment of system time across the organisations in scope networks.
1.14	How has your business monitoredand identified any vulnerabilities on your relevant systems, and if identified what steps have been taken to mitigate or remediate the vulnerabilities as soon as reasonably practicable? How often do you perform these vulnerability assessments?	Details around adherence to a documented procedure which may include: How you monitor and scan for vulnerabilities withinyour system; What patching is performed and how often this occurs.	Vulnerability scanning procedures Patch management procedures Operational evidence Audit/review documentation

1.14.1	Have you identified any material vulnerabilities? If yes have you notified the Code Manager and the Switching Operator in line with your processes?	Please provide details of the process you follow to notify the Code Manager and the Switching Operator of a material vulnerability, including how you will notify them, who performs this, what information will be provided and the relevant timeframe of the notification. If you have had to enact this process please provide details of this.	The REC Service User should have a clearly defined material vulnerability definition. The REC Service User should define a process that clearly details the steps taken upon identifying a material vulnerability. This should include: • The steps taken to notify the Code Manager and the Switching Operator. • The named individual(s) responsible for notifying the Code Manager and the Switching Operator • Steps on how the named individual would notify the Code Manager and the Witching Operator e.g. via an online form or the email address they would pass details to, • Reporting timeframes I.e. The length of time followingan incident that the named person(s) should notify the Code Manager and the Switching Operator of the occurrence. The reporting timeframe should be as soon as reasonably practical post the occurrence of the event, i.e. within 24 hours • The content and information required to be included within the notification e.g. details around the event, mitigation, remediation, impact of the vulnerability etc.
1.15	What processes does your business have in place in relationto incident management and how have you adhered to these?	Details around adherence to a documented procedure which details how incidents are dealt withwhich may include identification, triage, communication, reporting, management, resolution and review and review.	Incident management procedure Operational evidence Audit/review documentation

1.16	How have you ensured your datais held in a secure manner, retained for the necessary time required and deleted appropriately?	/Details around adherence to a documented procedure which may include details such as how data is classified based on its nature, how that data should be handled and stored based on its classification, how long it should be held for, and how it should be destroyed.	Data classification and retentionpolicy Operational evidence Audit/review documentation
1.17	How have you ensured data is only accessed for the purposes forwhich it is required?	Details around adherence to a documented procedure which may include details such as how access to data is restricted appropriately and how that access is monitored.	Data access policy Operational evidence Audit/review documentation
1.18	How have you adhered to your business continuity and disaster recovery arrangements in place within your organisation to ensure minimum disruption to service?	Details around adherence to a business continuity and disaster recovery arrangements procedure including details around any applicable resource training and exercises, failover testing and back up arrangements.	Disaster recovery and businesscontinuity plan Testing evidence Audit/review documentation
1.19	Please provide a completed up-to-date and relevant ICO checklist	A Completed ICO data protection self-assessments,these can be found here: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/checklists/data-protection-self-assessment/	Completed ICO checklists
1.20.	Have you reported any data breaches to the ICO in the lastyear?	Details of all data breaches you have provided to the ICO, along with any remedial actiontaken.	The REC Service User should have detailed any applicable reported data breaches that involve any inter-connected or similar systems, what happened and what they have done to ensure the reason for the breach does not happen again.

Appendix 4 – Maintenance of Qualification – System or Process Change Disclosure

If you declare that there are system or process changes in your annual statement, or as part the disclosure of a material event, you will need tomake this declaration:

- Management have documented any changes to systems or processes that may impact interfaces with other Market Participants, madesince the last Annual Statement or are it planned to be made in the next 12 months; and
- Management self-certify, based on reasonable enquiry, the categorisation of risks associated with any changes.

You will also have to complete the following additional questions about the changes, with answers captured on the REC portal.

#	Item to be Assessed	Your response	Evidence to Support…
	Nature of Change and Impact Assessment		
1	What is the nature of the change(s)that you wish to introduce into your operational systems?	Please describe the change in business terms and how it affects the processes you use in order to meetwith the requirements of the REC and to inter-operate with other Market Participants.	Change description. System architecture.
2	How do you intend to identify the items (procedures, instructions, applications etc.) that are impactedby the change(s)?	Please describe the analysis that will be carried outand the impact assessment records that will be available.	Change management impact assessment process and impact assessment records.
	What risks have you identified in the changes you propose to make, and how have you mitigated these?	Please describe how you have identified the risks and put in place arrangements to ensure these are minimised.	Change risk assessment. Change risk treatment plans.
	Change and Configuration Management		

3	What management processes do you intend to use to ensure that all necessary changes have been included?	Please describe the management processes that demonstrate that design of the change(s) will be effectively controlled.	Change management processes. Project plan. Review records.
	System/ User Acceptance Testing		
5	What management processes do you intend to use to ensure that the change(s) has been effectively tested?	Please describe the test management processes that demonstrate that the change(s) will be effectively tested.	Test strategy. Test plan. Test review records.
6	If changes include alterations to operational procedures and user activities, please confirm what involvement Business Users will have in the testing/acceptance ofthe changes?	Please provide a copy of the user acceptance processes.	Business review and approval records. Test strategy. Test results and review records.
7	Is any testing planned with other Market Participants with respect tothis change(s)?	If the answer to this question is 'Yes', please describe the tests.	Test strategy. Test plan. Test review records.
8	If the answer to 7 above is 'No', how will you ensure that the change(s) will allow you to inter- operate correctly with other MarketParticipants?	Please describe the management controls that will give you the confidence that the change(s) will allowyou to inter-operate correctly with other Market Participants.	Management controls or internal test strategy. Test plan. Test review records.
	Non-Functional Testing		

9	If high volume interaction is anticipated, what non-functional testing activities will be introducedto ensure system capabilities?	Please describe any high volume and load balancing testing that your organisation intends to complete.	Test Strategy. Test plans and results. Test completion approvals.
	Data Migration		
10	If the programme involves data migration of business records, howwill you ensure that data quality & integrity are maintained or improved?	Please describe the controls that are in place to monitor data integrity and quality at each stage of themigration process.	Migration strategy. Trial data migration plans. Data quality and integrity assessments. Data evaluation exercises & statistical evidence.
	Implementation		
11	How will you ensure that the cut-over to the changed processes does not cause disruption to the Market?	Please describe the controls that are in place to minimise disruption to services at the point of bringing the changed processes into operation in thelive Market, this could include phased implementation or parallel running.	Cut-over strategy and plan.
12	Will you be carrying out dress rehearsals prior to cut-over?	Please describe any plans for dress rehearsals.	Cut-over strategy and plan. Dress rehearsal detailed plan.
13	If the answer to 12 above is 'No', how will you ensure that all tasks inyour implementation plan can be completed in the appropriate time- frame?	Please describe any planning exercises in this area.	Detail relevant controls.
14	How will you ensure that complications that arise during cut-	Please describe any plans for recovery and/or roll-back.	Cut-over plan.

	over will not produce a detrimental effect on live operation?		Project business continuity plan.
15	Has your organisation planned to inform all interested parties of this change?	Please describe any contact your organisation intends to have with other Market Participants, informing them of the implementation of your programme.	Cut-over plan. Assessment of parties that may be affected by the changes. Letter containing operational contacts, dates.
16	Do you intend to carry out post go-live production proving?	Please describe any post go live proving strategy, processes & plans.	Post go-live monitoring and test plans.
17	If the answer to 16 above is 'No', how will you ensure that all tasks inyour Implementation Plan have been operationally verified as successful?	Please describe your production acceptance criteriaand any planned production acceptance tests.	Production acceptance criteria. Test plans. Test scripts.
	Business Training		
18	How will you ensure that all business users are fully conversantwith the new operational processesand procedures associated with this change?	Please describe your approach to user training.	Training strategy & plans. Training guides. Training records.
	Post Implementation		
19	How will you ensure that changes continue to be effective?	Please describe any ongoing operational monitoring activities planned by your organisation.	Operational monitoring plans & reports.

To find out more please contact:

enquiries@recmanager.co.uk

RETAIL ENERGY CODE