REFERENCE	**RECRIG_25_0110_04**
STATUS	**FOR DISCUSSION**
PAGES	**4**

MAINTENANCE OF QUALIFICATION REVIEW

1 BACKGROUND

Maintenance of Qualification is a key Performance Assurance Technique. The fundamentals of this approach are set out in Schedule 9 of the REC which includes the following requirements:

1. An Annual Statement attesting compliance with the Code.
2. An annual information security assessment which is either a lighter touch 'Compliance Statement' or a more detailed 'External Assessment'.
3. Requirements around specific events, including the disclosure of key changes and notification of security events, which may result in the Code Manager taking further action.

There are three reasons why we wish to review the qualification requirements.

1. There have been requests from Parties to transfer REC relevant data outside the European Economic Area (EEA), which is explicitly called out as requiring approval. There is no such requirement for processing within the EEA but outside of the UK.
2. There have been instances reported of Parties breaching anonymity of confidential tip offs.
3. Requests from REC Parties to reduce the overall level of activity in this area to reduce the workload on Parties.

We have discussed with the PAB options to improve this process, and PAB members asked that the Code Manager provide opportunities for industry to input via the REC Issues Group (RIG).

This review covers the scope of Maintenance of Qualification activities, with separate work being discussed with RECCo to make the practical processes of Maintenance of Qualification easier (e.g. the way uploads are made).

2 PURPOSE OF THE PAPER

This paper sets out the context around each of the reasons we have considered updating Maintenance of Qualification activities. It sets out the proposed approach in future as well as the options discounted. We have included the questions that we propose to ask of the RIG. During the RIG meeting we will:

1. Answer any clarification questions on this paper.
2. Facilitate a discussion on the questions posed.
3. Consider the feedback from industry.

If RIG attendees do not wish to provide input in an open forum they can provide their input to the Code Manager on qualification@recmanager.co.uk by 17th January or can contact PAB members (whose details can be found on the REC Portal).

3 EEA DATA TRANSFER

The Code requires that the RECCo Board approves any such transfer. Given the PAB is a component of this Board delegated to specify information security and data protection we consider it appropriate to involve the PAB in this process. The ICO has established a concept of 'adequacy'[1], essentially deeming other countries as having an essentially equivalent level of protections. We recommend the following delegated authority is established:

- REC Board – for unusual cases or complex cases, as escalated to by the PAB.
- REC PAB – for cases where there is no finding of adequacy.
- REC Code Manager – to approve cases where the ICO has found the country to have adequacy[2], subject to required controls being in place.

[1] See: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/

[2] Currently Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan (private-sector organisations only), Jersey, New Zealand, Switzerland and Uruguay.

In all cases before presenting for approval the Code Manager would request that the applicant fills in a form specific to this, and require the minimum criteria to be met:

- The transfer of data be covered by the Standard Data Protection Clauses set out in an International Data Transfer Agreement
- The organisation has shared the Data Protection Impact Assessment with the Code Manager and there are no identified concerns raised by either the Code Manager or their legal advisors.
- The organisation has agreed to any additional PATs (e.g. the provision of information or notification on specific events).

In developing this we collaborated with RECCo's Information Security & Data Protection Officer and consulted RECCo's legal advisor on the process and the standard information request we would issue.

Other Options Considered

The wording in the Code considers this a RECCo Board function, we considered all approvals could be routed to the RECCo Board, but discounted this due to the existing PAB role and delegations in relation to information security and data protection, and the frequency at which meetings are held.

Next Steps

The PAB supported the approach above, but raised queries around the impacts of organisations processing of data outside of the EEA on other organisations. They requested that we engage with the RIG to make sure that the matter is fully considered, and offer opportunities to engage with PAB members with any concerns if appropriate.

If approved we propose to present this to the RECCo Board for confirmation they are happy with this approach, and provide the form to be completed to initiate the process on the REC Portal.



INPUT REQUIRED FROM RIG

Are there any ways that others processing data outside of the EEA could negatively impact your organisation that we should take into consideration?

Do you have any comments or suggestions on the proposed process?

4 ETTOS CONFIDENTIALITY

Breaching ETTOS confidentiality could result in serious repercussions for the person tipping off. It can also deter people from submitting tip offs, which may result in safety risks for those near a tampered-with meter. There have been instances of Parties breaching ETTOS confidentiality, and we therefore want to take a comprehensive approach to tackling this issue. Working with RECCo we plan on issuing guidance relating to how to handle tip offs, whilst simultaneously adding a new question to the annual statement for Parties that receive tip-offs:

We are aware of the importance of keeping ETTOS tip offs confidential and have put in place relevant training, guidance and information security controls in order to achieve this.

In any detailed information security assessment we plan on adding the following question:

How do you ensure that ETTOS tip offs are confidential (please include information on relevant training, guidance and user access controls in order to achieve this)?

These new questions will be communicated to relevant Parties when they are provided this year's Maintenance of Qualification deadlines, alongside guidance prepared with RECCo.

We also will clarify the information Parties need to submit in the event of confidentiality having been breached to provide a specific information request in this instance.

Other Options considered

- We considered implementing only part of these processes, but given the importance and relatively low impact on organisations we did not feel this as appropriate.

- We considered raising a REC Change to specify requirements, but consider that incorporating this into Maintenance of Qualification, one of few REC interactions that involve Parties' senior management, as appropriate given the significance of the matter.

PAB members supported the above, options, but given the request to discuss the outside EEA matters with RIG asked we cover this with RIG.



INPUT REQUIRED FROM RIG

Do you have any feedback on this approach?

5 PROPORTIONALITY OF ANNUAL ACTIVITIES

We consider it to be essential that senior management are personally responsible for REC compliance, and consider an Annual Statement to be a critical activity for establishing accountability. Many organisations are completing MHHS qualification in the period and for those organisations we propose to allow them to submit their Annual Statement alongside their MHHS qualification forms, to be provided with a single piece of feedback. We will not require these organisations to complete Change notification related to MHHS.

There are currently 31 REC Service User Categories[3], which essentially requires organisations with access to REC APIs to have a more detailed assessment than those only accessing the online portal. This is because API access allows much faster access which means the impact of any confidentiality breach is likely to be more significant, as well as the possibility that security events can overwhelm services, making them unavailable for all users.

We have considered the following changes:

1. SEC Parties already undergo significant security assurance, although it does not cover the same data. We could reduce these organisations assurance activities to a Compliance Assessment with disclosure of the outstanding actions from SEC User CIO assurance (the specific security assurance activity) but would require an attestation that the Party operated a similar level of security controls for its REC activities as for the SEC User System. This would cover Energy Suppliers and electricity Distribution Network Operators.
2. Reducing the assurance activities of organisations populating REC data, or already privy to this data, namely Metering Equipment Managers, Meter Asset Providers and Shippers to Compliance Statements only.
3. Increasing the assurance of the highest risk organisations. We already conduct annual security assessments of CSS Interface Providers, as security issues with these organisations could have a significant impact on multiple Parties and directly impact the market. We propose to conduct a similar annual activity on Third Party Intermediary Service Providers. This approach would incur additional costs if proposed reductions are not approved.
4. Reducing the security assurance of other central bodies, including the BSC Technical Assurance Agent, the Authority, Industry Code Managers and Electricity Market Reform (EMR) Settlements, to only when required by the PAB's data access request process.

We note that some of the user types (e.g. Data Aggregators) will no longer exist following the completion of MHHS. We also assume that as part of R0148 (Introduction of classification-based access model into the REC in support of Open Data) that there may be further updates to this approach, as central controls over data are put in place that prevent inappropriate use and there is therefore less need for assessment of the controls of Service Users.

Other Options considered

- We considered reducing the frequency of the Compliance Statement for the least complex organisations, which would require a REC Change. Given this statement is attestation only we have discounted this option.
- We considered simplifying the Service User Categorisation and Assessment document to require those with API access to have an External Assessment and those without a lower assessment, although did not consider this was sufficiently tailored to the information provided.

[3] https://recportal.co.uk/documents/20121/0/REC+Service+User+Categorisation+V5.2.pdf/cb45a6ff-96e6-77e9-1eb5-21db101ce9ef?t=1732884147378

- We considered increasing the time between assessments for common Party types. For example Suppliers typically are subject to an External Assessment once every three years, but this could be increased to once every five years.
- We considered placing greater reliance on Parties (and related Service Providers) that have ISO27001, Cyber Essentials Plus, or additional accreditation, which would result in them answering a targeted shorter set of questions.

Next Steps

PAB members supported the above options, but given the request to discuss the outside EEA matters with RIG asked we cover this with RIG.

Should this be approved we would update relevant category 3 documents and communicate the requirements change as part of the annual maintenance of qualification deadline communication.



INPUT REQUIRED FROM RIG

Are there other things that we have not considered?

Are there other types of organisations that reflect a higher / lower risk profile where more / less activity should be prioritised?