EUROPEAN COMMISSION
DIRECTORATE-GENERAL
CLIMATE ACTION
Directorate A - International and Climate Strategy
CLIMA.A.3 - Monitoring, Reporting, Verification

Good practice: Application of EN ISO 14065 (management system)

The Accreditation and Verification Regulation - Outline of a verifier's management system

Final version, 18 December 2013

This document is part of a series of documents and templates provided by the Commission services for supporting the implementation of Commission Regulation (EU) No 600/2012 of 21 June 2012 on the verification of greenhouse gas emissions reports and tonne-kilometre reports and the accreditation of verifiers pursuant to Directive 2003/87/EC of the European Parliament and of the Council.

The guidance represents the views of the Commission services at the time of publication. It is not legally binding.

This example takes into account the discussions within meetings of the informal Technical Working Group on the Accreditation and Verification Regulation under WGIII of the Climate Change Committee (CCC), as well as written comments received from stakeholders and experts from Member States.

All other guidance documents and templates can be downloaded from the documentation section of the Commission's website at the following address: **http://ec.europa.eu/clima/policies/ets/monitoring/index_en.htm**.

Background

This note is aimed at providing a good practice example to supplement Key guidance note II.8 on the relation between EN ISO 14065 and the AVR. Both documents, the key guidance note and this example, are part of the suite of guidance documents developed by the Commission to explain the requirements of the EU ETS Regulation on Accreditation and Verification (AVR)[1]. The suite of guidance documents consists of:

- an explanatory guidance on the articles of the AVR (EGD I), including a user manual providing an overview of the guidance documents and their interrelation with the relevant legislation;
- key guidance notes (KGN II) on specific verification and accreditation issues;
- a specific guidance (GD III) on the verification of aircraft operator's reports;
- templates for the verification report and information exchange requirements;
- exemplars consisting of filled-in templates, checklists or specific examples in the explanatory guidance or key guidance notes;
- frequently asked questions.

Article 40(2) of the AVR requires the verifier to design, document, implement and maintain a management system to ensure consistent development, implementation, improvement and review of the procedures and processes required by the AVR and EN ISO 14065. More detail on what a verifier's management system should contain, is specified in section 12 of EN ISO 14065. These requirements have also been outlined in section 3.8 of Key guidance note II.8 on the relation between EN ISO 14065 and the AVR (KGN II.8). The example of a verifier's management system provided in the paragraphs below supplements that section in the key guidance note to assist the verifiers in understanding what a verifier's management system should cover.

Art. 40(2) AVR

1. Example of a verifier's management system

As mentioned in Key guidance note II.8 a verifier's management system should include a management policy, and processes for the control and filing of documents and records; planning and conduct of internal management system audits; corrective and preventive actions taken to ensure the management system is working properly; and management review. The table below indicates what should be included on these different elements of the verifier's management system.

Explaining the required elements of the verifier's management system
Management system policy – this policy should ensure that the management system is sufficiently robust and frequently reviewed to establish its effectiveness and capability of supporting consistent achievement of the requirements in EN ISO 14065 and the AVR. The review should be carried out by the most senior levels of management.
Control and filing of documents – verifiers should ensure that all documents (internal and external) are under control and properly filed. ▪ A process should be established to ensure proper controls of all documents (including archived) and to define responsibilities of all personnel involved, including top management;

[1] Commission Regulation (EU) No 600/2012 of 21 June 2012 on the verification of greenhouse gas emissions reports and tonne-kilometre reports and the accreditation of verifiers pursuant to Directive 2003/87/EC of the European Parliament and of the Council, OJ EU, L 181/1.

Explaining the required elements of the verifier's management system
▪ A master list of all controlled documents should be in place; ▪ Controls should be in place to ensure: - documents are frequently reviewed, updated as necessary, that revisions are correct and approved; and that old copies are archived; - documents remain legible, that unintended use of obsolete documents is prevented and that obsolete documents are available to personnel when needed; - effective change control processes, including suitable approval and authorisation of documents. This is particularly relevant for verification reports and official documents to be issued externally by the verifier. Changes to such client documents should be identifiable, recorded and justified in the supporting evidence files; - proper distribution of documents, and training on new and updated documents as well as control procedures. The verifier must ensure relevant versions of applicable documents are available to personnel, subcontractors, and accreditation assessors where necessary; ▪ Internal audits should include the whole document control process, including checks by the internal audit team that these aspects are implemented (the internal audit should also cover electronic records and control on electronic records, see further below).
Control and filing of records – the verifier should ensure that the following are taken into account in the verifier's process to ensure records are controlled and properly filed: ▪ How records are kept (electronic or paper or both), determines the types of controls a verifier should implement[2]; the verifier should assure itself that the most effective control is being applied; ▪ Who holds the records (employees/ contractors) determines what types of controls a verifier should implement[3] – the controls must ensure that the security and confidentiality of records is sufficiently safeguarded; ▪ There should be clear responsibilities allocated for retaining, collecting, disposing of records and other activities related to records; ▪ Records should be easily accessible and available to all relevant personnel, sub-contractors, accreditation assessors where necessary; ▪ A record retention policy should be in place – stating the number of years that documents are to be retained. Records associated with a specific verification must for example meet the MRR/AVR retention requirement (that documents have to be retained for 10 years); this should apply to both hard copy and electronic records systems.
Security of information – control processes should be in place to ensure that all electronic documents and records are held securely and confidentiality is safeguarded, including consideration of: 1. security of electronic information; 2. security and confidentiality of client information on lap tops and other mobile devices

[2] If there are electronic records then the scope of the checks needs to be much wider and take into account IT processes; archive management, backup and security of backups; IT change control etc.

[3] If it concerns records of internal staff then the relevant procedures would state what records are required and how they should be handled. If it concerns records of an sub-contractor, then the management of records may need to form part of the contract arrangements; contractors might be required to obtain and retain certain records; or they might be required to hand over to the verifier certain specified records to ensure that the verifier's files for a project are complete, accurate etc.

Explaining the required elements of the verifier's management system
etc.; 3. back up of electronic information. Please see also under internal audits. These elements are also covered in internal audits.
Internal audits – the verifier should establish a documented process for regular internal audits to ensure that it is in compliance with the AVR and EN ISO 14065. The following issues should be taken into account: ▪ Responsibility for the internal audit process should be properly defined; ▪ Schedule of internal audits should be available and documented, covering all requirements and system elements (regulations/ Commission guidance documents/ standards etc.). Usually internal audits are scheduled once a year; ▪ Trained and sufficiently competent auditors should be used that are: - independent and impartial; - different from those who perform the activity to be audited; ▪ Sufficient records should be maintained to demonstrate all areas have been covered by the internal audit; the status of the area covered and actions taken where non-conformance or weakness is identified; ▪ Systems should be in place to ensure that any issues identified in the internal audit are followed up in a timely manner and that any opportunities for improvement are acted upon.
Corrective actions – the verifier should implement a documented process for identifying and managing non-conformities in its own operations; whether these are identified formally (e.g. through internal audits) or informally (e.g. suggestions raised by staff). These processes should also include feedback from clients and the CA. When non-conformities are identified corrective action should be taken to address these with a focus on eliminating the root cause(s) of non-conformities and prevent reoccurrence. The process should include the following elements: ▪ A documented policy and controls in place in order to identify non-conformities; ▪ Clear definitions of who is responsible for actions to close out non-conformities; ▪ Clear definition of when the process of identifying and managing non-conformities is used and when corrective action is taken; ▪ Clarity on where information is recorded, including non-conformities identified; results of corrective action; and other activities related to the corrective action; ▪ Performance of root cause analysis to identify and determine the primary causes of non-conformities. This will enable the verifier to define specific and realistic actions to be taken to eliminate the causes and to prevent reoccurrence of non-conformities; ▪ Correct and timely implementation of corrective actions. Actions should be appropriate to the impact of the problems encountered and directed at the root cause(s); ▪ Timely closure of non-conformities and authorised sign-off of that closure; ▪ Review of the effectiveness of corrective actions and implementation of measures to avoid repeat issues; ▪ Review of trends, and the communication and escalation of major issues.
Preventive actions: the verifier should establish a formal process to identify opportunities for improvement in the system and controls; and to take preventive action to eliminate causes of potential non-conformities. Preventive action is avoidance of potential non-conformities. It is not used as a reaction to a non-conformance.

Explaining the required elements of the verifier's management system

The process should include the following elements:

- A documented policy and controls in place to identify potential non-conformities and other weaknesses;
- Clear definitions of who is responsible for preventive activities;
- Clear definition of when the process of preventive actions is used and when actions are taken in relation to improvements identified;
- Clarity on where information is recorded, including issues identified, and preventive actions taken;
- Performance of root cause analysis to identify the likely primary source of potential non-conformities so as to design effective control actions;
- Timely implementation of preventive actions, which should be appropriate to the likely impact of the potential problem;
- Timely closure of preventive action and authorised sign off of actions;
- Review of effectiveness of preventive actions taken.

Management review : the verifier should establish and document a formal process to review its management system, at planned intervals, to ensure continued effectiveness of the management system in controlling the verifier's areas of risk; and the verifier's conformance with its own management system and compliance with ETS requirements. The review of the verifier's management system should:

- Include standard input information e.g. –
  - results of internal/external audits;
  - feedback from CA's, clients and NAB/NCA;
  - status of agreed corrective and preventive actions;
  - follow up actions from prior management reviews;
  - internal/external changes to the verifier that could affect the quality management system and/or verification risks (including legal requirements);
  - recommendations for improvement to the verifier's management system that would increase the robustness of control over verification risks;
- Ensure that suitable personnel are involved in the planning, input to, and attendance at the review meeting(s); this should include senior management being present at the review meeting(s);
- Ensure annual review of all aspects of the verifier's management system and the verification risks they are designed to control;
- Include minutes of prior review meeting(s) and relevant other meetings, identifying attendees, resulting actions, defined timelines and responsibilities for actions agreed to be taken;
- Include records of all activities related to management review and a mechanism to track progress of closure of agreed actions.