CEIOPS-QIS5-13/10
5 November 2010

Process for analysing group data in QIS5

- main characteristics -

Purpose

1. The purpose of the centralised group database, both for cross border and national groups, is to analyse QIS5 groups results. This approach is needed as the size of samples will be too limited on a national level to have a sufficient quality of analysis.

Submission of results

2. The data of a given group will be submitted to CEIOPS using one of the 2 following procedures:
   - Sent to the group supervisor that will forward them to CEIOPS
   - Sent at the same time to the group supervisor and CEIOPS (option available in case the group agreement is in any case necessary to pass the data to CEIOPS)
3. **No data will have to be submitted only to CEIOPS.** If this were to happen, CEIOPS will immediately forward the data to the group supervisor.
4. Answers to the qualitative questionnaire preferably in English should also be submitted to CEIOPS as they are important tools for the analysis of the results.

Support to lead supervisors and Colleges for the analysis

5. Initial analysis of the group submissions available in the centralised database will be transmitted to the group supervisors including some global statistics coming out of the centralised database.
6. Theses initial analysis will:
   - Help group supervisors to structure their understanding and analysis of their group results in an harmonized way ;
   - Improve the quality of the analysis by showing to group supervisors whether their groups are outliers or not compared to the others groups ;
   - Ensure that the task force rely on group supervisors expertise to carry out an adequate analysis of the group results by allowing them to provide qualitative comments and interpretations.
7. In a second step, the group supervisor will send back to the task force, the template with qualitative analysis and possibly updated spreadsheets if quality of data has been improved following that analysis.
8. This second step is expected to be done in cooperation within Colleges for cross border groups.

9. Group supervisors will be the ones taking the initiative to contact their groups if mistakes are detected which raise the need for the group to re-submit the data. In such a case, re-submission should be done following the same process than the initial submission **(see 14)**.

Access

10. The database will be located in CEIOPS premises and only accessible from there to ensure the unity and integrity of the database.

11. The potential persons who can have access to the group database are the members of the QIS5 task force. This includes also the 2 CEIOPS Secretariat persons leading the task force.

12. Rules of access to the database aim to ensure a balance between Members with, at most, one person per authority involved in the task force will have access to the database.

13. All persons who will be granted access to the database will sign a dedicated confidentiality agreement.

14. The data will be stored for additional analysis only as long as necessary to answer all questions arising from the conduct of the QIS5 and destroyed thereafter.

IT solution to ensure a safe exchange and storage of data

15. The central database used for the analysis of groups submissions will be stored in an encrypted container and accessed using On-The- Fly-Encryption technology[1] to ensure that the sensitive content will be never stored in a non-encrypted form[2].

16. Passwords allowing access to this encrypted container will be disclosed to the defined list of people through physical meeting on a need-to-know basis.

17. The list of passwords used will be stored in the CEIOPS physical safe.

18. Encrypted data will be exchanged between CEIOPS and national supervisors using a dedicated CEIOPS e-mail address (qis5db@ceiops.eu), as normal e-mail with the sensitive data included in encrypted attachments created using the same technology[3]. Alternatively, the submission may be secured by the use of the popular encryption software PGP.

19. Passwords allowing access to the encrypted attachments will be disclosed using a different communication channel than the one used to transfer the encrypted data[4].

[1] Using the FreeOTFE (www.freeotfe.org) implementation of this technology.
[2] This goes a step further than the technology used to centrally store and analyse QIS3 and QIS4 data.
[3] Either the full version, or the "FreeOTFE Explorer" version that doesn't require being granted special IT rights to be used. Both are mutually compatible.
[4] Physical meeting, phone call or SMS for passwords related to encrypted e-mail attachments.