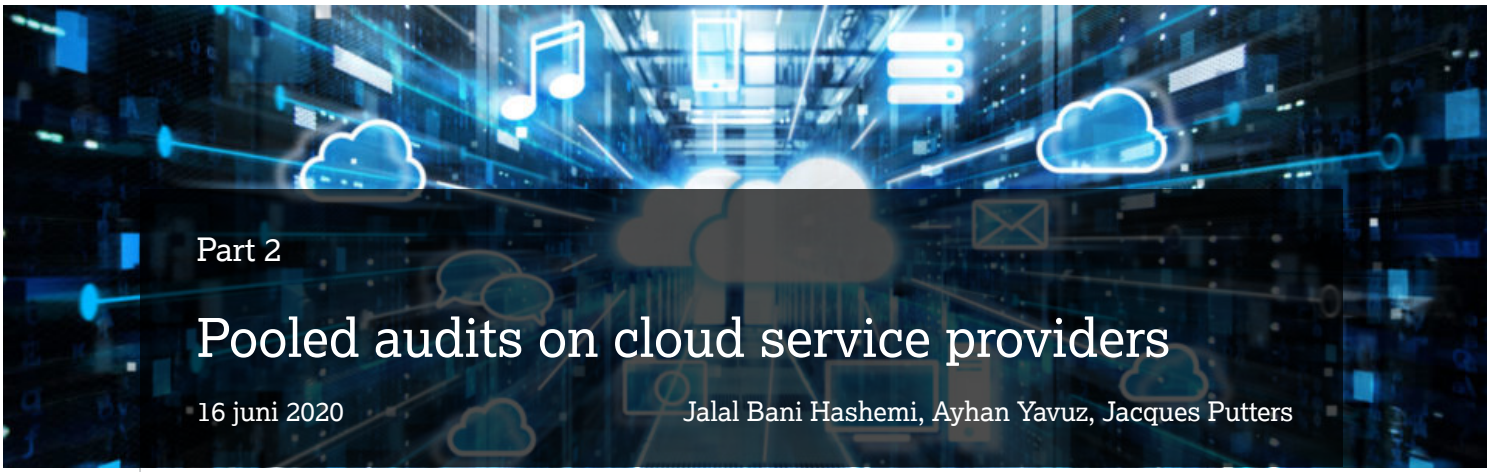

Part 2

# Pooled audits on cloud service providers

16 juni 2020

Jalal Bani Hashemi, Ayhan Yavuz, Jacques Putters

**This is the second part of our two-part article regarding pooled audits on Cloud Service Providers. It is based on our experiences with respect to the pooled audits we performed at two cloud service providers in 2018 and 2019.**

In Part 1, published on 11 March 2020, we outlined the context of these audits. We provided background information on cloud computing and outsourcing and the applicable laws, regulations, and guidelines relevant for financial institutions looking to utilise public cloud services. This was followed by a brief explanation regarding the most commonly used third-party certifications and the contractual framework we used for the pooled audits. In this second part we will present the audit framework, approach, organisation and testing procedures we used to perform the audits. In addition, we will present our experiences being part of such a pool of auditors – also in relation to the cloud service providers in question. Finally, we will share our conclusions and our notes for future audits.

## Audit framework, approach and organisation and testing procedures

The EBA Guidelines on outsourcing arrangements suggest using pooled audits as an option to acquire the required level of assurance regarding outsourced (cloud) services. However, the lack of experience in this area meant that the framework, the audit approach, the testing procedures, and the reporting practices needed to be built from the ground up by the Collaborative Cloud Audit Group (CCAG) Members. The core idea of the CCAG approach is to exercise unrestricted audit rights, and to maximise efficiency and effectiveness based on audit best practices. In essence, it enables individual audit rights to be executed in a group format (see figure 1) which benefits both the Cloud Service Provider (CSP) and the individual financial institutions.

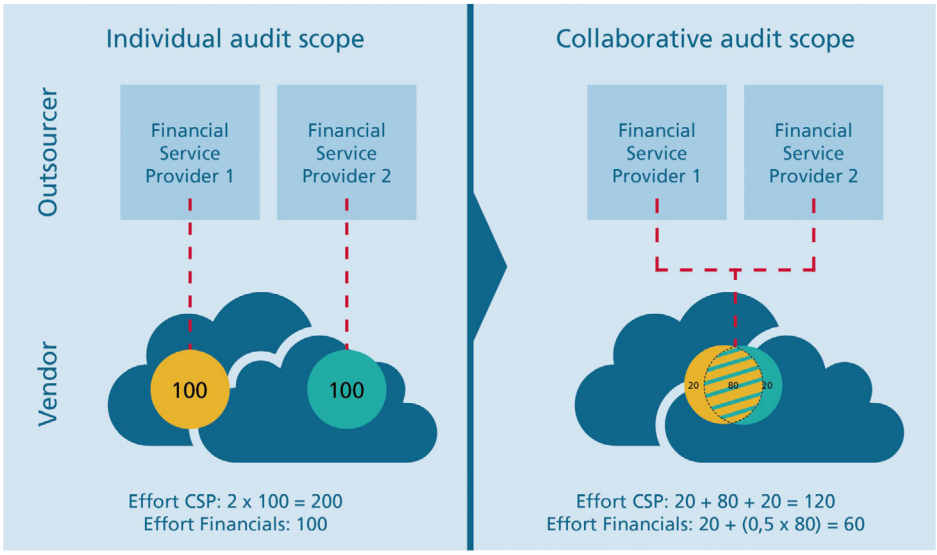


**Figure 1**: Effort required – individual audit scope versus collaborative audit scope

Not only is it much more efficient to do a pooled audit from a human resources perspective, it also means that the costs the CSP will allocate to the audit are shared between the participating institutions, thereby decreasing the costs per institution. Initially, the more institutions participate the lower the costs will be per institution. However, as the number of participating institutions increases, the more effort will be required for coordinating and aligning the audit activities between the participants and the more difficult it will become to take decisions. There will be a point where the increase in the number of participants will have a negative net effect on the efficiency of the audit. This will be elaborated on in the paragraph on future developments.

## Framework

While there are many frameworks available, we decided to use the Cloud Controls Matrix (CCM) of the Cloud Security Alliance (CSA) as the framework for our CSP audits. CCM is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles. The 16 control domains that CCM consists of are depicted in figure 2.


**Figure 2**: CSA CCM Control Domains

Every control domain consists of several controls and for each of these controls the architectural relevance (physical, network, compute, storage, app, data), the cloud service delivery model (IaaS, PaaS, SaaS) and the supplier relationship (Service Provider or Tenant) is indicated. Figure 3 shows this for one of the controls.

| Control Domain | Control Specification | Architectural Relevance | | | | | | Cloud Service Delivery Model Applicability | | | Supplier Relationship | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Phys | Network | Compute | Storage | App | Data | SaaS | PaaS | IaaS | Service Provider | Tenant / Consumer |
| | | | | X | X | X | X | X | X | X | X | |
| Application & Interface Security Application Security | Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations. | | | | | | | | | | | |

**Figure 3**: Example of a Control Specification as included in the CSA CCM

Although CCM was used as a basis for the audit, it was tailored to the needs of the Group whenever deemed necessary. For instance, we added controls when CCM seemed to be lacking in that area. And we excluded controls, for example when the control was already covered in one of the other control domains (we noted overlap in controls between the different control domains). In addition, for every control domain in scope the controls were translated into more detailed test procedures.

Finally, it is important to note that the audit activities described in this paragraph focus on the controls 'of the cloud' at the CSP's in question. 'Of the cloud' defines the environment managed by the CSP and made available to all customers of the cloud. This is illustrated by figure 4.

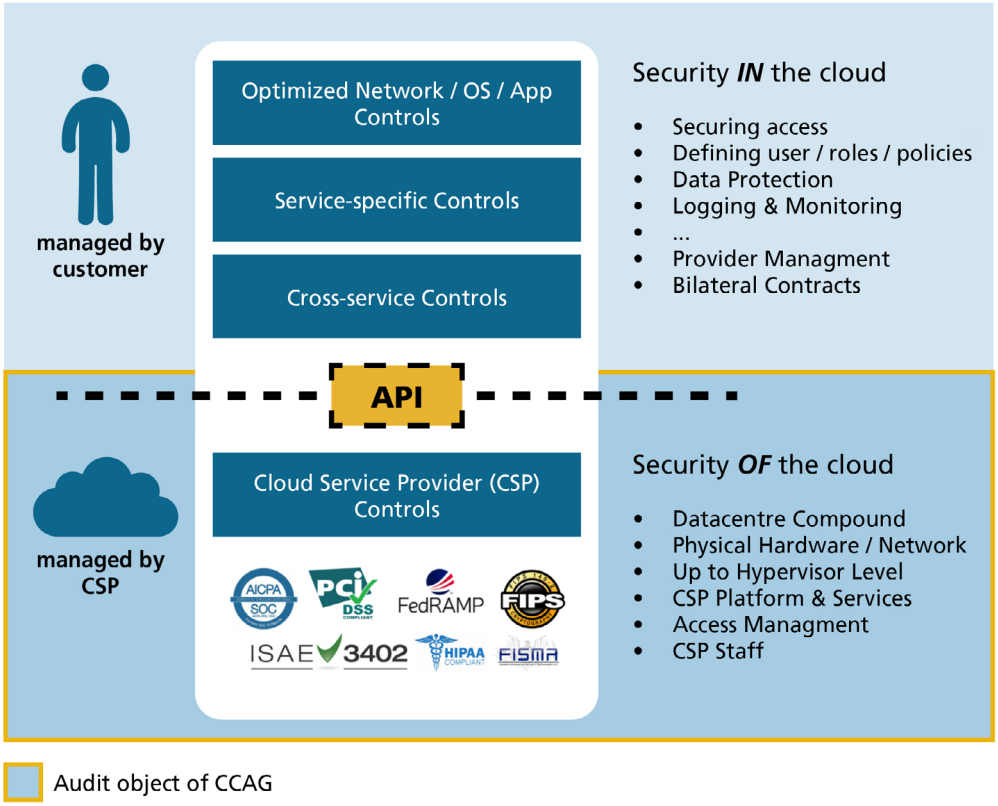


**Figure 4**: Security in the cloud versus security of the cloud

# Pooled audit organisation and approach

## Planning and organisation

Formally, the planning phase of the pooled audit starts with the 'Open Invitation Call'. The participants of the call are all CCAG members or companies who are planning to join the CCAG. The call is used by the financial institutions to express to what extent they are interested in auditing specific CSPs. After the call, this inventory of possible CSP audits is then distributed to all the (potential) CCAG members, requesting them to indicate which CSPs they would be interested in auditing. This results in an overall inventory of the CSPs with the financial institutions that are interested in joining the respective audits.

However, this does not mean that all included CSPs will indeed be audited. An important factor is whether there is sufficient interest in auditing a CSP. If only one financial institution is interested in auditing a specific CSP, then there will not be a pooled audit. This does raise the question: How many financial institutions need to be interested to make a pooled audit possible? Currently, the opinions vary between the CCAG members. Some have indicated that at least five financial institutions need to be interested, for such an audit to take place. Others have suggested that it only takes two financial institutions for it to be a pooled audit. Although we lean more towards the latter, the downside to such a small team is that the bargaining power towards the CSP diminishes.

The next step involves organising the kick-off meeting with all interested financial institutions for the CSP audit in question. The objective of the kick-off meeting is to establish a common information base within the audit team and to establish the general rules of engagement. This meeting is also used to vote for new Coordinators or to reconfirm the current Coordinators. Depending on the result of the vote, the new Coordinators take over or keep all the responsibilities and tasks of the coordinator role until the audit kick-off meeting next year. The same applies to the Project Management Officer who will support the Coordinators during the audit.

For each CSP audit, a (virtual) pooled audit organisation is established, consisting of CCAG members which all fulfil at least one role without formal authority or governance between the CCAG members. A short description of each role is provided below.

*Audit coordinator and backup*
The audit coordinator (per CSP) is tasked to coordinate the audit from start to finish. It is important to note that the coordinator has no formal authority or mandate over the CCAG members that participate in a pooled audit. The coordinator serves as a liaison for the CCAG members towards the CSP and vice versa. In practice, the coordinator also serves as an escalation path to decide on internal matters and to discuss problems with the CSP. He monitors the progress of the streams and makes sure that they finish in time. The second/backup coordinator ensures continuity of the audit as a fallback.

*Project Management Officer (PMO)*
The PMO volunteer assists the audit coordinator to schedule meetings and workshops, create and distribute meeting notes, and communicate decisions. The PMO is tasked to gather and distribute contracts, audit work-programs, and draft reports. And the PMO maintains the audit file repository, assuring that a full copy will be available for all participating members after the audit.

*Stream lead and buddy*
For each control domain to be covered in the audit, two CCAG members will have to volunteer to fulfil the role of stream lead and buddy. The stream lead ensures that the control domain objectives are covered. This includes defining controls for the related work-program, defining the Request For Information towards the CSP, gathering information during fieldwork, control testing and filing, and finally reporting. The stream buddy assists the stream lead by sharing the workload but also by serving as a sparring partner during each step. Where beneficial for quality or for coverage of the control domain, larger teams can be considered. The size of the team for a control domain should primarily be driven by the skill and qualification requirements, the planned coverage depth, and the complexity of the audited environment at the CSP. However, the mandatory minimum size is a team of two auditors.

The auditors who participate in the audit need to meet the minimum requirements with regards to experience, skills, and knowledge. The participating financial institutions are therefore requested to confirm that the auditors meet the minimum qualifications as established for each role.

## Preparation

Once the initial planning and organisation is done, the steps outlined in table 1 are taken as preparation for the on-site fieldwork.

| List of activities prior to on-site fieldwork | |
|---|---|
| 1. Individual risk assessments | All financial institutions perform a risk assessment regarding the CSA CCM control domains and the cloud services used by their organisations. |
| 2. Consolidation of risk assessments | The individual risk assessments are consolidated into one overall assessment regarding the control domains. A consolidated list of cloud services used is created. |
| 3. Determination of scope | During a workshop/call, the scope of the audit is determined in terms of control domains and cloud services, based on the consolidated overviews. |
| 4. Sourcing control domains | The control domains are sourced by stream leads and buddies from the participating financial institutions. |
| 5. Deliver first draft work program per control domain | Stream leads and buddies are tasked to create the draft work program for their control domain. |
| 6. Process feedback from CCAG members | All CCAG members participating in the audit are invited to provide comments and suggestions on the work programs and this initial feedback is processed by the stream leads and buddies. |
| 7. Discuss and approve work programs | The final draft work programs are discussed and approved by the CCAG members. |
| 8. Deliver mapping of work programs with available certification reports and notification towards CSP of relevant controls | Stream leads and buddies create a mapping between their work programs and the available certification reports (e.g. SOC 2, FedRAMP, etc.). Relevant controls are identified, and these alongside underlying evidence are listed in a Request for Information (RFI). |
| 9. Signed Project Collaboration Agreement | A Project Collaboration Agreement between CCAG members is signed by all CCAG members participating in the CSP audit. |
| 10. Signed Statement of Services | A Statement of Services is signed by all CCAG members and the CSP. |
| 11. Review available documentation and evidence | Available documentation and evidence for certification reports relating to the control domains in scope is made available for review by the CSP and analysed by stream leads and buddies. |
| 12. Determine scope of on-site fieldwork | After the desk study (previous step), stream leads and buddies create a proposal for the scope of the on-site fieldwork. All CCAG members participating in the audit are invited to provide comments and suggestions. After that, the scope of the on-site fieldwork is finalised. |
| 13. Share on-site fieldwork scope and RFI with CSP | The scope of the on-site fieldwork and the Request for Information (RFI) is shared and discussed with the CSP. |

**Table 1**: List of activities prior to on-site fieldwork

## On-site fieldwork

Up until this point, this description of the methodology has been theoretical and abstract. This paragraph describes our experiences regarding the on-site fieldwork. Although it pertains to different CSP audits we were involved in, these experiences were quite similar.

Based on the RFIs per stream/control domain, the CSPs made a schedule of presentations and meetings, covering the on-site fieldwork period of two weeks. In addition to this schedule, evidence requested via the RFI was gathered and made available for review on a share.

The presentations were mainly scheduled for the first two days to get the relatively new groups up to comparable – foundational – knowledge levels. However, all streams could join these presentations. When not attending these introductory presentations, the streams could read/analyse the information made available.

The remainder of the fieldwork period, specific meetings were scheduled per stream. When the schedule allowed, streams could attend each other's meetings. Typically, during the meetings, Subject Matter Experts (SMEs) from the CSP would elaborate on the questions of the RFI. Sometimes demonstrations or walk-throughs on the tooling/applications used were given. CSP internal control results were shared on-screen when applicable. Additional questions could be asked and when required, additional meetings were scheduled. It is important to note that we experienced a much more restricted and scripted environment than we as internal auditors are used to. In general, all meetings took place on a central location and all interviews were attended by the CSPs' audit coordination teams. It was not really possible to visit the CSP departments we had in scope and to ask questions to a broader set of employees working there.

While the auditors operated as a team, they primarily represented the interests of their companies. And for the team members to ensure that the work done by the other team members was sufficient and of adequate quality, it required all members to be involved in key steps of the audit process. These steps were: determining the scope of work (in terms of control domains, controls, services, and data centres), approving the work programs used to do fieldwork, reviewing and approving the test results, and finally reviewing and approving the report that would be shared with the CSP.

At the end of each day a wrap-up session chaired by the coordinator was held with the streams and after that another wrap-up meeting was held with the CSP representatives present. During the wrap-up sessions, progress was discussed and bottlenecks were identified. Ways to resolve the bottlenecks were proposed and discussed with the CSP. During the wrap-up session with the CSP, they were informed of overall progress,

experiences (good and bad) of that day, and changes required. The CSP valued the wrap-up sessions very much, because the sessions made sure that we received the information we requested and because the CSP's received a heads-up on the preliminary observations.

Per stream the observations were verified for factual accuracy with the CSP at the end of the on-site fieldwork as much as possible. In a few cases we did not succeed and additional conference call meetings were required with SMEs of the CSP after the on-site fieldwork period had ended.
A generic close-out meeting was held with representatives of the CSP on the last evening of the on-site fieldwork. Each stream prepared a presentation with their observations and shared them during this close-out meeting. The CSP was allowed to comment/give their view on the observations.

### Testing procedures

The audit team designed the testing procedures as they would do for any internal audit. The test of Design (ToD) was to be done based on the documentation made available for review in combination with interviews and walk-throughs during the on-site fieldwork, including a test of one.
Evidence for controls regarding Test of Effectiveness (ToE) needed to account for the scale of operations of the CSP. The highly automated nature of the CSP processes could justify smaller sample sizes. However, there are so many parties, processes, and software/tools involved that the audit procedures should ensure the automated controls applied to the processes and services in scope.

A highly specific topic was the extent to which reliance on the available external assurance reports would be possible. In order to alleviate the workload for the CSPs and ourselves, we decided to map our work programs and RFIs to the available SOC2 and FedRAMP reports. For the controls already covered by these assurance reports, the CSPs were offered the option to provide the same evidence as provided to the external auditors. For the controls that were not or not completely covered by these reports, additional work would have to be done.

To our disappointment, we were unable to rely on the work done by the external auditors based on the evidence that was provided. This was primarily caused by the fact that the evidence was incomplete: we did not have access to the external auditors' audit files which would probably also include their testing approach including process walkthrough information, meeting notes and observations done related to the controls tested. Consequently, both the CSPs and the audit team had to do more work than initially anticipated. Some SMEs also resisted: Why was the information that was sufficient for the external auditors not sufficient for our needs?

The Standard Operating Procedures, in combination with explanations, interviews, and walk-throughs during the on-site fieldwork in general provided sufficient basis for us to do the ToD. However, performing a (ToE) proved much harder for several reasons:

**a.** *We were not allowed direct access to any system but instead had to request for system output, which took relatively long and put our timelines under pressure.*
**b.** *Documentation and system output were often 'sanitised' by the CSP, mainly to protect the privacy of CSP staff and to protect highly confidential information that might expose the CSPs to threats. However, as this process also took time, timelines were put under pressure even more. In addition, some documentation was rendered (almost) useless by sanitising it as important data was now illegible.*
**c.** *Some documentation was deemed too confidential by the CSPs to share with the audit team. This meant that the required information was not provided, and testing could not take place.*

Of course, the limitations experienced during ToE had to be reflected in our report.

## Access to evidence and the audit file

Two repositories need to be distinguished: one that had to remain on premise at the CSPs and one that was used by the CCAG audit participants:

1. In general, CSPs do not allow their documentation to be taken off-premise. They are quite protective regarding what they consider to be their intellectual property. In the audits done, CSPs have therefore enabled viewing of the requested documentation via laptops provided by them. The auditors were not allowed to make copies of documents or any other material presented. As the provided evidence should still be available for review after the fieldwork, agreements needed to be made regarding which documents should be stored, the required retention time, and the access and integrity controls. An inventory of documents was provided by the CSP and all the streams compared the inventory with references to documents they made in their files (meeting minutes, work programs, etc.) and differences were reported back to the CSP.
2. The repository of the CCAG consisted of a Sharepoint environment made available by one of the CCAG members. Access was provided to all participating CCAG members and the streams were responsible for filing the required audit documents in that environment. Among others the following types of documents were filed: minutes of CCAG member meetings, work programs, RFIs, minutes of meetings with CSP, test results in work papers and (draft) report versions. At the end of the audit, every participating member copied the contents of the entire repository into his own company file. This, in combination with the file that is kept by the CSP, forms the complete audit file.

## Reporting

The reporting phase of collaborative CSP audits is split into two parts:

1. The first part involves sharing the results of the audit with the CSP. As a first step, a workshop was organised with all participating CCAG members to discuss the fieldwork results. For preparation, each stream lead ensured that the work papers for the related stream were complete. During the workshop the stream lead presented the results for the control domain to the other members and every participant had the opportunity to ask questions and provide comments. Based on the input of the streams, the audit coordinator then prepared the generic joint draft report that was first discussed extensively between the participating members. It turned out to be quite difficult to reach an agreement on items that could or should be reported, especially with larger audit teams. In particular in this phase the differences in backgrounds of the auditors showed. For example: where some members were used to reporting not only exceptions but also positive observations or controls tested without exceptions, other members rejected this as it would bring about an unnecessary audit risk for the auditors. Some members wanted to report 'issues' or 'findings' whereas other members insisted they be called 'observations'. Did we need to include agreed actions, or would formal management responses suffice? Did we need to express an opinion – overall or per control domain? In many cases members needed to compromise on these discussions, and usually the decision was made to choose the option that represented the least risk for the CCAG team. After the internal alignment, the report was discussed with the CSP. This was also not an easy task, as the audit coordination team of the CSP had to go back and involve the right SMEs again to verify our observations and provide the team with their responses. This took a number of iterations before the report could be finalised.
2. The second part of the reporting phase consisted of translating the generic report for the CSP into a specific report for the organisation that the participating CCAG member represented. For us it meant translating the generic report to the ABN Amro organisation. It involved using the organisation's risk appetite to determine which observations should be included in the report and which ones could be deleted, adding risk indications to the findings and writing an overall conclusion for senior management. This report was then discussed and distributed to the relevant ABN Amro stakeholders.

## Evaluation

Intermediate evaluations were performed during fieldwork to ensure that expectations were met for participating CCAG members as well as for the CSP. This helped to maintain alignment across all parties. After fieldwork and after sharing the draft report with the CSP, an evaluation was held with participating CCAG members to determine the strengths and improvement areas of the work performed. An additional evaluation was held with CCAG members together with the CSP to gather additional feedback for future audits. The key take-aways of these evaluations are included in section 'Conclusions and notes for future engagements'.

### Follow-up validation

Last year, one of the most frequently discussed points between CCAG members involved how to include follow-up validation on observations in the methodology. Initially, the idea was to collaborate up to and including the evaluation of the audit. After that the collaboration ended, so follow-up validation was to be done by the individual institutions. This resulted in dissatisfaction with the CSPs and also with many of the financial institutions. Why have all institutions approach the CSP for status updates separately and why have the institutions validate follow-up individually when this could just as well be done in collaboration? This is currently one of the many issues that are going to be addressed by a CCAG working group that aims to improve the methodology.

## Conclusions and notes for future engagements

Based on the results that were accomplished since the start of the CCAG we conclude that the pooled audit approach as suggested in the EBA Guidelines on outsourcing arrangements is a feasible option. During evaluations, almost all of the participating CCAG members have indicated that these pooled audits had been a very positive experience. Collaborating with people from other backgrounds, cultures, countries, experiences has been a great learning experience. One of the major benefits is that there are diversity effects: it proved possible to leverage the available, specific knowledge and experience of the participants. If there are auditors specialised in a certain topic, then why not use this? Also, due to the achieved synergies, the associated costs per financial institution have been a fraction of the costs that would normally be charged if a financial institution would cover the same scope on its own. Finally, and most importantly, the internal stakeholders have repeatedly expressed their appreciation for these audits.
Our experiences as to the collaboration with the CSPs have also been positive. The people we worked with were generally very professional and highly motivated to make these audits a success.
However, looking at the current (project-based) approach of the CCAG organisation and methodology, the following shortcomings are also clear:

- CCAG participants are relying on only a few key players to take the initiative. Resourcing of audits and legal preparatory activities are done ad hoc, and not all members are doing (have done) their fair share whereas others have done more than could be expected of them. For the people doing more than their fair share, balancing between 'business as usual' audits and these collaborative audits is cumbersome.
- The current project-based approach is not scalable: as more parties join and actively participate in audits, the limit of an effective and efficient audit team will probably be reached soon. Decision-making is cumbersome with too many people involved.

- The current project-based approach does not sufficiently support building a relationship with the CSPs and does not enable the audit teams to build upon experience and knowledge gained in previous audits. This is because the participating institutions as well as involved auditors can be different for every pooled audit.
- The current structure inadequately ensures the quality and consistency of the audit work performed across the different audits/CSPs because there hardly is an exchange of information between them.
- Knowledge and experience regarding public cloud technology and DevOps is still lacking with many auditors. This does not make a good impression on CSP staff and can be frustrating for the auditors who have to collaborate with these colleagues.
- CSPs and CCAG members have to get used to each other. CSPs are not familiar with the type of audits that internal auditors carry out. And the CCAG members are not used to the type of restrictions they have to deal with when doing a CSP audit.

As the abovementioned elements are widely recognised, work groups are trying to address them and regularly come with proposals to improve the overall governance, methodology and working practices. In addition, more and more participants have indicated to see additional opportunities for these types of audit. Why not use the same approach for audits on SaaS providers or vendors delivering HR, administrative or other back-office services?

In closing: as always, the start has been the most difficult part of our journey. But – with the ever-increasing relevance and importance of outsourcing – we are certainly hopeful that these pooled audits have a bright future.

## Drs. J. (Jacques) Putters RE CISSP CCSP CISA | Senior IT Auditor bij *ABN AMRO Bank NV*

Jacques started his career as mainframe / MVS system programmer at KLM. He has been working at Group Audit ABN AMRO as a technical IT Auditor since 2004. He has extensive experience in auditing IT infrastructure, such as OpenVMS, Tandem, HP-Unix, AIX, Solaris, Linux, Windows and z/OS and subsystems such as IMS and DB2.

## S.J. (Jalal) Bani Hashemi MSc RE CISSP CCSP CISA | IT Audit Manager bij *ABN AMRO Bank NV*

Jalal has been an IT Auditor at ABN AMRO Group Audit since 2010. He currently is the IT Audit Manager responsible for technical IT Audit coverage for IT infrastructure and platform services.

## A.J. (Ayhan) Yavuz RE | Senior IT Audit Manager bij *ABN AMRO Bank NV*

Ayhan started his career at ABN AMRO in 1995 as a management trainee. After that he worked in several positions within Group Audit, covering business lines, control functions and IT. He currently is the Senior Audit Manager for the Innovation & Technology audit team and spends a significant amount of time on audits on Cloud Service Providers.