Part 1

Pooled audits on cloud service providers

11 maart 2020 Jalal Bani Hashemi, Ayhan Yavuz, Delil Akdeniz, Jacques Putters

With this two-part article we aim to share our experiences with respect to the pooled audits we performed at two cloud service providers in 2018 and 2019. In Part 1 of the article we will outline the context within which these audits were performed. This relates to 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 is followed by a brief explanation regarding the most commonly used third-party certifications and the contractual framework we used for the pooled audit. In Part 2 (next edition) we will present our audit approach, framework and testing procedures. Finally, we will share our conclusions and notes for future audits.

Over the course of the past decade, cloud computing has become the foundation for disruptive trends such as the Internet of Things, data analytics and artificial intelligence. It is giving organisations a competitive advantage in digital transformation in terms of innovation, agility, resilience and skills. As more and more organisations are realising this, adoption of public cloud is taking place at a staggering rate. Gartner forecasts cloud computing to be a $300 billion business by 2021.[1]

Concerns regarding adoption of public cloud technology

The financial services industry was hesitant adopting public cloud technology at first. Security and compliance concerns prevented them from migrating critical workloads into the public cloud and made many of them instead choose for private cloud implementations. In addition, the financial services industry is heavily regulated, causing these companies to be very cautious.

The security and compliance concerns are usually related to the following:

- Data could be compromised or exploited by Cloud Service Providers (CSPs), by other clients of the CSPs (due to ineffective tenant isolation) or by federal law

enforcement offices that compel these CSPs via warrant or subpoena to provide requested data.
- Unavailability of applications due to Cloud Service Providers providing their services on standard terms, with limited guarantees.
- Vendor lock-in when:
    - access to cloud resources is gained through proprietary APIs and web interfaces (also known as ‘code level lock-in’);
    - use is made of cloud services that force the consumer into a CSP specific architectural style (also known as ‘architectural lock-in’);
    - shifting to a different cloud vendor would involve high costs.
- Inability to perform required control and audit activities to ensure cloud services are delivered in line with laws and regulations but also policies and standards of the outsourcing company.

The last listed concern is exemplary for the shift that outsourcing has made over the course of the past fifteen years.

Traditional vs modern-day outsourcing

Traditionally, outsourcing companies outsourced part(s) of their business or supporting processes ‘as is’, implying that the vendor took over the processes, systems, people and sometimes even physical infrastructure under a tailor-made contract. Nowadays however, outsourcing usually goes hand in hand with standardisation. Vendors are willing to take over the responsibility for a business process or supportive process only if they can standardise it in order to run it as efficiently as possible. Table 1 shows the main differences between traditional and modern-day outsourcing, of which public cloud computing is a good example:

Traditional outsourcing	Modern-day outsourcing
Outsourcing of service, process, system 'as-is'	Standardised service, process, system
Mainly aimed at reducing costs and improving performance	More aimed at deploying disruptive solutions faster, transforming the way business is done and supported
Vendor is only allowed to change the out-sourced service after approval from/notification to client	Vendor can change its services at his own discretion. Clients are not necessarily involved or informed
Bespoke contract, attuned to the needs of both parties	Standard contracts without tailor-made arrangements
Client has negotiating power	Vendors (especially CSP's) have negotiating power
Client's policies and standards apply	Policies and standards of vendors apply
Right to audit/examine can be agreed upon	Right to perform audits/inspections is difficult or impossible to establish
Bespoke service delivery reports	Standard reporting facilities
Second line of defence can perform its oversight and risk control duties	Second line of defence is not allowed access to perform regular oversight and risk control duties

Table 1: Traditional vs modern-day outsourcing

Notwithstanding the concerns raised, more and more financial services companies are considering the adoption of public cloud as vital if they are to survive in the highly competitive marketplace. In line with this trend, in 2016 ABN Amro decided to start working on the implementation of two public cloud platforms: one on Microsoft Azure and one on Amazon Web Services. During contract negotiations with both CSPs, it became apparent that they were reluctant to grant a right to audit to ABN AMRO. They suggested the bank rely on the available third-party certifications and assurance reports. In the meantime however, the European Banking Authority (EBA) published a consultation paper with recommendations on outsourcing to cloud service providers. These recommendations included the option that financial institutions use a so-called 'pooled' audit approach to exercise the – in the opinion of EBA – unquestionable right to audit. Nevertheless, we were not hopeful that this would put pressure on the leading Cloud Service Providers to such an extent that they would cave and allow us to do audits regarding the services they deliver.

However, based on regulatory considerations, Deutsche Börse Group took the initiative to establish the Collaborative Cloud Audit Group (CCAG) in 2017, with the aim to perform pooled audits on the main Cloud Service Providers. As we were interested, we decided to join this initiative and actively participate in the first pooled audit on Microsoft Azure, one of the largest Public Cloud Providers. Based on the success of that first audit, we continued being an active member and participated in audits on Amazon Web Services, and Microsoft Azure and Office 365 this year.

Applicable laws, regulations and guidelines

In general, legislators and regulators have had the following concerns regarding the (increased) outsourcing of (regulated) activities by financial institutions:

- It might impact their ability to manage their risks and monitor their compliance with regulatory requirements or to demonstrate to their regulators that they are able to do so.
- They might over-rely on outsourced activities that are critical to their ongoing viability as well as their obligations to customers.

These generic concerns have been addressed by legislators and regulators by putting in place several laws and regulations that in general all seem to apply the following rule: *Outsourcing of important operational functions may not be undertaken in such a way as to impair materially the quality of internal control and the ability of the supervisor to monitor the firm's compliance with all obligations*.

More specifically, the following laws, regulations and guidelines refer to the right to perform audits related to outsourced activities in the financial services industry (non-exhaustive list):

- In the Netherlands: Besluit Prudentiële Regels Wft (art. 27-32), Besluit Gedragstoezicht Financiële Ondernemingen (art. 36-38l).
- In Germany: Minimum Requirements for Risk Management (MaRisk) released by BaFin. Particularly relevant sections are AT 9, AT 4.4 paragraph 3 and 4, BT 2.1 paragraph 3, and BT 2.3 paragraph 1.
- Markets in Financial Instruments Directive (MiFIDII, Article 16-2).
- Basel Committee on Banking Supervision – Outsourcing in Financial Services (Guiding Principle III).
- European Banking Authority – Recommendations on outsourcing to cloud service providers (Section 4.3).
- European Banking Authority – Guidelines on outsourcing arrangements (as of the 30th of September 2019) (Section 13 (art. 75p and 85-97)).
- EU General Data Protection Regulation (Article 28, 3h).

The EBA recommendations for outsourcing to Cloud Service Providers (CSP) were first to present the option to perform pooled audits organized jointly with other clients of the same CSP, and performed by these clients or by a third party appointed by them. Main aim of these pooled audits is to use audit resources more efficiently and to decrease

the organisational burden on both the clients and the service provider. This option has also been included in the recently published EBA Guidelines on outsourcing arrangements.

Third-party assurance reports and certifications

CSPs generally prefer to provide their clients with assurance reports instead of allowing clients' auditors to perform audits. And it is easy to see why. CSPs such as Microsoft Azure, Amazon Web Services and Google service so many clients that they would be unable to run their business even if only a small portion of their clients would be allowed to perform on-site audits or inspections. And many of their clients also prefer to rely on available assurance reports instead of performing their own audits as these assurance reports will fulfil the generic assurance needs of the majority of clients. All significant CSPs nowadays provide for these assurance reports, many of which are based on the 'System and Organisation Controls' (SOC) reporting standards. The most commonly used assurance reports are the following:

- **SOC 1.** A SOC 1 report is a report on controls at a service organization which are relevant to user entities' internal control over financial reporting. The SOC 1 report is what you would have previously considered to be the standard SAS70 (or SSAE 16), complete with a Type I and Type II report, but falls under the SSAE 18 guidance (as of May 1, 2017).
- **SOC 2, SOC 3.** The SOC 2 and SOC 3 reports have been created to address controls relevant to operations and compliance. The SOC 2 report will be performed in accordance with AT 101 and is based upon the Trust Services Principles, with the ability to test and report on the design (Type I) and operating effectiveness (Type II) of a service organization's controls (just like SOC 1/SSAE 18). The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. The difference between a SOC 2 and a SOC 3 report is that a SOC 3 report is permitted to be freely distributed (general use) and only reports on whether the entity has met the Trust Services criteria or not (no description of tests and results or opinion on description of the system).
- **Security Assessment Report (SAR).** CSPs interested in having the U.S. Government as a consumer of their service must meet the FedRAMP (Federal Risk and Authorization Management Program) security requirements and implement FedRAMP baseline security controls. CSPs verify their compliance with FedRAMP security requirements by following the FedRAMP Security Assessment Framework and a third-party assessment organisation will verify implementation of the framework and will report on that in the SAR.

These assurance reports cover a large number of IT general controls and usually have a broad scope, but the depth of these reports will generally be more limited than that of internal audits. In addition, the audit of infrastructural components is generally not included in the scope of these reports.

The EBA Guidelines on outsourcing arrangements stress that institutions and payment institutions should make use of the aforementioned assurance reports only if they ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the financial institution or payment institution and the compliance with relevant regulatory requirements. In addition, they should be satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, reperformance/verification of the evidence in the underlying audit file) and that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operating effectiveness of the key controls in place.[2] We therefore included a basic assessment of the adequacy of the available reports in the methodology of the pooled audit approach.

Contractual framework

When Deutsche Börse Group took the initiative to establish the Collaborative Cloud Audit Group (CCAG) in 2017, they also established a contractual framework to govern the CCAG and the audits that would take place under its flag. This contractual framework consisted of two extensive agreements: The CCAG Collaboration Agreement and the Project Collaboration Agreement.

In addition to these agreements, which stipulate the way the relevant financial institutions organise public cloud audits, a separate agreement has to be negotiated for every audit with the relevant Cloud Service Providers. This agreement is usually called a ‘Statement of Work’ or ‘Statement of Services’. These agreements are presented in the following paragraphs.

CCAG Collaboration Agreement

Institutions that want to participate in one of the audits that take place each year need to first become part of the CCAG by signing the CCAG Collaboration Agreement. This Agreement governs the overall relationship between the Group Members of the CCAG. The Collaboration Agreement is open for accession by any regulated financial institution, subject to the terms set forth in the accession clause in the agreement. By entering into this Agreement, the Group Members commit to actively support collaborative audits. The Agreement also covers subjects such as how to split costs incurred in relation to the Collaboration, compliance with all relevant antitrust laws, liability, indemnification, intellectual property, publicity and announcements, confidentiality and representation.

Project Collaboration Agreement (PCA)

Pooled audits involve a collaborative effort by a group of auditors from different organisations. To clarify the nature and scope of the collaborative effort, a Project Collaboration Agreement is necessary. This is an agreement between at least two parties looking to work together on an audit on a collaborative or cooperative basis. The

agreement spells out the specific terms and conditions of the parties' working relationship including the allocation of responsibilities and division of costs related to the audit. The PCA outlines the collaborative activities including scope, volume, timelines, participation, preparation, execution, and follow-up activities. Group Members which agree to the PCA must provide sufficient and qualified resources and commitment to the collaborative audit. Audit results will only be shared between members that collaborate under a PCA and not with the other Group Members. It is important to note that Group Members which signed the CCAG Collaboration Agreement are not obligated to enter into a PCA.

Statement of Services

A prerequisite to enter into a PCA is the contractual right to audit that must have been negotiated by the individual financial institutions with the Cloud Service Provider in question. For Microsoft this implies having signed an M248/M399 addendum in addition to the Microsoft Online Service Terms. However, as the PCA is the agreement between the participating financial institutions only and does not include the CSP, an additional agreement is required with the CSP. This agreement – in case of the audit regarding Microsoft called a 'Statement of Services' (SOS) – includes the respective responsibilities of the participating financial institutions and Microsoft, the scope of work, the activities, the rules of engagement and an initial calculation of the related costs by Microsoft. This agreement, signed individually by all financial institutions, will also form the basis for the invoice after completion of the audit.

Summary Part 1 and outlook Part 2

Although the financial services industry had been hesitant using public cloud technology in the recent past, more and more of these companies are currently considering the adoption of public cloud as vital if they are to survive in the highly competitive marketplace. However, as legislators and regulators have had serious concerns regarding the (increased) outsourcing of (regulated) activities by financial institutions, several laws and regulations were put in place to address these concerns. More or less forced by these laws and regulations, cloud service providers have had to allow for audits by their financial services clients, even although they generally have a number of external assurance reports and certifications available. One way to do these audits is in a 'pooled' or 'collaborative' manner. In 2018 and 2019 we joined forces with a group of European financial institutions to perform audits at two of the largest cloud service providers using this pooled approach. However, in order to do so, the group had to start from scratch. An extensive legal framework had to be designed and implemented. This was all outlined in this first part of our article. The second part, that will be published in the next issue, will contain a description of the audit framework, and the approach, organisation and testing procedures we used to actually 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 give our view on the future of the collaborative approach.

Notes

[1] Gartner Press Release, August 15, 2018.

[2] We decided not to include the full text of article 93 of the EBA Guidelines on outsourcing arrangements but to only include the most relevant statements.

D. (Delil) Akdeniz Msc. RE CISSP CCSP | Information Security Consultant bij *RD IT Risk Control*

Delil worked as an information security consultant/auditor at PwC for more than five years before switching to Group Audit ABN AMRO in November 2016. There he focused on IT infrastructure and cloud computing in particular. In September 2019 Delil started working as an independent consultant.

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.