ABN·AMRO

Collaborative Cloud Audits

Specific assurance for the financial services industry

Ayhan Yavuz – February 2020

Table of contents

1. *Context & developments*
2. *Regulatory framework*
3. *Assurance*
4. *Pooled audits – the best way forward?*

1. CONTEXT & DEVELOPMENTS

From traditional to disruptive outsourcing

Traditional outsourcing is dead.

Long live disruptive outsourcing.

Deloitte Global Outsourcing Survey 2018

Outsourcing: traditional vs modern

Traditional

- *Outsourcing of process /system “as is”.*
- *Vendor is only allowed to change the outsourced service after approval from/notification to client.*
- *Bespoke contract, tailor-made to the needs of both parties.*
- *Client has negotiating power.*
- *Client’s policies and standards apply.*
- *Right to audit/examine can be agreed upon.*
- *Bespoke service delivery reports.*
- *2nd LoD can perform its oversight and risk control duties.*

Modern

- *Standardised (cloud) service, process/system.*
- *Vendors can change their services at their own discretion. Clients are not necessarily involved or informed.*
- *Standard contracts without tailor-made arrangements.*
- *Vendors have negotiating power.*
- *Policies and standards of the vendors apply.*
- *Limitations re right to perform audits/inspections.*
- *Standard reporting facilities;*
- *2nd LoD are not allowed the access to perform its regular oversight and risk control duties.*

Disruptive outsourcing

Disruptive outsourcing solutions—led by cloud and automation—are fundamentally transforming traditional outsourcing.

- *From cost reduction and performance improvement to disruptive outsourcing solutions.*
- *Focus shift from traditional work transfer to upfront transformation and automation.*
- *“Buying” capabilities in the marketplace is generally faster and more scalable than developing capabilities internally.*
- *Emerging solutions incorporating cloud and automation are empowering organizations to work smarter, scale faster, reach new markets, increase productivity.*
- *However, effort and expertise are needed to address security and cyber risks, changing regulations, organizational resistance, skill gaps, and to help flatten fragmented processes.*

Disruptive outsourcing: Public Cloud

Public Cloud adoption (including SaaS) will give organisations the competitive advantage in digital transformation in terms of innovation, agility, resilience and skills.

For many companies it is becoming a matter of survival!

2. REGULATORY FRAMEWORK

Regulatory requirements - assurance

Applicable laws, regulations and guidelines (non-exhaustive list):

- *Netherlands: Besluit Prudentiële Regels Wft (artikelen 27-32), Besluit Gedragstoezicht Financiële Ondernemingen (artikelen 36-38l).*
- *Germany: Minimum Requirements for Risk Management (MaRisk) released by BaFin. Particularly relevant sections are AT 9, AT4.4§3 and 4 and BT 2.1 §3, BT2.3§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 – 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).*

In general the following rule applies:

Outsourcing of important operational functions may not be undertaken in such a way as to impair materially the quality of its internal control and the ability of the supervisor to monitor the firm’s compliance with all obligations.

3. ASSURANCE

Assurance reports to cover the gap

- *CSP’s prefer to provide assurance reports instead of allowing clients’ auditors the right to audit.*
- *These assurance reports are supposed to fulfill the generic assurance needs of the clients.*
- *All significant CSP nowadays provide for these assurance reports, which are more and more based on the “Service Organisation Control” standards:*
  - *SOC 1: covers controls relevant for financial reporting.*
  - *SOC 2: covers 'Reporting on Controls at a Service Organisation, relevant to security, availability, processing integrity, confidentiality or privacy‘; standards are based on the “Trust Services Principles and Criteria”.*
  - *SOC3: Identical to SOC 2, but the published report can be considered to be a certificate.*
  - *FedRAMP (Federal Risk and Authorization Management Program): 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 Security Assessment Report (SAR).*
- *These assurance reports cover a large number of IT general controls and usually have a broad scope of services but the depth of these reports would normally be more limited than that of internal audits.*

EBA requirements for external certifications and pooled audits

Institutions and payment institutions should only make use of external certifications and pooled audits where they:

- *ensure that the scope of the certification or audit report covers the key systems and controls identified by the institution and payment institution and relevant regulatory requirements;*
- *thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the report is not obsolete 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;*
- *ensure that key systems and controls are covered in future versions of the certification or audit report;*
- *are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);*
- *have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls. The number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; and*
- *retain the contractual right to perform individual audits at their discretion.*

4. POOLED AUDITS – THE BEST WAY FORWARD?

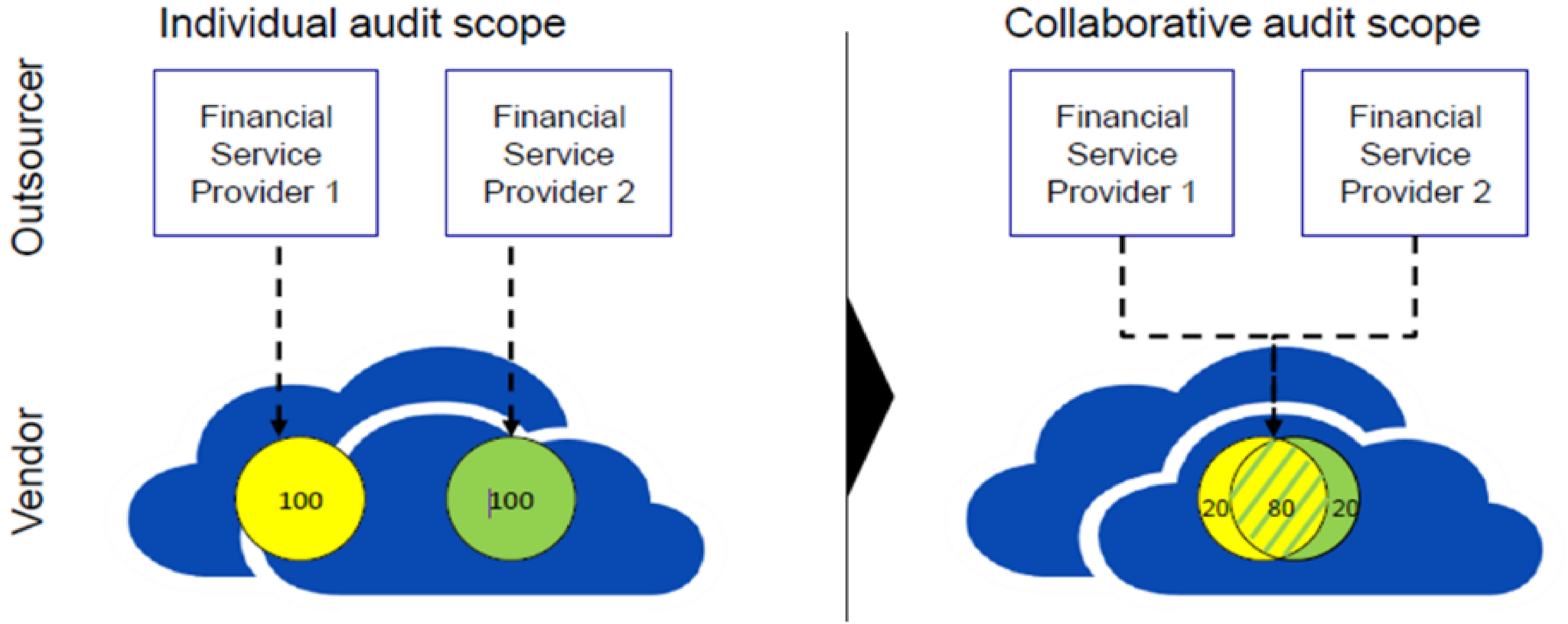
Establishing the Collaborative Cloud Audit Group to do pooled CSP audits

- *In June 2017 a Collaborative Cloud Audit Group was set-up on the initiative of Deutsche Börse.*
- *This collaborative audit group performed a proof of concept in Q3/Q4 2017 on Amazon Web Services (AWS) which confirmed that such a collaboration format is viable for audit collaboration.*
- *In 2018 we aimed to explore the possibility to perform a pooled audit according to EBA recommendations, taking into account regulatory requirements applicable to the respective financial institutions.*
- *In 2018 an audit on Microsoft Azure was performed by 8 FIs.*
- *In 2019 three CSPs were audited by the CCAG.*
- *2020?*

Cornerstones for the CCAG

- *Currently consists of almost 30 EU regulated Financial Institutions / Insurance companies.*
- *Audits are to be performed by Internal Auditors of the CCAG member group.*
- *Every financial institution must nominate one Auditor and one Legal contact.*
- *Active vs passive participation*
- *No contracting of a 3rd party audit firm on behalf of the CCAG Members.*
- *Comprehensive contractual framework for protection and disclosure of confidential information.*
- *Pre-requisite: an existing business relation with the CSP & respective audit rights.*
- *Each financial institution to cover it’s own costs and plan for respective (travel) budget.*

Pooled CSP audits - Advantages



Individual audit scope

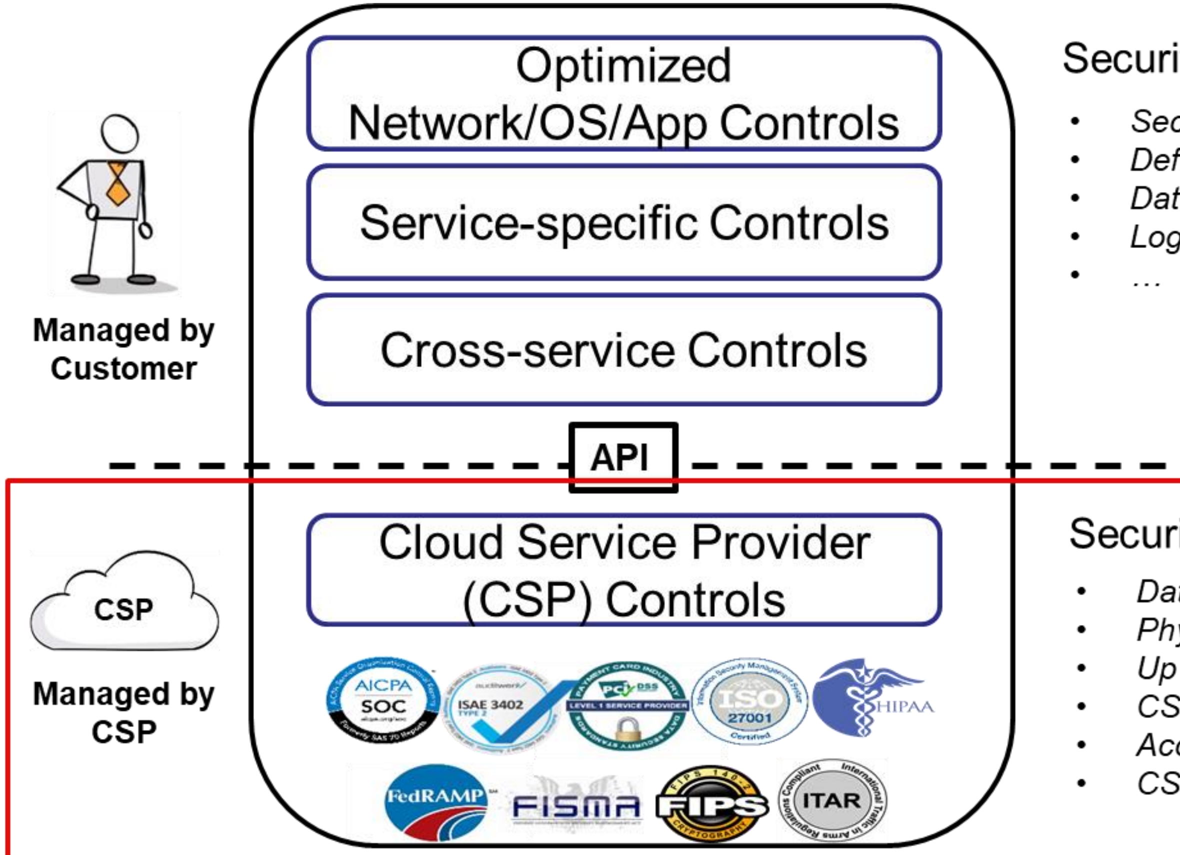
Collaborative audit scope

Outsourcer
Vendor
Financial Service Provider 1
Financial Service Provider 2
100
100
Financial Service Provider 1
Financial Service Provider 2
20
80
20

Effort CSP: 2 x 100 = 200
Effort Financials: 100

Effort CSP: 20+80+20=120
Effort Financials 20+(0,5x80)=60

Security of the cloud vs security in the cloud



Optimized Network/OS/App Controls

Service-specific Controls

Cross-service Controls

Managed by Customer

API

CSP

Managed by CSP

Cloud Service Provider (CSP) Controls

Security ***IN*** the cloud

- *Securing access*
- *Defining User / Roles / Policies*
- *Data protection*
- *Logging & monitoring*
- *…*

Security ***OF*** the cloud

- *Datacentre compound*
- *Physical hardware / network*
- *Up to hypervisor level*
- *CSP platform & services*
- *Access management*
- *CSP staff*

□ Focus of collaborative audit group

CCAG Audit Approach and Methodology: Scope determination

- *Cloud Controls Matrix (CCM).*
- *16 Control Domains mapped across various compliance criteria including but not limited to; SOC, COBIT, NIST, ISO and PCI.*
- *Data Centres – Relevant for the FI’s in question.*
- *Services – Relevant for the FI’s in question.*

CCAG Audit Approach and Methodology: Coverage

Application & Interface Security	Audit Assurance & Compliance	Business Continuity Management & Operational Resilience	Change Control & Configuration Management
Data Security & Information Lifecycle Management	Datacenter Security	Encryption & Key Management	Governance and Risk Management
Human Resources	Identity & Access Management	Infrastructure & Virtualization Security	Interoperability & Portability
Mobile Security	Security Incident Management, E-Discovery, & Cloud Forensics	Supply Chain Management, Transparency, and Accountability	Threat and Vulnerability Management

CCAG Audit Approach and Methodology: Coverage

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
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.			X	X	X	X	X	X	X	X	

Conclusions & lessons learned

General conclusions

- *Pooled audit approach is feasible*
- *Positive, special experience*
- *Shared costs >>> limiting costs per Institution*
- *Synergy: More efficient than performing individual audits*
- *Leveraging on knowledge and experience of other participants*
- *Unrestricted audit rights? >> Yes but some exceptions applied*

CSP Collaboration

- *Very professional*
- *Motivated to make it work*
- *Pleasant collaboration*
- *Transparency Centre – MS*
- *Sharing of documentation*
- *Getting used to each other*
- *Expectations*

Conclusions & lessons learned

Contractual foundation

- *Current CCAG contract allows for more members to join*
- *Lays a good foundation for future developments*
- *Structure with CCAG vs Project Collaboration Agreement*
- *Cooperation of Legal experts*
- *Time/effort for setting up the contracts is a generic bottleneck*

Team

- *Experienced internal auditors but…*
- *Willingness to cooperate*
- *Diversity effects*
- *Knowledge and experience regarding public cloud*
- *Knowledge of CSP services*
- *Balancing BAU vs CSP audits*
- *Cultural differences*
- *Decisiveness*

Next steps

How do we proceed from here?

Continuing seems to be a no-brainer, but how?

Next steps – main questions

- *Do we need a standing organisation next to the project-based approach for individual audits?*
- *What should be the scope (which CSP's) and mandate of the CCAG and what are the rules of the game?*
- *New entrants for the CCAG are allowed. But when does the group become too big to be effective?*
- *New entrants, new rules?*
- *Financial consequences?*
- *Whom does the CCAG represent? European financials? Who will be allowed to join?*
- *What approach for auditing CSP's should be used (No use reinventing the wheel or approaching each CSP differently)?*
- *How do we share results and lessons learned with group members that enter the group and that will actively participate in future audits?*

The future of CPS audits – Possible design

For any pooled audit to be acceptable, the requirements as outlined by EBA should be complied with >> should be part of the design of the CCAG

Of course there will be more than one answer to the questions and more than one design for the CCAG might work.

The future of CPS audits – Possible design

Questions?