JULY 2022

Cloud auditing
Assurance resources & pooled audits

TECHNICAL PAPER

www.ebf.eu

CONTENTS

EXECUTIVE SUMMARY

As consumer expectations and new technologies have emerged, so too have the opportunities cloud computing presents for all businesses, notably Financial Institutions (FIs). For the latter, adopting cloud computing is paramount but must be done in full compliance with the regulatory frameworks in force to safeguard data security and mitigate risk in this virtual environment.

The digital transformation underway continues to re-shape and advance cloud technology and – in turn – the auditing thereof. Indeed, while this technologically-driven advancement is happening, EU regulators are creating a more elaborate regulatory ecosystem for cloud adoption in Europe, addressing, among other aspects, cloud auditing. This paper focuses on the auditing of Cloud Service Providers (CSPs), where the FI directly outsources to the CSP.

REDEFINING AUDIT REQUIREMENTS IN CLOUD OUTSOURCING

For FIs to secure their risk-based approach to cloud technology, audit requirements are a central tool. For cloud outsourcing, the shared responsibility model differs from classical IT outsourcing (e.g., data centre hosting) and may also sometimes differ between cloud services themselves.

Given the cloud environment, the traditional Three Lines of Defence (TLoD) Model must be applied. That said, the consequent division of controls may be more complex to understand, implement, and audit, and require an updated assignment of responsibilities; these are outlined in the RACI matrix included in the Annex.

There is a 5-step auditing process for cloud computing, from audit trigger, to preparation, fieldwork, reporting, and lastly, follow-up actions. Auditing controls should assess control model design, model implementation, and control testing. To support the process-based approach to understanding the organisation of, and interactions with, CSPs, seven key principles are presented, feeding into the central risk-based approach for FI use of cloud computing.

Furthermore, boosted by the impact of Covid-19 on business operations, cloud auditing tools and processes are expected to further digitise and decentralise the workforce – including auditors – making remote cooperation an interesting feature to consider.

PRACTICAL GUIDANCE FOR POOLED AUDITS

The EBA Guidelines (GL) on Outsourcing (2019) outline supervisory expectations for cloud auditing today. While FIs and CSPs adhere to the EBA requirements establishing the foundation of FI cloud use and respective auditing, cloud service use by a large number of FIs with a concise number of hyperscale providers inevitably leads to certain questions being repeated in the FIs' audit execution process.

Section 2 of this paper explores the question of efficiency for cloud auditing, looking closely at assurance tools available, and the foundation and restrictions the EBA Guidelines offer. Completeness of audit results is arranged vis-à-vis the assurance tools' level of independence. Outlining benefits and drawbacks, different tools for FI consideration are presented, catering to bank risk-appetites in the risk-based approach.

Founded on the EBA GL requirements, the EBF Cloud Banking Forum Best Practices aim to help FIs and CSPs meet regulatory obligations while reflecting cloud service usage at scale. While they do efficiently offer understanding on hyperscale cloud services, third-party certifications and reports should not be relied on exclusively for several consecutive years.

CSPs' internal audit reporting can add to this picture, as appropriate under the EBA GL. Various factors need to be considered to gauge appropriateness, namely the: risks associated with the outsourcing arrangement; number of additional available assurance tools, consistency with FIs' internal audit functions; frequency of internal or pooled audits the FI intends, and mandate and objectives of the CSP's internal audit function.

Where the EBA GL lay out eight preconditions for using third-party reports and internal audit reports, FIs and CSPs need to define their understanding of said preconditions. Section 2.4.5 provides a common approach, highlighting key actions for FIs under each precondition.

Streamlining the audit process of a larger number of FIs towards the hyperscale CSPs reduces costs and saves resources. FI collaboration using a pooled audit approach – already included as part of the EBA GL – is steadily growing in the financial industry, benefiting both sides of the audit process. Structured work and extensive exchange of information to better understand risks and processes supports risk mitigation.

THE POOLED AUDIT PROCESS

The pooled audit process, its key conclusions, and the follow-up actions are based on eight governing principles. These are outlined in Section 3, which also provides guidance for the methodological setup of a pooled audit based on experience gleaned from prior pooled audit collaboration exercises in the market.

For an audit programme, preparation is key. When key factors are commonly understood, there are gains in efficiency. Testing procedures must be detailed, and timelines clearly communicated between FIs and the CSP in question. Section 3.2.3 outlines which details must be shared within the pool's audit group and which ones the pool must communicate with the CSP. The pool's auditors should provide the CSP with a list of required documents defining evidence requests such as specific types of written documentation, screenshots of internal tools, and data/metadata samples. Paired with public information sources by the CSP, both sides of a pooled audit thereby understand the instruments involved in the process very clearly.

Compliance certifications and attestations such as ISO and SOC reports provide auditors with helpful information upfront and a base from which to build according to their FI's risk-based approach to cloud. As part of the audit preparation phase, it is essential that the pooled audit aligns audit scope mapping with CSP controls which pool participants then assess based on the common audit approach agreed by the pool. The pooled audit's service scope should be defined based on each participant's use of the CSP service and their criticality.

Considering the potential number of pooled audit participants, audit fieldwork design and execution requires particular attention. Outlining the fundamental understanding and evidence types required in the fieldwork, Section 3.2.3 provides guidance in this regard such as best practices, testing modalities, and audit walk-throughs, all of which aim to create a harmonised understanding among FIs that are considering participating in a pooled audit.

A full pooled audit includes a finalised audit programme, executed audit fieldwork, and completed and comprehensive audit documentation. The pool's cooperation with the CSP, however, should always be considered as a learning process. In this regard, dedicated, post-fieldwork conversations should be held to drive cloud solution maturity.

Once the pooled audit is carried out, the group observation report establishes the final conclusions. FIs should consider the group report in individual audit reports, applying their individual risk appetites and respective cloud usage profiles. Audit follow-ups reflect the wide variety of nuances in cloud adoption by different FIs. Nevertheless, considerable options exist, including general (not customer-specific) control remediation by the audited CSP; individual mitigation actions with individual FIs from the audit pool; a CSP-standardised audit remediation report to the pooled audit members (commonly), and the pick-up of follow-up activities under the scope of a potential subsequent pooled audits (advancing the activities from bilateral to group level).

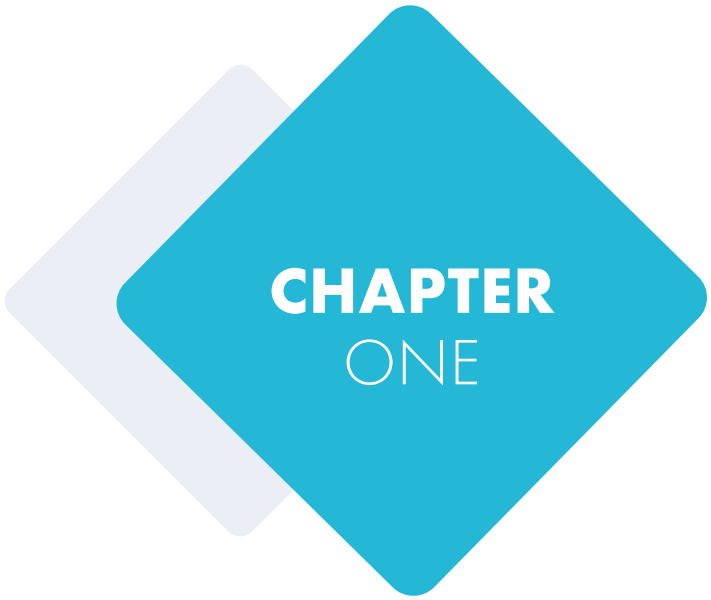
LEVERAGING DIGITALISATION FOR POOLED AUDITS

Digitalisation is increasingly enabling remote tool automation, greater efficiencies, and cost effectiveness. As the Covid-19 crisis confirmed, cloud auditing also offers remote options for health safety for any personnel involved in the process. However, pre-requisites for remotely conducting an audit should be clearly defined in the audit preparation phase. Section 3.2.3.5 offers procedural steps that should be included, ranging from remote interviews to live demonstrations, interactive virtual sessions, and the provision of evidence. Given the nascent and growing potential for the use of remote tools in audits, and audit automation overall, CSPs and auditors should regularly discuss this option for future pooled audits.

> "The pool's cooperation with the CSP should always be considered as a learning process."

ABBREVIATIONS

CSP	Cloud Service Provider
FI	Financial Institution
IA	Internal Audit
ICS	Internal Control System
NDA	Non-Disclosure Agreement
OWASP	Open Web Application Security Project
PII	Personal Identifiable Information
SME	Subject Matter Expert
SPARC Documentation	Security, Privacy, and Architecture documentation
TLoD	Three Lines of Defense
ToD	Test of Design Effectiveness
ToE	Test of operational effectiveness



1 Introduction to cloud auditing

Cloud auditing, as the term implies, is the independent and periodic examination of cloud service provider (CSP) performance and its ability to meet and adhere to established control frameworks. Cloud auditing ensures that CSPs are using best practices and complying with security policies and risk management and meeting certain industry benchmarks for service delivery. In the financial industry, this also considers CSP compliance with data security measures, privacy laws and regulations, and performance expectations.

With the ever-increasing digitalisation of the financial industry and the considerable importance of cloud computing as a key enabling technology for the digital transformation of FIs, the industry as a whole is coming under greater regulatory scrutiny.

Committed as they are to compliance and accountability under the financial regulatory framework, and in observance of established legal requirements and the risk-based approach to cloud technology it is important that those FIs that have outsourced functions to CSPs include audits thereof. Given the nature of cloud auditing, however, FIs should consider the technological and procedural differences cloud computing services present.

This paper examines cloud auditing in general terms, provides insights into the assurance resources available, and offers guidance on the structure and processes of pooled audits as a tool to enhance cloud audit efficiency. Pooled audits are collaborative efforts carried out by a group of auditors from different organisations with the goal of ensuring that a required level of assurance in outsourced cloud services is or has been met [1].

CHAPTER 1 elaborates on the scope of this paper, providing fundamental information relevant for **auditing cloud computing services**. Based on the Three Lines of Defence (TLoD) Model, it addresses audit steps at a general level, elaborates on the principle-based approach, and provides a collection of central principles for cloud audits.

[1] See for example under: https://www.deitauditor.nl/business-en-it/pooled-audits-on-cloud-service-providers-2/

CHAPTER 2 provides practical guidance on how available **assurance resources** can be used to implement audits on CSPs in compliance with the EBA Guidelines (hereafter, the EBA GL) on outsourcing, thus helping to ensure audit processes meet regulator expectations and the FIs' Internal Audit functions. The guidance addresses performing the audit as well as access and information rights but does not cover other activities performed by FIs such as implementing vendor management functions and controls to govern the CSP. It highlights how a more harmonised understanding of the use of assurance resources for cloud auditing will help FIs systematically execute proper audit processes across European jurisdictions.

CHAPTER 3 provides key principles and essential considerations for **pooled audits**. It presents relevant steps, offers best practices from a cross-sectoral perspective of FIs and CSPs, and contributes positively to regulators and supervisors across European jurisdictions accepting and facilitating pooled audits. Subsections highlight the structural setup, process steps and preparation thereof, and audit fieldwork.

1.1 Different scenarios for cloud use

Generally speaking, there are two main scenarios for FI use of CSP, namely[2]:

ONE A FI outsources directly to a CSP, using the offered cloud services (Scenario 1)

TWO A FI outsources service provision to a non-CSP entity, which in turn uses cloud services by one (or multiple) CSPs at the next layer of business operations. (Scenario 2)

Considering the possible constellations for industry cloud use and understanding the cooperation of FIs and CSPs as an ongoing journey with common learning experiences, these different constellations require separate, dedicated observation and guidance.

For this reason, the guidance in this paper relates specifically to Scenario 1 above, where the financial institution outsources directly to a CSP – with a typical example of this being a bank's use of a CSP to provide infrastructure as a service (IaaS)[3].

In the same vein, the terminology of "auditing the cloud" used in this paper relates to audit activity that addresses a CSP and its related services. It does not include audit considerations by a FI linked to a possibly private cloud solution.

1.2 Effective risk management: The financial industry's defence model

Audit is defined as a systematic, independent and documented process for obtaining objective evidence and evaluating it to determine the extent to which the audit criteria[4] are fulfilled[5].

In line with this, and to provide assurance of effective risk management over their operations, senior banking sector management and governing bodies typically use the **Three Lines of Defence (TLoD)** Model which key financial regulators and external auditors support globally.

As defined in the model, the three lines of defence each have particular areas of focus, as laid out in Figure 2.

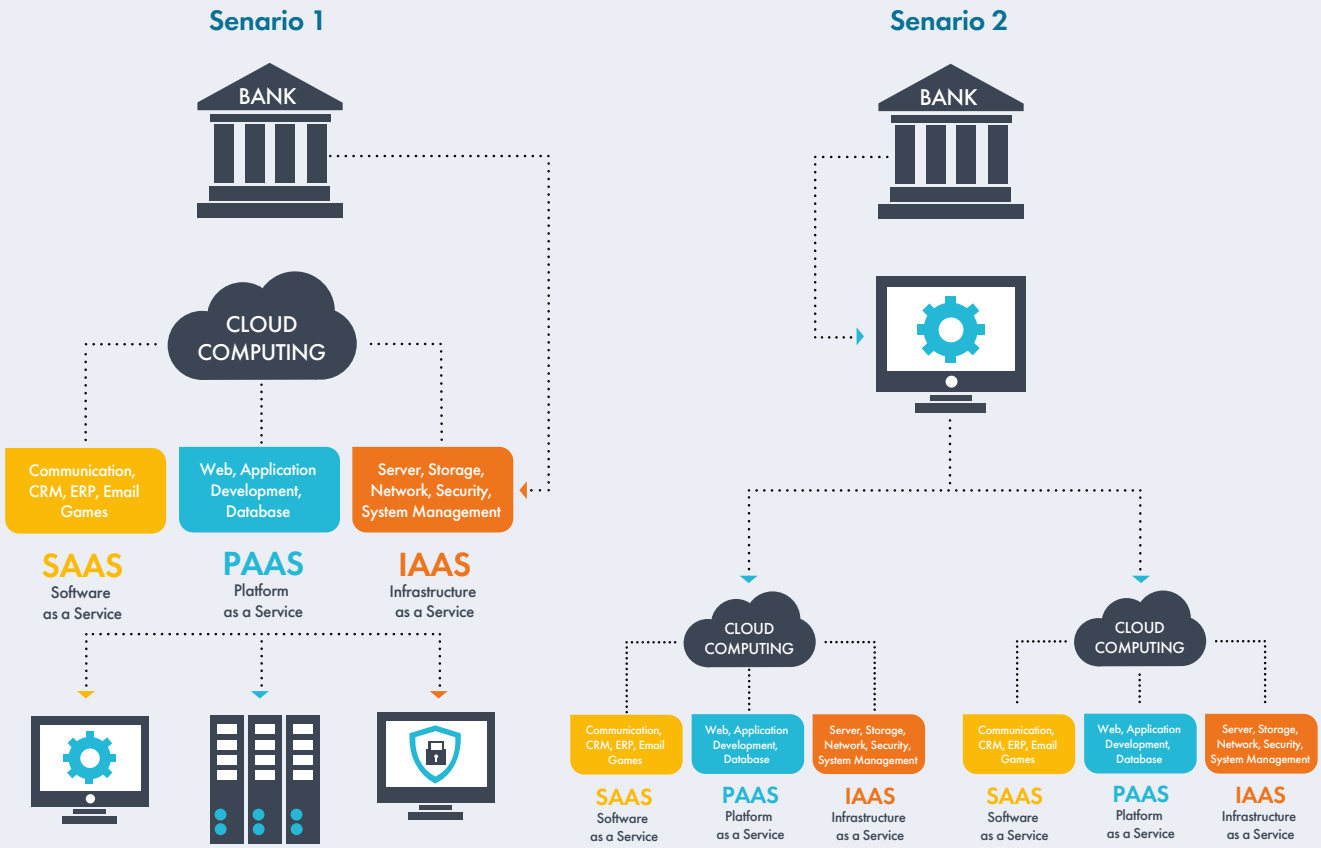
[2] Hybrid models and sub-outsourcing can advance the baseline scenarios further.

[3] Audit For general presentation and explanation of different cloud service constellations, please see the EBF Cloud Banking Forum's paper "The use of Cloud Computing by Financial Institutions"(2020), available for download here: EBF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf

[4] Audit criteria are a set of requirements used as a reference against which objective evidence is compared.

[5] ISO 19011:2018(en), Guidelines for auditing management systems

FIGURE 1



The responsibilities for the three lines are as follows:

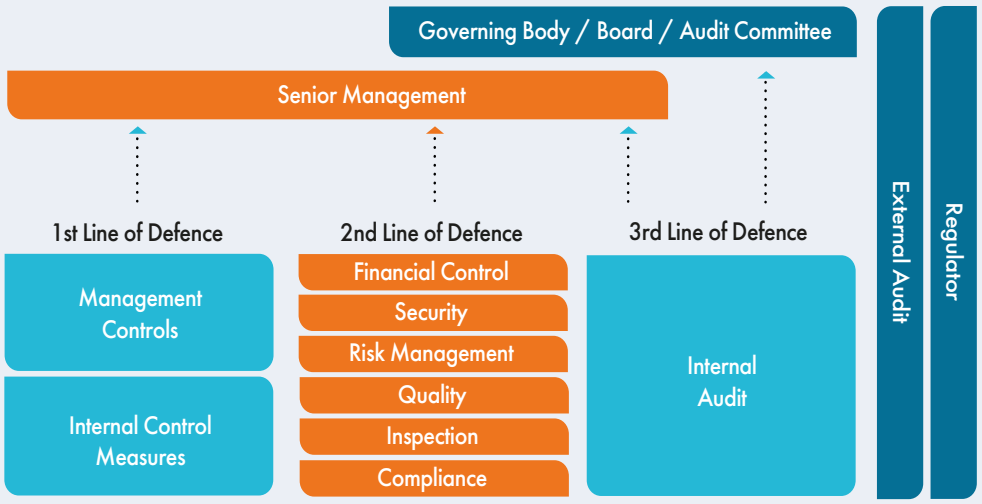
FIRST LINE OF DEFENSE
Operation Management
Own and manage risks. This line is responsible for: implementing corrective actions to address process and control deficiencies; maintaining effective internal controls, and executing risk and control procedures on a day-to-day basis.

SECOND LINE OF DEFENSE
Risk Management and Compliance Functions
Help to build and/or monitor the first line of defence controls and typically include a risk management, compliance, and controllership functions that monitor financial risks and financial reporting issues.

THIRD LINE OF DEFENSE
Internal Audit
Provides the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organisation.

FIGURE 2

The Three Lines of Defence Model



Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41

1.3 The Three Lines of Defence Model in a cloud context

This paper focuses on the FI's auditing procedures to review CSPs control measures. When it comes to cloud computing, the Three Lines of Defence (TLoD) Model is facing transformed technology controls. While controls pertaining solely to policy or procedure are generally the customer's responsibility, cloud services should **meet the same control objectives** as traditional application and infrastructure services.

When gaining assurance for an organisation, IT service consumption and delivery impacts how an audit should be performed. Indeed, depending on the organisation, all lines of defence could be auditing a CSP. Their relationship with the CSP is established within the FI's cooperative relationship with the CSP in the cloud environment overall.

Consequently, it is critical to understand the "**Shared Responsibility**" model between the CSP and the FI[6]. This model differentiates between technical, operational, and organisational measures managed by the CSPs and those managed by the FIs.

While conventional IT auditing and cloud auditing share many considerations, a cloud audit must address nuances typically absent from traditional IT audits. One major nuance is auditors needing sufficient knowledge of cloud computing; the other is the allocation of responsibilities for the various components of the cloud environment. Effective cloud auditors should be familiar with cloud computing terminology and have a working knowledge of a cloud system's construction and delivery method[7].

[6] For explanations and general considerations, see the EBF Cloud Banking Forum paper, "The use of Cloud Computing by Financial Institutions" (2020), available here

[7] See EBA Guidelines (or, EBA GL) on outsourcing, para. 97: "appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively".

One of the key differentiators between cloud and traditional IT is that the **public cloud uses a shared resource model**, where multiple tenants could use the same infrastructure, making application and security configuration controls more important than in traditional deployments[8].

Hence, the factors that must be taken into consideration are the:

- **Cloud service models** (SaaS, PaaS and IaaS)[9] aligned to traditional computing control areas, where the risk level relates to the selected cloud service model. In these models, risk management and the operation of IT activities are shared between CSP and cloud service customers (CSC). The "balance" of responsibility for IT control management shifts from cloud service provider to the service user as we move from the top of the stack (SaaS) to the bottom of the stack (IaaS);

- **Cloud deployment model** (internal, public, and hybrid)[10], where routine accountability remains primarily with CSCs who chose the model for their business, and where their data subject needs to be supportive and informed about data management, data location and network management, and

- **Specific characteristics of cloud computing** (self-service, accessibility across networks, resource pooling, rapid elasticity, metered services), where governance controls are necessary to provide timely management information and escalation/response in the event that defined thresholds are breached.

Shared Responsibility does not mean shared accountability.

Accountability remains with the financial institution, regardless of what services are being obtained from the cloud[11].

Responsibility is understood as a term allowing for clear definitions of who (the CSP or the FI) operates specific controls and FI visibility levels into how those controls work.

Having a well-defined approach with the CSP ensures that this can be accomplished in several ways.

The technological nature of cloud, paired with distinct roles for both CSPs and CSCs, requires a close look at the division of controls for a given cloud service. To reflect this evolving controls landscape in banking supervision, National Competent Authorities (NCAs) are invited to carefully consider Figure 10 in the EBF Cloud Banking Forum education paper on cloud use by FIs[12]. The cloud service PaaS and SaaS models are markedly different to other IT paradigms.

Projecting the understanding of the different roles in the controls landscape to the cloud service models available, please see Figure 12 of this Forum's paper[13]. Cloud Service Customers remain accountable for computing, although with cloud computing, they no longer operate all the IT controls in the cloud computing infrastructure themselves. The responsibility over the management and operation of IT controls may be shared with CSPs. The allocation of degrees of control depends largely on the cloud service model, with more controls managed and operated by CSCs in IaaS than in SaaS.

[8] EBA GL para. 96 makes protection of other customers' environments during audits in a multi-client environment an explicit call.
[9] For explanations and general considerations, see the EBF Cloud Banking Forum paper "The use of Cloud Computing by Financial Institutions" (2020), available here.
[10] Ibid.
[11] For background, please see the EBF Cloud Banking Forum paper, "The use of Cloud Computing by Financial Institutions" (2020), available here. For cloud auditing, this accountability leads to a supervisory expectation that FIs assess the need for an audit at some point in time, considering a risk-based approach.
[12] EBF Cloud Banking Forum paper "The use of Cloud Computing by Financial Institutions" (2020), page 19, available for download here.
[13] Ibid, page 20.

In the context of public cloud services, a typical deployment of the TLoD model can be outlined in a matrix on "Responsibility, Accountable, Consulted, Informed" (RACI) for a better overview. A comprehensive matrix is included in the Annex to this paper, presenting a match of tasks with lines of defence and CSPs.

BACKGROUND

Why is the cloud context so relevant today? Service migration to cloud: impact on daily FI functions

Regulators and authorities often interpret cloud computing as large-scale outsourcing contracts with extensive resource, asset, and knowledge transfer. While this can be the case with large IaaS and SaaS programmes, cloud can be systemic and broadly applied across banks in many critical and less critical functions[14]. Every day in FIs, hundreds of cloud solutions are used – from virtual desktops, to cyber capabilities, collaboration tools, and other SaaS applications. Banks need them to do their job.

There can be added value for FI operations and customers in the permanent migration of several service functions and processes to the cloud, for example (non-exhaustive):

- Collaboration tools (Zoom, GSuite, M365, Slack, and many more)
- Cyber security: prevention, detection, and response to cyberattack
- Vendor, asset, and real-estate management
- Third Party Risk Management
- HR applications and support (neural translation services, travel/expense management, logistics management, etc).
- Biometric authentication and digital signature capabilities
- Training & Development
- Document management
- Software development, testing, integration, and operations (DevOps/DevSecOps)

While technologically possible, a systemic reallocation of these functionalities back to on-premise solutions is unlikely as business efficiency and added value for customers and FIs would be lost.

1.4 Steps in the audit process

For a CSP, the auditing process usually consists of the typical steps, namely audit:

ONE

Planning (scope, timeline, resources, logistics alignments)

TWO

Start (often initiated by an audit letter and initial evidence request list)

THREE

Fieldwork ("auditing controls" such as evidence review, interviews, tests)

FOUR

Reporting (auditee management response, final audit report)

FIVE

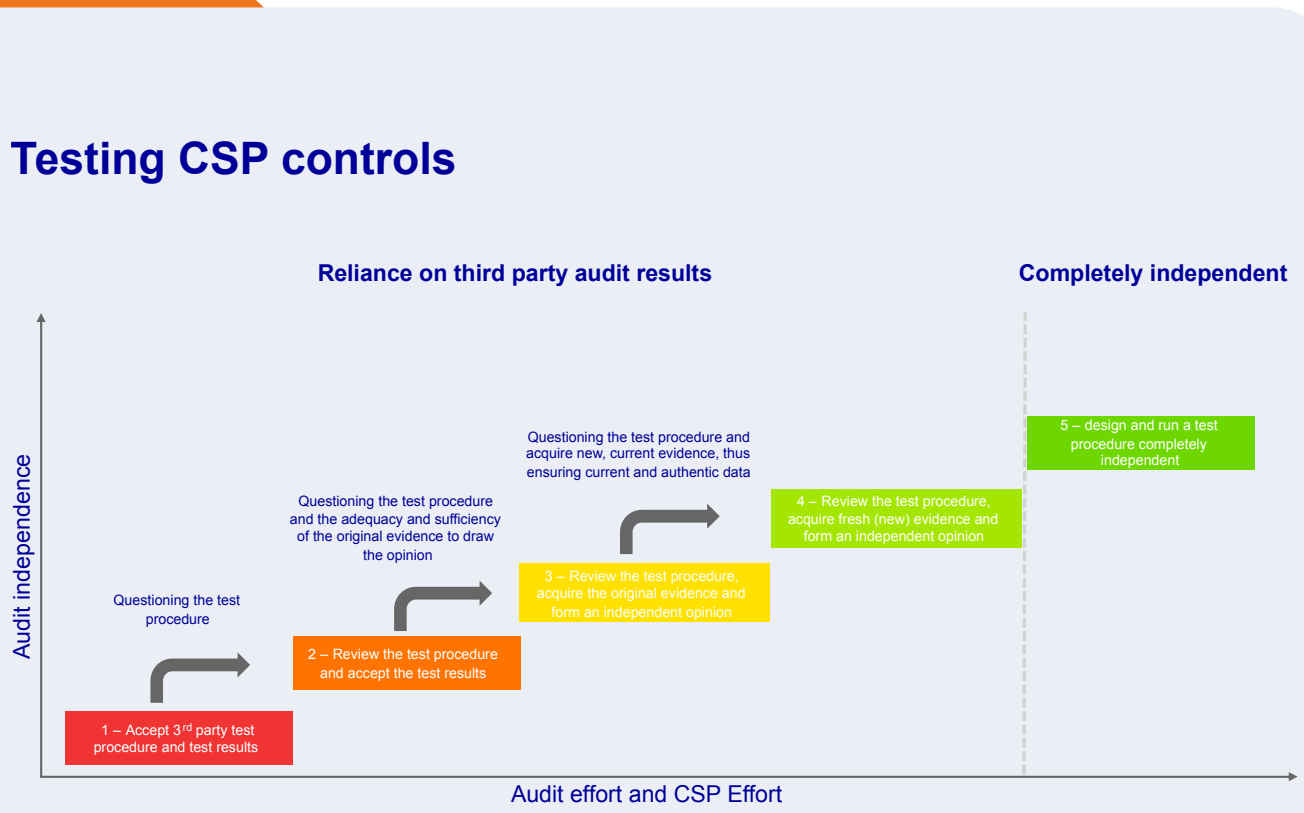
Follow-up (engaging with the CSP for post-report remediating measures; establishing an "audit trail" for FIs to revert to; CSPs offering specific functions such as evidence storage for a defined duration.

As part of the audit planning, auditors are responsible for creating their own work programme which clearly establishes the degree to which they will rely on pre-audited and third-party evidenced controls vis-à-vis the extent of their own control tests. Figure 3 shows the required steps and different levels of audit independence and describes different levels of audit assurance regarding audit test steps within an individual or pooled audit.

[14] EBF Cloud Banking Forum paper, "The use of Cloud Computing by Financial Institutions" (2020), available here

For orientation, please consider the following overview for required steps:

FIGURE 3



Under the applicable risk-oriented approach, the auditor can rely on third-party audit results or carry out their own audit procedures to evaluate and assess external auditor quality.

1.5 Auditing Controls

Audit-relevant knowledge can include a variety of pertinent features and facts, such as company risk levels, policies, and procedures as well as the regulatory requirements providing the framework. Within a given entity, an IT risk audit should in particular focus on control model knowledge. Analysis of the control model to verify its completeness, reasonability, and adequate implementation is critical to get a reasoned opinion of how IT risks are managed.

This approach is valid for reviewing on-premise platforms as well as cloud platforms in all their modes (IaaS, PaaS, SaaS). How the assurance activities are executed, however, is highly conditioned by the degree of technology process externalisation.

> “Within a given entity, an IT risk audit should in particular focus on control model knowledge.”

For reviewing a control environment and how it is impacted by externalisation, the audit process includes three complementary and non-exclusive approaches:

FIGURE 4

Control model design (also known as the "Risk and Control Framework"):
As IT providers, it is important that CSPs have a control model covering the risks they are exposed to which could also impact their customers. Based on regulatory requirements for the customers in question, this model should:

- Include a clearly identified control map (with control description) that is aligned with recognised standards (NIST, ISO 27000 series, etc).
- Link controls with CSP-provided services, ensuring that controls implemented in each service are clearly identifiable
- Guarantee control completeness
- Ensure appropriate periodical review of control execution and ensure evidence thereof is maintained
- Be measurable, including indicators showing controls status

The first step to determining how a CSP is managing technology risks is to review the definition of this control model design. While adequate to periodically carry out this review, it should not, in many cases, be the only action taken.

MODEL IMPLEMENTATION

Auditors must ensure the correct implementation of the designed control model; controls must be executed as expected, cover all the relevant services, and be sustainable over time. Given the nature of CSPs, controls are not client-specific, but defined and implanted agnostically. This is not incompatible with what is expected in an FI audit. It is, however, recommended that the CSP have mechanisms to ensure the control model is working specifically in the service the client is using, as well as evidence thereof. While auditors can recognise and factor in general controls on the supplier side, they need to ensure adequate and proper control execution on the CSP side. These have to be related to the service or platform utilised by the

service/platform affecting the FI, making it crucial that controls be mapped to the relevant services the FI is using. Model implementation review then requires evidence of control execution that can be linked to the services the FI is using.

CONTROL TESTING

Independent testing of the controls is a relevant added value that FI audit teams provide to the institution[15]. While a time-consuming process for the auditor and the technology team, it gives FI management a necessary independent opinion of the adequacy of the controls (not only by definition, but real effectiveness). In an on-premise platform, this independent testing is part of the assurance process. Different considerations apply, however, when a FI outsources IT services to a third-party provider.

When auditing a CSP using this approach, 1:1 audits or pooled audits should be carried out and include previously-defined evidences that will be shared or audit tests that will be executed. In general, professional care is important when performing audit test steps. Test steps should as far as possible be non-invasive, and not impact the production environment or affect the FI's "Business as usual" processes and controls. The auditor should also consider any impact(s) to the audited IT system which – if invasive in nature – could potentially increase risks.

CONTROL GAPS

During the review process, control gaps or exceptions can be identified (such as a CSP not implementing a specific control the FI expected, or the control's execution is not meeting expectations). While in an on-premise environment, control gaps can be directly closed by adding the new control, this may not be as straightforward when outsourcing to a hyperscale CSP running a very standardised environment for its large-scale operation. While CSPs generally align themselves with industry standards, individual processes or controls can still show differences to traditional on-premise environments. Where a gap is identified and accepted, CSPs are nonetheless committed to addressing it as part of the audit follow-up process in dialogue with the FI[16].

As part of the audit process, the CSP will formulate a "management response" to auditor findings. As with traditional audits, it will include the acceptance or rejection of the finding(s) along with a business justification as put forward by the CSP.

When a finding is:

- **Accepted**, an action plan and target resolution date are communicated.
- **Rejected**, this should be driven by risk-based considerations. CSPs should be expected to comment on the reasons behind the rejection. For example, it is not uncommon for a FI customer to flag a gap such as a missing control they would typically expect to have on-premises, but which the CSP identifies as not appropriate in the context of a cloud service, since the risk is being mitigated in a different way. In such case and to resolve the open issue, the CSP should show the FI auditors how this risk is mitigated.

The responses to control gaps or presented CSP exceptions will lead to the FI possibly accepting the finding under its risk appetite and, consequently, deciding to address the risk or not, following the fundamental risk-based approach.

[15] According to the EBA Guidelines on internal governance (2017), para. 199, the internal audit function (IAF) "should, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of an institution, including outsourced activities, with the institution's policies and procedures and with external requirements. Each entity within the group should fall within the scope of the IAF."

[16] Please see section 3.2.5.

Several factors should be included in this consideration; this is in general beneficial to all cloud audit participants. Understanding the differences in FI risk appetite, these factors can connect back to FI reflections prior to the contractual agreement being signed, and include:

- Focusing on risk mitigation and evaluating if other equivalent controls or processes are in place that address the same risks.
- Aligning internal controls with industry standards and best practices and determining if the gaps also exist against these standards and why.
- CSP reactions in direct conversation to gaps and related risks: it is strategically important for them to deliver high security and compliance. Where the CSP acknowledges these gaps as risky, they should be open to addressing them. When dealing with exceptions where a control was not in place (like in SOC audit reports), engage with the CSP and ask for clarification and an action plan.

1.6 A principle-based approach to cloud auditing

1.6.1 Cloud auditing compared to traditional auditing

Compared to traditional auditing, cloud auditing needs to respect important key factors in the risk-based and evidence-based approach, involving changes for auditors from their usual audit of internal processes.

When defining the audit scope, auditors typically take a **risk-based approach** to ensure audit work focuses on the key controls that mitigate risk for the organisation. As the technology, outsourcing and regulatory landscape continue to evolve, auditors are required to gain a thorough understanding of the organisation (including its processes, procedures, and interactions) to have a complete and holistic view of the risks. Consequently, the assessment should consider a process in isolation as well as the whole management system (in which the processes operate in relation to each other) and the relevance of said processes for achieving the defined objectives and mitigating risk.

When auditing a CSP, auditors not only have to keep their own organisation's risks in mind, but audit how CSPs mitigate those risks within their processes and established controls. Auditors also need to be open to the different approaches a tech company uses on mitigating their own and their customers' risks (in this case the FI[17]).

To evaluate how these controls mitigate the auditor's organization risks, cloud computing's new architectural model needs to be fully conceived prior to assessing the controls implemented by the cloud providers.

To help auditors gain this knowledge, access rights and transparency towards the customers should follow an **evidence-based approach** as this avoids incomplete information being used or provided which cannot be fully reliable for audit process purposes and objectives.

> "Auditors typically take a risk-based approach to ensure audit work focuses on the key controls."

[17] In turn, access and audit rights receive substantial attention during the negotiation of the contractual arrangement.

1.6.2 Principles for cloud auditing

To ensure an audit serve as an effective and reliable tool supporting management policies and controls, auditing should follow a risk-based approach and use a set of principles which are in some areas included in existing standards already[18].

This section further elaborates on important elements of the principles which – while a non-exhaustive list – are essential when considering the required FI cloud audits.

ONE
Integrity

- Perform audits with honesty, diligence, and responsibility.
- Observe and comply with applicable legal requirements.
- Demonstrate competence while performing audits.
- Operate on a knowledge basis, understanding differences in cloud computing services and audit teams recognising the need to deliver effective audit coverage.
- Perform audits in an impartial manner.
- Remain fair and unbiased in all dealings.
- Be sensitive to any influences placed on judgment during an audit.

TWO
Collaboration

- Recognise and accept the need for professionalism, remaining flexible and solutions-focused in seeking to mitigate identified risks.
- Establish and maintain mutual trust by showing the common value of collaborative efforts; set clear expectations and drive open discussions.
- Define clear roles and accountability; here, setting frequent meetings and using a tracking system could foster transparency and improve collaboration.
- Develop clear and realistic objectives and avoid ambiguity.
- Develop and maintain effective communication, understanding communication layers and using any available tools.
- Debrief post-audit to determine how or where audit activity can improve.
- Align and coordinate the available resources and timing to improve efficiency, minimise the duplication of efforts, and enable both parties involved in the audit to achieve their objectives.

THREE
Fair presentation

- Ensure audit findings, conclusions, and reports truthfully and accurately reflect audit activities.
- Share any significant obstacles encountered in the audit.
- Report any unresolved diverging opinions between the auditee and audit team.
- Communicate in a truthful, accurate, objective, timely, clear, and complete manner.

FOUR
Due professional care

- Exercise due care, reflecting task importance and confidence audit client places in you.
- In multi-client environments, avoid or mitigate[19] risks to another client's environment.
- In all audit situations, make reasoned judgments.

[18] In line with standard ISO 19011:2011: Integrity: foundation of professionalism. Fair presentation: obligation to report truthfully and accurately. Due professional care: application of diligence and judgment in auditing. Confidentiality: security of information. Independence: basis for impartiality of audit and objectivity of audit conclusions. Evidence-based approach: rational method for reaching reliable and reproducible audit conclusions in a systematic audit process.

[19] As reflected also by EBA Guidelines on outsourcing, para. 96.

FIVE
Confidentiality

To verify that controls at the CSP and other fourth parties are operating effectively, the auditor will have access to sensitive data which – if not protected – could impact the security of the cloud solution or expose client, customer, or sensitive business information. Further, the FI may be required to retain and store certain data to prove the review was conducted in line with policy and regulations.

In this regard, and when agreeing on evidence sharing between the CSP and FI as part of the pre-engagement activities, the following should be considered:

- Assess any legal and regulatory requirements in relation to relevant data access.
- Define as confidential any information the audit team prepares, including any findings, reports, conclusions, or other documentation.
- Establish Non-Disclosure Agreements (NDAs) to cover the handling of data and properly handle sensitive or confidential information in line with existing contractual obligations and other NDAs.
- Define data classification, right-to-know principles, and retention requirements.
- Agree on handling and data exchange processes, including how data will be transported physically and logically between the parties.
- Define procedures for viewing highly sensitive information (penetration test results, vulnerability assessments, log files, etc).
- Agree a process for sharing the audit evidence report or findings with third parties.
- Consider the use of obtained information during auditing for audit purposes (IP relevance and fair understanding). In all exchanges, the audit team should exercise discretion in using and protecting information acquired during audit duties.
- Use any information, responses, reports, or documentation disclosed to the audit teams or any other confidential information obtained or learned as a result of, or in connection with, the audit only for internal purposes in connection with the audit and for no other purpose.

SIX
Independence

- Avoid bias and conflict of interests. In particular, have auditors remain independent from the activity being audited: avoid bias of personnel responsible for both controls design and audit execution.
- Maintain objectivity throughout the audit process.
- Ensure findings and conclusions are evidence-based only (or signal any lack thereof).
- Before report finalisation, give the audited CSP the opportunity to engage with the auditors on audit results, facilitate exchanges and dialogue on findings and conclusions.

SEVEN

Insightful, Proactive & Future-Focused

- Do not focus audit attention exclusively on functions with a history of incidents.
- Complement the audit's attention to past and present with a forward-looking perspective in audits, considering the service's scalability. Fostering innovation requires a forward-looking approach to cloud computing. Reporting on the past shall be considered particularly where relevant to decisions and actions of today and for tomorrow (root cause considerations and continuous risk mitigation).
- Secure a professional role of internal auditors with management of the auditing party. The relationship should be defined by trust, allowing for a trusted advisor role of the internal audit function.
- Share information between the auditors and management of an auditing organisation in a timely manner. Audit findings should be communicated as part of a continuous exchange, not limited to one-off points in time.
- As an auditing organisation, be open to the conclusions and lessons learned from all audits, rather than focusing on a single, final report to foster an environment of continuous helpful exchanges with internal auditors.

1.7 Digital transformation and possible effects on auditing processes

Across many sectors, the Covid-19 impact in 2020 boosted the process of digital transformation. Digital communication tools and processes uniting a now more decentralised workforce are essential for continued cooperation and for business. The need for remote cooperation is an issue of interest in the auditing community as well as in cloud computing auditing processes, especially when it comes to pooled auditing. Access to audit-relevant information could – in part – theoretically be facilitated remotely, and exchanges between audit teams and CSP staff could leverage long-distance communication tools. This paper addresses the aspect of remote cooperation in Section 3[20], offering considerations to participants of pooled audits.

1.8 Digital Operational Resilience Act (DORA)

In September 2020, the European Commission published the **proposal for a Regulation on digital operational resilience for the EU financial sector (DORA)**[21] aiming to ensure that financial institutions withstand risks stemming from reliance on information and communications technology (ICT) and related threats which might impact financial stability.

[20] Please see section 3.2.3.5.

[21] https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/en/pdf

Covering contractual arrangements, the aspect of cloud auditing is directly affected by the outcome of DORA's legislative negotiations. Proposed Art. 27 (2) (h) establishes the requirement to include in the contractual arrangements rights of access, inspection and audit (i); rights to agree alternative assurance levels of other clients' rights are affected (ii), and the commitment to fully cooperate during the onsite inspections performed by the FI (iii). The latter also includes details on the scope, modality, and frequency of remote audits. In this regard, **assurance considerations and the cooperation of a pooled audit group and the CSP are of central importance, as explored further in Sections 2 and 3 of this paper.**

DORA introduces a crucial novelty: the proposed oversight to critical ICT service providers such as CSPs. The proposal foresees that a "Lead Overseer" would assess whether the ICT service provider has comprehensive, sound, and effective rules, procedures, and mechanisms in place to manage the ICT risks that it may pose to financial entities. The Overseer is considered to be provided with unrestricted right to access all information necessary to carry out its duties and conduct on-site inspections of any premises of critical ICT third-party service providers. Thus, the Regulation seeks convergence of the supervisory approaches to the ICT third-party risk in the financial sector, providing an oversight framework for critical ICT third-party service providers at European level.

With EU legislative negotiations ongoing in June 2022, **no definitive considerations can be made as to changes triggered by the final DORA text**. However, the EBF Cloud Banking Forum is aware of the upcoming impact for cloud auditing. Harmonisation of the regulatory and supervisory framework for cloud computing is perceived as a positive development, enabling better uptake by the financial industry with respect to scalability, legal certainty and – ultimately – economic viability[22]. While supporting the consideration of the Forum's education and guidance laid out in this paper by the EU legislator as potential background for DORA, we do not intend the following content to serve as input for the legislative process in particular. Instead, FIs and CSPs will closely follow the legislative procedure of DORA and the possible impact on European supervisory guidance today (i.e., EBA GL). Pending these developments, the Forum's cooperative and cross-sectorial guidance would be able to revisit audit aspects of cloud computing in the future, where deemed necessary.

> "Harmonization of the regulatory and supervisory framework for cloud computing is perceived as a positive development."

[22] For more comprehensive considerations, please see EBF Cloud Banking Forum paper "The use of Cloud Computing by Financial Institutions" (2020), available here.

CHAPTER
TWO

2 Service assurance

2.1 Introduction

Under existing financial regulation, banks are accountable for the management of the risks arising from consuming cloud services. Sound governance of outsourcing arrangements[23] is an integral requirement of this, including a rigorous outsourcing process, proper risk identification and management, as well as effective day-to-day management and oversight. As part of this governance, banks should ensure that "risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated" (EBA GL para. 40 c.). This includes "due diligence checks on prospective service providers" (EBA GL para. 42 c. iv.) and "the implementation, monitoring and management of outsourcing arrangements" (EBA GL para. 42 d.), including ongoing assessments.

The EBA GL emphasises the importance of FIs exercising their access and audit rights.

EBA GL PARA 90

Institutions and payment institutions should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.

The internal audit function of banks is part of the independent review of outsourced activities within the three-lines-of-defence model of banks[24]. This includes the bank having respective contractual audit rights within the written outsourcing arrangements[25] as well as the review of critical or important outsourced functions in its audit plan[26] **following a risk-based approach.**

According to EBA GL para. 87, the written outsourcing arrangement has to secure that for outsourced critical or important functions, the CSPs grant:

a. Full access to relevant business premises [...] ('access and information rights')

b. Unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights') [...]

[23] EBA GL para. 32 and following.
[24] EBA GL para. 50 and following; for the TLoD model, please see Section 1.2.
[25] EBA GL para. 85.
[26] EBA GL para. 50.

For non-critical or non-important functions, institutions shall ensure these access and audits rights under a risk-based approach, EBA GL para. 88.

As opposed to traditional IT outsourcing, however, public cloud services (IaaS, PaaS, SaaS) are often offered at scale and build on new and highly automated IT designs and operations, presenting FIs with both opportunities and concerns as they seek assurance over the services.

2.2 Efficiency in cloud auditing

FI auditing of CSPs must only deliver effective and efficient solutions to address (hyper-) scale cloud solutions but remain solidly within financial-sector regulatory requirements. FIs need to cater to regulatory expectations while adapting to processes and technology offered by third-party CSPs, an interaction that requires an evolved approach in auditing – one which is different from traditional on-premise IT infrastructure and even more focused on efficient risk mitigation for the services in question.

The increasing automation of service provision, the growing number innovative tech applications available, and sheer amount (set to increase) of CSP customers all trigger individual audit considerations for the same providers by each and every customer under regulatory obligations. This presents CSPs with the challenge of efficiency and limited scalability.

For numerous customers, auditor attention is focused on a limited number of CSPs. The possible efficiencies gained by applying common tools, standardised instruments, and pooled capacities are a legitimate topic for discussion, with the understanding that each tool must effectively serve its purpose. At the same time, and as a way to secure final accountability, customers are also, however, considering the efficiency and effectiveness in available assurance tools.

The possibilities offered in EBA GL para. 91 reflect supervisor desire to provide FIs with efficient auditing instruments under the risk-based approach, catering to increasing cloud adoption based on a common layer of control that can be audited by different customers at the same time, or benefit from a standardised understanding.

However, this understanding of the need for efficiency is directly connected to the supervisory understanding that these assurance resources are without prejudice to the FIs' ultimate responsibility regarding outsourcing arrangements[27].

This important distinction is continued in the restrictions for the assurance resource of third-party certifications and third-party or internal audit reports. EBA GL para. 92 obliges FIs to assess whether these resources adequately and sufficiently comply with regulatory obligations. FIs should not rely solely on these reports over time. Additionally, FIs should only make use of these assurance resources under the conditions of EBA GL para. 93.

Without reducing the assurance required, combining different assurance resources can be an appropriate way to enhance efficiency of assurance gain at scale, catering to the evolving cloud environment. For instance, pooled audits (addressed in Section 3) may be a good alternative for audit right execution compared to individual audits. Alternatively, the enhancement of CSP's third-party attestations may be sufficient for basic and even advanced assurance gain, depending on the inherent risk for the single FI, and in accordance with the principle of proportionality.

[27] See EBA GL para. 87 as referred to above.

2.3 Assurance tools

Assurance tools are resources or processes provided by the service provider or by a third party, available in different levels of independence, so that financial institutions can gain a deep understanding of the risks associated with outsourcing to third-parties such as cloud providers. Tools can target provision of information at scale and contain different levels of confidential information for the provider. In turn, providers may not share individual tools outside of a strictly controlled environment or must do so with safeguards such as NDAs.

With thousands of financial institutions consuming the same standardised cloud service, an opportunity exists to benefit from economies of scale when gathering assurance. Indeed, FIs are considering the effectiveness and efficiency of assurance tools for cloud auditing, with the quality and degree of independence of each being relevant factors for consideration.

More effective assurance tools can in turn foster efficiency for providers. Independently from FI size and service volume, customers of the same CSP operate in a common cloud environment, leveraging the same standards. Where assurance tools applied within the regulatory framework's conditions provide effective solutions, the cloud landscape could benefit from their efficient applications across all market players.

After all, even though there are differences in risk appetite or products being deployed across individual organisations, many of the operational risks remain largely the same when assessing – in particular but not exclusively – a cloud provider's control environment. Confidentiality, Integrity, Availability, Cybersecurity, and Privacy controls over the CSP side of the control environment must meet the highest standards to be used at such large scale. Once one party independently assesses and validates these, the question is then if the assurance obtained can be used to benefit others.

This is where standardised assurance tools come in, providing the opportunity of "1:many" assurance. Assurance tools focus on the common elements of the cloud provider's controls environment, thus avoiding a separate review by each individual FI as customer. The idea behind these tools is that an individual FI's risk organisation does not rely solely on these standardised assurance tools, but rather leverages them (as deemed appropriate) to optimise internal processes, accelerating the risk assessment and audit processes, and minimising the duplication of activities.

Different assurance tools exist for different use cases. Often, a mixture of these is used in practice to contribute to an overall assessment of outsourcing risks to cloud providers. Different assurance resources are available, including – but not limited to – the pooled audit, third-party certifications, and third-party/internal audit reports under EBA GL para. 91.

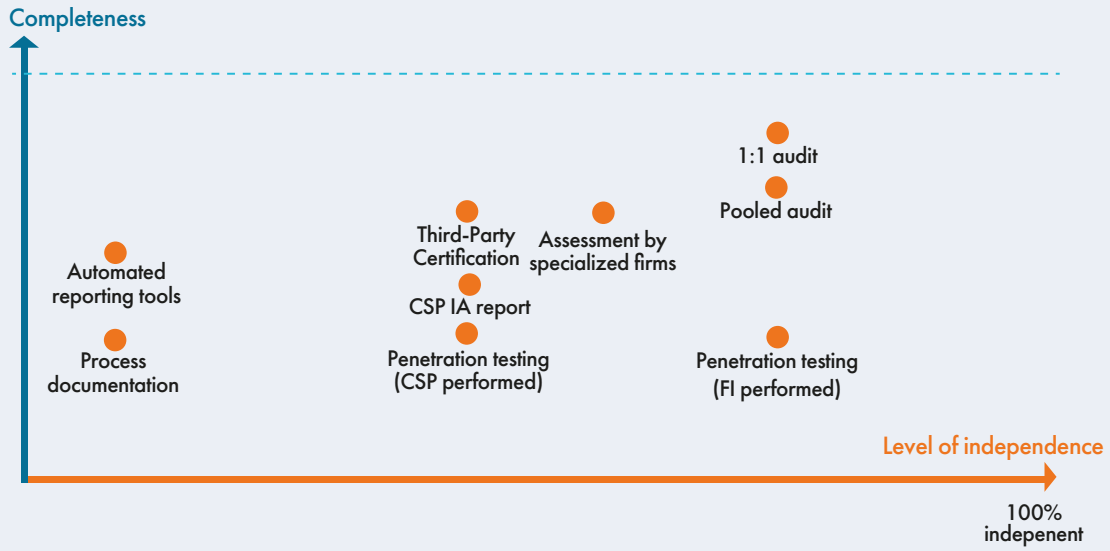
Even if the FI cannot rely unreservedly on third-party audit reports or internal audit reports provided by the CSPs[28], the size of many CSPs makes orchestrating different available assurance resources necessary to ensure sufficient overall independent audit coverage and depth aligned with the respective FIs' risk-based approach.

Figure 5 provides a visual overview mapping the main existing assurance tools by levels of **completeness (scope and testing depth)** and **independence (testing execution)**.

[28] See EBA GL para. 92, 93.

FIGURE 5

Consumption Completeness and level of independence of common assurance tools



Legend

Level of completeness

The value of completeness has been asserted by weighing several parameters:

- the level of depth of assurance that is available,
- the percentage of controls that are included, and
- continuous, scheduled vs. one-time assurance.

Level of independence

To which extent is it possible for an FI to have control over the assurance process, be it collaboratively with other financial institution or completely independently.

Source: Supplied by CSP. Disclaimer: strong variations occur on the positioning of these tools on the graph, in particular level of completeness is often influenced by scheduling/scoping exercises. Figure 5 only represents the optimal scenario (full scope, regular scheduling).

Financial institutions can consider the assurance audit resources within the regulatory framework, with particular consideration of the national competent authorities' expectations. Looking at the European level as a whole today, this consideration under possible different expectations and interpretations leads to an uncertain, fragmentated environment for the application for cross-border cloud services. Figure 6 aims to provide an educational overview of the tools available, outlining key benefits and drawbacks.

To ensure that assurance tools are fit for purpose according to the risks and relevance of the process for the FI that is running in the cloud, it is important to consider a risk-based approach[27].
Assurance tool effectiveness and efficiency both filter into this understanding. Leveraging automatic tools or CSP-provided reports can improve audit review efficiency. Following the logic of the EBA GL section 13.3, the FI assessment is considering process criticality. Frequency and results of previous audits can speak to this consideration, thereby becoming a relevant factor of its risk-based assessment.

Figure 6 includes a layered view of the different assurance tools that can be used as a reference when evaluating their use following an in-depth view (considering completeness and independence). Note that the use of these tools is a reference; it should not be considered exclusive but complementary. As main drivers for selecting the appropriate tool, FIs have to perform their own risk assessment and manage their risk appetite.

[27] See section 2.1: EBA GL para. 90.

FIGURE 6

	BENEFITS	DRAWBACKS
Process documentation	Good for understanding the CSP control environment and assessing control design. Allows initial assessment of control design suitability. May guide next steps in terms of assurance approach.	Good for assessing control design but not for control effectiveness.
Automated Reporting Tools	Obtaining a continuous view on controls through a tool or API. May be integrated with in-house risk management tools. Some of these tools may enable individual FIs to validate individual controls on a continuous basis.	Full set of individual controls. Not control testing, but reliant on the automatic information provided.
CSP's Internal Audit Plan; Audit Reports	May contain valuable information on risks as detected and flagged by the internal CSP auditor, recommendations, and improvement plans.	Internal audit plan not aligned with the risk assessment of the clients; scope of the audit not aligned; differences in methodology etc. May contain highly sensitive information not for disclosure to the CSP clients (e.g., possible exposure of security and privacy)
Penetration testing	Can be done by FI or by a third-party. Very hands-on way of testing effectiveness of controls environment against cyber risks. If done to "standards", it can provide a reasonable basis for initial readiness and fit-for-purpose consideration.	Testing scope and format may not be clearly defined. A CSP-led penetration test is not so independent. Limited scope to cyber risks, executed in a specific moment in time. May not discover all existing issues. Execution may impact other clients. May contain highly sensitive information not for disclosure to the CSP clients (e.g. possible exposure of security and privacy).

Third-Party certifications	
BENEFITS	**DRAWBACKS**
Assessment and attestation of control design and effectiveness by an independent third party. In many cases, these have a very wide scope and are sometimes aligned with government standards.	Pre-determined scope by the CSP, specific industry standards, or specific regulation. May not always meet all FI's specific requirements. May not always contain enough details to permit the FIs to challenge the third-party review.
Assessment by specialised firms	
The scope is determined by the external assessor in line with a defined standard or set of risk/control objectives. Report can be shared by multiple FIs.	Limited to a specific point in time (although it can be repeatable). Depth of the review may not always be aligned with expectations and depth of information provided could be lacking. Requires reliance on a third-party firm.
Pooled audits	
Limits overhead on both FI and CSP. Better availability of audit expertise as audit work is divided across a multidisciplinary team of experts. Teamwork brings opportunity for some FIs to gain expertise from peers and may ultimately save time and resources. Allows the definition of a specific scope according to participant FI requirements. For more details, please see Section 3 of this paper.	Requires expertise in cloud auditing. Scope must be defined with other participants and may not include all individual requirements. Evidences provided in the audit process could not meet individual FIs expectations. Possible transparency issues on the evidences provided. Coordination and alignment require dedicated attention (time) from the CSP. However it may result in benefits over longer timeframes.
1:1 audits	
Flexibility in determining scope and timing. Fitted to an individual FI audit plan, access to required evidence, and subject matter experts. Most independent audit.	Most expensive option for the FI. Time-consuming for the CSP. Complex process to execute periodically. Requires advanced expertise. Evidences provided in the audit process could not meet FI expectations. Possible transparency issues on the evidences provided.

In line with EBA GL para. 90, all exercise of the access and audit right, applying one or multiple of the listed assurance tools, should adhere to relevant, commonly accepted, national, and international audit standards.

A FOCUSED ASSURANCE TOOL:
The ENISA cybersecurity certification scheme for cloud services

The European Commission believes that certification plays a critical role in increasing trust and security[30]. A common framework for EU-wide valid cybersecurity certifications for cloud shall overcome fragmentation and barriers in the European Single Market. Based on the respective empowerment under the EU Cybersecurity Act, **the European Union Agency for Cybersecurity (ENISA)** is developing a certification scheme for cloud services, aiming at comprehensive technical requirements, standards, and procedures[31].

The voluntary scheme is expected to be applicable for all cloud services, ranging from infrastructure to applications. Leveraging industry input and support by an ad-hoc expert group, different assurance levels are envisaged under the scheme: basic, substantial, and high.

Offering a methodology for the particular cybersecurity aspect of cloud use by banks, **the ENISA scheme could be considered a central future resource to gain assurance in cloud auditing.** However, the scheme will not address all service aspects of outsourcing. Rather than offering a broad audit solution, this tool provides for specialised coverage for one out of many audit aspects. Nevertheless, the scheme's endorsement by ENISA and the cross-sectoral expertise involved in its creation could make this targeted certification a prime resource for auditor understanding of cloud security in place.

Works on the certification scheme are still ongoing, requiring a closer look once finalised. Nevertheless, the Forum appreciates supportive measures at the EU level that enhance harmonisation for cloud computing.

2.4 Leveraging assurance tools during audits

Working from the overview of assurance tools above, the following sections look at their use by FI auditors.

2.4.1 CSP audit scope planning

To determine the risk-based approach for cloud auditing, FIs should consider the following criteria when assessing assurance tools and possible combinations in an audit:

- Criticality and importance of the function as defined in para. 29 of the EBA GL. The requirements under the EBA GL Section 13.3 apply.
- Risk appetite.
- Incorporation of accepted national and international audit standards by the tool considered.
  Accepted industry standards can entail inter alia:
  - PCI DSS: The payment card industry data security standard contains mandatory controls to be completed by all companies processing payment card data.
  - NIST SP 800-53 and NIST Cybersecurity Framework: The control framework from the United States National Institute of Standards and Technology on ICT and Cybersecurity.
  - FedRamp: The US government's Federal Risk and Authorization Management Program containing controls to be fulfilled by governmental customers.
  - CSA CCM: The Cloud Security Alliance Cloud Control Matrix (CSA CCM) Cloud specific control framework.

Note that the above-mentioned control sets may need further enhancements according to FI-specific risk.

[30] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.
[31] https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme

- Quality of assurance resources
  - Depth of testing: Evaluate objectives performed within the assurance tool
  - Level of detail: Potential depth limitations
  - Independence: Tool's level of independence

The EBA GL paras. 92 and 93 provide conditions to the use of assurance tools for the outsourcing of critical or important functions. The use of assurance tools, either individually or as a compilation of tools, must adequately and sufficiently comply with an FI's regulatory obligations and must be an embedded part of an extensive assessment.

Audit mechanisms should recognise supervisory requirements, including options for a layered approach that builds on the assurance tools described earlier[32], allowing each FI to leverage increasingly "independent" assurance tools in a staged manner. This can, for example, include starting with public audit reports (ISO certificates), confidential audit reports (eSOC1/SOC2) and internal reports (penetration tests), moving over to pooled audits and 1:1 audits. The determination should be based on the risk-based approach by the FI and the supervisory obligations[33].

2.4.2 General information on CSP performance and quality

Similar to traditional third-party provider audits, there is a variety of general information which can be considered relevant information sources in CSP audits.

This includes (but is not limited to):

- Financial Accounting reports (for financial strength review)
- CSP service availability and performance metrics
- Public media coverage of the CSP and potential service impact
- Security bulletins provided by the CSP
- Provider assessments done by independent third parties

Auditors are encouraged to consider these – not individualised – information resources but must also consider that they have inherent limitations in terms of providing controls assurance.

2.4.3 CSP third-party certifications and reports

When considering applying a combination of assurance tools to gain the required understanding and assurance, the EBF Cloud Banking Forum believes it is helpful to offer more perspective on the conditions in EBA GL paras. 92 and 93.

This perspective is based on two main objectives, namely to:

- Satisfy the FI's regulatory obligations, i.e., providing the required assurance for the function outsourced to the cloud under the risk-based approach; and
- Allow for an efficient audit process in light of the hyperscale nature of cloud, leveraging available assurance resources which provide the assurance FIs require.

[32] See Section 2.3.
[33] EBA GL paras. 90, 92, 93, 94.

EBA PARA 92

For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.

If the CSP has third-party certifications and reports which audit and confirm the CSP's compliance to international recognised IT security standards, then such certifications could also serve as information and security assurance source. When considering the meaning of "adequate" and "sufficient" for outsourcing of critical or important functions, the factors in EBA GL para 93 should be considered. We provide further discussion of these factors in Section 2.4.5.

As stated in EBA GL para. 92, for the outsourcing of critical or important functions, FIs should not rely solely on the reports under EBA GL para. 91 (b) over time. Although FIs may use these certifications and reports during each audit cycle if they are "adequate" and "sufficient", they should not rely on them exclusively for several consecutive years without also conducting individual or pooled audits. As stated in EBA GL para. 90, the frequency of such audits and the areas to be audited should be determined taking a risk-based approach.

Using certifications/reports and conducting audits are not mutually exclusive. FIs may choose to leverage the provider's reports during (or prior to) individual or pooled audits. This helps to increase the FI's familiarity and understanding of the CSP's environment, which in turn increases audit efficiency and effectiveness.

2.4.4 CSP's Internal Audit report

In case the CSP has an Internal Audit function which is set up according to regulatory requirements that apply to the FI's own Internal Audit function, it could serve as additional compliance assurance.

EBL GL para 75 j contains a respective reference:

EBA GL PARA. 75 j.

The outsourcing agreement for critical or important functions should set out at least:
[...] and, as appropriate, the obligations to submit reports of the internal audit function of the service provider.

In determining whether access to the CSPs' internal audit reports* is appropriate*, the FI should consider:

- The risks associated with the outsourcing arrangement.
- The number of available assurance tools outside of internal audit reports (CSP service options, tools activated by the FI) as a factor of interest. Where the FI already considers available assurance high, the obligation for internal audit reports may decline in reliance with FI assurance requirements.
- If the CSP's Internal Audit function is set up in compliance with the FI's own Internal Audit function. The function's independence and status within the CSP organisation (for opinions and reports) are relevant.
- How frequently the FI intends to conduct individual/pooled audits of the provider.

The mandate and objectives of the CSP's internal audit function. In particular:

- The CSP's Internal Audit is mandated with providing assurance to its management and board of directors. It should not be assumed that the work performed by CSP's Internal Audit will contain relevant alignment of coverage of the risks identified by clients under the methodologies defined above. The primary objectives for CSP's Internal Audit function do not include obligations to provide assurance to CSP clients.
- The CSP's Internal Audit reports may cover more than individual service provision to a single financial institution. CSP's cannot indiscriminately share their own sensitive assurance exercise, since it is relevant for security and business operations of the entire multi-client environment. Even the contractually-agreed relationship with customers may not offer the foundation for full and indiscriminatory disclosure. In turn, the CSP's security considerations as well as service relevance to the outsourced functions are relevant factors for consideration. Here, a possible compromise is submitting redacted or protected internal audit reports using blank-out/black-out document tools or sharing, for example, relevant extracts of summaries. This ensures the FI only sees those parts of the report that cover the consumed services in scope of the FI's examination and the respective controls sets. However, when considering or applying this method, it is recommended to clearly share with the customer the rationale behind why redaction is required and who can be contacted in the event of questions and follow-ups on their inclusion. In light of internal audit report sensitivity, the CSP's take steps to share the non-redacted parts only via communication channels that are appropriate to safeguard confidentiality. While customers can receive them during formal audits, they will not be disclosed on websites.

2.4.5 Preconditions for third-party reports and Internal Audit report usage

The cumulative requirements in EBA GL para. 93 should be considered in order to determine if third-party certifications, third-party reports, and internal audit reports by the service provider are "adequate" and "sufficient" and can be used as an audit method.

EBA GL PARA. 93

Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they:

a. are satisfied with the audit plan for the outsourced function;

b. ensure that the scope of the certification or audit report covers the systems (processes, applications, infrastructure, data centres, etc). and key controls identified by the institution or payment institution and the compliance with relevant regulatory requirements;

c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

d. ensure that key systems and controls are covered in future versions of the certification or audit report;

e. are satisfied with the aptitude of the certifying or auditing party (with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/ verification of the evidence in the underlying audit file);

f. are satisfied that the certifications are issued, and the audits are performed against widely recognized relevant professional standards and include a test of the operational effectiveness of the key controls in place;

g. 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

h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.

The following guidance strives to provide a common understanding between FIs and CSPs of the supervisory conditions of the methods of para. 91 (b) and to facilitate the effective use of these methods.

a) are satisfied with the audit plan for the outsourced function;

Understanding of the timing of third-party or internal audit reports is important. FIs appreciate a forecast of the CSP's audit objects as well as the audit frequency and timeline.

For Internal and External Audit reports, to acquire the relevant assurance, a FI may want to validate the audit report by reviewing the charter, policies, and procedures of the CSP's internal audit department or the third party's audit methodology. The CSP should be able to provide the FI with sufficient information – including the scope of the respective audits. For Internal Audit reports, FIs should consider the potential differences between the mandate and orientation of the Internal Audit functions at the CSP and the Internal Audit function at the FI (e.g., coverage methodology versus risk-based methodology[34]).

Where a CSP offers the use of such third-party certification, the initial information of the availability to FI auditors should include the date of the certification's last update. The FI should also consider the expected version updates of the third-party certification.

b) 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 institution or payment institution and the compliance with relevant regulatory requirements;

FIs should review the scope of the CSP's third-party audit reports for sufficient cover of their own scope requirements, depending on the different services and regions they might use. FIs should also determine the extent to which the controls tested in available third-party attestations overlap with their own internal control framework. Since, in most cases, outsourced processes and/or functions need to be treated like internal processes, the scope of the requirements should always be aligned with the requirements on internal processes.

c) thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

FIs should implement a periodic monitoring/review process which ensures that the CSP's third-party certifications and reports are properly renewed and that the scope and result of respective subsequent audit reports matches their own requirements. Each FI needs to regularly assess the scope of the third-party certifications based on the identified processes and controls that are relevant to the FI.

[34] Please also see Section 2.4.4.

d) ensure that key systems and controls are covered in future versions of the certification or audit report;
In case FIs identify gaps in the scope of the third-party reports, they should align with the CSP on potential scope expansion within subsequent audits to include the necessary scope in the CSP's compliance programmes.

e) are satisfied with the aptitude of the certifying or auditing party (e.g., with regard to the rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);
The FI should take qualification and potential auditor rotation policies into consideration by assessing the extent to which they can rely on these audit reports. To ease such assessment, CSPs may provide FIs with information on their own auditor selection and review processes as additional information.

f) are satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;
FIs should review what baseline security standards are used for the respective certification and audit reports. Audit reports often differentiate between Type 1 reports which only test the proper control design, and Type 2 reports which also test the controls' operational effectiveness. If the operational effectiveness test is not part of the respective certification, the FI should evaluate the extent to which they may need to perform their own operational effectiveness testing if the CSP can provide alternative assurances for the operational effectiveness of such controls.

g) 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;
This right is to be secured as part of the contractual negotiations prior to service uptake by the FI. CSPs often cater to this regulatory expectation with a clause under the Financial Services Addendum.

h) retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.
Like point g), this right is to be secured as part of the contractual negotiations prior to service uptake by the FI. CSPs often cater to this regulatory expectation with a clause under the Financial Services Addendum.

> "Using certifications/ reports and conducting audits are not mutually exclusive. FIs may choose to leverage the provider's reports during (or prior to) individual or pooled audits."

CHAPTER
THREE

3 Best practice guide for pooled audits

The following technical guidance on best practices is based on the initial approach outlined in Chapter 1. The understanding of cloud auditing is founded on regulatory expectations to FIs, as codified in the EBA GL and presented in Chapter 2. Guidance is not limited to CSP controls only, but aims to support the reader in the approach to risk-mitigation measures in general.

3.1 Introduction to pooled audits

3.1.1 Advantages of pooled audits

Participants of the EBF Cloud Banking Forum agree that pooled audits can be very helpful. The Pooled Audit approach enables individual audit rights to be executed in a group format, benefitting both the CSP and the individual financial institutions (FIs): collaboration reduces costs and saves resources. For the CSPs, reducing the number of repetitive actions to provide the same insights for different clients drives effectiveness. At the same time, FIs require a lower number of auditors per institution to cover the same ground. Both sides can in turn allocate resources more effectively. The number of pool participants can streamline the complex preparatory actions required for carrying out a cloud audit.

Pooled audits also serve as common learning experiences for FIs and CSP, engaging both sides in dynamic cooperation from the outset. There are learning experiences in the different (plan-do-check-act) stages: project planning (plan); execution (do); lessons learned (check), and the continuous improvement through repetition (act). Shared pooled audit experiences drive a common language, and a deeper understanding of the approaches and methodologies used on both sides. Such larger-scale alignment of a growing number of FIs and CSPs engaging in pooled audits helps to scale up the efficiency for future audits to come.

3.1.2 Collaborative work between FIs and CSPs

To address their own risks and regulatory requirements, European FIs need to audit CSP processes and risk-mitigating measures (for instance, the controls part of CSPs' internal control system (ICS) that mitigate FI risks). This requires

careful consideration because both CSP processes and risk mitigation are quite different from what European FIs are used to audit in traditional IT systems. Consequently, a key prerequisite is that FIs understand CSP processes, failing which FIs cannot issue solid opinions and/or any assurances. This understanding incorporates the controls landscape and its evolution under the shared responsibility for cloud computing[35]. Collaboration is key to share the required understanding.

Two aspects are of central importance:

- A **structured work** between FIs in defining a scope in line with the pooled audit group members' different risk appetites.
- An **extensive exchange of information** between FIs and the audited CSP in terms of understanding risks, processes, and all risk-mitigating measures/controls.

Fundamentally speaking, a pooled audit expects:

- Transparency and trust on both sides (pooled audit group and CSP).
- Assurance that FIs will be provided with all relevant information and evidences needed to form a solid opinion.
- The opportunity for FIs to gain a greater understanding of CSP processes and further risk-mitigating measures.
- The possible application of audit techniques that are suitable for CSP processes.
- A balanced level of knowledge in the pool, enabling efficient cooperation. Where there are fundamental differences between pool participants (such as time needed for the exercise), efficiency gains may be jeopardised.

3.1.3 Methodological and organisational setup

An effective and efficient pooled audit requires a proper planning process and alignment among all participants.

Finding a common ground among the different FIs joining the pooled audit

Prior to the execution of the individual pooled audit project, an organisational and methodological structure must be rigorously defined. Even on highly sensitive aspects, this ultimately supports and facilitates the decision-making processes in a pooled audit group.

This definition includes in particular:

- The audit scope and respective alignment on a common framework.
- Agreement on necessary audit steps to be conducted.
- Contractual arrangement on collaboration by each group member.
- Cost distribution.
- Workload distribution methodology.

All aspects should be reflected within a common methodology agreed upon by each member of the pooled audit group.

Working understanding of cloud technology and processes to be audited

FIs and technology companies such as CSPs may have a different understanding of handling risk. While FIs mainly focus on classic IT Risk and Security management, relying on a combination of automated and manual controls as well as written procedures, CSPs focus more on automated risk mitigation, with less focus on written procedures and the use of technical measures to ensure risk mitigation.

[35] Please see shared responsibility model, Section 1.3.

It is therefore crucial that each auditor participating in a pooled CSP audit have solid knowledge of the technologies used[36].

FIs should carefully decide the right size and structure of the pooled audit group

The more parties join and actively participate in audits, the more important it is to ensure a clear decision-making framework within the group. The pool should be set up with efficiency considerations in mind.

Physical limitations and exponentially-increased complexity within larger groups may require a governance split of larger audit groups into "active" and "passive" audit members. The size of an "active" audit group conducting the audit fieldwork needs to be appropriate to the framework's designation of tasks (possible domain designation). To have efficient scope agreement processes, the size of the "passive members" (who contribute with high-level scope definition, audit cost coverage, and audit report access) might be scalable to a significantly larger extent but requires respective governance coordination within the audit group.

Any form of active/passive organisation is a form of delegation, covering at least audit execution. While to a certain extent, active members only rely on other active group members' work contributions, the degree of "delegation" and "reliance" on other auditors is stronger for passive members. Therefore, it is at each financial institution's discretion to determine the extent to which they feel comfortable joining a pooled audit as active or passive member. Involved as they are in the audit scoping process, and despite the name, "passive" members are still accountable for reflecting their needs. The pooled audit group must always ensure a reasonable balance between active and passive members.

3.1.4 Auditing Governing Principles

Auditing a CSP using a pooled audit approach should be based on principles aiming to secure a reliable audit result. Such principles further ensure the proper selection of viable FI candidates for participation in the pooled audit group ("Pooled Audit Participant"). Said principles should be regarded as specialised additions to the more fundamental principles for all cloud audits presented[37].

GUIDING PRINCIPLES

ONE
The Pooled Audit Participant has an existing contractual relationship with the CSP.

TWO
The Pooled Audit Participant intends to consume the Public Cloud Services of the designated CSP.

THREE
The Pooled Audit Participant commits to actively support the collaboration in the Pooled Audit Group (i.e. by signing a collaboration agreement).

FOUR
The Pooled Audit Participant should agree with the common methodology and standards to be used (if any) as defined by the Participant group as a whole, during the audit activity.

FIVE
The Pooled Audit scope is defined jointly based on the individual input provided by each Pooled Audit Participant in preparation of the audit.

SIX
Each Pooled Audit Participant shall have access to the joint audit documentation – including scope, testing approach, and other documentation – as well as audit results.

SEVEN
Each Pooled Audit Participant is committed to completing all audit steps necessary, until final evaluation of the pooled audit.

EIGHT
Each Pooled Audit Participant shall remain responsible and accountable for the final assessment (risk rating) and evaluation of the Pooled Audit results.

[36] As stated under the principle "integrity"; please see Section 1.6.2.
[37] Please see section 1.7.1.

3.2 Pooled Audit Process

3.2.1 Overview of the pooled audit process

The Pooled Audit scope is defined jointly based on the individual input provided by each Pooled Audit Participant. The focus of Pooled Audits is to verify that the CSP's processes and internal control systems adequately support the mitigation of the Pooled Audit participants' risks.

Figure 7 shows the audit process, the cooperation required for each step, and the output documents. There are five phases in the process, namely the Trigger, Preparation, Fieldwork, Reporting, and Follow-up:

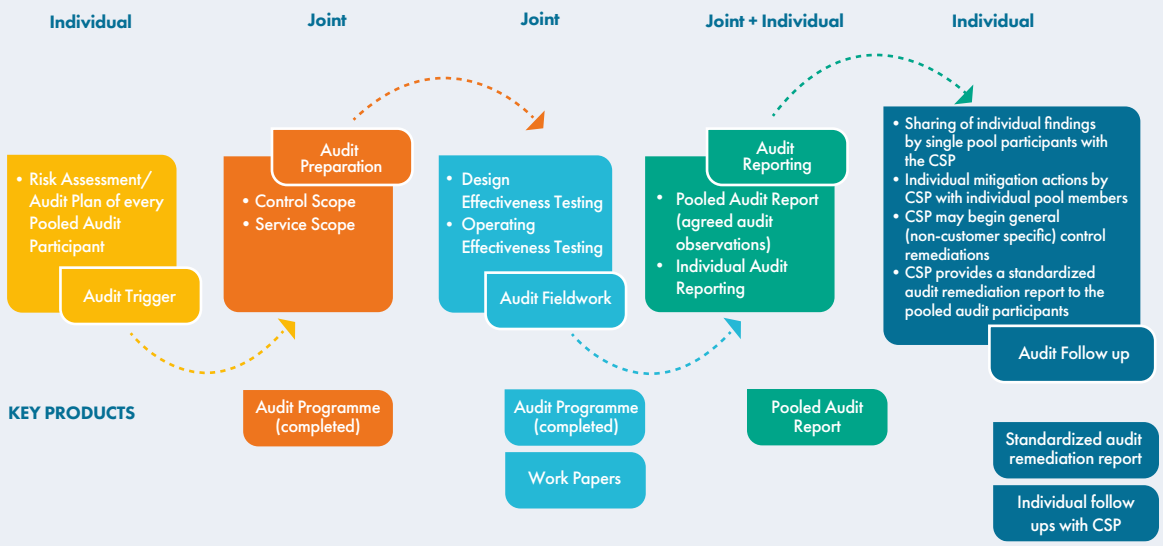
3.2.2 Pooled audit preparation

The audit preparation phase should be executed jointly by all Pooled Audit Participants, i.e., defining the control objectives and service scope based on input from all Pooled Audit Participants. In this phase, all Participants also agree on the common terminology and methodology for performing the audit activity.

Once understanding is secured, the control objectives should address the FI risks related to using cloud services. **A key product of the audit preparation phase is a formalised audit programme** which defines the agreed control objectives, associated risks, and service scope.

FIGURE 7

Pooled audit process steps and key deliverables



> Key product of the audit preparation phase is a formalized audit programme.

To ensure alignment on every part of the process, the programme should be discussed with the participating Pooled Audit Group (active and passive members). Should the discussion trigger comments and/or changes to the final version of the document, these should be clearly flagged for full transparency for all Pooled Audit participants.

Leveraging the understanding of the CSP's processes in scope, the **testing procedures should be part of the detailed audit programme**, with the latter being developed continuously as detailed information about the CSP's processes and control measures are received. For the auditors to understand the cloud technologies and CSP's control environment, gathering the right information as early as possible in the process is an important part of drafting the detailed audit programme. The Pooled Audit group and CSP should ensure sufficient time and resources are allocated to the preparation process, considering which information the auditors require, when and how the CSP can facilitate such information requests (within the audit preparation phase and/or in the audit fieldwork phase) and in which manner. The following sub-sections outline this in more detail.

3.2.2.1 Communication of timeline between FIs and CSP

Considering the complexity and cooperative nature of the pooled audit process and the number of participants, timelines should be communicated early on to provide clarity.

COMMUNICATING WITHIN THE AUDIT GROUP:

The timeline for the audit group should at least contain:

- General audit timeline, including audit start, preparation, fieldwork stages, auditor's documentation review, and reporting stages.
- Scoping workshop (scope definition and workload assignment).
- Audit programme development stages.
- Auditor team and CSP alignment meetings.

COMMUNICATION BETWEEN THE POOLED AUDIT GROUP AND THE CSP:

The Pooled Audit group should agree on a timeline for actions and expected information exchange and communicate details thereof to the CSP. The timeline should include information on the:

- Delivery of detailed information about CSP-implemented processes and controls to the group (in the preparation phase, and with more details in the fieldwork phase).
- Audit fieldwork and reporting.
- CSP delivery of documents and evidence.

To enhance communication and foster timely delivery of information, any difficulties hindering a timely delivery should be mentioned as early as possible. Any missing but required documentation should be mentioned immediately to avoid unnecessary delays. To prevent any misunderstandings and define possible alternatives, auditor requests should be discussed with the CSP as and when they arise.

3.2.2.2 Common understanding of relevant information for the pooled audit

To ensure alignment, auditors should provide CSPs with **a list of required documents** and hold **clarification calls** to confirm understanding of the request.

It is recommended that the list be subdivided into Prep phase and Fieldwork phase and include details on auditor evidence requests, such as:

- High-level written documentation describing the CSP processes such as:
  - Policies
  - Programmes (Business Continuity Programme, Disaster Recovery Programme, Incident Management Programme, etc).
  - Plans (Business Continuity Plan, Disaster Recovery).
- Detailed written documentation describing the CSP processes, for example:
  - Operating procedures
  - Runbooks
  - Playbooks
- Screenshots of the internal tools (redacted as needed for confidentiality). Screenshots should be taken during live sessions/interviews on auditor request.
- Proper samples of data and metadata, to prove that CSP processes work as designed/expected. Personally identifiable information (PII) and other sensitive data must be redacted and/or anonymised. Hash functions may be used to assure sample data cross-correlation integrity.

Considering the range of information with relevance for FIs, all FIs should already hold a signed contract with the CSP to audit. This contract should provide the basis for confidentiality and audit rights agreed, so that information sharing is secured.

Publicly-available documentation or customer-specific information – pending further authentication – will be important during all the audit phases[38]. CSPs invest heavily in making the information transparent and readily available.

MAKING INFORMATION AVAILABLE

Information by CSPs does not necessarily require a bilateral delivery to their customers. Public information can be a helpful source for FI auditors to research relevant information about CSP risk-mitigation measures early on.

CSPs make information available online, often with filter-function by country and industry. This can include security and audit information which can be useful to a bank and a Pooled Audit group's audit team.

Possible information available:

- Documents reflecting contractual commitments on:
  - Security safeguards
  - Privacy
  - Technical and organizational controls
  - Operational controls
- Commonly available information on system performance and security.
- CSP-specific features and functionalities to provide real time information.
- Customer-controllable security features (online guides).
- Information on additional security measures such as data encryption, monitoring, and access controls (whitepapers for download).
- Attestations of penetration tests and security assessments performed by third parties (available online at CSP website).
- Security Health Check: A standard feature which analyses CSPs security settings against a default or custom baseline. It provides a score and specific recommendations in help and training articles online.
- Publicly-available financial accounting information (depending on the CSP's public listing status).

Additional resources may be available via CSP online trainings and help services.

[38] Please see also Section 2.4.2.

3.2.2.3 Compliance Certifications and Attestations review

A helpful source of information for auditors upfront is a first review of the CSP compliance certifications and attestations – especially ISO and SOC reports. This reflects EBA GL para. 91 b., making third-party certifications and reports explicitly available for use to FIs. CSPs often make these reports available for all customers. If not, the Pooled Audit group can request these from the CSP directly.

Where reports include sensitive business information, the existing customer status of the requesting FIs can become relevant. Providers have a practice to request NDAs in such constellations. EBA GL para. 96 caters to providers' multiclient environments, stating explicitly that care be exercised to ensure that risks to another client's environment are avoided or mitigated. Limits to the use of third-party certifications and report under EBA GL para. 93 have been presented above[39].

Many CSPs have quite an extensive control framework aligned to industry standards like ISO 27001, SOC, C5, IIA standards and others. The better aligned the frameworks leveraged by the Pooled Audit group and the CSP are, the easier and faster controls- mapping can be done. This helps the CSP to better understand the risk and controls the pooled audit wants to audit and to provide the respective evidence.

3.2.2.4 Alignment and mapping of the audit scope with CSP's controls

The alignment and mapping of the Pooled Audit group's control auditing requirements and the CSP's control environment is a crucial part of the audit preparation phase. Since the setup and details of the CSP's (often highly automated) controls may significantly differ from traditional IT environments, Pooled Audit groups must clearly and precisely define the risks they intend to address with the audit procedures. Jumping directly into asking for specific controls or specific evidence without first discussing which risk is being address/audited may lead to inefficient exchanges of information.

An audit's success relies on a good Pooled Audit group/CSP alignment on the common audit approach which includes:

Step 1

Identification of the risks to be addressed

Step 2

Citing of the respective controls the CSP uses to address risks

Step 3

Definition of the type of evidence required to audit and confirm design and operational effectiveness

With the approach established, the Pooled Audit Participants should then **define control objectives to be assessed during the audit** in conjunction with the pooled audit participants' risks as outlined above. The suggested **control objective scope** for pooled audits should be defined based on industry standards and best practices as well as regulatory requirements[40]. The CSP should provide the description of processes and implemented risk-mitigating measures/controls in accordance with the communicated control objectives. This enables testing of the design and operating effectiveness of the control activities and processes implemented by the CSP.

Furthermore, the **service scope** for pooled audits should be defined based on each Pooled Audit Participant's use of the CSP services and their criticality. The defined audit scope should be clearly communicated to the audited CSP, together with the audit timeline and scope period as referred to above[41].

[39] Please see section 2.4.5.

[40] EBG GL on outsourcing: EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu) For ongoing regulatory activities please see section 1.8.

[41] Please see section 2.4.1 and 3.2.1.

The control objective scope and service scope should then be reflected in the audit programme together with the CSP risk-mitigating measures/ controls as well as relating risks to each of the control objectives.

3.2.3 Audit fieldwork

After the audit scope has been defined and preparation completed, audit fieldwork can begin. All "active" audit group members execute audit fieldwork jointly. To avoid any kind of "audit outsourcing" within the pool while working on different content in shared work forms, the respective "active/fieldwork group" should implement internal review and approval processes to create full transparency and approval of all details.

The following understanding is essential:

- The control scope is structured/divided into control topics, and
- Every control objective group is assigned to an auditor group from at least two different Pooled Audit Participants ("four-eyes inspection").

During fieldwork, **work papers** shall be produced, directly derived from the Audit Programme, giving a more granular view on the design effectiveness and operating effectiveness testing. The papers should include references to all CSP-provided evidences and may be used as the main source for all documentation for the audit fieldwork.

When fieldwork is being carried out, it is useful to document and track the identified observations (control deficiencies) for the respective control objective in a **separate list**. It allows pooled audit members to commonly discuss and agree on the observations while individually considering how the deficiencies may affect services relevant to FI risk appetite.

The list's content and accompanying explanations shall be transferred to the work papers created by the respective auditors. All the Pooled Audit participants should review these work papers during and at the end of the fieldwork – a review which entails each Pooled Audit participant looking at each work paper to ensure that each member's risk is reflected. Lastly, all participants should approve the workpapers.

EVIDENCE TYPES FOR FIELDWORK:

- Policies and procedures, standards, operating manuals.
- Organisational structure of the CSP team(s) responsible for the execution and monitoring of the controls related to the audit scope.
- Technical/operational documentation (infrastructure schemas, playbooks, runbooks, etc).
- Reports: Control execution reports, (executive) management reports.
- System screenshots: Evidence showing the system works as intended, with screenshots supported by additional live system sessions as needed.
- Meeting memos showing discussion content and participant roles with PII data redacted (for incident reporting).
- Agreements and contracts (including summaries and relevant extracts) with subcontractors (as far as possible, complying with the required care as defined in EBA GL para. 96).

Evidences can be distinguished according to their persuasive nature. Auditors consider two clusters according to the source's pre-existing history:

- **More persuasive**: organisational policies, procedures, operational manuals (each having a history).
- **Less persuasive**: interview notes, written confirmations, documents written during the course of the audit (having no history).

GOOD PRACTICES DURING FIELDWORK

- Timely and regular updates of the audit documentation after interviews and evidence delivery.
- Timely (or early) request-creation and regular delivery tracking to ensure timely escalation (if needed).

Since controls are tested during audit fieldwork, design effectiveness and operative testing must be distinguished.

3.2.3.1 Design effectiveness testing

A design effectiveness test should address if the control is designed to prevent or detect an error and therefore mitigate the risks identified and agreed upon as relevant for FIs.

A properly designed control should:

ONE

Satisfy the control objective, and

TWO

Enable a re-performance, meaning that, at least, the three following elements must be present:

i. control activity description
ii. frequency
iii. control owner

To evaluate a control's design, different testing procedures can be used, often in combination:

- **Inquire:** ask appropriate subject matter experts and/or control owners.
- **Observe:** watch operations or particular steps being carried out.
- **Inspect** relevant documentation: analyse policies, standards, operating manuals, technical documents, and internal control outputs.

During the design testing, the auditors may identify control deficiencies/deviations (gaps between the implemented control and the control objective and associated risk). These deficiencies should be discussed with the audited CSP to verify factual accuracy.

At the end of the design test, auditors should have all the elements to state whether they deem the control to be adequately designed. If not adequately designed (failed test), the control must be tested for effectiveness, as this may either show different results or confirm the design flaws.

> "At the end of the design test, auditors should have all the elements to state whether they deem the control to be adequately designed."

3.2.3.2 Operative effectiveness testing

The operative effectiveness test aims to test whether or not the risk-mitigating measures/controls operated consistently with the design over a past period in time. This can be done either through sampling or by gathering evidence that certain (automated) controls cannot be circumvented and are always conducted as designed. Control frequency and nature should be used as criteria on how to assess operative effectiveness.

IMPACT OF DIGITAL TRANSFORMATION? A LOOK AT AUDIT DATA ANALYTICS

Cloud audit is a relatively young domain that is being continuously enhanced by the cloud practices and standardisation communities to address all particular aspects of the architectural model. Auditors are challenged by one important aspect: the large-scale data and systems dimension of cloud computing and large-scale automation that derives from such an architecture model. This can impact practices in sampling, which might not always suffice for the required evaluation of CSP assurances of automated processes working as intended and how controls on automation are correlated to auditor organisation risks.

To tackle this challenge, recent progress on integrating data analytics and related technologies into the audit process has enhanced audit quality by working more effectively with large data sets. Applying audit data analytics may help to detect material anomalies by allowing all the items in a population to be examined, thereby effectively managing sampling risk. Audit data analytics can enable auditors to use data visualisation techniques and use it throughout the entire audit process, ultimately helping to form the overall conclusion.

Testing the operating effectiveness of controls can be based on different approaches with increasing levels of confidence or through an appropriate combination thereof. These tests ordinarily include procedures such as walk-through of the control, observation of the entity's operations, inspection of the system configuration, re-performance of the control, review/assessment of the specific control either on a sampling base or in a substantive way, to validate that it operated as defined along the audit period. **The auditor's evaluation of the design effectiveness of control procedures often influences the nature, timing, and extent of the tests of operating effectiveness.**

It can be quite challenging to assess automated controls, with CSPs often relying on automated controls of either preventive or detective nature.

It could help auditors to:

- Understand better how an automated control is performed by conducting an end-to-end walk-through of a control using a combination of inquiry, observation, and inspection, and identifying possible evidences (e.g., screenshots) on the way.
- Observe how the control owner performs the control in different scenarios.
- Inspect the configuration defined in an application/system.
- Inspect measures on how to circumvent the control. If applicable, conduct a test failing the control and observe the error message the application displays.

In order to rely on automated controls, **it is essential that a host of underlying IT general controls work effectively.**

No matter the approached type of control, the selected assessment method needs to be documented and the evidences stored. This might include documentation on how samples have been chosen, sample evaluations, or how a control might be circumvented.

As with design testing, during operating effectiveness testing, the auditors may identify control deficiencies/deviations (i.e., gaps between the implemented control and the control objective and associated risk). To verify their factual accuracy, these deficiencies should be discussed with the audited CSP.

3.2.3.3 Walk-throughs as part of the fieldwork

When testing the actual implementation of a control itself, a sample should be looked at:

- Perform a process/control walk-through by respective CSP Subject Matter Experts on the specific control objective to be shown to the respective control objective's auditors. Walk-throughs on an end-to-end process, ranging from first steps to the final approval (if applicable), are deemed most comprehensive.

Example: In terms of incident management, this might include showing incident reporting, triage, remediation actions, implementation approval, and lastly, incident closure.

- Templates can serve as support documents for the walk-through.
- The walk-through should include the inspection of a number of samples of control execution (Test of Effectiveness[42]).
- Where auditors are shown walk-through controls or risk mitigation measures, respective evidences should also be provided that also include walk-through screenshots.

3.2.3.4 Fieldwork outcome

Key products of audit fieldwork are:

- **Final audit programme** which can possibly advance the original version resulting from the preparatory phase of the pooled audit (update, a reason for which is the conducted test impact). The latter can result in the minor adjustments being included in the programme, reflecting testing outcomes accurately.
- **Completed audit documentation** (i.e., audit work papers) which includes a description of the work performed to assess the design and operating effectiveness of the controls from the audit scope and the identified agreed control deficiencies. As described earlier, all Pooled Audit Participants shall review this audit documentation.

In addition to the above, auditors and CSPs should conclude fieldwork with a dedicated conversation on the **lessons learned from the fieldwork cooperation.** Generally speaking, a constant communication between auditors and CSP on issues appearing during the audit – without undue delay – can maximise audit efficiency. As a final 'lessons learned' exercise, both sides should share positive and negative impressions from the exercise, advancing the common understanding and improving the starting point for future audits.

> A constant communication between auditors and CSP on issues appearing during the audit can maximize. audit efficiency.

[42] Please see Section 3.2.3.2.

3.2.3.5 Remote auditing procedures

While remote auditing remains a nascent discussion further accelerated by the demands and limitations of experienced Covid-19 restrictions, it is already being put into practice in limited capacity. It must, however, respect the audit principles outlined in this paper[43] and be solidly based on the regulatory requirements issued to FIs under EU law and supervisory guidance. Remote audit tools cannot be used at the cost of reduced audit functions or security. Indeed, financial entities carefully consider the added value of physical access as part of their auditing scope and execution. European banks and cloud service providers will consistently evaluate available instruments for auditing purposes.

There are of course benefits to remote auditing. It addresses any health-crisis-related need to limit physical interaction of personnel. Remote audits can simplify logistics, save costs, and increase environmental sustainability. Being able to perform interviews, reviews (of documentation and processes) and observation activities remotely maximises work time efficiency. The 24/7 availability of evidences could increase the efficiency of understanding CSP-implemented processes, while giving auditors the chance to study documentation at their own pace.

The key focus should, however, always be to meet audit objectives in line with the audit scope. Depending on the control objective, a remote audit may not always permit the auditor to complete the activity without physical presence such as physical controls (to security-relevant areas such as data centres) and documents requiring physical presence (emergency call lists used for business continuity purposes).

Performing remote audits also means auditors miss out on direct interactions with auditees and consequently the opportunity to strengthen the overall audit process. Long-distance communication is no substitute for exploring issues and audit trails

> “Remote auditing procedures must ensure that FIs' internal needs and regulatory requirements are met to the same degree as in on-site audits.”

in an on-site audit. The human element of real-world interaction builds stronger auditor/auditee relationships. An undifferentiated replacement of this interaction by remote communication would seem rash; the right balance between remote work and physical presence should be struck. Overall, audit activity cannot be entirely separated from a direct relationship with the audited structures.

If under these considerations remote audit action is considered, pre-requisites for doing so should be clearly defined in the audit preparation phase. Remote auditing procedures must ensure that FIs internal needs and regulatory requirements are met to the same degree as in on-site audits. The guidance presented in this paper therefore stands true for remote audit exercises as well. Considering the IT-based nature of a remote audit activity, however, no additional risks should be added due to the remote engagement.

The clear definitions under the audit preparation phase would need to include available technology supporting the activity and the accesses to evidences, along with their respective storage, to allow the auditors to exercise their audit rights and to have the needed access to the relevant systems and documentations.

[43] See section 1.6 and 3.1.4

The necessary audit procedures may include (amongst other aspects):

- Remote interviews with Subject Matter Experts on clarification of CSP processes and pooled audit participants requests leveraging audio and video conferencing.
- Live (screen) demonstrations of CSP systems while protecting the security, confidentiality, integrity, and privacy of CSP systems (showing PII should be prevented in any case).
- Interactive virtual sessions, including an availability of interactive work on data samples for auditors.
- Providing the evidences within a secure environment that is remotely accessible for all the pooled audit participants.
- The opportunity for auditors to take live evidences and store these appropriately.

3.2.3.6 Automated auditing processes

Even with efficiency gains under a pooled audit approach, manual and human-based audits face physical and logistical limitations. Scalability is not indefinite. CSPs are usually built on highly automated procedures and control processes. This provides a natural basis to discuss and evaluate automated test procedures in the future, without putting the usefulness of manual actions, per se, into question.

Control frameworks such as C5 have already started considering and evaluating the potential use of automated test procedures going forward – a topic that is too new and complex to be discussed in detail in this paper. It should, however, be noted that auditors and CSPs in future pooled audits should consider and discuss the potential use of automated and continuous auditing procedures.

3.2.4 Audit reporting

3.2.4.1 Audit group observation report

To finalise the audit, a **Pooled Audit Report** shall be created based on the identified agreed control deficiencies, as documented in the audit work papers (completed documentation), the CSP management response regarding a jointly-agreed remediation plan and a remediation target date. The final product of the pooled audit is the Pooled Audit Report and shall be provided to the CSP to formally conclude the conducted audit.

3.2.4.2 Individual FI's audit report

The audit report created by the pooled audit group cannot reflect each FI's own individual risk as the inherent and residual risk and control failure at the CSP will depend on the individual FI's (intended) cloud usage profiles, different risk assessment methodologies, and risk appetites. Consequently, pooled audit reports do not usually contain a risk assessment and classification of the observations/findings. The participating FIs therefore usually translate the group report into a risk-rated, FI-specific **Individual Audit Report**. Reflecting only the observations relevant for the respective FI, these individual audit reports may vary significantly between different pooled audit participants and are not shared among the pool members.

FIs usually review if the audit results lead to a potentially necessary update of their internal risk catalogue[44] due to decreased or increased risk perception.

[44] Such catalogue serves FI internal purposes and should not be mistaken for Reporting registers. For a template of a reporting register on cloud, please see the EBF Cloud Banking Forum paper "Outsourcing register: Cloud specific guidance" under https://www.ebf.eu/wp-content/uploads/2020/06/200604-EBF-Cloud-Banking-Forum_Outsourcing-Register-cloud-specific-guidance_final.xlsx.

3.2.5 Audit follow-up

In line with the previously presented differences between pooled audit participants, the follow-up measures will differ between individual FIs involved. Not all findings can be expected to apply to all group members alike. Individual reflection on the finding in question is therefore always necessary.

Re-negotiations of cloud contracts are not a general follow-up measure of a cloud audit. Nevertheless, it is recommended that the Pooled Audit Participants share their individual findings (conclusions/criticality assessments of potentials findings) with the CSP to allow the latter to understand priorities and consider these in their own audit-remediation prioritisation.

The wide variety of different audit follow-up needs prevents the application of a single "pooled audit follow-up approach".

Nevertheless, certain follow-up options present themselves:

- The CSPs may begin with implementing rather **general and not customer-specific control remediations** as potential audit follow-up to the pooled audit.
- On top of the **CSP's individual mitigation actions with individual group members**, the CSP can also provide an additional, more **standardised audit remediation report** to the pooled audit members commonly. It can invite the group to joint audit follow-up discussions to present and discuss evidences for completed audit remediations.
- Audit follow-up activities can be included in the scope of a potential subsequent pooled audit instead of performing additional audit follow-up activities on a bilateral basis in between the just-executed pooled audit and the subsequent one.

It is up to the individual pooled audit member to decide what degree of audit follow-up is necessary and what assurance/evidence for remediation is required to confirm closure of the potential findings.

ANNEX

Responsibility assignment (RACI) matrix – TLoD model

The following matrix focuses on the outsourcing by a FI to a single CSP.

Legend for the RACI matrix:	
Responsible (R)	The person responsible for completing the task, getting the work done, or a decision made. As a rule, this is one person such as a data processor, application owner, or technical architect.
Accountable (A)	The person who is accountable for the correct and thorough completion of the task. This must be one person and is often the data owner, contract owner, or project sponsor. This is the role that Responsible (R) is accountable to and approves their work.
Consulted (C)	The people who provide information for the project and with whom there is two-way communication. This are usually several people, often Subject Matter Experts.
Informed (I)	The people kept informed of progress and with whom there is one-way communication. These are people who are affected by task outcomes and must be kept up to date.

	First LoD				Second LoD						Third LoD		CSP
Task	Business Line	Information technology	IT Security	Management	Third Party Risk	IT Risk	Legal and Compliance	Data Governance	Regulatory Affairs	Financial Risk	Internal Audit	External Audit	
Pre-outsourcing phase - Planning and Strategy													
Define Cloud Policy as FI			C	C	A	C	C	C	I	I	I	I	
Establish Cloud Security Standards as FI	I	R	R	C	C	A	C	C	I	I	C	I	
Establish Cloud Governance as FI		R	R	R	A	C	C	C	I				
Define Outsourcing Requirements as FI	A	R	C	C							I	I	
Perform Risk assessment	A	R	R	R	R	C	C	C					C
Select Cloud Provider and perform due diligence	A	R		R									C
Approve Contract	A/R	C	C	C	C	C	C	C			I		R
Implementation													
Integrate IT Controls/Right Architecture	A	R	R										C/R
Train staff as required	A	R	R	R	R	R	R	R			R		C/R
Testing	A	R	R	I	I	I	I	I			I		C/R
Migration of processes or data into the cloud	A	R	R			C	C	C			I		C/R
Monitor Cloud Use	A		R	R	R	R	I	I					C
Business Continuity Management	A/R	R	R	C	C	C							C/R
Monitor Contractual Compliance	A/R			R	C								C
Monitor Control Effectiveness	A	R	R	R	I	I	I	I			R		C
Attest to the effectiveness of controls	A	R	R	R	R	R	R	R			R		C/R
Monitor Third Party Risks				R	A/R								C/R
Manage Fourth Parties	A	C	C	R	C		C						C/R

GLOSSARY

Assurance tool

Resources or processes provided by the service provider or a third party, available in different levels of independence, so that financial institutions can gain a deep understanding over the risks are associated with outsourcing to third parties such as cloud providers. Tools can target provision of information at scale and contain different level of confidential information for the provider. In turn, providers may not share individual tools outside of a strictly controlled environment or with safeguards such as NDAs.

Audit

Audit is defined as a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fullfilled (ISO 19011:2018 - Guidelines for auditing management systems). In the context of this paper, and if not stated otherwise, the term usually refers to review and testing activities conducted by the internal audit teams of a FI (3rd line of defence). However, audit activities by 1st or 2nd line are not categorically excluded in an audit.

Audit criteria

Audit criteria are a set of requirements used as a reference against which objective evidence is compared.

Audit fieldwork

Period of time where a team of auditors assesses the processes and controls on both design and operating effectiveness.

Audit finding

A finding may be derived by individual audit participants and can be addressed internally. It usually includes an assigned severity that indicates the risk-assessed criticality of an issue.

Audit program	Detailed testing steps of an audit linking back to the risks.
Cloud computing	An innovation in computing that allows for the use of an online network ('cloud') of hosting processors so as to increase the scale and flexibility of computing capacity. Cloud allows industries to tap into new service models, utilising its technological advancement for new and better services to customers, improving productivity, cost-efficiency and flexibility of internal business processes.
Control objective	Statements that shall address how risks should be effectively handled.
Design effectiveness	Showcasing that there are no gaps between FI requirement and the actual design within a CSP. Design in this sense includes all documentation like policies and procedures.
Evidence in a pooled audit	Information or data that are used or collected by IT auditors as part of their audit work so that they can conclude whether a control exists, is properly designed and operates as expected, within a defined audit period.
Evidences in audit fieldwork	Information or data used or collected by IT auditors as proof on controls/ processes/ risk mitigation measures.
Joint audit documentation	All documentation of the conducted pooled audit including scope documentation, test plans (audit program), test documentation (work papers), audit observations and the audit report.
Management system	Set of interrelated elements of an organisation that establish policies and objectives, and processes to achieve those objectives.
Observation in a pooled audit	The deviation between the control objective and the actual set-up (e.g., control/risk mitigating measure or process) at the CSP. An audit observation points to a potential control weakness, and it must be presented to the CSP who needs to agree to the factual accuracy before issuing the final audit report.

Operative effectiveness testing	Testing whether the CSP design is implemented according to the assessed documentation (policies/procedures) and the FIs requirements.
Pooled Audit	Pooled audits are collaborative efforts carried out by a group of auditors from different organisations with the goal of ensuring that a required level of assurance in outsourced services is or has been met.
Pooled Audit finding	A finding is an observation derived by an individual FI to address internally.
Pooled Audit Group	Group of individual FIs (Pooled Audit Participants) engaging in a collaborative audit.
Pooled Audit Participant	Pooled Audit Group members participating in a particular audit, including FI-candidates for participation.
Risk appetite	Cumulated risk that each individual company is willing to take.
Risk mitigation measure	Risk mitigating measures are designed to eliminate, reduce, or control the impact of known risks intrinsic with a specified undertaking, prior to any harm. Multiple risk mitigating measures may sum up to a risk mitigation strategy.
Samples of control execution	Sample to evidence that a control has been conducted the way it is designed.
Service scope for cloud	Defines the CSP-provided services that are going to be in scope for the audit.
Subject Matter Expert	A person who possesses a deep understanding of a particular control's design and execution.

Three Lines of Defense

Risk governing framework that splits responsibility for risk management across three different functions. The first line owns and manages risks directly, the second line must oversee the first line through setting up policies, defining risk tolerances and further risk mitigating measures. The second line is responsible for ensuring the implementation of the defined policies and risk mitigating measures through the first line. The third line (internal audit) is responsible to assess whether the first- and second-line functions are operating effectively. It is charged with the duty of reporting to the board and audit committee, in addition to providing assurance to regulators and external auditors.

Traditional IT systems

IT infrastructure typically connected to an on-premise server.

Work papers

Documents created by the auditors, directly deriving from the audit program. They give a granular view on design effectiveness and operative effectiveness testing. Relevant during pooled audit fieldwork, they shall include references to all evidences provided by the CSP. They may be used as main source for documentation of the audit fieldwork.

THE EBF CLOUD BANKING FORUM

European banks want to adopt innovative cloud technology, to allow them to operate in a fast-developing digital environment, to serve customers and to adapt their business in order to strive for the EU's digital leadership role. In December 2017, the European Banking Federation launched the EBF Cloud Banking Forum, a policy hub on cloud computing for European banks and Cloud Service Providers to support a harmonised supervisory approach towards cloud computing. This will facilitate the adoption of public/hybrid cloud computing by European banks on a larger scale.

The EBF Cloud Banking Forum focuses on specific regulatory developments related to cloud technology. The forum fosters the important exchange of IT architects, legal experts and cloud specialists from among EBF members (national banking associations and over 15 banks), Cloud Service Providers, and observers. The latter consist of Cloud Service Providers' trade associations and EU authorities (ECB, EBA, European Commission).

FOR MORE INFORMATION CONTACT

Alexandra Maniati
Senior Director of Innovation & Cybersecurity
a.maniati@ebf.eu

Julian Schmücker
Senior Policy Adviser - Digital Innovation
j.schmucker@ebf.eu

Drs. Patrick Maes
Chair of the Cloud Expert Group and Cloud Banking Forum
@ European Banking Federation
Managing Director – Global Head of Bank User Solutions
@ Credit Suisse
patrick.maes@credit-suisse.com | drspatrick.maes@gmail.com

European Banking Federation AISBL

Brussels
Avenue des Arts 56, 1000 Brussels
Belgium

Frankfurt
Weißfrauenstraße 12-16, 60311 Frankfurt
Germany

EU Transparency Register ID number:
4722660838-23