Position Paper

Requirements for standardisation
of compliant use of public cloud technology
in regulated European financial institutions

Version 1.0

12th of May 2021

Contact: consultation@ecuc.group

Document: ECUC_Position_Paper_May_2021.pdf

Content

1 Introduction

The European Cloud User Coalition (ECUC) was founded in 2021 to assist the compliant use of public cloud technology in European Financial Institutions (FI). Its primary objective is to develop a joint position on common challenges and solutions on Cloud Service Providers (CSP). This position is an aggregated view of the ECUC members and is derived from their experiences in public cloud adoption in recent years.

The aim of this Position Paper is to provide solutions to challenges we currently face to ensure long-term compliant use of cloud technology. The main challenges are:

- Overall public cloud adoption for FIs are challenging due to the specifics of cloud computing being regarded as outsourcing.
- Legislation such as Digital Operation Resilience Act (DORA) and rulings such as Schrems-II currently make it difficult for FIs to adopt public cloud services.
- FIs engaging CSPs individually leads to additional administrative effort and time, as well as misdirection of priorities.

Cloud computing is a key factor in transforming the financial sector. We see an opportunity to utilise public cloud solutions in this sector as they have high security standards, are readily scalable and robust. However, we need to address regulatory and other requirements to enable us to safely use public cloud to good effect. This will not only benefit FIs, but also CSPs and regulators. The CSPs can solve specific problems once and satisfy multiple customers at the same time, leading to compliant and secure cloud computing solutions for FIs. Regulators could leverage our requirements to formulate thresholds for CSPs in order to be appropriate for FIs.

The Position Paper consists of four different sections addressing requirements regarding Privacy, Security, Governance & Regulation, and Standard Contractual Clauses. There is also a section on the Digital Operational Resilience Act (DORA).

This paper is targeted to four different groups:

- The Requirements on cloud services are addressed to CSPs (EU and Non-EU) in their responsibility for offers to FIs.
- The interpretations on outsourcing are being brought to the attention of European Banking Authority (EBA) as a regulator.
- The enhancements on supervision are being brought to attention of European Central Bank (ECB) as a supervisor.
- The recommendations upon DORA are addressed to European Commission as the executive body.

European FIs are members of the ECUC. Amongst others there are: Allied Irish Banks, Bank of Ireland, BAWAG Group, Belfius Bank, Commerzbank AG, Deutsche Börse AG, EFG Bank AG, Erste Group Bank AG, Euroclear, ING Group N.V., KBC Bank NV, Landesbank Saar, Permanent TSB, Raiffeisen Bank International, Swedbank AB and UniCredit S.p.A.

The ECUC Position Paper is subject to regular updates and new releases. The requirements in this version must be regarded as a working response to the current challenges we face. Please refer to the ECUC website (https://ecuc.group) for the most recent version.

2 Requirements on Privacy

Information privacy is the right to have control over how personal information of the individual is collected and processed. This section specifies the requirements for privacy of individuals' data, both for employees and customers.

2.1 Data Privacy in Accordance with European General Data Protection Regulations

Responsibility CSP

Data protection in public cloud environments must conform to the relevant European data privacy laws and regulations such as General Data Protection Regulation[1] (GDPR). Within the European Economic Area (which includes the European Union), the GDPR data privacy law is applicable for both, FIs (data-controller as cloud consumers) as well as for CSPs (data-processor). In that regard, CSPs should prove that they are in strict compliance with the rules of GDPR when it comes to EU cloud consumers.

2.2 Technical Security Measures According to the EDPB Guidelines

Responsibility CSP

According to the recommendations[2] of the European Data Protection Board (EDPB) the stipulated use of Standard Contractual Clauses, data controllers and data processors should implement additional measures to compensate for gaps in protection of third country legal systems. These technical measures are typically data security, data minimisation, anonymisation or pseudo-anonymisation. These technical measures should work for all CSPs and cloud operating models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

2.3 Geographic Localisation of Data, Data Sovereignty and Regional Data Access

Responsibility CSP

With the invalidation of the EU-US Privacy Shield by the European Court of Justice (also known as Schrems-II), FIs as cloud consumers should be able to apply data restrictions to a certain country or geographic region, i.e. EEA. Furthermore, all cloud services should support storing and processing of consumer's data in a certain country or geographic region.

[1] https://gdpr-info.eu
[2] https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

3 Requirements on Security

Technical implementations rely on Information Security to ensure confidentiality, integrity, and availability of data and services. The following requirements should be fulfilled by the responsible CSP.

3.1 Strong and Transparent Data at Rest Security

Responsibility CSP

Data at Rest refers to the storing of data for various purposes. To fulfil this basic need of cloud customers, transparent and strong security in the cloud is a necessity. Therefore, CSPs should provide solutions to ensure adequate security is in place.

Firstly, a data encryption methodology should be implemented in such a way that the CSP cannot be forced to divulge the keys to decrypt customer data without approval, consent or knowledge of the data owners.

More precisely, a CSP should employ at least a level three, 140-2 Financial Information Processing Standard (FIPS) Hardware Security Module (HSM) which supports state of the art cryptographic processes as well as provides a scalable and managed Key Management System based on HSMs, including key import and re-import, rotation, re-encryption, grouping, and labelling. Plus, a CSP should offer multiple methods for customers to encrypt data at rest, for example, via Supply Your Own Key upon each request, Bring Your Own Key into CSPs HSM, External Key Management where key encryption keys reside outside CSPs HSM, and privately hosted HSMs in a co-location.

Secondly, it should be transparent to cloud customers what encryption keys are used when encrypting data assets and by whom, thus ensuring auditability.

A CSP should offer customers organisation-wide encryption policies and a central place to define Data at Rest encryption for all services, enable all services to support the cryptographic key management options mentioned above as well as provide access sovereignty and access transparency logs to justify usage of cryptographic keys and provide a holistic dashboard for all key involvement.

3.2 Strong and Transparent Data in Transit Security

Responsibility CSP

For FIs currently using public cloud services, it is often unclear where the data is transferred and how it is secured in transit. However, it should always be clear how data in transit is secured as well as how and where the data is being transfer.

The CSP should use state of the art security to secure Data in Transit for example Transport Layer Security version 1.3. To provide clarity on the data transport architecture, the CSP should provide a consistent, central place to configure and monitor data in transit security, rather than individually per service only. Also, a precise description of the CSPs internal communication channels and applied security measures should be made transparent.

3.3 Fully Featured Logging and Monitoring

Responsibility CSP

To ensure full control of customer data assets, robust, and complete audit logging of all cloud application and service activity is required. This applies to both customer and CSP actions. This includes customer service access (Access Transparency with approvals), including CSP and customer admin access (Admin Activity), as well as data addresses that have been accessed (Data Access). A CSP should for all services consistently log identity, performed action, service usage, corresponding purpose, and involved data. Cloud customers should be able to access logs of their own activity on the platform via an Application Programming Interface (API), a Graphical User Interface or some other mechanisms in order to integrate with their own security logging systems. Furthermore, customer log data should not be made public without the consent of the customer. With respect to monitoring, there is a lack of standardised monitoring interfaces across CSPs. Therefore, to leverage multiple CSPs, there should be a standardised monitoring interface provided across all services.

3.4 Data Exfiltration and Customer Policy Enforcement

Responsibility CSP

Since data sharing is quite effortless to perform on the cloud, customers are interested in strictly controlled data sharing capabilities to prevent data exfiltration to unwanted locations.

Hence, CSP should provide consistent visibility and control of all workloads and communication flow perimeters regardless of location, size, or architecture. This also applies to communication between CSP services and 'private endpoints', including the direction of data flow (ingress/egress). A CSP should also provide an effective set of security posture management tools to enable customers to assess security configurations at a global cloud control layer in line with their security frameworks and standards.

In addition, each configuration and policy defined for a cloud service by a customer should be applied automatically across all instances of that service run by that customer and be centrally monitored thereafter.

3.5 Service Certifications and Evidence

Responsibility CSP

Certifications for services assure an adequate level of security and therefore are one of the key requisites for all cloud users to rely upon. Hence, the services of a CSP should be independently certified by independent third-party auditors. The security certifications should at least include the de facto market standards[3], as well as further certifications that are specific to the financial industry[4].

A CSP should disclose evidence of certifications upon request to the customer. Furthermore, a CSP should provide its customers with the ability to conduct their own audits on the CSP.

3.6 Separation of Identities and Contacts

Responsibility CSP

If identities and contact information are the same, different contexts get mixed. A CSP should therefore provide the measures to associate federated and non-federated identities with valid routable contact information (i.e. email addresses) in order to ensure notifications are successfully delivered to the user. More precisely, identity identifier and contact information should be separated but able to be grouped by identities. For example, the identity internalNumber@ad.on-prem.customer.com cannot be routed, thus a valid and routable email address such as prename.surname@customer.com should be able to be associated and used to send any notifications to and from the CSP.

A CSP should provide specific communication channels for certain event types, such as critical data and service events, e.g., data breaches, security issues, or technical blockers. This should be provided, in addition to email by other channels that can be configured by the customer.

3.7 Maturity of Data in Use Security

Responsibility CSP

As of now, to achieve data in use security, the only generic and practical method in the industry is to rely on Trusted Execution Environments as part of the computer processors. Examples are Intel Software Guard Extensions, AMD Secure Encrypted Virtualization, and Advanced RISC Machines (ARM) Trust Zone. This functionality is often referred to as Confidential Computing.

Currently this feature is only offered by some CSPs for selected services restricted to specific hardware specifications. We are expecting Confidential Computing or similar implementations to be

[3] Cloud Security Alliance (CSA): Security, Trust & Assurance Registry Program (STAR) (CSA STAR); ISO/IEC: 27001, 27017, 27018; AICPA SSAE 18 / ISAE 3402 Type II: SOC 2.
[4] German Federal Office for Information Security: Cloud Computing Compliance Criteria Catalogue (C5:2020), Payment Card Industry Data Security Standards (PCI DSS).

available as an option for a broad set of hardware configurations as well as backends of managed services.

3.8 Backup Functionality, High Availability, and Disaster Recovery

Responsibility CSP

A CSP should provide a geo-redundant backup solution which is independent of the service's API enablement status. The backup functionality should not rely on third parties and should support service independent storage locations. Also, the backup measure should be coherent with the shared responsibility model for the cloud service models for IaaS, PaaS, SaaS. This functionality should be provided by all services storing customer data or service configurations and be manageable through a single interface.

For business continuity reasons, cloud services should be available in both High Availability and Disaster Recovery mode, so as not to create a single point of failure for FIs. Furthermore, if the CSP performs business continuity and resilience exercises affecting customers, they should be involved in the process.

4 Requirements for Governance and Regulation

This section covers requirements for the management of risk associated with outsourced services, as well as its regulatory framework. In the latter case, the intention is not to move responsibility away from cloud customers or to lower the given standards, but to point out a more effective way of operationalisation.

4.1 Control measures on Outsourced Services

Responsibility CSP

In order to control outsourced services and implemented systems on cloud platforms, the following is required for outsourced services:

- Contingency measures should be defined, implemented and tested for the used services and infrastructure.
- Information on outsourcing should be made available to the customer on near real-time basis or via adequate alerts with defined and transparent thresholds.
- The adequacy of the outsourced solutions should be proven and there needs to be contingency solutions in place to allow instant action and to keep the service running or to fix problems.
- Information needs to be provided on geographical/regional aspects, the provider landscape including their data centres.
- Supplied information should include the CSP supply chain and sub-outsourcing, if applicable.

4.2 Technical Portability and Vendor Lock-in

Responsibility CSP

The European Banking Authority (EBA) guidelines on outsourcing arrangements (EBA/GL/2019/02 §14/15) require FIs as part of their risk assessment to have an exit strategy in place when outsourcing "Critical / Important function" to CSPs. This is to cover relevant exit triggering events, e.g. bankruptcy of CSP, sanctions, or a changing legal environment. Another important aspect is vendor lock-in, CSPs using proprietary technology that makes transferring data and/or services to other providers infeasible.

At a minimum the following conditions should be met by CSPs:

- Provide open source components such as software stacks, interfaces and APIs.
- Standardised data formats for data extraction and transport to other environments and platforms.

- Licenses for on premise (or equivalent) solutions for a fair price with clients not forced into a cloud migration without the option of a return in an exit scenario.
- For SaaS the CSPs should offer a version/installation which is compatible with other cloud platforms or provides other alternatives such as licenses for desktop installations except for SaaS CSP proprietary solutions that needs cloud-native capabilities to provide services to the customer. Alternatives are especially relevant for Office products and should ensure that a migration during an exit is realistic and economically possible. CSPs should respect the requirement for FIs to have an exit plan.
- CSPs should inform customers on short notice about agreed exit triggering events which can be observed at their side.

4.3 Sound Governance of Third-Party Risk Management

Responsibility CSP

For a sound governance of third-party risk management, CSPs should provide FIs with the following information for the used cloud services and infrastructure:

- Overview of cloud services including a detailed supply-chain service mapping of underlying dependent sub-contractors or sub-hosting services.
- Supply-chain information detailing the roles and responsibilities of the underlying sub-contractors for the related cloud services.
- Supply-chain information detailing the dataflow, data exchange and data location/region between the CSP and each sub-contractor for the related cloud services.
- The information should be enough for a Financial industry specific Business Continuity Plan and Disaster Recovery Plan.

4.4 Exit Strategy Requirements

Attention EBA

We do not regard technical availability a relevant exit triggering event in using public cloud technology, when institutions' critical applications and services are hosted in three regionally different data centres, where two are used for production and one for recovery.

The remaining relevant exit triggering event types (see chapter 4.2) can be observed, and the occurrence anticipated. On that basis and empirical data from such an event, an exit and migration time slot can be defined to exit a cloud platform and migrate the bank critical service.

4.5 CSP Audits and Oversight

Responsibility CSP

We propose simplifications in audit procedures insofar, as the cloud service offerings are not checked by every FI, but centrally at the CSP. We want to facilitate the implementation of regulatory requirements at CSPs:

- Collaborative audits organised by the financial industry should become a generally accepted approach by CSPs and free of charge. Different institutions form a collaborative team to audit one specific CSP. The audit results can be regarded valid within the respective individual institution. Collaborative audits are already supported by the EBA Guidelines on Outsourcing Arrangements (chapter 13.3, Para. 91.a).

Attention ECB

Apart from the institutions' obligation to audit their CSPs, national and European supervision are asked to follow the private collaborative audit approach, that respective CSPs and their cloud service offerings to financial industry are audited once for all customers. This to replace the repetition of CSP individual audits and the related efforts along with each institutions' inspection. Moreover, the systemic risk of the whole industry with CSP being "hyper-scalers" cannot be managed by individual institutions. However, the institutions specific cloud adoption is still inspected individually and resulting observations are assigned to the respective institution.

5 Requirements on Standard Contractual Clauses

The following points require implementation by the CSP. Regarding standardised FI requirements, we would like to see a binding regulation of the Standard Contractual Clauses by the legislator and regulator.

The ECUC appreciates the European Commission's work on "Model Contractual Clauses for Cloud" and will align the positions below in the following public hearings on them.

5.1 Audit Rights for Customers

Responsibility CSP

To meet industry's obligations to audit, audit rights to data centres and its services, Customers Audit Rights should be granted per standard contractual clauses. There is also a need to audit the relevant infrastructure on a regularly basis.

5.2 Sub-Outsourcing

Responsibility CSP

In accordance with the EBA "Guidelines on Outsourcing Arrangements" (EBA/GL/2019/02 §14/15) the CSP provides information regarding sub outsourcing at any time without limitations. In addition, all changes are shown with a minimum advance of 90 days and a right of consultation. The CSP should ensure that the objections of FIs are examined favourably. In the event of use of unsuitable subcontractors, the FI should be granted a special right of termination including termination support.

5.3 Embedded URLs in Contracts and Service Level Agreements

Responsibility CSP

CSPs should offer contracts that include a cost cap for subsequent periods. Unilateral changes by the CSPs using embedded URLs in contract should not affect the agreed Terms and Conditions during the contract period. This prevents a sudden increase in cost which can occur after offering an attractive price model for the initial contract phase.

Likewise, the CSP should only change the service in a way that guarantees all cloud customer at least equal or improved services in terms of function, security, technology and data protection, or that a change or termination of the service will be announced with at least 18 months' notice.

In addition to availability, the Service Level Agreements (SLA) should also include performance metrics and reporting thereof. Both values require permanent monitoring and automation for reporting deviations without additional charge (without additional chargeable services).

The CSP should offer additional communication channels to transmit critical event and service level information (e.g. on data breaches, penetration test findings, logfiles for problem analysis) besides email and a definition of which channels are to be used for different types of information, e.g., via phone.

All deadlines, changes, and level of information should apply without exception to all consumers and not only to individual consumers.

5.4 CSP as Controllers or Processors

Responsibility CSP

There should be clarification on the categorisation of CSPs as controllers or processors. CSPs no longer limit themselves to just being a processor.

5.5 Insurance

Responsibility CSP

The contracts between CSPs and FIs should have an insurance clause that needs to increase with the number of assets on the cloud.

6 Digital Operational Resilience Act

The Digital Operation Resilience Act (DORA) has been published by the European Commission as a proposal for the Financial Sector. The aim is to make the financial sector safer, unifying and simplifying compliance with existing regulation on information and communication technology (ICT) risk management and security. Taking this into account and not to hinder the use of cloud computing, while respecting its particularities, we have the following recommendations. Generally, a period of 36 months should be provided for the implementation of DORA once it enters into force.

6.1 Lex Specialis

Addressed EU

DORA should be the "lex specialis" and requires clear precedence over the NIS 2 or the RCE Resilience of Critical Entities directive (RCE) proposals regarding scope.

- This should be clarified in the respective articles of NIS 2 / RCE and not only in recitals, further FIs shall be excluded from the list of entities within the respective annex of NIS 2 and RCE.
- This would unify ICT-related incident reporting and address overlapping reporting requirements.

6.2 EBA and ESMA Guidelines Should be Aligned with DORA Requirements

Addressed EU

The EBA" Guidelines on outsourcing and ICT and security risk management" (EBA/GL/2019/04) and the ESMA "Guidelines on outsourcing to cloud service providers" should be aligned once DORA requirements are published to avoid fragmentation and to maintain clarity.

6.3 TIBER Framework for Threat Led Pen Testing Should be Reused

Addressed EU

Given the positive experience with the ECB's TIBER-EU framework for cyber resilience testing, this framework should be used instead of developing new standards by the ESA's. Therefore, a reference to the Tiber-EU framework should be included. In addition, we advocate within the EU for mutual recognition of TLPT results.

6.4 DORA should be Aligned with Industry Standards

Addressed EU

The definitions of DORA should be aligned with industry standards to avoid regulatory fragmentation. We believe the industry should help define the "state of the art" of technology and terms used within DORA which should be aligned with global standards and key definitions. Here we advocate proportionality and a risk-based approach as well.

6.5 The Designation of critical ICT Third-Party Service Providers is not fully defined

Addressed EU

The scope of the oversight framework should be clarified regarding entities based outside of the EU and servicing EU FIs entities.

6.6 Intra-group Relationships should be out of Scope of DORA

Addressed EU

Intra-group relationships should not be classified as non-third-party relationships for the purpose of the DORA requirements. The principle of proportionality should be extended to all requirements considering a risk-based approach.

6.7 More Clarification is needed for the effective Assessment of sub-contracting Chains

Addressed EU

This requirement should be aligned with the EBA Outsourcing Guidelines for consistency with existing approaches. Further clarity on the roles and responsibilities of these different stakeholders should be provided to ensure regulatory certainty and efficiency of reporting and oversight.

6.8 Multi-vendor Approach is not necessary to mitigate Concentration Risks

Addressed EU

The multi-vendor approach requirement should be excluded in DORA. In the current market it is not feasible to enforce a multi-vendor strategy upon FIs in order to mitigate concentration risk and limit vendor lock-in as many ICT services are not easily interchangeable, and it negatively impacts complexity of the market, costs, and agility.

6.9 Acknowledged Certification Schemes should be promoted

Addressed EU

Acknowledged certification schemes, recognised by supervisory authorities for third party provider (TPP) as well as a central consortium for assessing TPP's risks, should be promoted.

6.10 Reviews and Assessments should take a risk-based Approach

Addressed EU

Reviews and assessments should be scheduled to take a risk-based approach and not on a uniform yearly cycle.

- There should be a certification scheme based on prescribed criteria to show the TPP is fit and certified to deliver services to FIs.
- It is important that oversight information is transparent and can be used by FIs to decrease their own monitoring on these providers as they can trust on the Lead Overseer.
- The termination of contractual arrangements by the competent authority should not be a standard enforcement tool.

7 Outlook

The publication of ECUC Position Paper 1.0 will be followed by a three-month consultative process before the next version will be published. The consultation phase serves to collect feedback from CSPs, regulatory bodies and other regulated institutions. The feedback will be incorporated into the next version of the position paper. The ECUC represents the position of the member institutions. We kindly ask you to use the following contacts:

consultation@ecuc.group	For questions upon the Position Paper e.g. from CSPs
press@ecuc.group	For inquiries form media and press

*

8 Glossary

AMD ..... *Computer processor manufacturer*
API ..... *Application Programming Interface*
ARM..... *Arorn RISC Machines*
BYOK..... *Bring Your Own Key*
CSA..... *Cloud Service Alliance*
CSP ..... *Cloud Service Provider*
DORA ..... *Digital Operational Resilience Act*
EBA..... *European Banking Authority*
ECB..... *European Central Bank*
ECUC..... *European Cloud User Coalition*
EDPB ..... *European Data Protection Board*
FIPS..... *Financial Information Processing Standard*
FI ..... *Financial Institution*
GDPR ..... *General Data Protection Regulation*
HSM ..... *Hardware Security Module*
IaaS..... *Infrastructure as a Service*
ICT ..... *Information & Communication Technology*
PaaS..... *Platform as a Service*
SaaS..... *Software as a Service*
SLA ..... *Software Level Agreement*
SOC ..... *Service Organization Control*
TPP..... *Third Party Provider*