Deloitte.

Regulatory News Alert

CSSF Circular 17/654 on cloud computing

18 May 2017

On 17 May 2017, the CSSF published Circular 17/654 (the circular) on IT outsourcing based on a cloud computing infrastructure. The circular intends to clarify the regulatory framework for recourse to cloud computing infrastructure supplied by an external service provider. Indeed, the circular reaffirms that CSSF considers that **cloud computing is a form of outsourcing**. The circular applies immediately to financial professionals, including credit institutions, investment firms, specialized PSFs, support PSFs, as well as payment institutions, and electronic money institutions.

Defining cloud computing

In order to distinguish cloud computing from other forms of outsourcing, CSSF provides a definition of cloud computing based on those of authoritative international organizations (i.e., NIST and ENISA). As per this definition, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of (i) five essential characteristics, (ii) three service models, and (iii) four deployment models:

- **Essential characteristics**
    - On-demand self-service

      A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
    - Broad network access

      Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

- Resource pooling

  The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- Rapid elasticity

  Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

- Measured service

  Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

- **Service Models**

  - Infrastructure as a Service (IaaS)

    The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

  - Platform as a Service (PaaS)

    The capability provided to the consumer is to deploy consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure. The consumer does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- Software as a Service (SaaS)

  The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- **Deployment Models**

  - Private cloud

    The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

  - Community cloud

    The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

  - Public cloud

    The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

  - Hybrid cloud

    The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Deloitte.

Applicability of the circular

An outsourcing will be considered as IT outsourcing based on a cloud computing infrastructure if all of the following criteria are met:

1-5. All of the **five essential characteristics of cloud** defined above are satisfied

6. Apart from exceptional situations, the external service provider's staff **does not access the data and systems** of their customers, unless the customers provide their consent to access and the service provider provides monitoring mechanisms

7. The external service provider performs day-to-day management of resources **without manual interaction** (i.e., an automated system provisions resources)

IT outsourcing arrangements satisfying all of these seven criteria will be subject to this circular rather than to Circular 05/178 as replaced by Circular 17/656, or to the sub-chapter 7.4 of Circular 12/552 as amended by Circular 17/655 (which remain applicable for other forms of IT outsourcing arrangements, as appropriate).

Roles foreseen in the circular

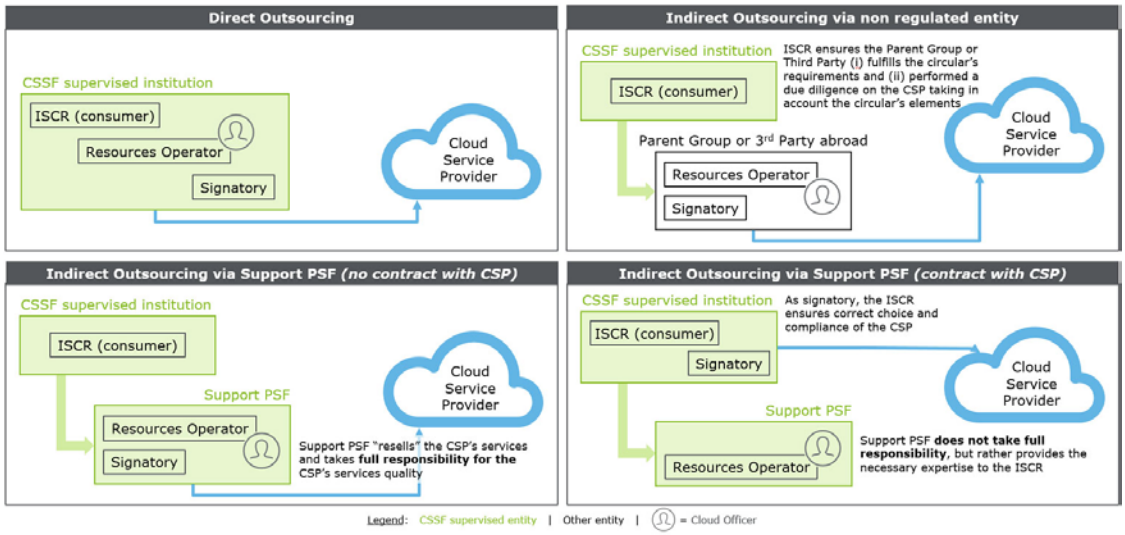
The circular foresees four roles:

Role	Description
ISCR or Consumer)	• An Institution Supervised by the CSSF Consuming cloud computing Resources for the purpose of carrying out its activities
Signatory	• The entity signing the contract with the Cloud Service Provider
Resources Operator	• Natural or legal person using the client interface allowing to manage cloud resources
Cloud Service Provider	• The Cloud Service Provider delivering the cloud solution in scope of this circular

Deloitte.

In addition, the resources operator shall name a **cloud officer** among its employees who will be mainly responsible for (i) use of the cloud solutions, and (ii) guaranteeing the competencies of the staff managing cloud resources. Thus, the cloud officer shall be qualified and understand the issues related to IT outsourcing in the cloud. The cloud officer function can be assigned to a person having other functions in the IT department. A resource operator cannot outsource the cloud officer.

The circular foresees certain authorized splits of these four roles and **creates opportunities for Support PSFs to play a role in the recourse to cloud solutions:**



Deloitte.

Requirements set forth in the circular

In addition to the above requirements related to roles, the circular sets forth requirements in the following domains; whereas most of the requirements consist in instantiating existing requirements on outsourcing in the context of cloud computing (i.e., in a detailed and prescriptive manner), the circular also introduces new requirements to address certain risks that are specific to cloud solutions.

Governance	• The circular instantiates existing requirements on outsourcing in the context of cloud computing (e.g., compliance with the ISCR's formal outsourcing policy, clear documentation on respective roles and responsibilities, etc.), but also introduces a **cloud officer** (as seen above)
Customers consent and notification	• **The circular refers to legal requirements** and thus paves the way for the changes foreseen concerning the obligation of professional secrecy (i.e. Bill of Law 7024) • The ISCR ensures whether it is necessary or not to inform its customers and to obtain their consent • The ISCR complies with data protection regulations • Encryption with localization of the encryption keys in Luxembourg is no longer mandatory
Prior authorization from or notification to the CSSF	• Entities in scope of the circular shall engage with the CSSF where they plan to recourse to the cloud. The nature of the communications will depend on the materiality of the activities outsourced in the cloud: o Cloud solutions supporting material activities require prior authorization o Other cloud solutions require notification • The termination of a cloud computing outsourcing needs to be notified to the CSSF • Support PSFs authorized as IT systems and communication networks operators shall obtain the prior authorization of the CSSF to offer cloud services

Outsourcing risk management	• The resource operator and its Cloud Officer need to ensure that the staff in charge of operating cloud resources, the internal audit, and the staff in charge of information security have been duly trained via training which is specific to the cloud solution's on cloud resources operations and security (there could be more than one cloud solutions in use) • The circular instantiates existing requirements on outsourcing in the context of cloud computing (e.g., prior and in-depth risk analysis), but also draws attention to specific risks, such as geopolitical risks where the cloud service provider hosts its systems abroad • The ISCR shall formally document its compliance with the requirements set forth in the circular (the CSSF may ask for this documentation at any time)
Business continuity	• The circular instantiates existing requirements on outsourcing in the context of cloud computing (e.g., continuity aspects and the revocable nature of outsourcing), but also draws attention to specific risks, such as data portability
Systems security	• The confidentiality and integrity of data and systems must be controlled throughout the IT outsourcing chain (i.e., at the ISCR, the resources operator, and the cloud service provider) • **The circular explicitly requires access to data and systems to comply with the "need to know" and "least privilege" principles**
Contractual terms	• The contract signed with the cloud service provider shall normally be **governed by the law of a EU member state** and shall normally **plan for resilience of cloud services in the EU** • In the event of contract termination, the CSP undertakes to **permanently delete the data and systems** within a reasonable time frame • The CSSF must have an **unconditional right** to audit the cloud service provider in the context of the services used by the ISCR and resources operator under its supervision

Outsourcing oversight	• The cloud service provider regularly provides **relevant indicators** (i.e., KPIs) to the signatory (and by extension to the ISCR) • **Proper isolation** of ISCR's systems and data must be regularly controlled by the cloud service provider
Right to audit	• The signatory may obtain sufficient assurance on the cloud service provider's compliance to its contractual obligations and suitable risk management practices through the **in-depth review of the cloud service provider's audit reports or certifications** • The signatory shall have the contractual **right to request reasonable adaptations in the scope of these audit reports or certifications** to fulfil their essential needs, and should retain the contractual **right to perform direct audits**

How can Deloitte help?

Disrupt. Transform. Repeat. That's the new normal. Done right, cloud not only drives that reality—it can turn it into your advantage. Deloitte's end-to-end capabilities and understanding of your business and industry help amplify the transformative value of cloud.

Our broad array of services include:

- **Compliance Assessment** – gap analysis of our client's cloud projects compliance against laws and regulations and pragmatic recommendations for improvement
- **Assisting in Communications with the Regulator** – preparation (or quality assurance) of application files and participation in meetings with the regulator, e.g.:

    - Notifications and authorization requests for financial professionals wishing to use cloud solutions

    - Authorization requests for Support PSFs wishing to offer cloud solutions

    - Gap analysis of CSSF requirements for cloud service providers wishing to expand in the Luxembourg financial sector

Deloitte.

- **Cloud Strategy and Readiness** – your journey into the cloud must navigate pitfalls and opportunities that are unique to your business alone. That makes mapping out a clear strategy and preparing your organization essential to achieving your business goals
- **Cloud Package Implementation** – multiple SaaS solutions exist on the market for every common business process. Each solution has its strengths and weaknesses, its best uses and fits. Knowing what those are and how they will affect your business is critical for success
- **Custom Migration Consulting Services** – a simple “lift-and-shift” approach to moving your applications to the cloud often bypasses the key benefits associated with the cloud—cost savings, scalability, increased speed, and flexibility
- **IT Operating Model with Cloud** – as the workload shifts to new and more business-aligned tasks, IT needs to adjust to a new reality. Governance, service delivery, integration architecture, supplier management, and service measurement are among the areas that require recalibration

Your contacts

Roland Bastin
Partner – Information & Technology Risk
Tel : +352 45145 2213
rbastin@deloitte.lu

Patrick Laurent
Partner – Technology Leader
Tel : +352 45145 4170
palaurent@deloitte.lu

Laurent de la Vaissière
Director – Information & Technology Risk
Tel : +352 45145 2010
ldelavaissiere@deloitte.lu

Jesper Nielsen
Director – Technology & Enterprise Application
Tel : +352 45145 3676
jespernielsen@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg